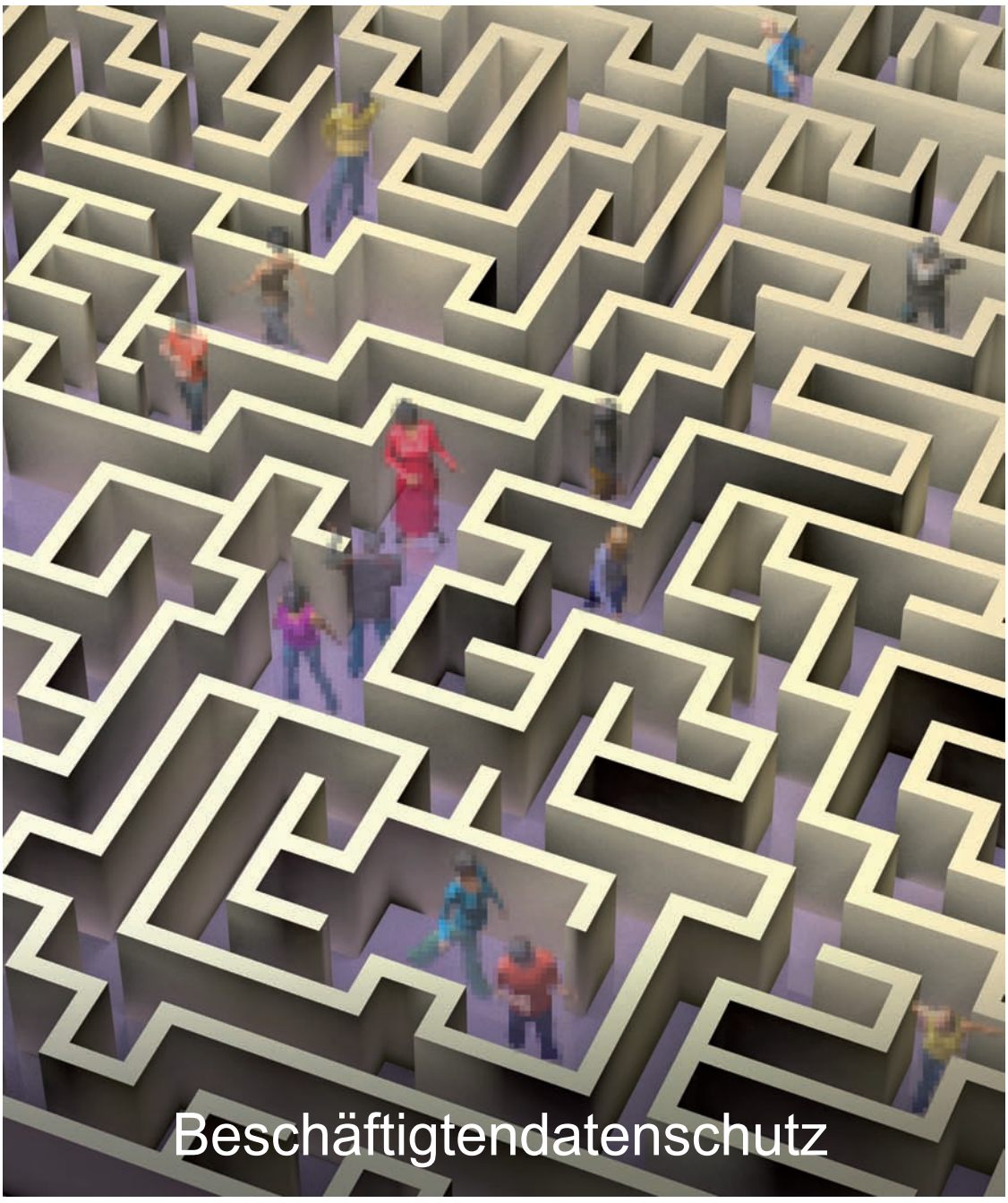
4/2010

Datenschutz Nachrichten

33. Jahrgang
ISSN 0137-7767
9,00 Euro



Beschäftigtendatenschutz

■ Datenschutz und Beschäftigungsverhältnisse ■ Anonyme Bewerbungen ■ Chronik der Kodifizierung des Arbeitnehmerdatenschutzgesetzes ■ Datenschutznachrichten ■ Rechtsprechung ■

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

Inhalt

Termine

Freitag, 31. Dezember 2010
Einsendeschluss für die Nominierungen zu den BigBrotherAwards 2011
http://www.bigbrotherawards.de

Samstag, 15. Januar 2011
DVD-Vorstandssitzung
Berlin. Anmeldung in der Geschäftstelle
dvd@datenschutzverein.de

Dienstag, 1. Februar 2011
Redaktionsschluss DANA 1/11
Thema: noch offen, Tagungsnachlese
verantwortlich: NN
Fragen und Anregungen bitte an:
dvd@datenschutzverein.de

Freitag, 1. April 2011
Verleihung der BigBrotherAwards 2011
Bielefeld
http://www.bigbrotherawards.de

Sonntag, 10. April 2011
DVD-Vorstandssitzung
Frankfurt. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 1. Mai 2011
Redaktionsschluss DANA 2/11
Thema: „Das Ende personenbezogener Daten als Auslöser von Datenschutz?“
verantwortlich: Karin Schuler
Fragen und Anregungen bitte an:
dvd@datenschutzverein.de

Sonntag, 3. Juli 2011
DVD-Vorstandssitzung
Stralsund. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Montag, 1. August 2011
Redaktionsschluss DANA 3/11
Thema: noch offen, verantwortlich: NN
Fragen und Anregungen bitte an:
dvd@datenschutzverein.de

Freitag, 28. Oktober 2011
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Samstag, 29. Oktober 2011
DVD-Mitgliederversammlung
Bonn

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

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

Redaktion (ViSdP)
Sönke Hilbrans
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.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

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. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

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

Abbildungen
Frans Jozef Valenta

Alle Jahre wieder...

Liebe Leserinnen und Leser,

diese Jahresendausgabe der DANA ist anders als die der letzten Jahre. Keine Laudationes und Hintergrundberichte zu den Big Brother Awards füllen mehr unsere Zeilen. Sie werden voraussichtlich auch in Zukunft auf die Schwerpunktausgabe der DANA zu den Big Brother Awards verzichten müssen, denn wir wollen jährlich vier redaktionelle Themenschwerpunkte setzen. Natürlich werden die BigBrotherAwards, inzwischen bekannt aus Funk und Fernsehen und ausführlich dokumentiert in Presse und Internet, auch im nächsten Jahr wieder vergeben werden. Die jährliche Gala wechselt den Takt und wird im Frühjahr stattfinden. Merken Sie sich doch schon mal den 1. April vor. Außerdem sind Sie wieder aufgerufen, preisverdächtige Datenschutzfehlleistungen zu melden (Näheres unter: www.bigbrotherawards.de), Einsendeschluss ist schon der 31.12.2010! Langeweile wird auch mit der Lektüre dieses Hefts kaum aufkommen. Neben den bewährten Nachrichten widmet sich Thilo Weichert unter anderem dem dramatischen Gesetzgebungsversuch für den Beschäftigtendatenschutz, dessen Zeuginnen und Zeugen wir dieser Tage werden. Der Blick in die Zukunft des Beschäftigtendatenschutzes bleibt spannend, auch wenn am Ende bei den Beschäftigten wohl kaum viele Sektkorken knallen werden. Zu guter Letzt seien noch die Vorstandswahlen auf der letzten Mitgliederversammlung am 7. November 2010 rekapituliert. Gewählt wurden: Karin Schuler (Vorsitzende), Sönke Hilbrans (Stellvertreter), Karsten Neumann. Die Amtszeiten von Roland Schäfer (Stellvertreter und Kassenwart) Frans Valenta dauern noch an. Der neue Vorstand dankt an dieser Stelle allen ausgeschiedenen Vorstandsmitgliedern herzlich für ihre engagierte und kompetente Mitarbeit und wünscht allen Leserinnen und Lesern ein gesundes, erfreuliches und datenschutzfreundliches 2011!

Ihr
Sönke Hilbrans

Autorinnen und Autoren dieser Ausgabe:

Kay Ann Gruling
Fachärztin (family medicine), Marshfield Clinic, Wausau Medical Center, Wisconsin, USA
Kontakt via Geschäftsstelle

Sören Jungjohann
Jurist, Hannover
soeren.jungjohann@web.de

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel
weichert@datenschutzzentrum.de

Dr. Thilo Weichert

Datenschutz und Beschäftigungsverhältnisse

Ein Überblick

I. Aktualität

Das Thema des Arbeitsnehmerdatenschutzes hat in den Jahren 2008/2009 eine bisher nicht gekannte öffentliche Aufmerksamkeit gefunden. Hintergrund sind große Überwachungsaktionen renommierter Unternehmen gegenüber ihren Mitarbeitenden, teilweise bis hinein in die Ebene des Vorstands und des Aufsichtsrates. Einige Beispiele für diese „Skandale“ sollen anhand von Presseüberschriften in Erinnerung gerufen werden:

- „Bespitzelungsaffäre bei Lidl“,
- „Auch Edeka und Plus bespitzeln Mitarbeiter“,
- „Überwachung von Mitarbeitern und Kunden erregt weiter die Gemüter“,
- „Betriebsversammlung vor laufenden Kameras“,
- „IKEA soll Mitarbeiter überwacht haben“,
- „Rasterfahndung bei der Bahn“,
- „Spitzelsoftware bei Honeywell“,
- „Daimler speichert Krankheitsdaten von Mitarbeitern“.

Diese „Skandale“ bzw. die öffentliche Wahrnehmung dieser Ereignisse führte kurzfristig zu Gesetzgebungsaktivitäten noch in der 16. Legislaturperiode des Bundestags. Dort waren ohnehin Überarbeitungen des Bundesdatenschutzgesetzes (BDSG) im Gesetzgebungsverfahren, und zwar insbesondere zur Regelung der Tätigkeit von Auskunfteien und von Scoringverfahren sowie zum Adressenhandel und zur Datennutzung für Werbezwecke. Die letztgenannte Gesetzesinitiative wurde v.a. unter dem Eindruck der Datenabgleiche der Mitarbeitenden der Deutschen Bahn AG um eine gesetzliche Regelung in einem § 32 BDSG ergänzt, in der eine Generalklausel für die Datenverarbeitung in Beschäftigungsverhältnissen aufgenommen wurde sowie in Absatz 1 Satz 2 eine Norm zur Aufdeckung von Straftaten. Hierbei handelte es sich erklärtermaßen um eine Notgesetzgebung, mit der vor der Bundestagswahl 2009 signalisiert werden sollte, dass weitergehender Regelungsbedarf besteht und dass der Beschäftigtendatenschutz einer umfassenden gesetzlichen Regelung zugeführt werden müsse. Hiergegen wehrten sich letztlich nur noch die Arbeitgeberverbände, die gegen ein Arbeitnehmerdatenschutzgesetz votierten. Ein solches sei Gesetz nicht nötig und einzelne Datenschutzverstöße dürften nicht zum Anlass genommen werden, die gesamte Arbeitgeberschaft in die Pflicht zu nehmen.

Über ein umfassendes Beschäftigtendatenschutzgesetz konnte sich die schwarz-rote Bundesregierung 2009 vor der Bundestagswahl nicht mehr einigen. Ein im SPD-geführten Bundesarbeitsministerium erarbeiteter Entwurf wurde vom Arbeitsminister Scholz kurz vor der Bundestagswahl veröffentlicht. Dieser fiel der Diskontinuität anheim und wurde in der 17. Legislaturperiode von der SPD-Fraktion in den Bundestag eingebracht (BT-Drs. 17/69). Die neue schwarz-gelbe Bundesregierung verabredete in der Koalitionsvereinbarung, den Beschäftigtendatenschutz im BDSG neu zu regeln (vgl. DANA 4/2009, 144). Inzwischen hat das Bundeskabinett am 25.08.2010 einen Gesetzentwurf vorgelegt, zu dem der Bundesrat am 05.11.2010 eine kritische Stellungnahme abgegeben hat. Hierauf wird die Bundesregierung eine Antwort vorlegen, die die weitere Grundlage für die Gesetzgebung im Bundestag sein wird. Es ist bei allen Beteiligten unstreitig, dass der Entwurf noch grundlegend geändert werden muss. So unterstützt etwa der DGB die kritische Stellungnahme des Bundesrats. Bündnis 90 / Die Grünen arbeitet an einem eigenen Gesetzentwurf. Der vorliegende Text rekapituliert die bisherige Diskussion und gibt einen Überblick über wesentlichen Konfliktthemen, ohne aber zu den aktuellen, noch Änderungen unterworfenen Entwürfen Stellung zu nehmen. Zur Gesetzgebungsgeschichte siehe auch den Überblick von Sören Jungjohann in diesem Heft.

II. Technischer Hintergrund

Die Notwendigkeit einer gesetzlichen Regulierung des Arbeitnehmerdatenschutzrechtes ergibt sich aus der technischen Entwicklung der Möglichkeiten und der Praxis bei der Arbeitnehmerüberwachung bzw. des Einsatzes von Informationstechnik im Arbeitsleben. In Bewerbungsverfahren greifen Personalchefs nicht nur auf die Bewerbungsunterlagen zurück, sondern nutzen im Internet verfügbare Informationen über Bewerber, um sich ein Bild von diesen zu machen. Zentrale Bestandteile fast jedes Arbeitsplatzes sind inzwischen komplexe Telekommunikationsgeräte, und zwar nicht nur das Festnetztelefon, sondern auch ein Handy und evtl. ein mobiler Arbeitsplatzcomputer als Recherche-, Schreib- und Kommunikationsgerät. Viele Arbeitsplätze sind in ein Unternehmensnetz integriert; nicht nur die klassischen Schreibtischarbeitsplätze, sondern auch in der Warenproduktion oder etwa im Fuhrpark. Über den Zugang zum Internet eröffnen sich neben der inzwischen schon klassischen E-Mail-Nutzung neue Formen der Kommunikation, wie z.B. die Internettelefonie mittels Voice over IP. An den digitalisierten Arbeitsplätzen fallen Verkehrs- und Inhaltsdaten an, die analysiert werden können und eine umfassende Arbeitskontrolle, eine Verhaltens- und Leistungskontrolle, ermöglichen.

Auch an anderen Stellen hinterlassen die Beschäftigten digitale Spuren, die sich für den Arbeitgeber zur Kontrolle eignen: Der Einsatz von evtl. mit Funktechnik (RFID) ausgestatteten Betriebsausweisen oder von Biometrie ermöglicht die Erstellung von Bewegungsprofilen. Noch lückenloser ist dies mit Hilfe von Lokalisierungsdiensten auf Mobilfunkbasis möglich und evtl. gar mit Satellitenortung, die sowohl innerhalb des Betriebsgeländes, vor allem aber im Außendienst genutzt wird. Videoüberwachung im Kundenbereich dient v.a. der Diebstahlsbekämpfung, eignet sich aber auch zur Mitarbeiterüberwachung. Auch auf dem Betriebsgelände findet Videoüberwachung zunehmend Einsatz: zur Objektsicherung, zur Aufklärung von Straftaten, zur Gefahrenabwehr oder zur Verkehrsregulierung. Die Kameras sind offen, manchmal aber auch verdeckt installiert. Vernetzte Kamerasysteme mit Mustererkennungsverfahren ermöglichen das automatische Verfolgen von Personen über das gesamte Betriebsgelände.

Eine besondere Form der digitalen Mitarbeiterkontrolle erfolgt bei der Heimarbeit, wo im Rahmen der Arbeitskontrolle zwangsläufig in die Wohn- und Privatsphäre der Beschäftigten eingedrungen werden muss. Bei Arbeitsverhältnissen, in denen die Beschäftigten mit Geld in Berührung kommen, finden zunehmend Bonitäts- und Zuverlässigkeitsprüfungen statt. Die Methode des Scorings wird genutzt, um Eigenschaften der Beschäftigten zu bewerten. Zunehmender „Beliebtheit“ bei Arbeitgebern erfreuen sich fragwürdige Gesundheits-, Drogen- oder gar Genscreenings. Oft werden die Mitarbeiterdaten in einer umfassenden HR-Datenbank gespeichert. HR steht für Human Resources (Personalwesen). Die dort gespeicherten Daten werden nach unterschiedlichen Fragestellungen analysiert, wobei diese sich nicht ausschließlich auf die Produktivität und Organisation beziehen, sondern auch auf die Mitarbeiterselektion und -ausleuchtung. Eingesetzt werden teilweise sogar Data-Mining-Werkzeuge, mit denen aus HR-Datenbanken Antworten auf noch nicht präzise formulierte Fragestellungen gegeben werden können.

III. Verfassungsrechtlicher Datenschutz

Verfassungsrechtlicher Ausgangspunkt des Datenschutzes ist das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG), dessen Relevanz in der Informationsgesellschaft zunimmt. Dieses Recht findet historisch Konkretisierungen im Schutz am eigenen Bild, im Recht am gesprochenen Wort oder im Schutz der Privatsphäre, besonders der Intimsphäre. Eine moderne Ausgestaltung ist das durch das Volkszählungsurteil im Jahr 1983 vom Bundesverfassungsgericht (BVerfG) abgeleitete Grundrecht auf informationelle Selbstbestimmung, also das Recht des einzelnen Menschen grundsätzlich. selbst bestimmen zu dürfen, wer was wann bei welcher Gelegenheit über ihn weiß: „Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten vom allgemeinen Persönlichkeitsrecht […] umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. [...] Einschränkungen dieses Rechts auf ´informationelle Selbstbestimmung` sind nur im überwiegenden Allgemeininteresse zulässig“ (BVerfG NJW 1983, 422).

Schon im Jahr 1990 stellte das BVerfG klar, dass es sich bei dem Recht auf informationelle Selbstbestimmung nicht nur um ein individuelles Abwehrrecht gegenüber dem Staat handelt, sondern dass dieses im Privatrechtsverkehr beachtet werden muss und insofern eine staatliche Gewährleistungspflicht begründet (BVerfG NJW 1991, 2411). Dies gilt insbesondere in Privatrechtsbeziehungen zwischen ungleichen Partnern, wie das BVerfG 2007 anschaulich darlegte: „Das allgemeine Persönlichkeitsrecht […] entfaltet als Norm des objektiven Rechts seinen Rechtsgehalt auch im Privatrecht. [...] Ist ersichtlich, dass in einem Vertragsverhältnis ein Partner ein solches Gewicht hat, dass er den Vertragsinhalt faktisch einseitig bestimmen kann, ist es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt“ (BVerfG NJW 2007, 3707). Diese Aussagen gelten uneingeschränkt für das Verhältnis zwischen Arbeitgeber und Arbeitnehmer.

Das BVerfG hat in einer Vielzahl von Entscheidungen das Recht auf informationelle Selbstbestimmung präzisiert und im Hinblick auf spezifische Kontrollszenarien interpretiert. Für Eingriffsmaßnahmen werden bestimmte gesetzliche Grundlagen gefordert, die verhältnismäßig sein müssen. Von diesen Ermächtigungen darf nur unter Beachtung des Verhältnismäßigkeitsgrundsatzes Gebrauch gemacht werden. Dabei stellt sich nicht nur die Frage des „Ob“ des informationellen Eingriffs, sondern auch des „Wie“: In den Normen sind technische, organisatorische und prozedurale Vorkehrungen vorzusehen, die Rahmenbedingungen für den Schutz des Rechts auf informationelle Selbstbestimmung schaffen. Das BVerfG hat spezifische materielle Schranken des allgemeinen Persönlichkeitsrechtes definiert, die nicht überschritten werden dürfen. So wurde schon früh das Erstellen von ganzen oder teilweisen Persönlichkeitsprofilen verboten. Während dieses Verbot vorrangig eine zeitliche Dimension hat, zielt das Verbot einer Rundumüberwachung auf eine Sektorbeschränkung von Überwachungsmaßnahmen. Das Verbot der anlasslosen Kontrolle, der Überwachung „ins Blaue hinein“, wird heute plakativ als Verbot einer Vorratsdatenverarbeitung beschrieben. In jüngster Zeit musste das BVerfG einige grundlegende Entscheidungen zum Schutz des „Kernbereichs persönlicher Lebensgestaltung“ treffen.

Dabei stehen zwei Fallgestaltungen, die auch im Arbeitsverhältnis von großer Relevanz sind, immer wieder im Fokus: Die heimliche Erfassung, bei der die Betroffenen den Eingriff in ihre Privatsphäre überhaupt nicht erkennen können, und die daher nur ausnahmsweise und klar reguliert erlaubt sein kann, und die anlasslose Kontrolle. Im Hinblick auf den Einsatz von Videoüberwachung stellte das BVerfG im Jahr 2007 hinsichtlich des zweitgenannten Themas Folgendes fest: „Verdachtlose Eingriffe

mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und die Eingriffe durch ihr Verhalten nicht veranlasst haben, weisen grundsätzlich eine hohe Eingriffsintensität auf. Die geplante Videoüberwachung ist ein intensiver Eingriff. Sie beeinträchtigt alle, die den betroffenen Raum betreten. [...] Videoüberwachung (kann) materiell verfassungsgemäß sein, wenn für sie ein hinreichender Anlass besteht und Überwachung sowie Aufzeichnung, insbesondere in räumlicher und zeitlicher Hinsicht und im Hinblick auf die Möglichkeit der Auswertung der Daten, das Übermaßverbot wahren“ (BVerfG 23.02.2007, 1 BvR 2368/06).

2008 leitete das BVerfG in der Online-Durchsuchungsentscheidung ein Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit eigengenutzter informationstechnischer Systeme ab, mit dem – analog zu den räumlichen und sozialen Privatsphären Wohnung und Familie – eine besonders geschützte informationstechnische Privatsphäre definiert wurde (BVerfG NJW 2008, 822).

Nicht ausgeblendet werden dürfen die klassischen Grundrechte, die in unserer technisierten Welt eine technische, genauer eine digitale Komponente erhalten. Dies ist am offensichtlichsten beim Post- und Fernmeldegeheimnis bzw. dem Telekommunikationsgeheimnis nach Art. 10 GG. Seit der Entscheidung des BVerfG zum Lauschangriff ist allgemein anerkannt, dass dem Schutz der Wohnung auch eine informationelle Komponente zukommt. Die berufliche Vertrauensbeziehung, etwa eines Arztes, eines Rechtsanwaltes oder eines Geistlichen, genießt den Schutz des Art. 12 GG. Vielseitigen Schutz bietet außerdem Art. 5 GG, der den Zugang zu Informationen und die individuelle Meinungsäußerung gewährleisten soll. Auch allen weiteren analogen Grundrechten kann eine digitale Komponente zukommen.

IV. Gesetzliche Grundlagen

Das deutsche Datenschutzrecht geht auf die 70er Jahre des letzten Jahrhunderts zurück. 1978 trat das erste Bundesdatenschutzgesetz in Kraft, das von Anfang an sowohl den öffentlichen wie auch den privaten Bereich der personenbezogenen Datenverarbeitung erfasste. Spätestens seit dem Volkszählungsurteil 1983 steht die Forderung nach einem spezifischen Arbeitnehmerdatenschutzgesetz im Raum. Und tatsächlich haben die Regierungskoalitionen seit Mitte der 80er Jahre regelmäßig verabredet, ein solches Gesetz zu erlassen. Dem widersetzten sich die Arbeitgeberverbände von Anfang an – mit Erfolg. So äußerte sich z.B. der Gesamtverband der deutschen Versicherungswirtschaft im Jahr 1989 wie folgt zu einem Gesetzgebungsvorhaben: „Die Vorschrift stellt […] eine Entmündigung des Arbeitnehmers dar, indem sie ihm verwehrt, selbst darüber zu entscheiden, was mit seinen Daten geschieht.“

1995 verabschiedete die Europäische Union (EU) eine europäische Datenschutzrichtlinie (EU-DSRL), mit der der grenzüberschreitende Datenverkehr im Binnenmarkt erleichtert und hierfür ein einheitliches Datenschutzniveau in den EU-Mitgliedsländern erreicht werden sollte. Diese Richtlinie, die 2001 im BDSG national umgesetzt wurde, hat direkte Auswirkungen auf die Verarbeitung von Beschäftigtendaten z.B. in internationalen Konzernen. Im neuen Jahrhundert nahm die Diskussion in der EU über die Schaffung europäischer bereichsspezifischer Regelungen zum Arbeitnehmerdatenschutz Fahrt auf. Im Jahr 2001 wurde hierzu die erste Stufe eines EU-Konsultationsverfahrens gestartet, im darauf folgenden Jahr die zweite Stufe. Diese v.a. von Arbeitnehmerseite stark geförderte Initiative wurde aber weder von der Öffentlichkeit noch von der Politik aufgegriffen, so dass sie im Sande verlief. Ein Grund hierfür mag sein, dass es in der EU für ein Arbeitnehmerdatenschutzgesetz bisher kaum nationale Vorbilder gab. Lediglich Finnland erließ 2001 ein solches Gesetz, das aber, nicht zuletzt durch bestimmenden Einfluss des Großarbeitgebers Nokia, von einem Schutzgesetz für die Arbeitnehmerinnen und Arbeitnehmer zu einem Kontrollgesetz für die Arbeitgeber mutierte.

Der Widerstand der Arbeitgeber gegen eine Regelung in Deutschland hielt bis ins Jahr 2009 an, als z.B. der Arbeitgeberverband BDA sich wie folgt äußerte: „Es würde die Koordinaten im Arbeitsrecht empfindlich verschieben, wenn unter dem Deckmantel des Datenschutzes die Rechtsbeziehung zwischen Arbeitgeber und Arbeitnehmer wie in einem Arbeitnehmervertragsgesetz verregelt werden würde. […] Es ist zu überlegen, die Zustimmungsnotwendigkeit des Betriebsrates partiell durch eine nachträgliche Informationspflicht zu ersetzen. Der Datenschutz im Konzern muss erleichtert werden. Schließlich muss das Verhältnis von Kriminalitätsbekämpfung und Datenschutz nachgebessert werden.“

Unter der Fiktion einer gleichgewichtigen Vertragsbeziehung zwischen Arbeitgeber und Arbeitnehmer haben es die Verbände der Erstgenannten praktisch bis heute geschafft, eine umfassende Regulierung des Datenschutzes im Beschäftigungsverhältnis zu verhindern. Dies ändert aber nichts daran, dass es eine Vielzahl von Regelungen gibt, die heute anwendbar sind, die aber den Nachteil haben, dass sie oft sehr unspezifisch sind und damit keine klaren und oft sogar schlechte Antworten auf die bestehenden datenschutzrechtlichen Problemlagen geben. Dies gilt insbesondere für die allgemeinen Datenschutzgesetze. Während für öffentlich Bedienstete in den Ländern über die dortigen Landesdatenschutzgesetze (LDSG) teilweise analoge Regelungen zum Beamtenrecht gelten, geben andere LDSG und das BDSG keine wirksamen rechtlichen Sicherheiten. Für den Wirtschaftsbereich ist im BDSG vorrangig der 4. Abschnitt anwendbar, der sich auf den Hinweis der Erforderlichkeit der Datenverarbeitung im Arbeitsverhältnis und ansonsten auf eine Abwägung zwischen Arbeitnehmer- und Arbeitgeberinteressen beschränkt.

Daneben gibt es aber für viele Einzelfragen spezifische Regelungen. Dies gilt insbesondere für die Sozialgesetzbücher (SGB), in denen bereichsbezogen festgelegt ist, welche Daten für die Gewährung von Sozialleistungen – vom Arbeitslosengeld bis zur Unfall- und Krankenversicherung – von den Arbeitgebern und den Betroffenen bereitgestellt und genutzt werden dürfen. Einen Paradigmenwechel nimmt insofern das aus Datenschutzgründen höchst umstrittene ELENA-Gesetz aus dem Jahr 2009 vor, das an die Stelle der Selbstbeibringung der relevanten Sozialdaten durch die Betroffenen einen

umfassenden, von den Arbeitgebern einzuspeisenden **El**ektronischen **Le**istungs**na**chweis (ELENA) vorsieht, der von den Sozialbehörden für die Leistungsberechnung vorrangig herangezogen werden soll. Damit würde die Schaffung einer bundesweiten Einkommensdatenbank der gesamten Erwerbsbevölkerung einhergehen. ELENA wurde Anfang Juli 2010 aus finanziellen Gründen von der Bundesregierung in Frage gestellt. Unabhängig davon steht seine Verfassungsgemäßheit auf dem Prüfstand.

Gesundheitsdaten, auch solche beim Betriebsarzt, werden nach dem Arbeitssicherheitsgesetz und nach einer Vielzahl von spezifischen Verordnungen erhoben. Das aus dem Jahr 2009 stammende Gendiagnostikgesetz regelt u.a. die Frage, inwieweit Arbeitnehmer zu genetischen Untersuchungen bzw. zur Offenlegung ihres Gencodes für arbeitsrechtliche Zwecke veranlasst werden dürfen.

Eine Rolle spielen das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG). Insbesondere Letzteres führt dazu, dass Arbeitgeber, wenn sie die private Nutzung der betrieblichen Kommunikationsmittel erlauben, wie TK-Zugangsanbieter behandelt werden, und das mit der wenig sachgerechten Konsequenz, dass, abgesehen von Abrechnungsprüfungen, keinerlei Kontrollen durchgeführt werden dürfen und das Telekommunikationsgeheimnis umfassend anwendbar ist.

Von großer Bedeutung im aktuellen Arbeitnehmerdatenschutzrecht ist das Betriebsverfassungsgesetz (BetrVG), das zur Vermeidung von übermäßigen Arbeitnehmerkontrollen kollektivrechtliche Instrumente vorsieht. Gemäß § 75 Abs. 2 BetrVG gehört es zu den Aufgaben des Betriebsrates wie auch des Arbeitgebers, die Persönlichkeitsrechte der Arbeitnehmerschaft zu wahren. Gemäß § 80 Abs. 1 Nr. 1 BetrVG überwacht der Betriebsrat die Einhaltung sämtlicher zugunsten der Arbeitnehmer bestehenden Gesetze. Hierzu gehören auch die allgemeinen Regelungen des BDSG sowie spezifische Datenschutzvorschriften. Schließlich kommt dem Betriebsrat nach § 87 Abs. 1 Nr. 6 BetrVG ein generelles Mitbestimmungsrecht bei sämtlichen technischen Einrichtungen eines Unternehmens zu, die zur Verhaltens- und Leistungskontrolle von Arbeitnehmern geeignet sind. Da dies inzwischen praktisch bei dem Einsatz jedweder Informationstechnik am Arbeitsplatz der Fall ist, begründet diese Regelung die Pflicht des Arbeitgebers, vor dessen Einführung die Zustimmung des Betriebsrates einzuholen.

Die Rechtsprechung des Bundesarbeitgerichtes (BAG) hat mehrfach und schon früh festgestellt, dass diese Mitbestimmungspflicht unabhängig davon besteht, ob mit den technischen Einrichtungen Verhaltens- und Leistungskontrollen tatsächlich beabsichtigt sind. Selbst die theoretische Möglichkeit für derartige Kontrollen genügt, um den Betriebsrat beteiligen zu müssen (BAG 09.09.1975, Az. 1 ABR 20/74). Insbesondere in den letzten Jahren hatte das BAG immer wieder Veranlassung, sich mit der informationellen Arbeitnehmerkontrolle zu befassen. So stellte es im Jahr 1997 fest, dass heimliches und unbemerktes Abhören von Telefongesprächen zum Zweck der Arbeitskontrolle unzulässig ist (BAG 29.10.1997, Az. 5 AZR 508/96). Wenig später stellte es klar, dass Arbeitnehmer nicht pauschal und anlasslos zu ärztlichen Untersuchungen zwecks Blutalkoholfeststellung verpflichtet werden dürfen (BAG 12.08.1999, Az. 2 AZR 55/96). Etwas später äußerte sich das BAG gleich zweimal umfassend zur Arbeitskontrolle per Videoüberwachung, die nicht umfassend, sondern nur ausnahmsweise erfolgen darf und begründungspflichtig ist, insbesondere wenn diese heimlich vorgenommen wird. Das BAG fordert vor dem Einsatz eine nachvollziehbare und an Datensparsamkeit orientierte Verhältnismäßigkeitsprüfung (BAG 14.12.2004 Az. 1 ABR 34/03; 2 AZR 51/02; BAG 26.08.2008, Az. 1 ABR 16/07).

Bewegung in die Diskussion um den Beschäftigtendatenschutz kam mit den Überwachungsskandalen bei renommierten großen Arbeitgebern in Deutschland, u.a. bei Lidl, bei der Deutschen Bahn und bei der Telekom. Der Arbeitskreis „Recht & Praxis“ des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. legte im Juni 2008 einen „Vorschlag zu notwendigen Regelungen für ein Gesetz zum Schutz der Persönlichkeitsrechte im Arbeitsverhältnis (GSPA)“ vor, der aber noch keine größere Resonanz fand. Die Datenschutzskandale im Arbeitsbereich und eine Vielzahl weiterer öffentlicher Hingucker führten erst einige Monate später dazu, dass die ohnehin geplanten, auch auf Skandale zurückgehenden BDSG-Änderungen zur Datennutzung für Werbezwecke und zum Adressenhandel um eine Regelung zum Arbeitnehmerdatenschutz ergänzt wurden. Damit sollte noch vor der Bundestagswahl 2009 Handlungsbereitschaft signalisiert werden.

Die in direkter Reaktion auf Rasterfahndungen bei der Deutschen Bahn zum Zweck der Korruptionsbekämpfung formulierte Regelung des neuen § 32 BDSG lässt die heiße Nadel beim Stricken erkennen und wirft mehr dogmatische Fragen auf, als sie Rechtssicherheit zu schaffen in der Lage ist:

Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die

Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

V. Gesetzgebungsbestrebungen

Nicht einigen konnte sich zum Ende der 16. Legislaturperiode die rotschwarze Bundesregierung auf einen Gesetzentwurf des damaligen SPD-Arbeitsministers Scholz, den dieser kurz vor der Wahl der Öffentlichkeit vorstellte und der in der darauffolgenden Legislaturperiode von der SPD-Bundestagsfraktion als Oppositionsentwurf in die parlamentarische Debatte eingebracht wurde (BT-Drs. 17/69). Dieser Entwurf zielt weitgehend auf eine Vollregelung der Thematik in einem Spezialgesetz, also nicht nur auf eine Ergänzung des BDSG. Der Entwurf benennt mit seinen Regelungen einige wichtige Fragestellungen, weshalb es sinnvoll ist, diese hier kursorisch zu referieren:

§§ 6 f. Datenverarbeitung im Einstellungsverfahren

§ 8 Datenerhebung nach folgenden Grundlagen: Gesetz, Vertrag, zur Wahrnehmung von Rechten, zur Überprüfung eines Straftatverdachts und zur Feststellung der Gesundheitseignung ohne Diagnosen

§ 9 Abs. 2 Übermittlung an Dritte zu Zwecken der Gefahrenabwehr und Strafverfolgung sowie nach Interessenabwägung oder auf Basis der Einwilligung des Betroffenen

§ 11 Videoüberwachung für spezifische Sicherungs- u. Kontrollzwecke mit Sicherung der Transparenz und der Datenlöschung, Zulassung heimlicher Kontrolle bei konkretem Tatverdacht

§ 12 Einsatz von Ortungssystemen für Sicherheitszwecke und zur Einsatzkoordinierung

§ 13 Einsatz von Biometrie nur zur Autorisierung und Authentifikation

§ 14 Regelung des Einsatzes von Telekommunikations-(TK-)Dienstenauf der Basis von Betriebsvereinbarungen, Trennung zwischen dienstlicher (Kontrollen als Stichprobe oder bei konkretem Anlass) und privater Nutzung (Verarbeitung zwecks Abrechnung oder Sicherheit)

§ 15 Bei Telearbeit: Verbot dauerhafter Fernüberwachung und Normierung einer spezifischen Geheimhaltungsverpflichtung

Spezifische Verschlüsselungspflichten (z.B. § 14 Abs. 2 Nr. 4 Schweigepflicht, TK-Daten, § 17 Abs. 1 Biometriedaten)

§ 18 Generelle Benachrichtigungspflichten, v.a. bei sensiblen Verfahren

§ 19 Benachrichtigungspflicht bei Datenpannen

§ 25 Datenverarbeitung im Auftrag

§ 26 Konzern-Datenverarbeitung

§ 33 Datenverarbeitung durch Interessenvertretung (Betriebsrat)

Nicht vorgesehen waren bzw. sind spezifische Regelungen zum Scoring, zum Screening bzw. zu Rasterfahndungen und zum Whistleblowing. Auch das immer wieder diskutierte kollektive Klagerecht ist in dem Entwurf nicht enthalten.

Nicht nur in der Opposition, auch in der Bundesregierung werden nun Überlegungen zur Regulierung des Beschäftigtendatenschutzes angestellt. Ende März 2010 legte das Bundesinnenministerium Eckpunkte zur Neuregelung des Beschäftigtendatenschutzes im Bundesdatenschutzgesetz vor. Hieran gab es sofort heftige Kritik, die z.B. in „Eckpunkte eines Beschäftigtendatenschutzgesetzes“, formuliert von AOT, DVD, BIT, FoeBud, Forba, FORBIT u.a., Eingang fand (DANA 2/2010, 72; AuR 7-8/2010, 314 f.). Ende Mai wurde dann vom Ministerium ein Regelungsentwurf vorgelegt, der in die Anhörung interessierter Verbände ging. Diese reagierten wenig schmeichelhaft auf die Ergänzung des § 32 um einen ganzen Unterabschnitt von § 32 bis zu § 32l im BDSG (z.B. DVD DANA 2/2010, 73). Am 17.06.2010, einen Tag vor einer Anhörung im Bundesinnenministerium, veröffentlichte der Deutsche Gewerkschaftsbund einen „DGB-Entwurf für ein Arbeitnehmerdatenschutzgesetz“ (http://www.soliserv.de/presse-DGB-2010_01.htm; AuR 7-8/2010, 315ff.). Am 19.07.2010 lud die Fraktion Bündnis 90/Die Grünen zur „Mitarbeit am grünen Gesetzentwurf“ ein (http://beschaeftigten-datenschutz.de/). Am 28.08.2010 beschloss dann das Bundeskabinett einen gegenüber den Referentenentwürfen leicht verbesserten Gesetzentwurf (BR-Drs. 535/10). Dieser Entwurf wurde umgehend von Arbeitgeber- wie Arbeitnehmerseite sowie von der Opposition heftig kritisiert. Eine umfassende Kritik an dem Entwurf wurde z.B. vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (https://www.datenschutzzentrum.de/presse/20101012-arbeitnehmerdatenschutz.htm) oder von der Neuen Richtervereinigung (http://www.nrv-net.de/main.php?id=171&stellung_id=89&lv_id=&fg_id=) veröffentlicht.

Der Bundesrat entwickelte in den Ausschüssen eine Vielzahl äußerst positiver Verbesserungsvorschläge (BR-Drs. 535/2/10, dazu LfD Baden-Württemberg http://www.baden-wuerttemberg.datenschutz.de/lfd/pm/2010/10_28.htm), die aber nur teilweise am 05.11.2010 vom Bundesrat beschlossen wurden. Gefordert ist nunmehr wieder die Bundesregierung, aber dann vor allem der Bundestag und die öffentliche Diskussion.

VI. Rechtsfolgen

Die Rechtsfolgen von Verstößen im Arbeitnehmerdatenschutzrecht werden nicht durch den in der Diskussion befindlichen Entwurf berührt. Insofern sind die bestehenden Gesetze anzuwenden. Grundlegendes Datenschutzrecht aller Arbeitnehmer und die Grundlage sämtlicher individual- und kollektivrechtlichen Ansprüche ist ein aus dem Recht auf Einsicht in die Personalakte weiterentwickelter Auskunftsanspruch des Arbeitnehmers gegenüber dem Arbeitgeber auf umfassende Mitteilung der zu seiner Person gespeicherten Daten. Gemäß dem allgemeinen Datenschutzrecht besteht bei falscher, rechtswidriger oder nicht mehr erforderlicher Datenspeicherung ein Recht auf Berichtigung, Sperrung und Löschung bzw. in arbeits- bzw. zivilrechtlicher Lesart auf Unterlassung und Beseitigung. Als materielle Kompensation immaterieller Persönlichkeitsverletzungen sind grundsätzlich Schadenersatz- und Schmerzensgeldansprüche möglich. Da jedoch zivilrechtlich hierfür eine schwerwiegende Persönlichkeitsbeeinträchtigung verlangt wird und die Frage der Erheblichkeit bei Datenschutzverstößen bis heute weitgehend ungeklärt geblieben ist, hat dieses Instrument

auch im Arbeitsrecht keine wesentliche praktische Bedeutung erlangt.

Denkbar sind weiterhin direkte Auswirkungen eines Datenschutzverstoßes auf den Arbeitsvertrag. So ist eine Anfechtbarkeit der Willenserklärung bei Abschluss des Vertrages möglich, wenn z.B. der Arbeitgeber den Arbeitnehmer über die Zulässigkeit bestimmter Datenerfassungen getäuscht hat. Auch ein Kündigungsanspruch steht im Raum. Bei Aufrechterhaltung des Arbeitvertrages wird darüber gesprochen, dass bei bestimmten Datenschutzverstößen dem Arbeitnehmer ein Zurückbehaltungsrecht seiner Arbeitsleistung zusteht.

Von praktischer Relevanz ist bisher v.a. die Frage, inwieweit die auf illegaler Datenerhebung und -auswertung basierende Begründung einer Kündigung ein Verwertungsverbot und damit faktisch einen Kündigungsausschluss zur Folge hat. Dies ist grundsätzlich bei wesentlichen Verstößen anerkannt; Ausmaß und Begründung sind aber in Rechtsprechung wie in der Literatur äußerst umstritten.

Neben diesen zivil- und arbeitsrechtlichen Konsequenzen gibt es datenschutzrechtliche bis hin zu strafrechtlichen Sanktionsmöglichkeiten von Datenschutzverstößen. Die einfachste und zugleich folgenloseste Sanktion ist die reine Feststellung der Rechtswidrigkeit durch die Aufsichtsbehörde, die sog. Beanstandung nach § 38 Abs. 1 BDSG. In der Praxis als äußerst wirksames Instrument für die Aufsichtsbehörden hat sich bei den Datenschutzskandalen in den Jahren 2008/2009 die Veröffentlichung über die genaueren Umstände erwiesen. Neben der Veröffentlichung von Beanstandungen sind auch schon während des Verfahrens im Interesse einer Gefahrenabwehr vorläufige Bewertungen und Warnungen zulässige Praxis.

Während die Pressearbeit von Aufsichtsbehörden eher eine unförmliche Sanktionsform ist, gilt dies nicht für das Durchführen von Ordnungswidrigkeitenverfahren nach § 43 BDSG, was bei Formverstößen zu einem Bußgeld bis zu 50.000 Euro und bei materiellrechtlichen Verstößen bis zu 300.000 Euro führen kann. Bei Bereicherungs- und Schädigungsabsicht kann die Aufsichtsbehörde den Fall nach § 44 BDSG zur Strafverfolgung an die Staatsanwaltschaft abgeben. Bisher wenig erprobt sind Zwangsgelder und Unterlassungsverfügungen, die bis zum 01.09.2009 nur hinsichtlich technisch-organisatorischer Mängel möglich waren. Seither kann auch ein materiellrechtlicher Verstoß zu einer verwaltungsrechtlichen Verfügung führen. Inwieweit dieses Instrument genutzt wird und wirksam ist, muss sich noch erweisen.

VII. Schlussbemerkung

In den ersten 30 Jahren des Bestehens des Datenschutzrechtes war der Beschäftigtendatenschutz in einen Dornröschenschlaf versunken. Dies hat dazu geführt, dass trotz und auch wegen der zunehmenden technischen Kontrollmöglichkeiten die Dreistigkeit der Arbeitgeber bei der Mitarbeiterkontrolle zunahm. 2008 – auch ansonsten für die öffentliche Bewusstwerdung für den Datenschutz in Deutschland ein wichtiges Jahr – kam das Fass zum Überlaufen, so dass die Arbeitgeberseite mit ihren Abwehrgefechten gegen eine rechtsklare Normierung nicht mehr gehört wurde. Doch hat die Arbeitgeberseite bis heute immer noch nicht verstanden, dass ein hohes Datenschutzniveau im Betrieb und die damit einhergehende Freiheit der Mitarbeiter eine grundlegende Bedingung für eine hohe und innovative Produktion ist oder zumindest sein kann. Es wird in Kürze ein mehr oder auch weniger streng normiertes Beschäftigtendatenschutzrecht geben. Mitarbeiterkontrolle wird immer mehr in den Fokus der Auseinandersetzung zwischen den Parteien von Kapital und Arbeit geraten. Dies wird zwangsläufig zu einer intensiveren Befassung auch der Arbeitsgerichte führen, die bis heute mit ihrer Rechtsprechung ein valides materiell-rechtliches Fundament für den Datenschutz gelegt haben, das sich aber wegen der Einzelfallbezogenheit und dem fehlenden Bewusstsein in den Betrieben noch nicht in eine entsprechende Praxis umgesetzt hat. Insofern bleibt vieles zu tun: beim Gesetzgeber, den Parteien im Betrieb wie in der Arbeitswelt generell und auch bei den Aufsichtsbehörden.

Kay Ann Gruling

Anonyme Bewerbungen

In die alte Debatte um den Beschäftigtendatenschutz mischt sich seit einiger Zeit die Diskussion um die Erforderlichkeit so genannter anonymer Bewerbungen. Die Forderung nach der Möglichkeit, ohne Nennung von Namen, Geschlecht, Alter und Hautfarbe sowie ohne ein Foto eine Bewerbung abgeben zu können, wird in unseren Breiten noch skeptisch beäugt. Zu sehr sind wir an unsere Standardabläufe bei Bewerbungsverfahren gewöhnt, um den pseudonymen Einstieg in eine Stellenauswahl als gleichwertig zu empfinden.

Dabei wird in vielen Diskussionsbeiträgen scheinbar vergessen, dass die Pseudonymität von Bewerbern ja nur bis zu einem bestimmten Zeitpunkt aufrechterhalten wird. Spätestens beim Bewerbungsgespräch wird, das liegt in der Natur der Sache, die Pseudonymität aufgehoben. Beschwerlich und polemisch vorgetragene Befürchtungen, man könne möglicherweise genötigt sein, sich quasi im Blindflug den „falschen" Bewerber einzustellen, entbehren bei genauerer Betrachtung jeder sachlichen Grundlage.

Auch wenn solche Bewerbungsverfahren in erster Linie unter dem Gesichtspunkt der Vermeidung von Diskriminierung diskutiert werden, so handelt es sich hierbei auch um Gestaltungsfragen im Bewerbungsprozesses, bei dem Erforderlichkeit und Zweckbindung der personenbezogenen Bewerberdaten eine wesentliche Rolle spielen. Ein anfangs pseudonymer Bewerbungsprozess würde auch das Gebot der Datensparsamkeit als zentrale Anforderung des Datenschutzes angemessen umsetzen.

Dass eine solche datensparsame Gestaltung keine Qualitätseinbußen bei der Stellenbesetzung mit sich bringt, ist in anderen Ländern seit langem bekannt. Zum Blick über den Tellerrand soll die folgende kurze Darstellung aus Sicht einer amerikanischen Ärztin animieren. Kay Ann Gruling verbrachte während Ihres Studiums selbst ein Jahr in Bonn und lebt heute in Wausau in Wisconsin.

I have followed with interest the current discussion in Germany about the so-called "anonymous job application." Truthfully, I initially was surprised to discover that there needed to be such a discussion! Germany is such a progressive country in so many respects.

First some background information about myself. I reside in Wausau, Wisconsin and am of German heritage. Early in my university career, I studied German and culminated those studies with a year-long study in Bonn, Germany in 1983-84 as a Rotary Scholar and Goodwill Ambassador. I ultimately finished my studies in the United States and graduated as a medical doctor. Currently, I am practicing family medicine as part of a large medical clinic.

From an American standpoint, our system of the "anonymous job application" works well. In a formal job application process, the organization offering the job prepares a detailed description of the requirements of the job. This includes formal educational requirements, associated job related experience, physical demands of the job, etc. Later, references are obtained. This is usually from an individual who is able to comment on the applicant's job qualifications as well as character and so forth. Thereafter, the applicant typically completes a formal, written job application. Most often, this application allows the job candidate to list his or her job qualifications and other pertinent information about him or her. Job references may be obtained either initially on all the applicants or may be limited to those applicants who were deemed the most promising candidates.

The above information is then utilized to determine which candidates will be interviewed for the job. At this point, the interviewer can then discover the applicant's skin color, approximate age, as well as any obvious disability. Specifics about race, ethnicity, religion, etc. still are only presumed based on appearance. For instance, a candidate dressed as an orthodox Jew, can likely be assumed to be of that faith. However, someone who appears to be Arabic cannot be presumed to be of the Islamic faith. Note that gender can often be determined with the original job application, although this too cannot be for certain. For instance, my name, 'Kay,' is generally considered a man's name in Germany even though I am a woman. This is an issue with multiple names in most languages.

Under American law, there is no option at any time to legally request information from a job applicant or hired employee regarding gender, age, race, sexual orientation or religion. It is based upon the belief that as long as the applicant/employee is qualified for the job and/or performs the job adequately, the above issues do not matter. I have personally been involved in multiple hires for staff at our clinic and have never had any problems as a result of the "anonymous job application." This system really works well.

Hopefully, the above helps clarify the "anonymous job application" issue. Likewise, hopefully it also dispels concern about it as well. The system does in fact generally work well. The best part is that it actually can help procure the best applicant/employee because the initial screening process frees us from our own personal biases about gender, religion, race, etc. These factors only potentially become an issue during and after the interview. Unfortunately, this is still leaves an opening for the potential for discrimination. However, the "anonymous job application" itself is progressive and ideal for all involved.

Sören Jungjohann

Chronik der Kodifizierung des Arbeitnehmerdatenschutzes

2009

18. Februar 2009

Angesichts verschiedener so genannter Datenskandale beschließt die CDU/CSU-SPD-Bundesregierung, umgehend eine Grundsatzregelung zum Datenschutz der Arbeitnehmer in das Bundesdatenschutzgesetz aufzunehmen. Parallel dazu sollen die Arbeiten an einem Arbeitnehmerdatenschutzgesetz wieder aufgenommen werden.

1. Juli 2009

Der Innenausschuss des Deutschen Bundestags empfiehlt dem Bundestag, den Entwurf eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften zu verabschieden. Art. 1 Nr. 12 des Gesetzentwurfs enthält mit § 32 BDSG eine Generalklausel zum Schutz von Arbeitnehmerdaten.

3. Juli 2009

Der Deutsche Bundestag beschließt das Gesetz zur Änderung datenschutzrechtlicher Vorschriften.

10. Juli 2009

Das Gesetz passiert den Bundesrat.

18. August 2009

Das Gesetz zur Änderung datenschutzrechtlicher Vorschriften wird im Bundesgesetzblatt I S. 2814-2820 verkündet.

1. September 2009

Der neue § 32 BDSG (Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigtenverhältnisses) tritt als Bestandteil des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften in Kraft.

4. September 2009

Unmittelbar vor der Bundestagswahl legt Bundesarbeitsminister Olaf Scholz einen Diskussionsentwurf für ein Gesetz zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG) vor. Der Entwurf wird vom Bundeskabinett nicht mehr behandelt.

26. Oktober 2009

Die neue Regierungskoalition aus CDU/CSU und FDP kündigt in ihrem Koalitionsvertrag an, den Arbeitnehmerdatenschutz in einem eigenen Kapitel im Bundesdatenschutzgesetz zu regeln.

25. November 2009

Die SPD-Fraktion bringt den Scholz'schen Diskussionsentwurf für ein Gesetz zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG) als Gesetzesvorlage in den Bundestag ein.

2010

31. März 2010

Bundesinnenminister Thomas de Maiziére stellt die Eckpunkte der Bundesregierung für die geplante Novellierung des Arbeitnehmerdatenschutzrechts vor.

31. Mai 2010

Das Bundesinnenministerium legt einen Referentenentwurf für ein Gesetz zur Regelung des Beschäftigtendatenschutzes vor. Der Entwurf wird von Gewerkschaften und Datenschützern heftig kritisiert.

25. August 2010

Die CDU/CSU-FDP-Bundesregierung verabschiedet den Gesetzentwurf des BMI, nachdem dieser zuvor in wesentlichen Punkten überarbeitet worden war. Arbeitgeberverbände und Gewerkschaften kritisieren den Entwurf gleichermaßen.

3. September 2010

Die Bundesregierung bringt den Entwurf des Gesetzes zur Regelung des Beschäftigtendatenschutzes in den Bundesrat ein.

5. November 2010

In seiner Stellungnahme schlägt der Bundesrat vor, den Gesetzentwurf der Bundesregierung in wesentlichen Punkten zu ändern und zu ergänzen.

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund

Elektronischer Aufenthaltstitel für Drittausländer

Deutsche StaatsbürgerInnen müssen sich damit abfinden, dass auf ihrem Reisepass mit Funkchip, dem ePass, Fingerabdrücke gespeichert sind. Auf dem nPA, dem neuen Personalausweis, ist die digitale Speicherung der Fingerabdrücke freiwillig. Wenn es nach dem Willen des Bundesinnenministeriums (BMI) geht, sollen alle nichteuropäischen AusländerInnen in Deutschland vom 01.05.2011 an mit einem „elektronischen Aufehthaltstitel" ausgestattet werden, auf dem auch zwei digitalisierte Fingerabdrücke und ein digitales Foto gespeichert werden. Der Beschluss für diesen eAufenthaltstitel geht auf zwei Verordnungen der Europäischen Union aus den Jahren 2002 und 2008 zurück, wonach sogenannte Drittstaatenangehörige ein Dokument ähnlich dem biometrischen Personalausweis besitzen müssen. Bislang mussten AusländerInnen ihre Aufenthaltsberechtigung mit einem in den Pass geklebten Dokument oder einer Klappkarte nachweisen, was weniger als einen Euro kostet. Die neue Karte soll 10 Jahre gültig sein. Ab Mai 2011 müssen die DrittausländerInnen bei deutschen Behörden vorstellig werden, ein biometrisches Foto und, so sie älter als sechs Jahre sind, zwei Fingerabdrücke abgeben. Dafür bekommen sie einen Ausweis ähnlich dem neuen Personalausweis, der nach Angaben des BMI 28,80 Euro kosten soll. Die Bundesländer fordern über den Bundesrat aufgrund der hohen Kosten für Verwaltung und Technik noch höhere Gebühren von bis zu 90 Euro. Wie im nPA soll ein kontaktlos auslesbarer RFID-Chip die Daten speichern. Die Ausländerbehörden sollen die Daten einlesen und an die Bundesdruckerei übermitteln, die dann die Karten herstellen soll. Ziel ist die Verhinderung und Bekämpfung der illegalen Einwanderung und des illegalen Aufenthalts. Eine zentrale Speicherung von Fingerabdrücken im Ausländerzentralregister ist laut BMI nicht vorgesehen. Eine Zusatzfunktion der neuen Karte soll als Identitätsausweis im Internet dienen.

Memet Kilic, integrationspolitischer Sprecher der Grünen-Bundestagsfraktion, hält die Erfassung für unverhältnismäßig: „Fingerabdrücke sind erkennungsdienstliche Behandlungen von Personen. Dies haben die Immigranten in unserem Land nicht verdient". Die Linke erklärte, der Bundesinnenminister stelle so die Schwächsten unter „Generalverdacht". Der Bundesvorsitzende der Türkischen Gemeinde in Deutschland, Kenan Kolat, bestätigte: „Gerade vor dem Hintergrund der rauen Integrationsdebatte ist es fatal, jetzt einen Generalverdacht gegen ganze Bevölkerungsgruppen auszusprechen." Der Vorsitzende des Bundeszuwanderungs- und Integrationsrats, Karama Diaby, ergänzte: „Mit der geplanten Maßnahme werden Menschen aus Drittstaaten zunehmend als potenzielle Kriminelle gesehen. Auch wenn dies eine Maßnahme ist, die nicht von der Bundesregierung initiiert wurde, hätten wir von der Regierung erwartet, sich gegen diese Abschottungspolitik starkzumachen." Für Jan Korte von den Linken ist es „inakzeptabel und skandalös", dass auch von Kindern Fingerabdrücke erfasst werden: „Das ist ein verlogenes Spiel: Die deutsche Bundesregierung setzt sich zuerst in Brüssel vehement dafür ein und verweist dann auf die reine Umsetzung von EU-Recht." Der SPD-Innenpolitiker Dieter Wiefelspütz verteidigte dagegen die Pläne: „Ich sehe darin keine diskriminierende Wirkung. Fingerabdrücke und biometrisches Foto sollten Standard für jeden Menschen sein, der in Deutschland lebt."

Nach Auskunft des BMI werden jährlich etwa 1,1 Millionen Menschen die neue elektronische Karte benötigen, unter anderem auch US-BürgerInnen und SchweizerInnen. Insgesamt leben 4,3 Mio. sog. DrittausländerInnen in Deutschland. Die Schweiz empörte sich über die Planungen; bisher sind die Menschen aus diesem Land nach einem Abkommen mit der EU aus dem Jahr 1999 davon befreit, sich einen solchen Aufenthaltstitel besorgen zu müssen. Sie dürfen sich hier niederlassen, ohne dies zuvor zu beantragen. Trotzdem sollen sie sich künftig dieses „Recht auf Freizügigkeit" durch eine „Aufenthaltserlaubnis" bestätigen lassen. Gemäß Medienberichten überlegt das schweizerische Außenministerium (EDA), gegen die Maßnahme vorzugehen, da diese bilaterale Verträge verletze. Die Basler Zeitung titelte „Deutschland will von Schweizern die Fingerabdrücke" und meinte weiter: „Dem EDA ist derzeit kein anderer EU-Staat bekannt, der für Schweizer Bürger eine solche Ausweispflicht vorsieht." Die Schweiz plant entsprechend den EU-Vorgaben einen ähnlichen Ausweis für dort lebende AusländerInnen – Deutsche sollen aber davon nicht betroffen sein (Biermann www.zeit.de 20.10.2010; SZ 20.09.2010, 5; Omnicard Newsletter 10/2010, 3; Kaul www.taz.de 20.09.2010).

Bund

Politiker fordern verstärkte Einwanderungskontrolle

Bei einem Treffen am 15.10.2010 forderten die Innenminister der unionsregierten Bundesländer ein schärferes Vorgehen gegen illegale Einwanderer. Das Bundeskriminalamt (BKA) sowie Sprachgutachter sollten zur Klärung der Identität von AusländerInnen eingesetzt werden. Außenminister Guido Westerwelle (FDP) plädierte dafür, über den Nutzen von ZuwandererInnen

offen zu debattieren: „Wir haben als Staat ein wohlverstandenes nationales Interesse zu fragen, wen wir einladen wollen, in Deutschland zu leben. Und wir haben ein Recht zu fragen, welchen Beitrag Einwanderer leisten wollen, damit nicht nur sie, sondern das ganze Land einen Gewinn davon hat“ (SZ 16./17.10.10.2010, 5).

Bund

CDU/CSU pocht auf Visadatei

Bei einem Treffen von InnenpolitikerInnen der Koalition und den drei beteiligten Ressorts Innen, Außen und Auswärtiges Amt am 05.10.2010 sind, so eine teilnehmende Person, „die Fetzen geflogen“, als über die Visa-Warndatei diskutiert wurde. Es habe keine Annäherung gegeben (vgl. Weichert, DANA 1/2008, 24). Die Unionsfraktion sei verärgert, so ihr innenpolitischer Sprecher Hans-Peter Uhl: „Nun werden die drei Parteivorsitzenden die Einhaltung des Koalitionsvertrags durchsetzen müssen“. Dort haben Union und FDP vereinbart, eine Datei einzurichten, in der Visa-Betrügende, Menschenhändler und Menschen, die durch Einreisevergehen aufgefallen sind, geführt werden. Laut Uhl sperre sich insbesondere Justizministerin Sabine Leutheusser-Schnarrenberger dagegen, den Sicherheitsbehörden Zugriff auf die Datei zu geben, was die Union fordert. Mit Hilfe der gemeinsamen Datei von Auswärtigem Amt und Innenministerium sollen Visa-Anträge deutlich schneller bearbeitet werden können. Umstritten ist zudem, wer in die Datei aufgenommen werden soll – nur verurteilte Straftäter oder auch Verdachtsfälle und Menschen, die auffällig oft AusländerInnen einladen (SZ 07.10.2010, 6).

Bund

Journalistenverbände gegen Sicherheitschecks

In einem Brief an die Innenministerkonferenz haben sich TV-Sender, Zeitungsverleger und Journalistenverbände (ARD, ZDF, BDZV, Deutscher Presserat, VDZ, DJV, ver.di, VPRT) gegen die Praxis der Zuverlässigkeitsprüfung von JournalistInnen bei Großereignissen wie Fußball-WM, NATO-Gipfel oder Leichtathletik-WM gewandt. Diese Checks würden pauschal bei allen JournalistInnen durchgeführt und gefährdeten den Rechtsanspruch auf Akkreditierung. Ein Akkreditierungswunsch dürfe nur versagt werden, wenn es konkrete Anhaltspunkte gibt, dass die Person die Veranstaltung stören oder die Gesundheit von Teilnehmenden gefährden wolle. Die betroffene Person müsse Gelegenheit haben, zu den Sicherheitsbedenken Stellung zu nehmen (Der Spiegel 35/2010, 143).

Bund

Jahresstatistik zum Großen Lauschangriff

Am 22.09.2010 wurde der Jahresbericht zum Großen Lauschangriff von Bundesinnenminister Thomas de Maizière (CDU) und seiner Kollegin im Justizressort, Sabine Leutheusser-Schnarrenberger (FDP), vom Bundeskabinett angenommen. Danach haben Strafverfolger 2009 in sieben Bundesländern in acht Ermittlungsverfahren insgesamt neun „akustische Wohnraumüberwachungen“, also eine Verwanzung von Wohnräumen, durchgeführt. 2008 waren es laut der offiziellen Jahresstatistik sieben Verfahren. Die Zahl der Genehmigungen für einen Großen Lauschangriff liegt seit mehreren Jahren auf einem relativ niedrigen Niveau. 2005 ordneten Richter in sieben Verfahren eine akustische Wohnraumüberwachung an, 2006 in drei, 2007 in zehn Ermittlungsfällen. Davor lag die Zahl der genehmigten Wanzeneinsätze jeweils bei rund 30 pro Jahr. Den Rückgang hat hauptsächlich das Urteil des Bundesverfassungsgerichts zur Eingrenzung des Großen Lauschangriffs vom März 2004 sowie dessen gesetzliche Umsetzung im Jahr darauf bewirkt. Zu den Beschwerdeführern zählte damals Leutheusser-Schnarrenberger, die zuvor Anfang 1996 aus Protest gegen den Beschluss des Gesetzes zur akustischen Wohnraumüberwachung durch die damalige schwarz-gelbe Koalition ihre erste Amtszeit als Bundesjustizministerin vorzeitig beendet hatte. Der Rücktritt wäre angesichts der Zahlen der vergangenen Jahre aber gar nicht nötig gewesen, meinte nun der Vize der CDU/CSU-Bundestagsfraktion Günter Krings. Die Wohnung sei als privatester Bereich des Bürgers sehr gut geschützt. Polizei und Staatsanwaltschaften gingen mit ihren Befugnissen verantwortungsvoll um, was auch für ein anderes umstrittenes Fahndungsinstrument gelte. So habe das Bundeskriminalamt bislang nach wie vor keine heimliche Online-Durchsuchung durchgeführt, obwohl die prinzipielle gesetzliche Möglichkeit dazu seit Anfang 2009 bestehe (Kremp www.heise.de 22.09.2010).

Bund

Zoll nutzt Quellen-Telekommunikationsüberwachung

Das Bundesfinanzministerium hat auf Anfrage der FDP eingeräumt, dass die Zollfahndung im Verdachtsfall bei Internet-Telefongesprächen über den beliebten Anbieter Skype die „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ) einsetzt. Dabei spielen die Ermittler auf den Rechner von Verdächtigen heimlich ein Programm zum Mitlauschen auf. Nötig ist eine richterliche Anordnung. Der parlamentarische Staatssekretär Hartmut Koschyk schreibt in seiner Antwort: „Mittels einer speziell entwickelten Software können solche Gesprächsinhalte, noch bevor sie verschlüsselt werden, auf einen bestimmten Server ausgeleitet werden“. Die Überwachung beziehe sich „ausschließlich auf Daten aus laufenden Kommunikationsvorgängen“ und stehe damit im Einklang mit dem Urteil des Bundesverfassungsgerichts zur sog. Online-Durchsuchung. Dies sieht Gisela Piltz, innenpolitische Sprecherin der FDP, anders. Die Verfassungsrichter hätten deutlich gemacht, dass schon mit der Quellen-TKÜ die entscheidende Hürde genommen sei, das System insgesamt auszuspähen (Der Spiegel 41/2010, 16).

Bund

Stasi-Überprüfung bis 2019

Die schwarz-gelbe Koalition hat sich auf eine Verlängerung der Stasi-Überprüfungen im öffentlichen Dienst bis 2019 verständigt (vgl. DANA 2010, 119). Der stellvertretende Vorsitzende der CDU/CSU-Bundestagsfraktion Arnold Vaatz, informierte, dass die 2011 auslaufende Frist verlängert werde: „Darüber sind wir uns mit der FDP einig." Vaatz sprach sich dafür aus, 2019 eine „Zäsur" zu machen und die Zuständigkeit für die Stasi-Unterlagen von der zuständigen Behörde an das Bundesarchiv zu überführen. 2019 laufe auch der Solidarpakt aus: „30 Jahre nach der Wiedervereinigung wäre das Thema dann erledigt" (SZ 06./07.11.2010, 6).

Bund

Gesetzentwurf gegen Internet-Abzocke

Bundesjustizministerin Sabine Leutheusser-Schnarrenberger hat am 29.10.2010 einen Referentenentwurf für ein Gesetz zum besseren Schutz der VerbraucherInnen vor Kostenfallen im elektronischen Geschäftsverkehr präsentiert. Bei kostenpflichtigen Online-Angeboten sollen Nutzende künftig mit einem deutlichen Hinweis vor versteckten Kosten gewarnt werden. Vor einer Bestellung sollen die VerbraucherInnen mit einem Klick ausdrücklich bestätigen, dass sie die Erläuterung gesehen haben. Die KundInnen könnten sich, so die Ministerin, so leichter gegen unberechtigte Zahlungsaufforderungen zur Wehr setzen. Mit der „Button-Lösung" werde die Transparenz beim E-Commerce insgesamt verbessert und unseriösen Geschäftsmodellen der Boden entzogen. Bislang hatte die Bundesregierung für eine europäische Lösung plädiert und Forderungen der Bundesländer für einen nationalen Alleingang zurückgewiesen. Ein Vorschlag aus Berlin, die Regelung gegen Internet-Abzocke in die geplante Verbraucherrechte-Richtlinie der EU aufzunehmen, liegt in Brüssel auf dem Tisch. Doch rechnet Leutheusser-Schnarrenberger mit einer Verabschiedung der Direktive nicht vor Ende 2012. Diese müsse zudem anschließend noch in innerstaatliches Recht umgesetzt werden. Da dieser Zeitrahmen deutlich zu lang sei, solle nun zunächst eine nationale Regelung geschaffen werden. Weil Abofallen im Netz nicht an Staatengrenzen haltmachten, sei eine europaweite Lösung weiterhin notwendig.

In einem von Rheinland-Pfalz eingebrachten Entschließungsantrag im Bundesrat wird gefordert, mit einer Button-Lösung für Online-Verträge Kostenfallen im Netz entgegenzuwirken: „Ein auf eine entgeltliche Gegenleistung gerichteter Vertrag im elektronischen Rechtsverkehr soll nur dann wirksam sein, wenn der Verbraucher vom Unternehmer einen Hinweis auf die Entgeltlichkeit und die mit dem Vertrag verbundenen Gesamtkosten in deutlicher, gestaltungstechnisch hervorgehobener Form erhalten hat und diese Kostenmitteilung in einer von der Bestellung gesonderten Erklärung bestätigt" (Krempl www.heise.de 29.10.2010).

Bund

ELENA-Start auf 2014 hinausgeschoben

Die Bundesregierung will gemäß einer Bekanntgabe vom 19.11.2010 die Testphase für die umstrittene Arbeitnehmer-Datenbank ELENA um zwei Jahre bis Ende 2013 verlängern. Als Realstart ist nun der 01.01.2014 vorgesehen. Mit ELENA (Elektronischer Entgeltnachweis) soll lästiger Papierkram im Bescheinigungswesen der Arbeitswelt gegenüber Sozialleistungsträgern abgeschafft werden. Anfang Januar 2010 startete die erste Phase: Unternehmen müssen mit ihren monatlichen Gehaltsabrechnungen für jeden ihrer Beschäftigten zahlreiche Eckdaten wie Name und Anschrift, Versicherungsnummer, Gesamt-, Steuer- und Sozialversicherungs-Bruttoeinkünfte, Abzüge für die Sozialversicherung sowie steuerfreie Bezüge verschlüsselt an die zentrale Datenbank der Deutschen Rentenversicherung übermitteln. Ursprünglich sollten mit Beginn des Regelbetriebs ab 2012 die für die Bewilligung von Anträgen auf Arbeitslosengeld, Wohngeld und Bundeselterngeld erforderlichen Daten elektronisch abgerufen werden können, papierne Arbeitgeberbescheinigungen sollten dann nicht mehr nötig sein. Rund 3,2 Millionen Arbeitgeber erstellen jährlich etwa 60 Millionen Bescheinigungen über Einkommen und Beschäftigung ihrer Mitarbeiter. Diese werden bisher ausgedruckt und von Ämtern zur Bewilligung von Sozialleistungen später wieder per Hand eingegeben. Die Kommunen hatten gewarnt, dass die Kosten für den Aufbau von ELENA aus dem Ruder laufen. Ihnen drohten durch das Verfahren Mehrkosten von bis zu 250 Millionen Euro. Die Entlastungen für Unternehmen und Bürger seien dagegen äußerst gering, hieß es. Der Bundestag hatte sich Ende September 2010 gegen ein ELENA-Moratorium ausgesprochen. Das endgültige Schicksal von ELENA wird nun der 2013 neu gewählten Bundesregierung überlassen. Was mit den bisher gespeicherten Daten passiert, ist unklar. Da diese nicht auf Vorrat gespeichert werden dürfen, müssen sie wohl wieder gelöscht werden (www.heise.de 19.11.2010; KN 20.11.2010, 2; SZ 20./21.11.2010, 6).

Bund

„Tatort Internet" missbraucht Pädophile

Die seit Anfang Oktober 2010 ausgesendete und von der Ehefrau des Verteidigungsministers Stephanie zu Guttenberg ko-moderierte RTL2-Sendung „Tatort Internet" nimmt es beim Kampf um Einschaltquoten mit dem Persönlichkeitsschutz nicht so genau. Die Sendung will dokumentieren, wie pädophile Männer im Internet Kontakt zu minderjährigen Kindern und Jugendlichen suchen, sie in Chatrooms belästigen und zu persönlichen Treffen auffordern bzw. sich mit ihnen verabreden. Von Frühjahr 2010 an wurde in Köln, München und in kleinen Orten gedreht. Die Produktionsfirmen und die Redaktion ließen fiktive Minderjährige als Jungen oder Mädchen im Internet auftreten. Die Kommunikation in den

Chatrooms wurde von Redakteuren geführt. Die Absicht war immer eine Verabredung mit dem Pädophilen, wobei die fiktiven Minderjährigen selbst nie um eine persönliche Begegnung baten. Wenn die Männer, es gab wohl auch Ehepaare, in einer Wohnung, auf Plätzen oder an sonstigen Orten eintrafen, wurden sie mit dem RTL2-Team, zu dem als Moderator oft der ehemalige Innensenator Udo Nagel zählte, gefilmt und zumeist auch mit dem Vorwurf konfrontiert.

Die Sendung stößt auf viel Kritik. So meinte Sabine Verheyen, die sich als CDU-Abgeordnete im EU-Parlament für die Bekämpfung des Kindesmissbrauchs einsetzt, „Tatort Internet" schüre ausschließlich Ängste, ohne den Gefährdeten zu helfen. Die Sendung verzichte weitestgehend auf Information, wo und wie sich Jugendliche und ihre Eltern schützen und helfen lassen können. Die Täter versuche man zwar unkenntlich zu machen. Ein junges Mädchen, das belästigt worden war, sei hingegen ganz offen interviewt worden.

In der Sendung am 14.10. wurde ein grauhaariger Mann mit verpixeltem Gesicht gezeigt, der sich mit einem vermeintlich 13jährigen Mädchen trifft. Die beiden sprachen darüber, ob er in der Wohnung des Mädchens im Gästezimmer übernachten könne. Wegen der unzureichenden Anonymisierung war der Name des derart dargestellten über eine Google-Suche mit nur einem Suchbegriff als erster Treffer zu finden. Der Mann wurde als 61jähriger Kinderdorf-Leiter bei der Caritas erkannt und wurde umgehend gekündigt, nachdem er auch sofort zugab, dass er der dargestellte Mann ist. Danach verschwand der Mann; seine schwer kranke Frau meldete ihn als vermisst. Der Würzburger Caritas-Chef Clemens Bieber zeigte sich empört, dass die Redaktion die Caritas fünf Monate lang nicht über das Fehlverhalten des Kinderdorf-Leiters informiert hatte. Es stelle sich die Frage, „ob es dem Sender wirklich um den Schutz der Kinder geht oder doch nur um die Einschaltquote". Der Produzent der Sendung, Daniel Harrich, erwiderte, da der Mann nur eine „straflose Vorbereitungshandlung" begangen hätte, wäre es „nicht rechtens" gewesen, den Arbeitgeber zu benachrichtigen. Das Material sei stattdessen an zuständige Behörden weitergeleitet worden. Der Kinderdorf-Leiter selbst war von RTL2 nicht darüber unterrichtet worden, dass er gefilmt worden war. Er wurde von der Sendung überrascht. Danach, so berichtete er der Presse, sei bei ihm zu Hause „die Hölle" losgebrochen: „Telefonterror, Beschimpfungen", seine Familie sei massiv bedroht worden. Die Kommission für Zulassung und Aufsicht der Landesmedienanstalten (ZAK) beanstandete die beiden ersten Ausstrahlungen am 07. und 11.10. des Sendeformats, das am 22.11. beendet wurde. Die ZAK kritisierte, dass in diesen Sendungen die potenziellen Täter nicht hinreichend unkenntlich gemacht worden seien, so dass ihr soziales Umfeld sie identifizieren konnte.

Auf der Webseite der Bild-Zeitung, die seit dem Start der Sendung ausführlich über „Tatort Internet" berichtete, tauchte in einer Bildergalerie ein Foto des angeprangerten Mannes auf, das aus seinem Facebook-Profil stammt. Trotz einer Verpixelung war der Mann mit einem Vergleich über das Originalbild sofort zu identifizieren. Dennoch behauptete Bild-Sprecher Tobias Fröhlich: „Wie Sie der Gestaltung unserer Berichterstattung unschwer entnehmen können, war es unsere Absicht, die betroffenen Personen nicht identifizierbar werden zu lassen."

Die Kontaktanbahnung zwischen Pädophilen und Kindern im Internet ist als „Cyber-Grooming", also die sexuell motivierte Kontaktanbahnung zu Kindern über Internetdienste, bereits seit 2004 nach § 176 Abs. 4 Nr. 3 StGB strafbar. Die bayerische Justizministerin Beate Merk (CSU) fordert eine weitere Strafverschärfung, was aber von StrafrechtlerInnen abgelehnt wird, zumal jetzt schon, so der Konstanzer Strafrechtler Jörg Eisele, eine reine Vorbereitungshandlung sanktioniert wird, was eine „extreme Vorverlagerung des Strafrechtsschutzes" darstelle, wie sonst nicht einmal bei Mord. Der Hallenser Strafrechtsprofessor Joachim Renzikowski meinte deshalb auch: „Das Hauptproblem sind nicht die Internetkontakte, sondern die Reitlehrer und die Verwandten". Zum „Tatort Internet" meinte Eisele: „Die Diskussion geht am eigentlichen Problem vorbei. Da hat man eine Sendung gemacht, ohne vernünftig juristisch zu recherchieren." Das RTL2-Programm profiliert sich auch sonst nicht gerade durch emanzipatorische Beiträge, sondern u.a. mit Sendungen wie „Frauentausch" und Titeln wie „Grenzenlos geil – Deutschlands Sexsüchtige packen aus".

Stephanie zu Guttenberg hat ein Buch über Kindesmissbrauch geschrieben mit dem Titel „Schau nicht weg". Sie ist Präsidentin der deutschen Sektion von „Innocence in Danger". Der Verein wurde 1999 unter dem Dach der UNESCO gegründet und kämpft gegen den Kindesmissbrauch. Das Prinzip, nach dem „Tatort Internet" funktioniert, stammt aus den USA. Von 2004 bis 2007 lief beim Network NBC „To Catch a Predator". Schon in den USA wurde über die Zulässigkeit der Sendung gestritten. Das Original stellte die angelockten Pädophilen ins Kameralicht. Häufig wartete bereits der Sheriff. Doch die allermeisten mussten wieder freigelassen werden, weil ein Treffen noch keine Straftat ist. Einer der derart an den Pranger gestellten beging Suizid. 2008 einigte sich NBC finanziell mit der Familie. Ein großes Geschäft war die Sendung offensichtlich nicht; Werbekunden hatten Bedenken geäußert und wollten in diesem Kontext nicht erscheinen (Keil SZ 08.10.2010, 15; Boie/Deininger SZ 18.10.2010; SZ 24.11.2010, 17; Der Spiegel 42/2010, 16; Der Spiegel 43/2010, 18; Lischka/Pilarcyk/Stöcker/Kühn www.spiegel.de 13.10.2010).

Bund

Bahn AG schließt Mitarbeiterdatenschutzvereinbarung mit Betriebsrat

Die Deutsche Bahn hat eine neue Vereinbarung zum Mitarbeiterdatenschutz mit dem Betriebsrat des Unternehmens getroffen. Das Unternehmen zieht damit die Konsequenzen aus der Bespitzelungsaffäre, die im Frühjahr 2009 aufgedeckt worden war. Damals war bekannt geworden, dass die Deutsche Bahn rund 173.000 Mitarbeiter mit einem Datenabgleich überprüft hatte (DANA 1/2009, 20 ff.).

Mit der neuen Vereinbarung soll vor allem sichergestellt werden, dass etwa bei Korruptionsverdacht frühzeitig Arbeitnehmervertreter einbezogen werden, so Bahn-Rechtsvorstand Gerd Becht: „Wenn wir den Verdacht einer schweren Straftat haben, werden wir Mitarbeiter befragen und Daten überprüfen. Aber wir werden keine Ermittler einsetzen, die mit zweifelhaften Methoden arbeiten." Zudem würden in der Vereinbarung Datenschutz-Bestimmungen erläutert und verständlich gemacht. Der Zweck einer Datensammlung müsse vorher genau festgelegt sein. Grundsätzlich dürfen Daten nur noch für einen vorher eindeutig definierten Zweck erhoben werden. Die Bahn werde zudem in den kommenden Monaten unter Leitung der Datenschutzbeauftragten Chris Newiger eine flächendeckende Datenschutzorganisation mit mehr als 100 Beteiligten installieren. Man habe sich darauf verständigt, dass aus sozialen Netzwerken wie Facebook keine Daten von Bewerbern erhoben würden. Ziel sei, möglichst wenige Mitarbeiterdaten zu speichern. Die 37 Seiten starke Vereinbarung gilt für rund 160.000 Beschäftigte in Deutschland.

Becht lobte die Vereinbarung als „ein Zeichen des kulturellen Wandels" im Unternehmen. Nun müsse innerhalb des Unternehmens mit rund 1.000 Tochtergesellschaften „verloren gegangenes Vertrauen wieder zurückgewonnen werden". Das Ansehen der Bahn hatte durch jahrelange heimliche Erhebung persönlicher Daten und Überwachung seiner rund 173.000 Beschäftigten schwer gelitten. „Die neue Kultur besteht darin, dass man vorher informiert wird", betonte stellvertretende Konzernbetriebsratsvorsitzende Jens Schwarz. Die Bahngewerkschaften Transnet und GDBA erklärten, ihr „Kampf um einen echten Arbeitnehmer-Datenschutz hat sich zumindest im DB-Konzern ausgezahlt." Der Datenschutzskandal war nach Auffassung der Bahn entstanden, weil die Konzernführung mit der Überwachung glaubte, Korruption unterbinden und Lücken im Vertraulichkeitssystem schließen zu können. Beides sei seinerzeit nicht gelungen, resümierte Becht. Die Affäre bei der Bahn mit dem Datenabgleich fast aller Mitarbeiter in Deutschland sowie einer E-Mail-Überwachung hatte zum Zerwürfnis zwischen Betriebsräten, Gewerkschaften sowie Ex-Bahnchef Hartmut Mehdorn geführt. Neben der angeführten Korruptionsbekämpfung versuchte die Bahn im Vorfeld des geplanten Börsengangs auch Kontakte zu Journalisten und Unternehmenskritikern aufzuspüren. Letztlich musste Mehdorn im Zuge der Affäre im Frühjahr 2009 seinen Posten räumen. Die Bahn zahlte später wegen Verstoßes gegen Datenschutzbestimmungen ein Bußgeld von 1,2 Millionen Euro (www.tagesschau.de 25.11.2010; Kuhr SZ 26.11.2010, 26).

Bund

Pilotprojekt zu anonymisierten Bewerbungsverfahren in Deutschland gestartet

Seit dem 25.11.2010 führen in Deutschland einige Großunternehmen wie die Deutsche Post, die Deutsche Telekom, Konsumgüterhersteller, das Bundesfamilienministerium, die Bundesagentur für Arbeit in Nordrhein-Westfalen und die Stadtverwaltung Celle einen Pilotversuch mit anonymisierten Bewerbungen durch. Nach Angaben der Antidiskriminierungsstelle des Bundes (ADS) werden ca. 225 Arbeits- und Ausbildungsplätze mit voraussichtlich einigen tausend BewerberInnen mit verschiedenen Anonymisierungstechniken so durchgeführt, dass auf Name, Alter, Geschlecht, Herkunft und Familienstand der BewerberInnen und auf Fotos in der ersten Bewerbungsphase verzichtet wird. Die teilnehmenden Unternehmen und Behörden werden dabei verschiedene Modalitäten der Anonymisierung einsetzen. Erst zu Vorstellungsgesprächen sollen die Daten den potentiellen Arbeitgebern bekannt werden. Das Pilotprojekt, das bis März 2012 läuft, soll wissenschaftlich begleitet und ausgewertet werden. Die ADS verspricht sich Erkenntnisse über die Wirksamkeit und Praktikabilität anonymisierter Bewerbungen bei der Bekämpfung von Diskriminierungen nach Alter, Geschlecht, ethnischer Herkunft usw. bei der Besetzung von Arbeitsplätzen (Antidiskriminierungsstelle des Bundes, Pressemitteilung Nr. 29/2010 v. 25.11.2010).

Baden-Württemberg

Große Nachfrage nach Schleckers Datenleck-Entschädigung

Bei der Drogeriekette Schlecker hatte nach Unternehmensangaben schon nach wenigen Tagen eine «fünfstellige Anzahl» von Online-KundInnen den als Entschädigung für ein Ende August 2010 bekannt gewordenes Datenleck gedachten Einkaufs-Gutschein im Wert von je fünf Euro eingelöst (DANA 3/2010, 119 f.). Datensätze von 150.000 Online-KundInnen waren im Internet zugänglich mit Vor- und Nachnamen, Adresse, E-Mail-Adresse und Kunden-Profil für Werbezwecke, zudem 7,1 Millionen E-Mail-Adressen von Newsletter-KundInnen. Die Daten lagen auf dem Server eines externen Dienstleisters mit Sitz in Bonn. Ein Mainzer Internet-Unternehmer hatte das Leck durch Zufall entdeckt und öffentlich gemacht. Schlecker erstattete Anzeige gegen Unbekannt; die Bonner Staatsanwaltschaft ermittelt. Schlecker vermutet, dass es zuvor einen «internen Angriff» auf den Server gegeben habe. Hinweise auf eine Einzelperson mit «einschlägigen internen Kenntnissen» über den beauftragten Dienstleister hätten sich dabei «weiter erhärtet». Fahrlässigkeit oder sicherheitstechnische Fehler könnten mittlerweile ausgeschlossen werden. Bei dem Dienstleister habe man eine «Verbesserung der Sicherheitsstandards» veranlasst. Das gelte auch für den eigenen Online-Shop (portal.gmx.net 08.09.2010).

Bayern

Bayerische Datenschutzgesellschaft gegründet

Am 18.05.2010 wurde in München die Bayerische Gesellschaft zur Förderung

des Datenschutzes („Bayerische Datenschutzgesellschaft“) gegründet. Zweck des Vereins ist die Förderung von Wissenschaft und Forschung auf dem Gebiet des Datenschutzes und der Datensicherheit, sowie die Vermittlung von Datenschutzbelangen gegenüber BürgerInnen, öffentlichen und nicht-öffentlichen Stellen, politischen und anderen gesellschaftlichen Vereinigungen, der Wirtschaft und den Medien. Auf der Gründungsversammlung wurden in den Vorstand der Gesellschaft gewählt: 1. Vorsitzender: Florian Thoma (Rechtsanwalt, Datenschutzbeauftragter der Siemens AG; Vorsitzender des Arbeitskreises Datenschutz des BITKOM), 2. Vorsitzender: Markus Stamm (Rechtsanwalt, Berater Alcatel-Lucent Deutschland AG). Die Datenschutzgesellschaft wird zur Förderung ihrer Ziele von einem Beirat unterstützt, der sich wie folgt zusammensetzt: Dr. Oliver Draf, Rechtsanwalt (Datenschutzbeauftragter der Allianz SE), Professor Dr. iur. Ulrich M. Gassner (Universität Augsburg), Dr. Sibylle Gierschmann, LL.M. (Rechtsanwältin, Taylor Wessing) und Dr. Stefan Hanloser (Rechtsanwalt, HOWREY LLP) (www.dsg-bayern.org).

Bayern

Verfassungsschutz kämpft vergeblich vor dem Landtag gegen Islamisten

An der Pforte des Bayerischen Landtags sind am 22.10.2010 zwei Herren erschienen, die mit einem Dienstausweis wedelten. Der Pförtner ließ sie nicht rein, da sie weder ihren Namen zu sagen bereit waren, noch wohin sie wollten. Der Pförtner meinte, „Dann kommen´S auch nicht rein“ und holte die Polizei, denn die Herren hatten sich hinter einer Tanne und einem Trambahnhäuschen zurückgezogen. Der Landtagsvizepräsident Franz Maget kam vorbei und verfolgte zusammen mit einer Polizistin die beiden Herren ins Unterholz. Dabei stellte sich heraus, dass zwei Verfassungsschützer gerade bei der Arbeit waren, nämlich beim Observieren eines Islamisten. Der sollte angeblich im Landtag arbeiten, für eine Fraktion. Das änderte nichts daran, dass sie nicht eingelassen wurden. Später stellte sich dann auch noch heraus, dass sie den falschen Islamisten observiert hatten (SZ 23./24.10.2010, 40).

Brandenburg

Datenschutzaufsicht über Privatwirtschaft bei der Landesbeauftragten

Mit der Verabschiedung des neuen Brandenburgischen Datenschutzgesetzes im Mai 2010 ist die bisherige Trennung der datenschutzrechtlichen Aufsicht aufgehoben worden. Die Landesbeauftragte für Datenschutz und Akteneinsicht ist nicht mehr nur für die Kontrolle der öffentlichen Verwaltung zuständig. Ab 01.06.2010 besteht auch die Zuständigkeit für den nichtöffentlichen Bereich (PE LDA Brandenburg 07.05.2010; GDD-Mitteilungen 5/2010, 6).

Hamburg

Bauer-Verlag ignoriert Hinweise auf Sicherheitsleck

Der Bauer-Verlag („Das Neue Blatt“, „Tina“, „Laura“) ignorierte offenbar mehrere Monate lang ein Sicherheitsleck in seinem Online-Abo-Shop. Gemäß internen Unterlagen wird die Datenbank „nicht den zeitgemäßen Sicherheits- und Datenschutz-Anforderungen gerecht“. Im April 2010 wurde das Problem bei einer Strategiepräsentation in Gegenwart der Verlegerin Yvonne Bauer angesprochen, aber bis Oktober nicht behoben. Die Sicherheitslücken waren von einer externen Firma festgestellt worden, die sich um eine Zusammenarbeit mit Bauer beworben hatte. Bereits „oberflächliche Checks“, so die Firma an den Verlag in einer E-Mail, „seien beunruhigend“. Mitte Oktober 2010 war bekannt geworden, dass die AbonnentInnen der Wochenzeitung „Die Zeit“ über das Internet ausspioniert worden waren. Der Zeit-Verlag informierte seine KundInnen darüber per E-Mail und gab an, die Datenbank „vor weiteren Zugriffen gesichert“ zu haben. Dem gegenüber ließ der Bauer-Verlag lediglich wissen, die Sicherheitsvorkehrungen im Abo-Shop würden „intern regelmäßig überprüft und angepasst“. Darüber hinaus vertraut das Zeitschriftenhaus eher auf das Gute im Menschen: „Ein unberechtigter Zugriff auf geschützte Daten des Abo-Shops ist ohne kriminelle Energie ausgeschlossen“ (Der Spiegel 43/2010, 185).

Hamburg

Haspa erstellt psychologische Kundenprofile

Die Hamburger Sparkasse (Haspa), Deutschlands größte Sparkasse, nutzte Erkenntnisse der Hirnforschung und erstellte psychologische Kundenprofile, um ihre Produkte unters Volk zu bringen. Die KundInnen wurden sechs Charakterprofilen zugeordnet, auf die im Beratungsgespräch gesondert eingegangen werden sollte. Dem Typ „diszipliniert“ gegenüber sollte etwa die „rationale Haspa“ hervorgekehrt werden, der „Hedonist“ dagegen mit der Karte fürs Rockkonzert gelockt werden. Nach den einer Berichterstattung hierüber beendete die Haspa das Projekt mit dem Namen „Sensus“ nach eigenen Angaben am 04.11.2010. Hinter Sensus steht der in der wissenschaftlichen Marktforschung neue Ansatz des Neuromarketings. Hierbei werden, so die Website der „Gruppe Nymphenburg“, „Erkenntnisse der Gehirnforschung, der Psychologie und der Evolutionsbiologie mit empirischer Konsumforschung verknüpft“. Die Unternehmensberatung lieferte mit ihrem System „Limbic“ das Vorbild für Sensus.

Für jeden Kundentyp gab es Schlüsselwörter zum ködern:

- Performer: außergewöhnliche Chancen und Renditen, leistungsstark, hochwertig, exklusiv
- Disziplinierter: korrekt, bewährt, Qualität, Zahlen, Fakten
- Bewahrer: Sicherheit, bewährt, verlässlich, traditionell
- Genießer: sicher, bequem, angenehm, etwas Besonderes, aber durchaus bewährt

- Hedonist: neu, innovativ, außergewöhnlich, Spaß, flexibel
- Abenteurer: neu, innovativ, ungewöhnlich; riskant aber extrem chancenreich, herausfordernd, zielführend.

Nymphenburg-Vorstandsmitglied Hans-Georg Häusel erläuterte: „Das ist alles kein Geheimnis und heute im Marketing gang und gäbe." Die Haspa habe Limbic für ihre Bedürfnisse modifiziert. Als Grundlage dienten Informationen darüber, welche Haspa-Produkte wie Aktien oder Immobilienfonds jemand gekauft habe. Außer der Haspa gehörten auch andere Finanzdienstleister zum Kundenkreis seiner Firma. Das System ermögliche es, Zielgruppen noch besser zu segmentieren und entsprechend ihrer bewussten wie auch unbewussten Bedürfnisse anzusprechen. Die Haspa teilte über ihre Unternehmenssprecherin Stefanie von Carlsburg mit, ihr sei es ein Anliegen, so individuell wie möglich auf die Wünsche ihrer KundInnen einzugehen. „Die Haspa hat Sensus genutzt, um die Bedürfnisse ihrer Kunden noch besser zu verstehen. Obwohl Sensus im Interesse unserer Kunden ist, stellen wir es nun ein." Eine Sprecherin des Deutschen Sparkassen- und Giroverbandes erklärte, die Unterteilung von Sparkassen-KundInnen nach deren Lebensstil und Konsumgewohnheiten sei keine generelle Vorgehensweise der Sparkassen.

Kritik kommt von Edda Castello von der Verbraucherzentrale Hamburg: Das Neuromarketing nutze die meist unbewussten Wünsche und Bedürfnisse von Menschen, um diese zu bestimmten Entscheidungen zu veranlassen. Gerade bei Finanzprodukten seien jedoch rationale Entscheidungen wichtig: „Die ganze Diskussion um Beratungsprotokolle und Verbesserungen bei der Beratung zu Finanzprodukten entlarvt sich als Farce." Karin Baur vom Magazin Finanztest hält es für „erschreckend, was die da machen, weil es das Beratungsgespräch entmenschlicht". Man bemächtige sich der psychologischen Struktur eines Menschen, um diesen zu manipulieren. Und Bernd Voß, grüner Landtagsabgeordneter in Schleswig-Holstein meinte: „Spätestens seit der Finanzkrise, der Pleite von Lehman Brothers, muss die Anforderung an eine Finanzberatung sein, dass sie objektiv informiert und im Interesse der KundInnen handelt. Die BürgerInnen müssen ihr Auskunftsrecht stärker wahrnehmen, und dies nicht nur bei abgelehnten Kreditverträgen, sondern auch allgemein darf sich eine Bank beim Verlangen nach Auskunft über die Speicherung von eigenen persönlichen Daten der KundInnen nicht hinter Betriebs- und Geschäftsgeheimnissen verstecken." Wie die Haspa an die nötigen Daten gelangt ist, wollen jetzt die Datenschützer wissen. „Wir vermuten, dass das von der Kontoführung kommt", sagt der stellvertretende hamburgische Datenschutzbeauftragte Joachim Menzel. „Das wäre eine nicht erlaubte Nutzung dieser Daten" (www.ndr.de 04.11.2010; www.taz.de/1/nord 04.11.2010; www.fr-online.de 04.11.2010; EZ SHZ 05.11.2010, 4).

Hamburg

Bußgeld gegen Haspa wegen Kundendatenzugriff und Neuromarketing

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat am 23.11.2010 gegen die Hamburger Sparkasse (Haspa) ein Bußgeld in Höhe von 200.000 Euro verhängt. Die Bank hat sich bei der Aufklärung des Datenschutzverstoßes kooperativ gezeigt und das beanstandete Vorgehen eingestellt. Die Haspa hatte von Ende 2005 bis August 2010 ihren als selbständige Gewerbetreibende eingesetzten sog. mobilen KundenberaterInnen den Zugriff auf Daten der BankkundInnen ermöglicht. In einer nicht näher bekannten Anzahl von Fällen konnten diese über den gesamten Zeitraum ohne Einwilligungserklärung der KundInnen auf deren Kontodaten zugreifen. Dies war bankintern auch bekannt, da anhand der Logdaten seit 2007 regelmäßig Stichproben der Zugriffe erfolgten. Ferner hatte die Bank Charakterprofile der Kunden, die auf Erkenntnissen der modernen Hirnforschung beruhen, unter Nutzung von Kundendaten erstellt, auf die ebenfalls alle mobilen Kundenberater Zugriff hatten. Hierzu wurden sowohl soziodemographische Daten als auch die Produktnutzungsdaten der Kunden herangezogen (s.o.). Dazu gehörten u.a. Salden etwa von Girokonten wie auch die Anzahl von Buchungen. Die Erstellung der Kundenprofile und deren Nutzung erfolgten ohne Wissen der Bankkunden.

Der HmbBfDI Johannes Caspar erläuterte: „Bei den Bankdaten handelt es sich um sehr sensible Daten, die sehr viel über die einzelnen Kunden aussagen. Wir haben uns bei der Verhängung des Bußgeldes an Schwere und Ausmaß des Datenschutzverstoßes sowie daran orientiert, dass dessen Höhe den daraus resultierenden wirtschaftlichen Vorteil übersteigen soll. Ferner setzen wir hiermit ein Zeichen gegen den Einsatz moderner Methoden des Neuromarketing unter Außerachtlassung des Datenschutzes und gegen einen gläsernen Bankkunden." Die Haspa hatte den MitarbeiterInnen des mobilen Vertriebs am 09.07.2010 die Berechtigung des Kundendatenzugriffs entzogen. Seit dem 30.08.2010 werde ein geändertes technisches Verfahren eingesetzt, das den Anforderungen des Datenschutzes gerecht wird (www.datenschutz.de 23.11.2010; PE HmbBfdI 23.11.2010; Läsker SZ 24.11.2010, 28).

Hessen

Fußballspielverweigerung wegen „falschem" Geburtsort

Ein 53-jähriger Fußballfan wollte gemeinsam mit seinem 10jährigen Sohn Ende November 2010 das Drittliga-Spitzenspiel zwischen Wehen Wiesbaden und dem FC Hansa Rostock besuchen. Der Vater durfte nicht ins Stadion, weil er im „falschen" Postleitzahlengebiet geboren ist. Genauer: Weil Rostocker Fans in Dresden randaliert hatten, durfte ein Familienvater, der in Sachsen geboren ist und in Hessen wohnt, in Wiesbaden nicht ins Stadion. Hintergrund war ein Beschluss des Deutschen Fußballbundes (DFB) und des SV Wehen Wiesbaden. Anlass waren Ausschreitungen von Rostocker Hooligans beim Auswärtsspiel im Oktober 2010 in Dresden. Der DFB hatte Hansa Rostock als „Wiederholungstäter" anschließend die

Auflage erteilt, die beiden folgenden Auswärtsspiele beim SV Sandhausen und beim SV Wehen Wiesbaden ohne seine Fans zu bestreiten. Um diese Maßnahme umzusetzen, dachte sich der SV Wehen ein besonderes System aus. Demnach sollten Fans, die außerhalb der Postleitzahlenbereiche 60 bis 65, 55/56 und 34 bis 36 wohnen oder dort geboren sind, keinen Zutritt in die Arena erhalten. Also hätten auch Fans beispielsweise aus Bremen, Stuttgart oder München nicht kommen dürfen.

Der Personalausweis des Familienvaters legte offen, dass er vor 53 Jahren in Bischofswerda in Sachsen geboren wurde. Der Betroffene: „Das Sicherheitspersonal am Stadioneingang belehrte mich, dass meine Herkunft respektive meine Geburt in Sachsen auf Weisung des DFB einen Zugang zum Stadion und damit zum heutigen Spiel unserer Wehener Mannschaft nicht zuließe." Auch sein Hinweis, er würde ja in dem „richtigen" Postleitzahlengebiet wohnen, konnte die Ordnungskräfte, die mit elektronischen Geräten die Postleitzahlen der im Personalausweis angegebenen Orte ermittelten, nicht überzeugen, so dass er draußen bleiben musste. Er war nicht der Einzige; es gab weitere rund 20 Beschwerden. Ein Vereinssprecher meinte, man habe keine andere Wahl gehabt, als das Urteil zu akzeptieren und die Maßnahmen umzusetzen. Dass es dabei zu Unannehmlichkeiten gekommen ist, täte ihm leid. Er selber habe sich ein halbes Jahr auf das Spitzenspiel gegen den Zweitliga-Absteiger gefreut, doch statt eines Fußballfestes erlebte er eine chaotische Woche und ein Wochenende, das einen ganz faden Beigeschmack hinterließ. Eigentlich sollte der FC Hansa Rostock wirksam bestraft werden, doch bekam so plötzlich Wiesbaden den Schwarzen Peter. Der DFB bestätigte, das Postleitzahlen-Konzept abgenickt zu haben, verweist ansonsten aber auf den Gastgeber. Es läge am Verein, das Hausrecht umzusetzen. Beim DFB will man die Vorwürfe der Fans, in Wiesbaden habe es eine Mischung aus Rasterfahndung und Sippenhaft gegeben, nicht gelten lassen. Schließlich sei die Maßnahme im Vorfeld kommuniziert worden und habe sich – von den 20 Betroffenen einmal abgesehen – als sinnvoll erwiesen.

Norbert Weise, stellvertretender Vorsitzender des DFB-Kontrollausschusses, meinte darum auch: „Die Umsetzung des Urteils hier in Wiesbaden hat sehr gut funktioniert". Er selbst habe sich vor Ort ein Bild gemacht: „Der Verein und die Ordnungskräfte haben im Vorfeld und am Spieltag selbst alles dafür getan, dass die disziplinarischen Maßnahmen gegen Hansa Rostock greifen und haben so die Forderungen des DFB erfüllt." Zudem gebe es kaum Alternativen zu den Geisterspielen. Heimpartien unter Ausschluss der Öffentlichkeit würden noch viel mehr Unbeteiligte für das Fehlverhalten einer kleinen Gruppe bestrafen, hieß es beim DFB. Rechtsanwalt Rüdiger Zuck hält die Maßnahme für unverhältnismäßig und riet den Betroffenen, gegen diese Behandlung zu klagen: „Solche Maßnahmen mögen bei einem Massengentest greifen, wenn ein Mörder gesucht wird, sind jedoch in diesem konkreten Fall vollkommen überzogen, weil sie sehr undifferenziert sind". Der Jurist setzt sich seit Jahren für Fanrechte ein und betreut derzeit einen Fan des FC Bayern München, der vor dem Verfassungsgericht gegen seiner Meinung nach willkürliche Stadionverbote klagt (Glindmeier www.spiegel.de 22.11.2010).

Niedersachsen

Polizei-Überwachungsdrohnen gegen Anti-Atom-DemonstrantInnen

Bei den Demonstrationen gegen den Transport von Castoren in das Atommülllager Gorleben Anfang November 2010 wurden von der niedersächsischen Polizei erstmals Überwachungsdrohnen, sog. Unmanned Arial Systems (UAS), eingesetzt. Der auch „Drehflügler" genannte Mini-Flieger verfügt über eine Tageslichtkamera und eine Dämmerungskamera. Die Bilder werden in Echtzeit an eine Bodenstation übertragen und können dort aufgezeichnet werden. Insgesamt hatte es vier Starts eines unbemannten Quadrokopters gegeben, darunter ein Test- und drei Aufklärungsflüge. Das Fluggerät vom Typ „md4-200" der Firma Microdrones war im Jahr 2008 vom niedersächsischen Innenministerium für 47.000 Euro angeschafft worden. Als Einsatzbeispiele nannte Innenminister Uwe Schünemann damals etwa die „Vorbereitung von Maßnahmen der Spezialeinheiten der Polizei gegen bewaffnete Straftäter sowie die Verhinderung oder Verringerung der Schadensausweitung für die Bevölkerung bei Gefahrenlagen".

Laut Innenministerium war die Drohne beim Castor-Transport zum ersten Mal im „echten Einsatz", zuvor habe man lediglich die Flugeigenschaften des Quadrokopters und seine optischen Fähigkeiten getestet. Früheren Angaben zufolge wurden insgesamt sechs Polizeibeamte als sogenannte Luftfahrzeugfernführer eingewiesen und zertifiziert. Erworben hatte man damals ein Microdrones-Paket: den Quadrokopter „md4-200", ein „Base Station Set" mit Videobrille, Software sowie zwei Kameras. Die Drohne kann 500 Meter weit fliegen. Ministeriumsangaben zufolge liefert die Drohne bei „Einsätzen in normaler Flughöhe" lediglich Übersichtsaufnahmen, auf denen „einzelne Demonstranten nicht identifizierbar" seien. Dies widerspricht allerdings dem erklärten Ziel, die Drohnen einzusetzen, um mit den Aufnahmen „eine nachträgliche Aufklärung von Straftaten zu ermöglichen". Bei der Präsentation eines Quadrokopters vom selben Typ, den die sächsische Polizei 2008 angeschafft hatte, war zu erkennen, dass es möglich ist, Gesichter von Personen selbst aus einer Höhe von 50 Metern noch „gestochen scharf" zu erkennen. Auch Kfz-Kennzeichen konnten identifiziert werden. Nötig ist dafür lediglich eine Erweiterung des optischen Systems um eine Digitalkamera.

Nach Ansicht des Innenministeriums des Landes war der Einsatz zulässig. Für Luftaufnahmen der Drohne gälten die gleichen Rechtsgrundlagen wie bei anderen von der Polizei durchgeführten Videoaufzeichnungen. Ob Videobilder bei einer Demonstration nun von einem bemannten Hubschrauber aus oder von einer unbemannten Drohne erstellt würden, mache rechtlich keinen Unterschied. Die Bürgerinitiative Umweltschutz Lüchow-Dannenberg bezeichnete „die Ausspähung des Protestgeschehens durch Drohnen" als „rechtlich äußerst

problematisch“. Ein Sprecher des niedersächsischen Datenschutzbeauftragten Joachim Wahlbrink erklärte, die Flüge seien aus rechtlicher Sicht grundsätzlich zulässig. Auch habe eine datenschutzrechtlich erforderliche Vorabkontrolle des Gerätes stattgefunden, eine technische Beschreibung liege ebenfalls vor. Sogar Porträtaufnahmen dürften mit der Drohne angefertigt werden, sollten konkrete Hinweise auf Straftaten oder erhebliche Ordnungswidrigkeiten vorliegen. Zuvor hatte Wahlbrink noch behauptet, der Einsatz sei unzulässig: „Es besteht die Gefahr, dass die Kamera direkt in Wohnungen hineinfilmt. Das wäre ein verbotener Eingriff in die Privatsphäre“.

Das Innenministerium betont hingegen, das System habe gar nicht die Fähigkeit, Gesichter einzelner Personen heranzuzoomen. Es sei aber „wohl technisch möglich“, aus den Videoaufzeichnungen „später Bildausschnitte zu vergrößern“. Innenminister Schünemann hatte schon 2008 entsprechende Systemerweiterungen im Auge, als er mit Bezug auf die Warnmöglichkeiten bei Gefahrenlagen meinte: „Ein mit Kameras oder Gas- und Sensortechnik ausgestattetes UAS kann den Einsatzkräften hilfreiche Dienste leisten.“ Der innenpolitische Sprecher der SPD Klaus-Peter Bachmann warf Schünemann eine „Geheimaktion“ vor, über die nicht einmal der oberste Einsatzleiter informiert worden sei. Er habe den Eindruck, dass die Drohne unbedingt eingesetzt werden musste, „damit der Minister den Makel der nutzlosen Anschaffung widerlegen kann.“ Der Grünen-Innenpolitiker Ralf Briese forderte eine „einwandfreie rechtliche Regelung“. Es sei nicht klar, für welche konkreten Einsatzzwecke das „fliegende Auge“ eingeplant werden solle. „Die Verwendung der Drohne darf unter keinen Umständen zu einer abschreckenden Wirkung auf Teilnehmer von Protestveranstaltungen führen.“ Auch dürfe die Drohne nicht zur Herstellung und Speicherung verdeckter Demonstrationsteilnehmer benutzt werden. Der Einsatz müsse zuvor von der Polizei bekannt gegeben werden (vgl. DANA 3/2010, 129; www.heise.de 17.11.2010 u. 16.11.2010; Schneider SZ 18.11.2010, 1, 4, 6).

Niedersachsen

Atlas videokontrolliert Metallerstreik

Im Tarifkonflikt beim niedersächsischen Bagger- und Kranhersteller Atlas Maschinen GmbH hat die Gewerkschaft IG Metall Küste eine einstweilige Verfügung gegen die Videoüberwachung von Streikaktivitäten beantragt. Der Tarifkonflikt begann beim Werk Ganderkesee bei Oldenburg und weitete sich dann auf die Betriebsstätte Delmenhorst aus. Atlas hatte mit einer eigens in Ganderkesee aufgestellten Videokamera das Streikgeschehen an den Werkstoren gefilmt, war auch anderweitig gegen Streikende und Betriebsräte vorgegangen und hatte u.a. Hausverbote erteilt. Der Arbeitsrechts- und Datenschutzexperte Wolfgang Däubler, Jura-Professor an der Universität Bremen, kritisierte: „Das ist ein Eingriff in das Streikrecht. Das Filmen ist eine Einschüchterung.“ In einer „Parallel-Entscheidung“, dem legendären „Brokdorf-Beschluss“ von 1985, habe das Bundesverfassungsgericht das systematische Filmen einer Demonstration durch die Polizei als Eingriff ins Demonstrationsrecht bezeichnet. Zwar gebe es zur Videoüberwachung vor Betrieben keine höchstrichterliche Entscheidung. Doch werde eine solche Videoüberwachung selbst von „konservativen Kommentatoren“ als rechtswidrig bezeichnet. Außerdem verletze das Filmen das Recht am eigenen Bild.

Der IG-Metall Sprecher Heiko Messerschmidt meinte: „Wir sehen hier einen eklatanten Verstoß gegen den Datenschutz und einen unzulässigen Eingriff in das vom Grundgesetz garantierte Streikrecht.“ Eine Sprecherin des eingeschalteten niedersächsischen Landesdatenschutzbeauftragten sagte: „Wir prüfen den Fall und sehen den Vorgang sehr kritisch.“ Die IG Metall fordert für die 650 Beschäftigten in den drei Atlas-Werken Ganderkesee, Delmenhorst und Vechta einen Haustarifvertrag. Der neue Inhaber Fil Filipov versuchte seit Februar 2010 durch neue Arbeitsverträge, die sozialen Standards zu senken. Anstelle der 35-Stunden-Woche möchte er 40 Wochenstunden ohne Lohnausgleich durchsetzen (von Appen www.taz.de/1/nord/ 04.11.2010).

Nordrhein-Westfalen

Telefonüberwachung nimmt ab

Die Zahl der Telefonüberwachungsmaßnahmen (TÜ) in strafrechtlichen Ermittlungsverfahren sinkt in Nordrhein-Westfalen. Im Jahr 2009 ordneten Richter diese Maßnahme in 526 Verfahren an. Das waren 9% weniger als 2008. Für den Justizminister des Landes Thomas Kutschaty (SPD) belegt der Rückgang, dass die Staatsanwaltschaft bei ihren Aufträgen auf TÜ großes Verantwortungsbewusstsein zeige. In mehr als 83% der Fälle habe die Überwachung beweiskräftige Erkenntnisse gebracht. Anordnungen zur Verfolgung schwerer Drogendelikte stellten mit 45% weiter die häufigsten Fälle; 15% betrafen andere Bereiche der organisierten Kriminalität (SZ 01.10.2010, 6).

Nordrhein-Westfalen

Verbraucherzentrale warnt vor „Paid4“

Die Verbraucherzentrale Nordrhein-Westfalen (VZ NRW) warnt vor unseriösen Nebenverdienst-Angeboten im Internet. Wer sich für die „Paid4-Dienste“ im Internet anmelde, müsse oft sensible Daten preisgeben, eine Menge Werbung ertragen und das in der Regel für wenige Cent. Im Internet gibt es inzwischen zahlreiche Firmen, die Surfern leicht verdientes Geld für ihre Aktivitäten im Netz versprechen: etwa für den Empfang und das Öffnen von Reklame-E-Mails, das Anklicken von Internet Seiten oder das Anschauen von Werbebannern. Einige dieser Internetportale sichern sich schon bei der Anmeldung das Recht, Daten wie Name, Geburtsdatum, Handynummer und Hobbys für Wettbewerbe, Werbe-SMS und andere Marketingaktionen weiterzuverkaufen und machen so selbst gute Geschäfte, so die VZ NRW. Außerdem seien die Aussichten der Surfer gering, wirklich Geld zu verdienen. So müsse der Internetnutzer bei

der sogenannten Paid-Mail eine E-Mail mit Werbung öffnen, mindestens 20 Sekunden auf der Seite verbleiben und dann noch einige Fragen beantworten. Der Lohn der Mühe ist allerdings gering. Um auch nur 20 Euro ausgezahlt zu bekommen, müssten viele Surfer etwa eineinhalb Jahre lang Werbung klikken, rechnete die Verbraucherzentrale am Beispiel eines großen Anbieters vor. Wer sich von einem anderen Bieter für das Anschauen und Kommentieren von Videos bezahlen lasse, müsse für zehn Euro im Monat rund 2800 Videos samt Werbung ertragen – also fast 100 am Tag. Wenig lukrativ sei es auch, sich dafür bezahlen zu lassen, dass die eigene Internet-Startseite mit Werbe-Bannern versehen wird. Wer dreimal am Tag ins Internet gehe, komme gerade einmal auf einen Lohn von 2 Euro – im Jahr (www.az-web.de 08.09.2010; SZ 09.09.2010, 24).

Schleswig-Holstein

Heimliche Mitarbeiter-Videoüberwachung bei Billigdiscounter Krümet

In einem Fernsehbericht schilderte ein ehemaliger Bezirksleiter des norddeutschen Billig-Discounters Krümet, dass in den Sozialräumen von Filialen heimliche Videoüberwachungsmaßnahmen durchgeführt und auf dieser Basis detaillierte Protokolle über Beschäftigte angefertigt wurden. In fünf der insgesamt elf Filialen in Schleswig-Holstein, Hamburg und Niedersachsen sollen MitarbeiterInnen so ausspioniert worden sein. Die Kameras, bis zu 18 pro Filiale, waren in Rauchmeldern oder hinter toten Steckdosen der Pausenräume versteckt; die Angestellten hatten davon keine Ahnung. Es wurde protokolliert, wann und wie lange sie telefonierten und wann sie rauchten. Ein Mitarbeiter steckt ein Cuttermesser in seine Hosentasche und wurde des Diebstahls verdächtigt. Die Angestellten der Krümet Sonderpostenmärkte nutzen solche Messer zum Öffnen von Kartons. Dass sich der Mitarbeiter eines Marktes in Schleswig-Holstein dieses Werkzeug vom Tisch des Pausenraums in die Tasche steckte, hat eine versteckte Kamera gefilmt. Den Verdacht des Diebstahls hatte dann eine Detektei in der Auswertung des Videomaterials geäußert.

Der frühere Bezirksleiter, der dort 16 Jahre lang tätig, war, wollte „sein Gewissen erleichtern“: „Ich war ausführendes Organ.“ Die Bespitzelung sei seine Aufgabe gewesen – auf Anweisung. Die Krümet Handelsgesellschaft mit Sitz in Bönningstedt im Kreis Pinneberg sieht sich dagegen als Opfer einer Schmutzkampagne in einem Arbeitsrechtsstreit: Im Mai wurde der Bezirksleiter fristlos entlassen. Zu den Gründen sagt das Unternehmen in einer Stellungnahme nichts: „Dies ist Gegenstand eines derzeit anhängigen Rechtsstreits.“ Es sei richtig, dass Kameras in fünf Filialen angebracht wurden, nachdem Diebstähle nicht auf andere Weise aufgeklärt werden konnten. Aber: „Die Prüfung geschah allein auf Veranlassung des entlassenen Bezirksleiters und betraf nur Teile der von ihm geführten Filialen.“ Die Geschäftsleitung habe nur den von ihm erteilten Auftrag an das Überwachungsunternehmen freigegeben. „Die konkrete Ausgestaltung oblag unserem früheren Mitarbeiter.“

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) führt nun gegen Krümet ein Verfahren durch ebenso wie gegen das für Krümet tätige Kieler Überwachungsunternehmen Visako. Dessen Anwältin Susanne Becker beteuert, dass die Sicherheitsfirma das Datenschutzgesetz stets einhalte. „Die Mitarbeiter sind geschult. Wir prüfen, ob es für die Installateure der Kameras ersichtlich war, dass es sich um Sozialräume gehandelt hat. Wenn in so einem Raum gefilmt wurde, ist das nicht in Ordnung.“ Laut Stellungnahme von Krümet soll der Ex-Bezirksleiter die Visako-Mitarbeiter falsch informiert haben. Diese seien davon ausgegangen, dass es sich um zulässige Bereiche gehandelt habe. Protokolle über Mitarbeiter seien von Krümet nicht in Auftrag gegeben worden, teilt die Geschäftsleitung des Familienunternehmens mit. „Wurden sie dennoch erstellt, sind sie sogleich vernichtet worden.“ Dies halten die Datenschützer vom ULD für wenig plausibel. Gemäß Sven Polenz offenbaren die Auswertungsprotokolle von Visako, dass Mitarbeiter (Ma) durchnummeriert und ihr Verhalten auf Minute und Sekunde genau beschrieben wurden: „Ma 8 kommt in den Raum, zündet sich eine Zigarette an. Ma 23 und Ma 14 unterhalten sich. Und Ma 4 schminkt sich“, jedesmal dahinter in Versalien der Vermerk „Unproduktivität“. Der frühere Bezirksleiter wehrt sich gegen die Behauptung, er sei für die Videoüberwachung allein verantwortlich gewesen: „Diese Behauptung ist völlig absurd.“ Er habe Strafanzeige gegen Krümet gestellt (Mormann www.shz.de 19.10.2010; Alves, www.kn-online.de 19.10.2010; www.kn-online.de 20.10.2010; SHZ 22.10.2010, 11; Metschies KN 27.11.2010, 7).

Datenschutznachrichten aus dem Ausland

Österreich

ORF-Sprecher tritt nach Lausch-Affäre zurück

Der Sprecher der österreichischen Rundfunkanstalt ORF Pius Strobl trat am 19.11.2010 nach heftiger einwöchiger Kritik durch Redakteure, Betriebsräte, Direktoren und FPÖ-Politikern wegen einer „Lausch-Affäre“ von seinem Amt zurück. Strobl hatte kurz zuvor eine ORF-Mitarbeiterin angewiesen, Gespräche zwischen Direktoren des Senders und JournalistInnen mitzuschneiden – für eine „interne Bewertung“, wie er dies zu erklären versuchte. Der Verein Medienjournalismus Österreich sprach von „völlig indiskutablen“ Aussagen. Die rechte FPÖ hatte eine Klage angekündigt. ORF-Generaldirektor hat das Rücktrittsgesuch akzeptiert. Stroble erklärte, der Rücktritt sei seine Idee gewesen; er sei hierzu nicht gedrängt

worden. Die ganze Sache sei „hochgebauscht“ worden und entbehre jeder Substanz: „Ich habe nie Journalisten oder Stiftungsräte bespitzelt. Der ORF, den ich sehr mag, verdient und braucht einen Kommunikationschef, der zumindest ein so respektvolles Verhältnis zu den Führungskräften des Hauses hat, dass er mit ihnen arbeiten kann“ (SZ 20./21.11.2010).

Österreich

Kfz-Kennzeichenerfassung auf Autobahnen

Am 27.09.2010 sind in Niederösterreich die ersten drei Kameras eines stationären Kamerasystems auf Autobahnen durch die Polizei in Betrieb genommen worden, die alle vorbeifahrenden Fahrzeuge fotografieren. Die erfassten Kennzeichen werden automatisch mit der Fahndungsdatenbank Elektronisches Kriminalpolizeiliches Informationssystem (EKIS) abgeglichen. Der Landeshauptmann Erwin Pröll (ÖVP) vom größten Bundesland Östereichs hatte die Kameras Anfang 2010 angefordert; vier weitere Kamerasysteme werden angeschafft; danach sollen weitere Bundesländer versorgt werden. Die Standorte werden regelmäßig gewechselt. Ergänzend verfügt die österreichische Polizei über mobile Kennzeichenerfassungssysteme. Vorrangiges Ziel der automatisierten Videoüberwachung ist laut Innenministerium die Bekämpfung des Kfz-Diebstahls. Jede Kamera kostet 50.000 Euro; hinzu kommen Installationskosten im fünfstelligen Bereich. Der Autobahnbetreiber ASFINAG stellt neben Strom und Glasfaseranbindung auch die Überkopfbrücken, die meist für die LKW-Mauterfassung errichtet wurden, kostenlos zur Verfügung. Löst das System Alarm aus, wird das Foto an einen Polizisten zur Überprüfung weitergeleitet, der gegebenenfalls die Fahndung veranlasst und Kollegen in der Gegend verständig. Handelt es sich um einen Fehlalarm, so das Innenministerium, „wird der Datensatz sofort gelöscht; der Datenschutz bleibt gewahrt“ (Sokolov www.heise.de 28.09.2010).

Dänemark

Aufforderung zur Denuziation von Sozialbetrügern

Kommunen in Dänemark verschärfen ihre Bemühungen, SozialbetrügerInnen auf die Schliche zu kommen und setzen darauf, dass hierfür andere BürgerInnen denunzieren. Die Dänen können Verdächtige mittels eigens eingerichteter Mail-Adressen oder Online-Formulare an die Behörden melden. Berit Forum von der süddänischen Gemeinde Haderslev erläuterte: „Wir sind auf die Unterstützung der Bürger angewiesen, weil wir nicht bei den Leistungsempfängern vorbeischauen können“. Lange war Nordeuropa in der Sozialpolitik Vorbild für andere Staaten. „Fordern und fördern“ galt in Dänemark schon vor den Reformen der rot-grünen deutschen Bundesregierung. So ist das Land für sein starkes soziales Netz mit einem relativ hohen Arbeitslosengeld, aber auch für besonders kurze Kündigungsfristen bekannt.

Die Idee, gegen Sozialmissbrauch vorzugehen, hat in jüngerer Zeit schnell viel Unterstützung gefunden. Gemäß einer Sprecherin von Vejle, einer Stadt in der Region Süddänemark, die eine kommunale Arbeitsgruppe gegen Sozialmissbrauch leitet, hat binnen einem Jahr etwa jede dritte dänische Gemeinde Anschwärzmöglichkeiten im Netz geschaffen. In Haderslev mit seinen rund 21.000 Einwohnern haben, so Gemeindemitarbeiter Forum, die Onlinehinweise geholfen, die Stadtkassen zu füllen: „Im laufenden Jahr haben wir auf diese Weise 3 Mio. Kronen (rund 0,4 Mio. Euro) eingespart“. 90% der Hinweise hätten sich als richtig erwiesen. Bei den Hinweisen handele es sich zum Beispiel um Personen, die Wohnzuschuss als Alleinstehende beziehen, aber mit einem gut verdienenden Partner leben. Oder um Krankgeschriebene, die Geld beziehen, obwohl sie nebenher arbeiten. Esbjerg in Westdänemark macht seinen BürgerInnen das Verpetzen besonders einfach. Gleich auf der Stadt-Startseite sticht eine Panzerknackermaske ins Auge, daneben steht „Betrugsverdacht“. Der Link führt zu einem schlichten Formular. „Um wen geht es?“, wird da gefragt, „Worin besteht der Betrug?“ und „Was haben Sie konkret beobachtet?“. Eigene Kontaktdaten müssen nicht mitgeliefert werden. Proteste gegen eine „Blockwartmentalität“, wie sie wohl in Deutschland zu erwarten wären, hat es in Dänemark bislang nicht gegeben. JuristInnen kritisieren nur, dass die Kommunen den Betrug nicht beweisen müssen; es obliegt den Verdächtigten, Einspruch einzulegen.

Schleswig-Holsteins Datenschützer Thilo Weichert kommentierte das dänische Modell damit, dass dort der Datenschutz „bei weitem nicht so ernst genommen wird wie hierzulande.“ Deshalb liefen dort „weder die dänischen Datenschutzkollegen noch die Bevölkerung oder Betroffene Sturm gegen die Denunziationsaufforderungen“. Vergleichbare Versuche bei Sozialbehörden und vor allem der Polizei seien zudem in Deutschland erfolglos geblieben: „Die meist anonymen Denunziationen hatten oft weder Hand noch Fuß und dienten oft ausschließlich dem Zweck, jemanden zu schädigen. Auch wenn es in Dänemark „mehr Verantwortungsbewusstsein und eine besser funktionierende Sozialkontrolle“ gebe, das globale Internet sei dazu das „denkbar falscheste Instrument“ (Bomsdorf www.ftd.de 12.10.2010; Höver EZ SHZ 13.10.2010, 1).

Großbritannien/Frankreich/Italien

Personalausweise in europäischen Rechtskulturen

Ab 01.11.2010 gibt es in Deutschland elektronische Personalausweise mit Funkchip. Dies lädt zur Frage ein, wie mit dem Thema in anderen EU-Staaten umgegangen wird. Während Italien ebenso auf Chipkarten setzt, genügt in Frankreich die Stromrechnung zum Identitätsnachweis; die neue britische Regierung lehnt Ausweise strikt ab. In einer ihrer ersten Amtshandlungen kippte die konservative Regierung in London den Beschluss ihrer Vorgänger. Innenministerin Teresa May erklärte, es werde keine Personalausweise im Königreich geben: „Es geht um das Prinzip des Personal-

ausweises: Wir glauben, es ist nicht richtig. Sie funktionieren nicht, verstoßen gegen die Freiheitsrechte, und es wäre falsch, sie den britischen Bürgern aufzuzwingen.“ Die Debatte hierüber wird in Großbritannien seit Jahrzehnten leidenschaftlich geführt. Immer wieder war die Einführung eines solchen Dokumentes mit dem Argument abgelehnt worden, dies sei ein Übergriff des Staates in die Freiheit des einzelnen Bürgers. Das scheint sehr erstaunlich in einem Land, wo Datenschutz ansonsten nicht sehr ernst genommen wird, wo jeder Schritt von Videokameras festgehalten und jeder Kreditkartenkauf gespeichert wird. Doch die Widerstände gegen den Ausweis blieben stark. Erst Premier Tony Blair schaffte es mit seiner Labour Regierung im Jahr 2006 im Rahmen seiner ausufernden Anti-Terror-Maßnahmen, im Parlament mit knapper Mehrheit die Einführung von Personalausweisen zu beschließen (DANA 2/2006, 88 f.). Die scheiterte allerdings dann an der Umsetzung und wegen immer weiter steigender Kosten. Es hatte offensichtlich Blockaden im Behördenapparat gegeben. Als im Frühjahr 2010 die Konservativen gemeinsam mit den Liberalen ans Ruder kamen, brachte die Absetzung der unbeliebten Ausweise Applaus in allen Lagern. Wer in Großbritannien ein Bankkonto eröffnen oder eine Wohnung mieten will, beweist mit seiner Strom- oder Gasrechnung seine Identität.

Die Franzosen haben einen Ausweis, der aber im täglichen Leben kaum eine Rolle spielt. Der Personalausweis ähnelt dem bisher Üblichen in Deutschland. Eine plastifizierte Karte, deutlich größer als eine Kreditkarte, angeblich fälschungssicher; links das Foto, rechts die persönlichen Daten und die Unterschrift des Inhabers, auf der Rückseite die Adresse. Da es in Frankreich keine Einwohnermelderegister gibt, werden zwecks Ausweiserstellung alle möglichen Dokumente akzeptiert, aus denen die Anschrift hervorgeht. Am beliebtesten ist die Stromrechnung, die man auch bei vielen anderen Gelegenheiten vorlegen muss, etwa, wenn man ein Konto eröffnen will. Wer in einer Wohngemeinschaft lebt, in der die Stromrechnung an einen anderen Mitbewohner adressiert ist, kann sich mit einer Telefonrechnung behelfen. Der französische Personalausweis ist kostenlos und gilt zehn Jahre, danach muss man einen neuen beantragen. Im täglichen Leben spielt er eine viel geringere Rolle als in Deutschland. Als „pièce d’identité“ werden viele andere Ausweise mit Foto akzeptiert, der Führerschein etwa oder die Monatskarte für die U-Bahn. Die 13-stellige persönliche Sozialversicherungsnummer, die Franzosen bis zum Tod dauernd begleitet und mit der man beim staatlichen Statistikamt registriert ist, hat dagegen eine erheblich größere Bedeutung. Nach ihr wird häufiger gefragt.

Italien setzt wie Deutschland auf den Chip. Die ItalienerInnen erhalten für ihren elektronischen Personalausweis eine Geheimnummer; ab 2011 soll der alte Papierausweis in Italien Geschichte sein. Der auszumusternde alte Personalausweis besteht noch aus Papier. inzwischen kann man in 180 Kommunen Italiens den neuen elektronischen Personalausweis erhalten. Fast zwei Millionen Bürger können sich schon „elektronisch“ ausweisen. Von Januar 2011 an werden keine Papierausweise mehr ausgegeben. Der neue Scheckkartenpass verfügt über einen Chip, mit dem die BesitzerIn auch elektronisch identifiziert werden kann. Auf dem Chip können auf Wunsch weitere persönliche Daten gespeichert werden: die biometrischen Daten, die Blutgruppe, aber nicht die DNA der BesitzerIn. Für die BürgerInnen kostet der neue Ausweis statt bisher 5,42 Euro stolze 25,42 Euro, wobei bei manchen Behörden die Erstellung des Passfotos gleich mit eingeschlossen ist (Wesel/Wöß/Kleinjung www.tagesschau.de 02.11.2010).

Frankreich

„Genitale Fingerabdrücke“

Mit einem netten Versprecher sorgte der französische Innenminister Brice Hortefeux für Spott und Heiterkeit. In einem Fernsehinterview sprach er von „genitalen Fingerabdrücken“ – ein Lapsus, der danach im Internet massenhaft reproduziert wurde. Hortefeux sagte: „Es gibt zwei wichtige Dateien: die Datei der genitalen Fingerabdrücke und die Datei der genetischen Fingerabdrücke.“ Offenbar meinte er den Unterschied zwischen Polizeidateien mit digitalisierten Fingerabdrücken Verdächtiger und Datenbanken mit DNA-Angaben, also Genanalysedateien, vermischte also genetisch und digital zu genital. Siegmund Freud hätte seine Freude gehabt (SZ 19.10.2010, 9).

Großbritannien

Jedermensch-Videokontrolle über das Internet

In Großbritannien macht ein Internet-Überwachungsprojekt Furore, mit dem Internet-Nutzende von zuhause aus Ladendiebe stellen sollen. Das Unternehmen „Internet Eyes“ wirbt mit dem Slogan „Ein Verbrechen erkennen, wenn es passiert“. Die Beobachter lassen sich auf ihren Bildschirm die Bilder von Überwachungskameras in britischen Geschäften übertragen, und zwar vier Kameras gleichzeitig. Bemerken sie einen Ladendiebstahl, klicken sie auf einen Button – der Besitzer oder das Sicherheitspersonal erhalten dann sofort per SMS eine Benachrichtigung mit einem Screenshot der Kameraaufnahme und können den mutmaßlichen Dieb daraufhin stellen. Die Macher meinen, mit dieser Methode lasse sich ein echtes Problem lösen: Einer Statistik des Centre for Retail Research zufolge wird der Einzelhandel in Großbritannien im Jahr 2010 durch Ladendiebstahl Waren im Wert von fast 1,9 Milliarden Pfund verlieren. Internet-Eyes-Geschäftsführer Tony Morgan erläuterte: „Die kleinen Läden an der Ecke sterben. Viele müssen pro Woche Waren im Wert von 500 Pfund abschreiben.“ Sein Dienst sei vor allem Hilfe zur Selbsthilfe. Das Geschäftsmodell ist vor allem für Morgan lukrativ: 75 britische Pfund kostet es monatlich, sein Geschäft von Internet Eyes überwachen zu lassen. Und auch die Nutzer zahlen knapp 13 Pfund im Jahr dafür, dass sie als Hobby-Ladendetektive am Bildschirm aktiv werden dürfen.

Für mehr als 60 Monatsstunden Beobachtung erhalten sie 1,50 Pfund. Jeder

erfolgreiche Hinweis gibt Bonuspunkte; der erfolgreichste Internet-Spion kassiert am Ende des Monats die ausgelobte Prämie von 1000 Pfund (umgerechnet etwa 1150 Euro).

Britische Einzelhändler investieren pro Jahr derzeit 977 Millionen Pfund, um Warendiebstahl zu verhindern; Sicherheitsleute erhalten den gesetzlichen Mindestlohn. Seit Oktober 2010 wird die Internet-Überwachung in 30 Geschäften getestet, unter anderem in Spar-Märkten. Die Branchenverbände halten sich bislang offiziell mit einer positiven Bewertung von Internet Eyes zurück. Die britischen Handelskammer stellte klar, dass deren Mitglieder dazu keine einheitliche Meinung haben. Vertreter der größten britischen Supermarktkette Tesco wollen sich zu einem möglichen Test nicht äußern. Beim bekannten Einzelhändler Marks & Spencer schweigt man zu der „heiklen Thematik". Alexander Hanff von der britischen Bürgerrechtsgruppe Privacy International kritisierte: „Es ist schlimm genug, wenn die Behörden die Menschen verfolgen, sollen nun auch noch Bürger ihre Mitbürger ausspionieren?" Internet-Eyes-Chef Morgan hält solche Einwände für übertrieben: „Bereits jetzt kann jeder Mensch über Webcams sehen, wer sich gerade an Plätzen wie dem Picadilly Circus aufhält." Die Nutzer könnten die Kameras im Laden weder steuern, noch die Geschäfte auswählen – die Beobachtung eines Objekts im Bereich der eigenen Postleitzahl sei ausgeschlossen. Zudem werde das Bild nach Auslösen des Ladendieb-Alarms eingefroren, eine mögliche Verhaftung wäre also nicht zu sehen. Bei mehrmaligem Fehlalarm werde ein Nutzer gesperrt.

Nicht verhindern lässt sich, dass die Internet-Ladenbewacher die Videos mitschneiden und beispielsweise später auf YouTube eine Hitparade der seltsamsten Einkaufsgewohnheiten zusammenstellen – in der sich dann unwissentlich jeder Kunde wiederfinden kann. Hierzu Hanff: „Es ist eine Sache, ob ein Ladendetektiv solches Material sieht, eine andere ist es, ob irgendjemand anderes darauf zugreift, dessen Motive nicht bekannt sind." Nach nur vier Wochen hatten sich bereits mehr als 1800 Nutzende registriert, um mit Hilfe der Überwachungskameras nach Dieben zu suchen. Nach Angaben von Internet Eyes kommen viele davon aus Frankreich und Deutschland. Das passt in die Geschäftsstrategie, wonach mittelfristig die Augen aus dem Internet auch Geschäfte auf dem Kontinent überwachen sollen (Kuhn www.sueddeutsche.de 03.11.2010).

Tschechien

Datenschutzbehörde stoppt Google Street View

Die tschechische Datenschutzbehörde lehnte erneut einen Antrag von Google zur Sammlung von personenbeziehbaren Daten für seinen Straßenbilddienst „Street View" durch Kamerafahrzeuge wegen Zweifeln an der datenschutzkonformen Datenverarbeitung ab. Seit Oktober 2009 zeigt der Google-Dienst Bilder aus der Hauptstadt Prag sowie 3 weiteren Städten. Diese Daten sind von der Anordnung nicht betroffen. Die Aufsichtsbehörde in Prag untersagte vielmehr Google, das Street-View-Programm fortzuführen (DSB 10/2010, 6).

Schweiz

Massiver Rechtsverstöße bei Staatsschutz-Datensammlung

Der Staatsschutz verarbeitete Daten von über 200.000 Personen „nicht gesetzeskonform". Ein Bericht der Geschäftsprüfungsdelegation (GPDel) des Schweizer Parlaments kommt zu diesem Ergebnis und forderte am 30.06.2010 in Bern den Einsatz eines externer Datenschutzbeauftragten. Der solle nun bestimmen, welche Daten in der Datenbank ISIS (Informatisiertes Staatsschutzinformationssystem) gelöscht oder behalten werden dürfen. GPDel-Präsident Claude Janiak rügte, bei der Geheimdienstdatensammlung sei vor allem die Pflege und Systematik der Datenbank über Jahre hinweg enorm vernachlässigt worden. Daten von heute 120.000 erfassten Personen „mit eigener Staatsschutzrelevanz" seien nicht richtig überprüft worden, häufig seien falsche Daten eingetragen worden. Um Kontrollen vorzutäuschen, seien Daten auch verfälscht worden. Rund die Hälfte der 200.000 Datensätze des Nachrichtendiensts seien überhaupt nicht direkt von Belang. Unter den in ISIS gespeicherten Personen sind etwa auch 83.000 sog. Drittpersonen, die in der Mehrheit nicht staatsschutzrelevant seien. Ihre Speicherung entspreche daher nicht den rechtlichen Vorgaben. Drittpersonen sind etwa erfasst, weil sie eine Verbindung zu einer registrierten Person oder zu einer Meldung in der Datenbank haben. Vor allem handelt es sich um über 50.000 Personen, die aufgrund der sogenannten Fotopasskontrolle registriert wurden. Im Rahmen dieses präventiven Fahndungsprogramms werden Personen aus einem Dutzend Staaten an der Grenze erfasst, wenn sie in die Schweiz ein- oder ausreisen.

Mängel bei der Qualitätskontrolle stünden im Zusammenhang mit einer Umstellung auf ein neues Datenbanksystem. 2005 wurden die Daten aus dem alten, hierarchisch organisierten ISIS-System in eine relationale Datenbank mit dem Namen ISIS-NT (Neue Technologie) übertragen. Die Nachrichtendienste haben zudem laut GPDel in großem Ausmaß vernachlässigt, die gesetzlich alle fünf Jahre vorgeschriebene Überprüfung vorzunehmen. Das vernichtende Fazit der parlamentarischen Kontrolleure ist, dass die Datenverarbeitung „in keiner Art und Weise" den rechtlichen Anforderungen entspricht, was „Zweifel an der Richtigkeit und Relevanz der Daten" aufkommen lasse. Die GPDel forderte eine provisorische Datensperre aller Daten, die nicht ordnungsgemäß überprüft wurden. Der Eidgenössische Datenschutzbeauftragte (EDÖB) Hanspeter Thür hatte der GPDel entsprechende Hinweise gegeben: „Die Größenordnung zeigt, dass eine gewisse Eigendynamik entsteht, wenn Amtsstellen verpflichtet werden, Daten zu sammeln." Thür forderte eine Stärkung der beiden Aufsichtsorgane GPDel und EDÖB.

Januiak stellte mit Blick auf die sog. „Fichenaffäre" fest, dass ein Kulturwandel beim Staatsschutz wohl nicht stattgefunden habe. Die der Affäre den Namen gebende Personenkartei hatte Ende der 1980er Jahre einen der größten politischen Skandale der Schweiz ausgelöst. Dabei stellte sich heraus, dass

Bundespolizei und Nachrichtendienst rund 900.000 Personen, Organisationen und Ereignisse bespitzelt hatten. Jede zwanzigste SchweizerIn und jede dritte AusländerIn war in der Kartei erfasst, die 1994 von ISIS abgelöst wurde (Sperlich www.heise.de 01.07.2010).

Schweiz

Grundstückseigentümer Luzern georeferenziert online

Seit Ende August 2010 haben Internetbenutzende Zugang zum überarbeiteten Geoportal des Kantons Luzern mit Rauminformationen einschließlich Grundstücksnummer und EigentümerInnen, Zonenpläne und vieles mehr. Der Auftritt basiert auf neuesten Webtechnologien mit einem schnellen Kartenaufbau und einer guten Darstellungsqualität der Fach- und Hintergrundkarten. Die dargestellten Bilder sind aktueller und schärfer als die von Google Maps. Die Benutzenden können sich dank einer reduzierten Anzahl von Bedienelementen schnell zurechtfinden. Das Geoportal macht Daten mit Raumbezug für die Öffentlichkeit zugänglich. Dabei gehört der Kanton Luzern zu den Pionieren. Bereits 2002 hat das Geografische Informationssystem (GIS) Kanton Luzern die erste Online-Karte aufgeschaltet. Thomas Hösli, Leiter Geoinformation und Vermessung Kanton Luzern, hat unter anderem für seine innovative Leistung beim Geoportal einen Preis in den USA erhalten (www.zisch.de 27.08.2010).

USA

Bürgerrechtsorganisation fordert Infos zu Google-NSA-Kooperation

Die Bürgerrechtsorganisation Electronic Privacy Information Center (EPIC) hat beim „United States District Court for the District of Columbia“ einen Antrag auf Herausgabe von Dokumenten nach dem Freedom of Information Act (FOIA) zur Zusammenarbeit zwischen dem Internet-Dienstleister Google und dem US-Geheimdienst NSA (National Security Agency) gestellt: Welche Vereinbarungen wurden im Zusammenhang mit der Abwehr und Aufklärung von Hacker-Angriffen auf die eigene Netzwerkinfrastruktur getroffen? Welche Konsequenzen hat die Zusammenarbeit mit dem Information Assurance Directorate (IAD) der NSA für die Millionen Nutzenden des Google-Mail-Dienstes Gmail? Die Antworten auf diese Fragen wurden EPIC bisher verwehrt. EPIC meint, die Öffentlichkeit habe das Recht, „Details der Partnerschaft zu erfahren, um wichtige Entscheidungen hinsichtlich persönlicher Daten und der Nutzung von E-Mail treffen zu können“. Google hatte im Januar 2010 mitgeteilt, von China aus sei ein technisch hochkomplexer Angriff auf die eigene Netzwerkinfrastruktur durchgeführt worden, der zum „Diebstahl geistigen Eigentums“ geführt habe. Im Mittelpunkt hätten Gmail-Konten von chinesischen Menschenrechtsaktivisten gestanden. Kurz darauf gab das Unternehmen bekannt, man habe die für Spionagefälle zuständige NSA eingeschaltet und der Behörde Zugriff auf fallrelevante Daten gewährt.

EPIC kritisiert Google unter anderem, erst nach dem Angriff, der zu erheblichen Dissonanzen zwischen dem Unternehmen und der chinesischen Regierung führte, eine standardmäßige Verschlüsselung des Gmail-Datenverkehrs implementiert und Nutzende des Mail-Dienstes damit einem „sehr realen Datendiebstahl-Risiko ausgesetzt“ zu haben. Eine diesbezügliche Beschwerde hatte die Organisation bereits im März 2009 bei der Federal Trade Commission (FTC) eingereicht. EPIC will nun wissen, welche Rolle die NSA, die seit Jahren wegen fragwürdiger Abhöraktionen im Zusammenhang mit Maßnahmen zur Terrorismusbekämpfung in den USA in der Kritik steht, bei der Ausgestaltung der Sicherheitsstandards von Gmail und anderen Google-Webdiensten spielt (www.heise.de 14.09.2010).

USA

SDU spioniert im befreundeten Ausland

Die US-amerikanische Regierung lässt US-Einrichtungen in Deutschland und auch in vielen weiteren „befreundeten Staaten“ von einer geheimen Organisation überwachen. Für die US-Botschaft in Berlin ist eine „Surveillance Detection Unit“ (SDU) tätig, in der neben US-amerikanischen offenbar auch deutsche Sicherheitsexperten beschäftigt sind. Diese sollen – wie in vielen anderen Staaten – verdächtige Personen in der Nähe von US-Einrichtungen beobachten, um möglichen Terroranschlägen vorzubeugen. Das deutsche Bundesinnenministerium teilte auf Anfrage mit, ihm sei die Existenz einer solchen Einheit nicht bekannt. Tatsächlich finden sich Angaben zum „Surveillance Detection Program“ (SDP) auf Webseiten der US-Regierung. Die SDUs wurden im Jahr 2000 als Reaktion auf Anschläge auf zwei US-Botschaften in Afrika 1998 gestartet.

Erstmals bekannt wurde die SDU in Norwegen. Nach Fernsehberichten von Anfang November 2010 operiert die bei der US-Botschaft in Oslo im Geheimen aufgebaute Überwachungsorganisation in einer „eigenen Sphäre außerhalb der norwegischen Gesetze“. Ihre Aufgabe sei die Registrierung von Personen, die Terroranschläge auf amerikanische Einrichtungen planen könnten. Danach ist die Gruppe von 15 bis 20 norwegischen und amerikanischen Sicherheitsexperten für den Geheimdienst SDU seit 10 Jahren aktiv. Viele von ihnen hatten für heimische Dienste gearbeitet, ehe sie sich von der US-Agentur anheuern ließen. Der Leiter der Gruppe in Norwegen sei der 71-jährige Olaf Johan Johansen, pensionierter Chef der Antiterroreinheit der norwegischen Polizei. Seine KollegInnen kommen teils von der Kripo, vom Militär und von der Zivilbereitschaft. Hunderte NorwegerInnen landeten in der von der SDU aufgebauten Datenbank. Die Überwachungsgruppe registrierte rund um die Uhr Autos und Personen, die in der Nähe von US-Einrichtungen auffielen, fotografiert und filmt „verdächtige Handlungen“ und Demonstrationen und sammelt detaillierte Daten über die Verdächtigen bis hin zu Augenfarbe und Namen der Eltern. Die Daten wurden an die Sicherheitsverantwortlichen der US-Botschaft weitergeleitet. In Oslo lösten die Enthüllungen heftige Reaktionen aus. Justizminister Knut Storberget und Außenminister Jonas Gahr Støre er-

klärten, man habe von der geheimen Überwachung nichts gewusst. Hingegen behauptete ein Sprecher des State Department in Washington, dass der Einsatz mit norwegischen Stellen abgesprochen sei. Støre berief daraufhin den US-Botschafter ein, um Auskunft zu fordern, erhielt jedoch keine befriedigende Antwort. Sollte sich herausstellen, dass der Dienst die norwegischen Gesetze verletzt habe, sei dies „sehr ernst".

Storberget kündigte eine Untersuchung an und schaltete auch das Parlament ein. Dort nannten Politiker aller Lager die Existenz eines aus dem Ausland gesteuerten Parallel-Geheimdienstes „schockierend" und „erschreckend". Helga Hernes, die Vorsitzende des Kontrollausschusses für Sicherheitsdienste, meinte: „Das ist nicht die Art, die wir von einem befreundeten Land erwarten." Die norwegische Polizei bezeichnete die Existenz der SDU als „völlig unbekannt", obwohl man Teile der Tätigkeit gekannt habe. Verletzungen des norwegischen Rechts habe man nicht feststellen können. Bjørn Erik Thon, der Chef der Datenschutzbehörde, meinte dagegen: „Norwegische Regeln wurden zur Seite geschoben". Das Sammeln von persönlichen Daten in privaten Registern sei verboten, und nur die Polizei und norwegische Behörden dürften eine Überwachung in Gang setzen. „Polizeioperative Maßnahmen" seien ausschließlich Sache der heimischen Justiz, betonte die Sicherheitspolizei. Es mag natürlich sein, dass die US-Botschaften ihre eigene Sicherheitsbereitschaften haben, nicht aber, wenn mit Hilfe ehemaliger Polizisten eine eigene Spionageorganisation aufgebaut wird. Der US-Botschaftssprecher in Norwegen, Tim Moore sicherte den Behörden intensive Zusammenarbeit bei der Aufklärung zu. Am 05.11.2010 stellt SDU in Norwegen seine Überwachungsaktivitäten vorläufig ein.

Moore bestätigte, dass es ähnliche Operationen „seit längerer Zeit in mehreren Ländern" gebe. „Es gibt einen offensichtlichen Bedarf dafür; schließlich sind amerikanische Botschaften mehrmals attackiert worden." Die Überwachung geschehe stets „in Zusammenarbeit mit den Behörden der betroffenen Länder". Die SDU ist auch in weiteren Staaten Nordeuropas aktiv. In Schweden leitete die Staatsanwaltschaft eine Voruntersuchung wegen des Verdachts auf „ungesetzliche nachrichtendienstliche Tätigkeit" ein. Justizministerin Beatrice Ask wie auch der Chef des Geheimdienstes Säpo Anders Danielsson beteuerten, noch nie etwas vom SDP gehört zu haben. Danielsson räumte ein, es könne durchaus sein, dass einzelne Polizisten eingeweiht wurden: „Aber bei Tätigkeiten dieser Art muss man auf der richtigen Ebene informieren." In Finnland will der Geheimdienst Supo die Überwachungsaktivitäten unter die Lupe nehmen. In Island wurde die Polizei mit Nachforschungen beauftragt. Der Rundfunk berichtete, die Einheit habe rund um die US-Botschaft in Reykjavik den Hausmüll durchsuchen lassen (Herrmann SZ 11.11.2010, 8; Herrmann SZ 08.11.2010, 8; ND 06./07.11.2010, 7; www.heise.de 08.11.2010; Gamillscheg www.fr-online-de 04.11.2010).

USA

Obama-Regierung will Internet-Überwachung verstärken

Die US-Regierung arbeitet gemeinsam mit Sicherheitsbehörden wie FBI und der National Security Agency (NSA) an einem Gesetzesentwurf zum einfacheren Abhören von Internet-Telefonaten, verschlüsselten E-Mails und Chat-Nachrichten. Gemäß Presseberichten müssten Kommunikationsdienstleister, die den Austausch verschlüsselter Botschaften ermöglichen, Strafverfolgern und Geheimdiensten dann verdächtige Nachrichten im Klartext vorlegen. Ausländische Anbieter, die ihre Dienste in den USA anbieten, sollen demnach verpflichtet werden, ein Büro in den Vereinigten Staaten zu unterhalten, um darüber die Abhör- und Entschlüsselungsaktionen sicherzustellen. Entwickler von Software zur „Peer to Peer"-Kommunikation wie Instant Messaging würden angehalten, ihre Anwendungen schon vom Design her abhörfreundlich zu gestalten. Klassische Telekommunikationsanbieter stehen in den USA mit dem „Communications Assistance for Law Enforcement Act" (CALEA) von 1994 bereits in der Pflicht, Überwachungsschnittstellen für die Sicherheitsbehörden bereitzuhalten. Seit Jahren findet ein auch vor Gericht ausgetragener Streit statt, ob diese Bestimmung auch auf Provider von Voice over IP (VoIP) und Breitbandzugängen auszudehnen ist. Dies bejahten 2006 ein Washingtoner Berufungsgericht sowie die US-Regulierungsbehörde, die Federal Communications Commission (FCC). Technologiefirmen und Bürgerrechtsvereinigungen sind dagegen seit Längerem der Ansicht, dass die bestehenden Regelungen zur Überwachung des Internetverkehrs ausreichend sind. Ermittler und Staatsschützer würden schon jetzt alle Daten erhalten, die sie für ihre Arbeit benötigen.

Sicherheitsbehörden befürchten angesichts der wachsenden Beliebtheit von Geräten wie den Blackberrys, die für eine verschlüsselte E-Mail-Übertragung sorgen, sowie sozialen Netzwerken wie Facebook und ihren Chatmöglichkeiten, ins Hintertreffen zu geraten. Ihre traditionellen Möglichkeiten zum Abhören von Kriminellen und Terroristen mit der zunehmenden Online-Kommunikation reichten nicht aus. Sie wollen daher von den Diensteanbietern verlangen, dass diese gerichtlichen Abhörgenehmigungen in allen Fällen nachkommen und ihnen unverschlüsselte Nachrichten an die Hand geben können. Die Gesetzesinitiative, die zeitnah eingebracht werden soll, reißt die alten Gräben zwischen Datenschützern, Internetwirtschaft und Behörden neu auf. James Dempsey vom Center for Democracy and Technology (CDT) warnt, dass der Vorstoß letztlich ein „komplettes Redesign der dezentralen Internetarchitektur" verlange. Diese solle wieder so funktionieren, wie das alte Telefonsystem. Die Bürgerrechtsorganisation ACLU warnte vor einem „enormen Eingriff in die Privatsphäre". Die Electronic Frontier Foundation (EFF) wies darauf hin, dass die geplanten Gesetzesvollmachten viel umfassender sind, als bisher. Bei 2400 Überwachungsanträgen, die US-Behörden 2009 gestellt wurden, habe es sich nur in einem Fall um verschlüsselte Daten gehandelt. Sicherheitsexperten warnen davor, dass die ausgeweiteten legalen Abhörschnittstellen von Computerkriminellen leicht missbraucht

werden könnten. Providervertreter verweisen darauf, dass die Implementierung der Überwachungsfunktionen eine enorme technologische und finanzielle Herausforderung für die Anbieter mit sich bringen würde. Die Entwicklung innovativer Dienste werde so behindert.

Die FBI-Justiziarin Valerie Caproni hält dagegen, dass es nicht um eine Ausweitung von Befugnissen, sondern um deren Anwendungsmöglichkeit im Interesse der inneren Sicherheit gehe. Derzeit brauche man bei einigen Anbietern oft Monate, um überhaupt Abhörmöglichkeiten ausfindig zu machen. Bei verschlüsselten Botschaften käme man häufig gar nicht weiter. Angst vor Wirtschaftsspionage bräuchten die Nutzer auch künftig nicht haben. Die Provider und Gerätehersteller könnten ihren Kunden weiter „starke Verschlüsselung versprechen. Sie müssen nur einen Weg finden, uns mit dem Klartext zu versorgen“ (Klüver SZ 29.09.2010, 8; Krempl www.heise.de 27.09.2010).

USA

Facebook-Entwickler verkauften Nutzerdaten

Anwendungsentwickler für das soziale Netzwerk Facebook haben nach Angaben des Unternehmens am 29.10.2010 offenbar Nutzer-IDs gesammelt und an einen Datenhändler verkauft. Die fragwürdige Praxis sei bei der Untersuchung einer datenschutztechnisch problematischen Lücke aufgefallen, über die Anwendungen ungewollt individuelle Nutzer-IDs preisgaben. Facebook betonte die eigenen Datenschutzregeln, nach denen Anwendungen keine persönlichen Nutzerdaten einschließlich der ID für Anzeigendienstleister oder Datenhändler preisgeben dürften. Nachdem bekannt wurde, dass dies in einigen Fällen unbeabsichtigt geschieht, habe Facebook die Regeln angepasst. Darüber hinaus will der Betreiber den Programmierern eine anonyme Identifikationsmöglichkeit für Anwendungen über das API bereitstellen. Bei der Untersuchung der unbeabsichtigten ID-Weitergabe sind laut Facebook einige Entwickler aufgefallen, die sich von einem Datenhändler für Nutzer-IDs bezahlen ließen. Es handele sich um „weniger als ein Dutzend“ auffällig gewordene Entwickler, über die eine sechsmonatige Sperre verhängt wurde. Künftig will der Betreiber den Umgang mit Daten dieser Entwickler genauer überprüfen. Es seien keine privaten Daten der Nutzenden verkauft worden, auch erlaubten die IDs keinen Zugriff auf persönliche Daten. Anhand der IDs lassen sich Nutzernamen ermitteln und die auf den Seiten der betroffenen Nutzer öffentlich zugänglichen Informationen zur Profilbildung erfassen. Facebook erklärte, dass der Datenaggregator RapLeaf eingewilligt habe, alle Nutzer-IDs in seinem Besitz zu löschen und der Plattform künftig fernzubleiben (www.heise.de 01.11.2010).

USA

Locationslabs vertreibt Positionsdaten von potentziell 250 Mio. Mobilgeräten

Die US-Firma Locationlabs kann den Standort von über 250 Millionen Mobiltelefonen in den USA bestimmen und verfolgen. Nachdem der Mobilfunkanbieter Verizon seine Entwickler-Schnittstellen für Locationlabs geöffnet hat, arbeitet das Unternehmen nun mit den vier großen US-Anbietern (AT&T, Sprint und T-Mobile) zusammen. Locationlabs-Geschäftsführer Tasso Roumeliotis warb: „Bei diesem Verbreitungs-Grad gibt es nichts, das Entwickler davon abhalten kann, eine ganze Reihe von neuen, aufregenden ortsbezogenen Diensten für die breite Masse anzubieten“. Seine Firma verkauft diese Daten unter dem Titel „Universal Location Service“ an Entwickler, die mit Hilfe dieser Daten ortsgebundene Dienste erstellen und anbieten. Locationlabs versteht sich selbst als Dienstleister, der die Standortbestimmung für andere Anbieter ermöglicht. Somit werden derzeit nicht tatsächlich 250 Millionen Handys geortet – es besteht aber die Möglichkeit dazu. Geortet werden den Nutzungsbedingungen zufolge nur Mobiltelefone der Personen, die dem zuvor bei einem der Dienste zugestimmt haben, den Service von Locationlabs zur Lokalisierung zu nutzen. Beispiele für Unternehmen, die mit Locationlabs-Daten neue Dienste betreiben, sind Kurierdienste, die den Ortungsservice nutzen, um KundInnen den Standort ihrer Lieferungen anzuzeigen. Dazu wird das Handy des jeweiligen Kurierfahrers geortet. Ein Wettanbieter nutzt den Ortungsdienst, um Sportwetten nur von KundInnen in Nevada anzunehmen, weil das Wettangebot in diesem Bundesstaat legal ist. Der Anbieter Finsphere verspricht eine zusätzliche Absicherung von Kreditkartenzahlungen. Das Unternehmen gleicht den Standort des Mobiltelefons einer NutzerIn mit dem Ort ab, an dem gerade mit der Kreditkarte bezahlt wird und warnt, wenn die Standorte nicht übereinstimmen. Der Preis für diese Absicherung ist, dass man Finsphere Einblick in das Kaufverhalten und die Position seines Mobiltelefons gewährt. Die NutzerIn sollte zudem stets sein Telefon beim Bezahlen dabei haben. Und wenn einem beides – Handy und Kreditkarte – geklaut wird, funktioniert die Warnung nicht. Besonders interessant sind die Daten natürlich für Werbeanbieter – auch hierfür werden die Handy-Ortungsdaten bereits genutzt (www.spiegel.de 23.09.2010).

China

Internet-Zensur und -Kontrolle lückenhaft

Chinesische Internet-Nutzende tummeln sich in einem unüberschaubaren Raum, wo auch sie die „New York Times“ lesen und harte Pornografie herunterladen können. Dazu kommen Websites für Spiele, Klatsch und Tratsch, akademische Foren und illegale Software. Mit 384 Millionen Menschen hat China die meisten Internet-Nutzenden der Welt. Während Nachrichten auf Englisch – auch solche mit Kritik an China – meist abgerufen werden können, bleiben gewisse soziale Netzwerke wie Facebook sowie eine Reihe ausländischer Blogs ausgesperrt. Zu groß ist aus Sicht der Behörden die Gefahr, die von der blitzschnellen Verbreitung von Nachrichten über diese Kanäle ausgehen könnte. Auch Websites, die sich eingehender mit sensiblen Themen wie dem Massaker

auf dem Platz des Himmlischen Friedens 1989 oder der verbotenen Gruppe Falun Gong beschäftigen, werden blockiert. Eine völlige Sperre bleibt jedoch die Ausnahme.

Stattdessen setzt der Staat auf ein ausgeklügeltes System, das abweichende Meinungen zwar eindämmen, der wirtschaftlichen Entwicklung aber gleichzeitig genug Raum lassen will. Erste Anlaufstelle sind die Redakteure und Autoren von Websites. Sie erhalten regelmäßig von den Behörden detaillierte Anweisungen, wie sie mit den Inhalten umzugehen haben. Als Folge dessen kann es passieren, dass Themen von der ersten Seite genommen, die Kommentar-Funktion ausgestellt oder nur die Veröffentlichung von offiziellen Berichten erlaubt werden. Beobachtende vermuten, dass China zusätzlich eine „50-Cent-Armee" unterhält, die für minimales Entgelt regierungsfreundliche Kommentare in Foren stellt. Viele ChinesInnen scheinen sich von Zensur und Kontrolle nicht beeindrucken zu lassen. Wer genügend Geld hat, kann seinen Computer mit Hilfe der VPN-Technologie (Virtual Private Networks) direkt an das Internet außerhalb der Zensurmauern ankoppeln. In einer High-Tech-Version eines Katz-und-Maus-Spiels versuchen Internet-Nutzende, Blog-Postings schneller zu verbreiten als die Zensur sie aus dem Netz nehmen kann. Gelöschte Nachrichten werden dabei scherzhaft „harmonisiert" genannt – eine satirische Anspielung auf Präsident Hu Jintaos Vision einer „harmonischen Gesellschaft" (derstandard.at 23.03.2010).

Internet

Fälschlich wegen Tötung von Hundwelpen weltweit am Pranger

Im Portal YouTube wurde ein 44 Sekunden dauerndes Video veröffentlicht, das ein blondes Mädchen mit einem roten Pullover, das mehrere fiepende schwarz-weiße Welpen einzeln aus einem Eimer herausnimmt und in einen Fluss wirft. Mit dieser Tat wurde schnell fälschlich eine Ayinger 18jährige Schülerin in Verbindung gebracht, deren Namen veröffentlicht und tausendfach weltweit verbreitet wurde. Das Mädchen wurde mit Morddrohungen und übelsten Beschimpfungen überzogen und flüchtete ins Ausland. Günter Mäser vom Landeskriminalamt Bayern berichtete: „Natürlich haben wir mit der Videoplattform YouTube Kontakt aufgenommen und den Film mit dem Mädchen, das die Hundewelpen ertränkt, löschen lassen." Doch inzwischen war der Streifen tausendfach kopiert worden und an anderen Stellen im Netz verfügbar. Die umstrittene Tierschutzorganisation Peta setzte 2.000 Dollar Kopfgeld auf die Hundetöterin aus. Auf der Seite dieser Organisation meldete sich dann Michael Bay, der Regisseur des Hollywood-Films Armageddon zu Wort und bot 50.000 Dollar für Hinweise auf die Tierquälerin.

Dass Menschen im Internet beleidigt, bedroht und diffamiert werden, ist inzwischen ein Phänomen, das nach der Rechtsanwältin Kerstin Piller-Simon ständig zunimmt. Es komme immer öfter vor, dass intime Bilder ins Netz gelangen, Menschen geoutet werden oder sich nach einer Trennung der Partner via Web rächt. Für die Opfer sei dies oft mit massiven beruflichen Einschnitten verbunden, „oder sie werden auch im sozialen Umfeld gemieden". Mäser ergänzte: „Es gibt Leute, die sitzen den ganzen Tag am Computer, suchen nach interessanten Videos und informieren andere User. Dies funktioniert aber auch in die andere Richtung. Auf Facebook posteten Nutzende Hinweise, dass das Mädchen aus Aying unschuldig ist. Die bosnische Polizei meinte inzwischen, das auf dem Video gezeigte Mädchen identifiziert zu haben. Das Mädchen stamme aus Bugojno im Zentrum Bosniens. Den Namen der Jugendlichen wollte die Polizei nicht mitteilen. Bei der Untersuchung des durch das Videoportal Youtube bekannt gewordenen Falles werde „das vorgeschriebene Verfahren" eingehalten, sagte ein Sprecher. In Bosnien steht auf Tierquälerei eine Geldstrafe von umgerechnet 15 bis 5000 Euro. Die Misshandlung von Tieren ist allerdings durchaus verbreitet und erregt die Gemüter der Bosnier kaum. Bosnische Medien berichteten, das Mädchen sei von seiner Großmutter angestiftet worden, die erst drei Tage alten Hunde zu ertränken (www.stern.de 04.09.2010; Haimerl/Wimmer SZ 03./04.09.2010, 39).

Technik-Nachrichten

DIN übernimmt innerhalb der ISO Normungskoordination zu ‚Privacy' und Datenschutz

Oktober 2010 fand in Berlin die „First ISO Privacy Standards Conference", deren Leitthemen die aktuellen und künftigen Standardisierungsaktivitäten auf dem Gebiet „Datenschutz" und „Wahrung der Privatsphäre" innerhalb von ISO, IEC und JTC 1 waren. Es nahmen ExpertInnen u.a. aus den Sektoren Bankwesen, Intelligente Transportsysteme, Medizinische Informatik, Sicherheitsverfahren teil. Mit der Einsetzung des Lenkungskomitees „ISO/TMB/PSC" im Technischen Beirat der ISO wurde bereits 2009 ein Forum ins Leben gerufen, das die Richtung der Standardisierungsarbeit für den Datenschutz und die Privatsphäre bestimmen soll. Das Sekretariat, das die Arbeit auf diesem Gebiet koordiniert, hat Deutschland bzw. das Deutsche Institut für Normung (DIN) übernommen. Zu den Aufgaben des PSC gehört es, diejenigen ISO-Normen und ISO-Komitees zu identifizieren, die vom Thema Datenschutz tangiert werden. Dies sind u.a. ISO/TC 68 „Financial Services", ISO/TC 204 „Intelligent transport systems", ISO/TC

215 „Health informatics“, ISO/TC 247 „Fraud Countermeasures and Controls“ und ISO/IEC JTC 1 „Information Technology“ mit dem Unterkomitee 27 „IT Security Techniques“. Das PSC wird ein Dokument erarbeiten, in dem die Terminologie des Datenschutzes ISO-weit definiert wird. Dies ist, so TeleTrust, wichtig, weil divergierende Begriffswelten in unterschiedlichen Komitees den umfassenden Koordinierungsansatz der ISO verhindern würden. Einheitlich definierte Fachbegriffe seien eine Voraussetzung für die Erarbeitung von Leitlinien zur Einbindung von Datenschutzaspekten in ISO-Normen (Mühlbauer PE TeleTrust 28.10.2010).

Gefahrenereignis-Detektion per Video-Mustererkennung

Das Fraunhofer-Institut für Angewandte Informationstechnik in Sankt Augustin bei Bonn hat eine Software entwickelt, die bei Videoüberwachungsaufnahmen auffällige Ereignisse gezielt erkennen und markieren kann. Dieses „Smart Eyes“ getaufte System, das mit einer festen und zwei beweglichen Kameras arbeitet, analysiert zunächst die typischen – als unproblematisch detektierten – Bewegungsmuster der jeweiligen Szenerie, im Fußballstadion also z.B. Fahnenschwenken oder jubelnde Fans. Was sich davon abhebt, z.B. eine Prügelei oder ein Einzelner, der aus der Menge ausbricht, markiert das System auf den Security-Monitoren farblich und in Echtzeit. Sofort richten sich zudem die beiden beweglichen, ultraschnellen Kameras auf das verdächtige Muster und liefern eine Aufnahme in besonders hoher Auflösung (Der Spiegel 39/2010, 150).

Mit Firesheep kinderleicht WLAN scannen

Mit der im Internet kostenlos herunter zu ladenden Software „Firesheep“ ist es möglich, automatisch nach ungesicherten WLAN-Verbindungen in der Umgebung zu schnüffeln. So ist es z.B. einfach möglich auszuspähen, wer sich über ein ungeschütztes WLAN in einem Café anmeldet und kann so fremde Daten abgreifen. Eric Butler, ein Programmierer als Seattle/USA, der „Firesheep“ geschrieben hat, erläuterte, er wolle auf Gefahren hinweisen, die ohnehin existieren. Der Tübinger Sicherheitsberater Sebastian Schreiber rät, ausschließlich verschlüsselte Verbindungen zu nutzen: „Vielleicht führt die Debatte dazu, dass Firmen wie Facebook endlich Verschlüsselung anbieten“ (Der Spiegel 44/2010, 131).

Micochip kontrolliert Medikamenteneinsatz im Körper

Die Novartis AG, einer der größten Pharmakonzerne weltweit, kündigte an, bald damit zu beginnen, im Rahmen einer Smart-Pills-Technologie Mikrochips in Medikamente einzubauen. Die Mikrochip-Technologie wird vom Unternehmen Proteus Biomedical im kalifornischen Redwood City lizensiert. Sobald der in die Tablette eingebaute Mikrochip durch die Magensäure aktiviert wird, beginnt er damit, seine Umgebung abzutasten. Die gewonnenen Daten werden dann an einen Empfänger gesendet, den der Patient bei sich trägt. Dieser Empfänger kann Daten über das Internet auch an einen Arzt senden. Das Konzept der „Smart Pills“ zielt darauf ab, direkt Informationen über das Körpergeschehen an den behandelnden Arzt zu senden. Novartis will zunächst Medikamente gegen die Abstoßung nach Organverpflanzungen mit Mikrochips ausstatten und diese Technologie dann auch auf andere Bereiche seiner Produktpalette auszuweiten.

Von Novartis wurde die Chiptechnologie an einem Blutdrucksenker getestet zur Detektion, ob eine Pille im Körper ankommt. 20 ProbandInnen schluckten das Mittel Valsartan, das so präpariert war, dass bei der säureabhängigen Zersetzung der Pille im Magen ein elektrisches Signal erzeugt wurde. Dadurch bekommt ein Chip, der als Pflaster auf der Schulter des Patienten klebt, die Information: „Pille eingenommen“. Fehlt das Signal, sendet der Chip z.B. eine Erinnerung per SMS an die PatientIn selbst, an einen Verwandten oder Arzt. Der Chip lässt sich auch in ein Funknetzwerk (WLAN) integrieren. Der Sandkorn-große Pillenchip enthält eine Minibatterie, die aus Nahrungsbestandteilen hergestellt und, so Proteus Biomedical, gut verdaulich sei. Kommt sie mit Wasser in Kontakt, entsteht das elektrische Signal, das durch das Gewebe weitergeleitet wird. Das koste nur einen Cent pro Pille. Unklar ist der Preis für das Chip-bestückte Pflaster, das auch Herzrate oder Atemfrequenz ermitteln kann.

Das kalifornische Unternehmen Proteus Biomedical entwickelt bereits implantierbare Chips. Es wirbt, seine Technologie ermögliche es, das „patientenspezifische Medikamenten-Einnahmeverhalten und physiologische Antworten zu kommunizieren“. Dies könnte für Demenzkranke, die ihre Tabletten leicht vergessen, nützlich sein. Viele Medikamente würden nicht geschluckt, sondern landeten im Müll. So nehme jeder zweite Schizophreniekranke ein Jahr nach Entlassung aus der Klinik seine Arznei nicht mehr ein. Unter Bluthochdruckpatienten schluckt auch nur jeder Zweite sein Medikament.

Nick Peters, Kardiologe vom Imperial College London, sieht die Technologie positiv, weil sie Patienten und ihre Familien stärker mache. Es bestehe Hoffnung, mit der Chiptechnologie Kosten zu sparen. Jochen Schuler von der Universitätsklinik Salzburg gibt aber zu bedenken: „Der Fokus liegt auf der Nicht-Einnahme und Ziel ist es, diese zu verhindern.“ Das sei problematisch, weil der Patient seine Medikation womöglich verweigert, da er sie nicht verträgt. „Bevor man Druck ausübt, muss man der Sache auf den Grund gehen.“ Chronisch Kranke und PatientInnen mit psychischen Problemen brauchten statt Technik die Nähe zu ihren Behandlern: „Durch Gespräche lässt sich wahrscheinlich besser verhindern, dass arzneimittelbedingte Probleme entstehen.“ Eine Überwachung per Telekommunikation könne womöglich Gegenteiliges bewirken. Bei psychiatrischen PatientInnen sei eine Überwachungsparanoia zu befürchten.

Novartis plant offensichtlich keine klinischen Versuche, um zu abzuklären, ob es gefahrlos ist, Mikrochips zu schlukken. Die Nachrichtenagentur Reuters be-

richtete: „Novartis geht nicht davon aus, dass für den Nachweis der Wirksamkeit der neuen Produkte umfangreiche klinische Studien erforderlich sind. Stattdessen will das Unternehmen sogenannte Bioäquivalenz-Tests durchführen, die zeigen, dass sie wie das Original wirken."

Proteus Biomedical behauptet, die Signale der Chips könnten nicht von außen abgefangen werden. Der Pflasterchip auf der Haut spreche nicht auf Pillensignale einer anderen Person an, selbst „wenn beide in physischem Kontakt sind". Die von den Mikrochips versandten Daten können aber grundsätzlich aufgefangen werden. Theoretisch ist es denkbar, dass ein am Eingang einer Apotheke installierter Mikrochipdetektor die Daten erfasst, um daraus Empfehlungen zum Kauf von Medikamenten abzuleiten. Behördenmitarbeitende könnten sich heimlich mittels eines Miniscanners darüber informieren, welche Medikamente das Gegenüber so einnimmt. Denkbar ist auch die Anwendung der Chips in Kombination mit Medikamentenscannern durch Personalsachbearbeiter bei Bewerbenden zwecks Feststellung im Vorstellungsgespräch, ob signalgebende Mikrochip-Tabletten geschluckt wurden. Medikamentenscanner ließen sich auch bei Verkehrsunfällen durch die Polizei einsetzen zur Feststellung, ob ein Unfallbeteiligter durch Medikamenteneinnahme nur eingeschränkt verkehrstüchtig war (Adams info.kopp-verlag.de 15.11.2010; Brüsker www.sueddeutsche.de 30.10.2009).

Nachruf

Andreas Pfitzmann ist tot

Prof. Dr. Andreas Pfitzmann, Inhaber des Lehrstuhls für Datenschutz und Datensicherheit an der Technischen Universität (TU) Dresden, ist am 23.09.2010 nach kurzer schwerer Krankheit im Alter von 52 Jahren gestorben. Pfitzmann war Leiter der Datenschutz- und Sicherheitsgruppe an der TU Dresden. Zu seinen Forschungsinteressen gehörten Datenschutz und multilaterale Sicherheit in Kommunikationsnetzen, mobiler Kommunikation und verteilten Anwendungen. Letzte Forschungsprojekte waren „anonymes Websurfing" (JAP), „Privacy and Identity Management in Europe for Life" (PrimeLife) und „Steganographie". Er war Mitglied in den Organisationen ACM (Association for Computing Machinery), Institute of Electrical and Electronics Engineers (IEEE) und der Gesellschaft für Informatik (GI). Bei Letzterer wirkte er lange Zeit als Vorsitzender der Fachgruppe „Verläßliche IT-Systeme". Nach dem Informatik-Studium und der Promotion an der Universität Karlsruhe über „Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz" (1989) arbeitete er als Dozent an der Universität Hildesheim, bis er 1993 nach Dresden berufen wurde, wo er zuletzt als Dekan der Fakultät für Informatik tätig war.

In einem Nachruf des Prodekans der Fakultät Informatik, Oliver Rose, heißt es: „All unsere gemeinsamen Hoffnungen haben sich schlagartig aufgelöst. Bis zuletzt hat er noch so viel für seine Mitmenschen getan und Visionen für die Zukunft entwickelt. Wir alle verlieren in ihm einen wirklichen Menschenfreund, einen hervorragenden Wissenschaftler, engagierten Hochschullehrer und weitsichtigen Dekan." Der Chaos Computer Club erklärte: „Pfitzmann prägte in Deutschland die technischen und politischen Diskurse zu Selbstdatenschutz und informationeller Selbstbestimmung und besaß auch international Renommée. Dabei vermochte er stets, über die Grenzen seiner Disziplin hinweg die Auswirkungen von Technik begreifbar zu machen. Wir verlieren mit ihm einen einzigartigen Verteidiger der Anonymität und der informationellen Selbstbestimmung als Grundvoraussetzung für die gelebte Demokratie und einen herausragenden Wissenschaftler." Für das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), mit dem Pfitzmann bei einer Vielzahl von Projekten zusammenarbeitete, erklärten dessen Leitung Thilo Weichert und Marit Hansen: „Mit Andreas haben wir einen ebenso freundlichen wie hartnäckigen und konfliktfähigen Streiter für das Recht auf informationelle Selbstbestimmung verloren. Er war belehrend im besten Sinne des Wortes, einfach weil er nicht nur die Technik, sondern auch die gesellschaftlichen Rahmenbedingungen von Kontrollnotwendigkeiten und -gelüsten kannte. Wir haben viel von ihm gelernt. Zugleich war er eine liebe und liebenswerte Person, ernsthaft, selbstbewusst und selbstkritisch und voller Lebensfreude. Er wird uns fehlen."

Pfitzmann hatte sich immer wieder in die politischen und juristischen Diskussionen zum Datenschutz eingemischt. So war er 2001 gemeinsam mit Hans-Jürgen Garstka und Alexander Roßnagel einer der Autoren des vom Bundesinnenministerium in Auftrag gegebenen Gutachtens zur Modernisierung des Datenschutzrechtes. Er formulierte gegenüber dem Bundesverfassungsgericht eine Kritik am Instrument der staatlichen Online-Durchsuchung, was eine wichtige Grundlage für das höchste Gericht bei dessen kritischen rechtlichen Bewertung im Jahr 2008 war. ULD-Mitarbeiter haben im Juni 2010 mit Andreas Pfitzmann ein umfangreiches Interview zu seinen Erfahrungen und Vorstellungen durchgeführt, das als Video im Internet abrufbar ist unter https://www.datenschutzzentrum.de/interviews/pfitzmann/ (www.heise.de 25.09.2010; www.datenschutzzentrum.de 27.09.2010).

Rechtsprechung

EuGH

Veröffentlichungen von Agrarsubventionen verstoßen gegen Datenschutz

Der Europäische Gerichtshof (EuGH) in Luxemburg hat mit Urteil vom 09.11.2010 entschieden, dass die Namen der Empfänger von EU-Landwirtschaftsbeihilfen nicht länger in der bisherigen Form veröffentlicht werden dürfen (Az. C-92/09 und C-93/09). Wegen Verletzung des Datenschutzes erklärte der EuGH die entsprechende EU-Verordnung für ungültig. In Deutschland wurden bislang die Namen von Landwirten und die Summe, die sie aus dem Agrartopf erhalten, von der Bundesanstalt für Landwirtschaft und Ernährung ins Internet gestellt. Die Inhaber zweier Betriebe hatten dagegen geklagt. Von deutschen Gerichten war die Praxis bislang unterschiedlich bewertet worden. Das Verwaltungsgericht in Wiesbaden legte die beiden Klagen der Landwirte dem EuGH vor. Dieser betonte in seinem Urteil zwar, das Ziel, Transparenz über die Verwendung von EU-Mitteln sicherzustellen, sei legitim – die Veröffentlichung der personenbezogenen Daten der Subventionsempfänger in der bisherigen Form sei aber, in Abwägung mit dem Recht auf Datenschutz, unverhältnismäßig. Unverhältnismäßig sei vor allem, dass in den Veröffentlichungen nicht nach Bezugsdauer, Häufigkeit, Art und Umfang der erhaltenen Beihilfen unterschieden werde. Somit ließ der EuGH die Möglichkeit einer differenzierteren Neuregelung offen. Ein Sprecher der EU-Kommission in Brüssel erklärte, es werde nun geprüft, wie die entsprechenden Verordnungen geändert werden könnten, um die Transparenz auch künftig sicherzustellen.

Die Agrarsubventionen der EU sind seit langem umstritten. Die Kommission gibt jährlich 55 Mrd. Euro aus. Doch nur ein geringer Teil der Gelder landet bei Bauern; das meiste geht an Großbetriebe und Konzerne; in Deutschland z.B. Südzucker oder die Großmolkerei Nordmilch. Umweltschützer empfanden die Veröffentlichung als hilfreich, weil sie ihrer Ansicht nach zeigte, wie fehlgeleitet die EU-Agrarpolitik ist. Landwirte befürchteten dagegen eine Neiddebatte, hielten die Daten für wenig aussagekräftig und fühlten sich zu Unrecht an den Pranger gestellt. Die Entscheidung des EuGH gilt nicht für Unternehmen – deren Daten dürfen weiterhin veröffentlicht werden. Auch die bisher ins Netz gestellten Listen müssen laut EuGH nicht gelöscht werden. Landwirtschaftsministerin Ilse Aigner erklärte dennoch, bis zu einer EU-weiten Neuregelung werde die Veröffentlichung von Bund und Ländern mit sofortiger Wirkung ausgesetzt. Auf der Website www.agrar-fischerei-zahlungen.de war 4 Stunden nach dem Bekanntwerden der Entscheidung statt der ungeliebten Empfängerliste des EU-Agrarfonds nur noch der Hinweis auf das EuGH-Urteil zu sehen (www.tagesschau.de 10.11.2010; Kuhr SZ 10.11.2010, 4, 17).

BVerfG

Anlassbezogener Videobeweis gegen Verkehrssünder zulässig

Gemäß einem Nichtannahmebeschluss des Bundesverfassungsgerichts (BVerfG) vom 12.08.2010 ist die Anfertigung von Videoaufnahmen zum Beweis von Verkehrsverstößen auf der Grundlage von § 100h Abs. 1 Satz 1 Nr. 1 StPO verfassungskonform (Az.: 2 BvR 1447/10). Der in solchen Aufnahmen liegende Eingriff in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG sei durch den Zweck gerechtfertigt, die Sicherheit des Straßenverkehrs aufrecht zu erhalten und damit Rechtsgüter mit erheblichem Gewicht zu schützen. Der Beschwerdeführer war von einem Amtsgericht wegen fahrlässiger Unterschreitung des erforderlichen Sicherheitsabstandes im Straßenverkehr zu einer Geldbuße in Höhe von 320 Euro verurteilt worden. Die Verurteilung stützte sich im Wesentlichen auf das Ergebnis einer Abstandsmessung mittels einer geeichten Anlage und die dabei angefertigten Videoaufnahmen, auf denen der Beschwerdeführer zu erkennen ist. Das Oberlandesgericht (OLG) hatte dessen Rechtsbeschwerde als unbegründet verworfen. Die daraufhin erhobene Verfassungsbeschwerde rügte insbesondere eine Verletzung seines Grundrechts auf informationelle Selbstbestimmung und des Willkürverbots aus Art. 3 Abs. 1 GG. Der Eingriff sei mangels gesetzlicher Grundlage nicht gerechtfertigt. § 100h Abs. 1 Satz 1 Nr. 1 StPO in Verbindung mit § 46 Abs. 1 OWiG könne nicht als Rechtsgrundlage herangezogen werden, da diese Befugnis nur bei der Herstellung von Bildaufnahmen zu Observationszwecken greife.

Das BVerfG meinte, der Beschwerde käme weder grundsätzliche Bedeutung zu noch verletzten die angegriffenen Entscheidungen den Beschwerdeführer in seinen Grundrechten. Es sei verfassungsrechtlich nicht zu beanstanden, dass die Gerichte die Vorschrift des § 100h Abs. 1 Satz 1 Nr. 1 StPO als Rechtsgrundlage für die Anfertigung von Videoaufnahmen zum Beweis von Verkehrsverstößen herangezogen haben. Die Norm erlaube die Anfertigung von Bildaufnahmen ohne Wissen des Betroffenen, wenn die Erforschung des Sachverhalts auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Dies gelte sowohl für die Anfertigung von Einzelaufnahmen als auch von Videoaufnahmen. Der in den Bildaufnahmen mittels einer Identifizierungskamera liegende Eingriff in das Grundrecht des Betroffenen auf informationelle Selbstbestimmung sei auch verhältnismäßig. Der Zweck derartiger Maßnahmen der Verkehrsüberwachung, nämlich die Aufrechterhaltung der Sicherheit des Straßenverkehrs und damit der Schutz von Rechtsgütern mit erheblichem Gewicht, rechtfertigte eine Beschränkung der grundrechtlichen Freiheiten. Dabei sei zu berücksichtigen, dass – auch wenn es sich um verdeckte

Datenerhebungen handelt – nur Vorgänge auf öffentlichen Straßen aufgezeichnet würden, die grundsätzlich für jedermann wahrnehmbar seien. Die Maßnahme ziele nicht auf Unbeteiligte, sondern ausschließlich auf Fahrzeugführer, die selbst Anlass zur Anfertigung von Bildaufnahmen gegeben hätten, da der Verdacht eines bußgeldbewehrten Verkehrsverstoßes besteht. Schließlich entfalte die Maßnahme über die Ahndung der Verkehrsordnungswidrigkeit hinaus grundsätzlich keine belastenden Wirkungen für den Betroffenen. Denn es bestünden in § 101 StPO hinreichende grundrechtssichernde Verfahrensvorschriften über die Benachrichtigung sowie zur Kennzeichnung und Löschung von Daten.

Soweit im vorliegenden Fall auch Übersichtsaufnahmen von einer Brücke aus angefertigt wurden, verneinte das BVerfG bereits einen Eingriff in das Grundrecht des Beschwerdeführers auf informationelle Selbstbestimmung. Denn zum einen sei nach den amtsgerichtlichen Feststellungen eine Identifizierung der Fahrer oder Kennzeichen anhand der dauerhaft angefertigten Übersichtsaufnahmen nicht möglich gewesen. Zum anderen seien die Übersichtsaufnahmen nach ihrer Zweckbestimmung nicht auf eine Individualisierung des Betroffenen ausgerichtet. Diese sollten vielmehr ausschließlich durch die verdachtsabhängige Anfertigung von Bildaufnahmen mittels der am Fahrbahnrand aufgestellten Identifizierungskamera erfolgen (beck-aktuell.beck.de 03.09.2010; KN 04.09.2010, 14; SZ 04./05.09.2010, 12).

BVerfG

Spickmich-Bewertung nicht verfassungswidrig

Das Bundesverfassungsgericht (BVerfG) hat im Rechtsstreit um das Lehrerbewertungsportal spickmich.de die Verfassungsbeschwerde einer Lehrerin mit Beschluss vom 16.08.2010 ohne inhaltliche Begründung nicht zur Entscheidung angenommen (Az. 1 BvR 1750/09). Damit bleibt das Urteil des Bundesgerichtshofes (BGH, BGHZ 181, 328 ff.; NJW 2009, 2888; DANA 2009, 75) bestehen, der das Modell der Lehrerbewertung grundsätzlich für zulässig erachtet hatte. Der BGH hatte im Juni 2009 die Lehrerbenotung für zulässig erklärt, da sie „weder schmähend noch beleidigend“ sei. Die Bewertungen der namentlich genannten LehrerInnen auf spickmich.de entsprechen den Schulnoten 1 bis 6 und orientieren sich an Kriterien wie „cool und witzig“, „beliebt“, „motiviert“, „menschlich“, „gelassen“, und „guter Unterricht“. Timo Keller, einer der Betreiber des Internetportals, meinte: „Mehr Transparenz verbessert das Schulsystem in Deutschland, und Bewertungen der Schul- und Lehrqualität sind dazu unbedingt notwendig“. Das BVerfG habe dies indirekt bestätigt. Der Deutsche Lehrerverband hatte vergeblich Hoffnungen auf das BVerfG gesetzt. Enttäuscht reagierte auch der Verband Bildung und Erziehung (VBE). Auf Spickmich würden „Aburteilungen“ von LehrerInnen ermöglicht, die allein auf Stimmungslagen und Meinungsmache basieren.

Dass das meinungsfreiheitsfreundliche BVerfG sich nicht gegen die Abwägungsentscheidung des BGH gestellt hat, ist nicht überraschend, wohl aber, dass es es ablehnte, die Verfassungsbeschwerde überhaupt zur Entscheidung anzunehmen. Ein solches Verfahren ist zur Entlastung des Gerichts möglich, wenn der Verfassungsbeschwerde keine grundsätzliche verfassungsrechtliche Bedeutung zukommt (§ 93a Abs. 2 BVerfGG). Sogar auf eine Begründung der Nichtannahme verzichtete das BVerfG (vgl. § 93d Abs. 1 S. 3 BVerfGG). Es ging bei seiner Entscheidung offenkundig davon aus, dass der Fall durch die bisherige Rechtsprechung des Gerichts zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht bereits hinreichend verfassungsrechtlich geklärt ist, trotz entsprechender Zweifel teilweise in der juristischen Literatur und in tagespolitischen Kommentaren. Bewertungen im Internet, die nicht nur im Schutze der Anonymität erfolgen, sondern auch für jedermann leicht zugänglich sind, können sich für den Betroffenen in ihrer Wirkung durchaus von einer kritischen Beurteilung in klassischen Medien, etwa einer Schülerzeitung, unterscheiden.

Es muss dennoch davon ausgegangen werden, dass die Grenzen der rechtlichen Zulässigkeit von Bewertungsportalen damit noch nicht abschließend geklärt sind. So bleibt abzuwarten, ob die Rechtsprechung etwa das von der AOK angekündigte Portal zur Bewertung von Ärzten an den gleichen Maßstäben messen wird (dazu jetzt Gundermann, VuR 2010, 329). Aufschlussreich wird auch der Umgang der Rechtsprechung mit Bewertungsportalen für JuristInnen sein. So bietet z. B. die Seite marktplatz-recht.de eine Möglichkeit zur Bewertung von Richtern und Gerichten. Zugang zu den Bewertungen sollen allerdings nur Angehörige juristischer Berufsgruppen haben, die eine entsprechende Ausbildung nachweisen können. Auch sollen die Ergebnisse nicht über Suchmaschinen auffindbar sein. Die Macher haben sich somit bereits am Urteil des BGH zu spickmich.de orientiert. Trotz der eindeutigen Positionierung des BVerfG werden sich also zumindest die Fachgerichte mit solchen und ähnlichen Konstellationen auch in Zukunft zu befassen haben (Greve, Schärdel, www.telemedicus.info 22.09.2010; SZ 23.09.2010, 10; www.spiegel.de 22.09.2010).

BVerfG

Beschwerde gegen Volkszählung 2011 nicht angenommen

Das Bundesverfassungsgericht hat mit Beschluss vom 21.09.2010 eine Beschwerde von vier Bürgern gegen das Gesetz über den registergestützten Zensus im Jahre 2011 nicht angenommen (Az. 1 BvR 1865/10). Die Verfassungsbeschwerde genüge nicht den Anforderungen, die im Bundesverfassungsgerichtsgesetz gestellt werden. Nicht das gesamte Gesetz könne Gegenstand einer Verfassungsbeschwerde sein; vielmehr müssten die angegriffenen Bestimmungen genau bezeichnet werden. Die Beschwerdeführer hatten beantragt, das Zensusgesetz insgesamt als unvereinbar mit ihren Grundrechten zu erklären. Sie kritisierten, dass die für den Zensus 2011

vorgesehene Datenerhebung und Datenzusammenführung nach den §§ 3 bis 9 ZensG „ein nicht zu rechtfertigender Grundrechtseingriff“ sei. Das BVerfG meinte, die „undifferenzierte Nennung dieser Vorschriften“ reiche angesichts ihres „umfangreichen und detaillierten Regelungsgehalts für eine hinreichende Bezeichnung des angegriffenen Hoheitsakts nicht aus“. Die Klage wurde von 13.000 Personen unterstützt.

Gemäß der 40 Seiten umfassenden Verfassungsbeschwerde sehen die Beschwerdeführer einen schwerwiegenden Verstoß gegen die Vorgaben des Bundesverfassungsgerichts durch die Zuordnung der zu erhebenden Datensätze und persönlichen sensiblen Daten unter einer Ordnungsnummer, die bis zu sechs Jahren und länger vorgehalten werden könnten. Beim Zensus 2011 sollen rund 17,8 Millionen Immobilien-Besitzer per Post einen Fragebogen zu ihren Häusern oder Eigentumswohnungen erhalten. Außerdem soll eine Stichprobe von höchstens 10 % der Bevölkerung erhoben werden. Für den Zensus werden in erster Linie Daten aus bestehenden Registern der Verwaltung genutzt. Mit der Befragung von Immobilien-Besitzern und der Stichprobe aus der Bevölkerung sollen in Registern wie zum Beispiel den kommunalen Melderegistern enthaltene Fehler über die Zensusergebnisse statistisch bereinigt werden (www.heise.de 01.10.2010; SZ 02./03.10.2010, 6; Beschwerebegründung: http://wiki.vorratsdatenspeicherung.de/images/VB_Zensus_anonymisiert.pdf).

VG Wiesbaden

Sicherheitsübermittlung für Presseakkreditierung durch BKA an NATO unzulässig

Das Verwaltungsgericht (VG) Wiesbaden hat mit Urteil vom 06.10.2010 entschieden, dass das Bundeskriminalamt (BKA) im Rahmen der Erteilung einer Presseakkreditierung für den NATO-Gipfel vom 03. bis 04.04.2009 kein Negativvotum an die NATO durch Übermittlung personenbezogener Daten eines Journalisten abgeben durfte (Az. 6 K 280/10.WI). Der Kläger, ein freiberuflicher Journalist aus Polen, der für die polnische Ausgabe der internationalen Monatszeitschrift „le monde diplomatique“ und andere Zeitschriften vom NATO-Gipfel vom 03. bis 04.04.2009 in Straßburg, Baden-Baden und Kehl berichten wollte, beantragte am 29.01.2009 online bei der NATO seine Akkreditierung als Journalist für das Gipfeltreffen. Dort erklärte er sich damit einverstanden, dass seine persönlichen Daten gespeichert und in Verbindung mit seiner Akkreditierung verwendet würden. Die NATO lehnte die Akkreditierung ohne Angabe von Gründen ab. Hintergrund der Ablehnung war, dass die NATO dem BKA im Rahmen des mit der NATO vereinbarten standardisierten Akkreditierungsüberprüfungsverfahrens für den NATO-Gipfel 2009 die persönlichen Daten des Klägers zur Überprüfung übermittelt hatte. Der automatische Datenabgleich im polizeilichen Informationssystem INPOL führte dazu, dass das BKA eine Empfehlung zur Nichtzulassung des Klägers gegenüber der NATO abgab, die daraufhin die Ablehnung des Klägers aussprach.

In dem die Klage stattgebenden Urteil stellte das VG Wiesbaden fest, dass die vom BKA vorgenommene Gefährdungsprognose an die NATO und die Datenübermittlung mangels einer gesetzlichen Ermächtigungsgrundlage rechtswidrig gewesen sei. Das BKA-Gesetz enthalte keine Norm, die es ermöglicht, Daten an die NATO zu übermitteln. Es sei berechtigt, für die eigenen Aufgaben des Schutzes von Mitgliedern von Verfassungsorganen auf die gespeicherten Daten beim BKA zuzugreifen und diese zu nutzen. Auch gebe es eine Berechtigung im BKA-Gesetz, personenbezogen Daten an Dienststellen der Stationierungsstreitkräfte oder an eine internationale kriminalpolizeiliche Organisation zu übermitteln. Diese Voraussetzungen träfen aber allesamt nicht auf das NATO-Hauptquartier in Brüssel zu. Eine vergleichbare Berechtigung, wie sie das Bundesamt für Verfassungsschutz für die Übermittlung personenbezogener Daten an ausländische öffentliche Stellen besitzt, habe das BKA nicht.

Eine Berechtigung des BKA zur Übermittlung personenbezogener Daten sei auch nicht nach dem Bundesdatenschutzgesetz gegeben, da der Kläger eine – grundsätzlich – schriftliche Einwilligung zur Übermittlung seiner Daten dem BKA gegenüber gerade nicht erteilt hat. Die Einwilligung der NATO gegenüber habe nicht die Weitergabe seiner Daten an Dritte enthalten. Das VG ließ die Revision zum BVerwG gegen das Urteil zu; die Beteiligten können auch einen Antrag auf Zulassung der Berufung stellen, über den der Hessische Verwaltungsgerichtshof (VGH) zu entscheiden hat. Im Frühjahr 2009 hatte ein anderer Journalist, ein freiberuflicher Fotograf aus Berlin, in gleicher Sache ein Eilverfahren gegen das BKA angestrengt. Er hatte damit jedoch kurz vor dem Gipfel vor dem Hessischen VGH keinen Erfolg. Das Gericht hatte damals aber nicht in der Sache entschieden (PE VG Wiesbaden 12.10.2010 Nr. 12/2010; SZ 13.10.2010, 6; www.tagesschau.de 12.10.2010).

LG Wuppertal

Reines „Schwarzsurfen“ nicht strafbar

Gemäß einem Beschluss des Landgerichtes (LG) Wuppertal vom 19.10.2010 ist das heimliche Surfen in unverschlüsselt betriebenen fremden WLAN-Funknetzen nicht strafbar (Az.: 25 Qs 177/10). Das Gericht stellte sich damit gegen ein älteres Urteil des Amtsgerichts (AG) Wuppertal gegen einen „Schwarzsurfer“. Anlass der LG-Entscheidung des Landgerichts war eine sofortige Beschwerde der Staatsanwaltschaft Wuppertal gegen einen Nichteröffnungsbeschluss. Die Staatsanwaltschaft hatte vor dem AG die Eröffnung der Hauptverhandlung gegen einen Angeschuldigten beantragt, dem sie vorwarf, mit seinem Laptop einen Ort in Wuppertal aufgesucht zu haben, an dem er sich in ein über einen WLAN-Router unverschlüsselt betriebenes fremdes Funknetzwerk

eingewählt haben soll, um die Kosten für einen eigenen Internet-Anschluss zu sparen. Weil der Beklagte sich dazu mit seinem Laptop vom Bürgersteig aus einwählte, konnte der Besitzer des WLAN-Hotspots den Schwarzsurfer ausfindig machen und bei der Polizei anzeigen. Das AG hatte in dem angegriffenen Beschluss eine Strafbarkeit dieses Verhaltens verneint und eine Eröffnung der Hauptverhandlung aus rechtlichen Gründen abgelehnt. Die 5. große Strafkammer des Landgerichts bestätigte diese Bewertung und verwarf die sofortige Beschwerde der Staatsanwaltschaft als unbegründet.

Die Kammer verneint die Strafbarkeit des Einwählens in ein offenes und über einen WLAN-Router unverschlüsselt betriebenes fremdes Funknetzwerk unter jedem rechtlichen Gesichtspunkt. Eine Strafbarkeit gemäß §§ 89 Satz 1, 148 Abs. 1 Nr. 1 Telekommunikationsgesetz (TKG) sei nicht gegeben, weil der Einwählende nicht zwischen anderen Kommunikationspartnern vertraulich ausgetauschte Nachrichten wahrnehme, die § 89 Satz 1 TKG unterfielen, sondern selbst Teilnehmer eines Kommunikationsvorgangs wurde. Das Verhalten erfülle auch nicht den Tatbestand des unbefugten Abrufens oder Sich-Verschaffens personenbezogener Daten gemäß §§ 43 Abs. 2 Nr. 3, 44 Bundesdatenschutzgesetz (BDSG). Weder bei dem Einwählen in das unverschlüsselt betriebene Funknetzwerk noch der anschließend hierüber erfolgenden Nutzung des Internetzugangs würden personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG abgerufen. Eine Strafbarkeit wegen des Ausspähens von Daten gemäß § 202a StGB, oder des Abfangens von Daten gemäß § 202b StGB, oder gar wegen eines versuchten Computerbetruges gemäß §§ 263a Abs. 1 und 2, 263 Abs. 2, 22 StGB sei nicht gegeben. Auch für das Erschleichen von Leistungen gemäß § 265a StGB sahen die Richter keinen stichhaltigen Anhaltspunkt. Auch wenn der Schwarzsurfer den WLAN-Hotspot gegen den Willen des Besitzers genutzt hat, so ist diesem letztlich kein Schaden entstanden, weil er eine Flatrate für den Internet-Zugang nutzte. Außerdem können die Betreiber ihre Hotspots gegen eine unbefugte Mitnutzung sichern (Winter, www.teltarif.de 21.10.2010; www.faz.net 20.10.2010; Knoke www.spiegel.de 21.10.2010).

AG Franfurt/Main

IP-Adress-Ermittlung mit „Filesharing Monitor“ beweissicher

Das Amtsgericht (AG) Frankfurt am Main hat im Rahmen eines Urheberrechtsprozesses mit Urteil vom 14.04.2010 entschieden, die Software „Filesharing-Monitor“, mit der die IP-Adressen der Urheberrechtsverletzer ermittelt wurden, sei beweissicher (Az. 30 C 562/07). Ein vom AG beauftragter Sachverständiger kam in seinem Gutachten zu dem Ergebnis, dass mit Hilfe der Software zuverlässig festgestellt werden könne, von welchem hinter einer bestimmten IP-Adresse stehenden Anschlussinhaber eine bestimmte Datei zum Herunterladen angeboten wird. Er bestätigte die lediglich „theoretische“ Möglichkeit von Fehlerquellen (Verfälschen von IP-Adressen, Produzieren des gleichen Hashwertes), dies sei aber praktisch ausgeschlossen. Daher sei von der Beweissicherheit der durch die Software gewonnenen Ergebnisse im Sinne des § 286 ZPO auszugehen. Lediglich wenn konkrete Tatsachen vorgelegt werden könnten, wäre der durch die Software „Filesharing Monitor“ erbrachte Beweis des ersten Anscheins zu erschüttern. Der Landesdatenschutzbeauftragte von Schleswig-Holstein Thilo Weichert zeigte sich irritiert über das Ergebnis des Gutachtens: „Es ist leicht, IP-Adressen zu fälschen. Eine ermittelte IP-Adresse kann m.E. keinesfalls genügen, um jemanden zu verurteilen“. Wie die Verbraucherzentrale Schleswig-Holstein warnt aber auch er vor dem illegalen Herunterladen bzw. Wiederzurverfügungstellen von Musik, Filmen, Software etc. Tatsächliche wie vermeintliche Urheberrechtsverletzer werden in einem gewaltigen Umfang abgemahnt und mit hohen Schadensersatzforderungen konfrontiert (PE Verbraucherzentrale Schleswig-Holstein 22.06.2010; www.jurpc.de/rechtspr/20100105.htm; Mormann www.shz.de 22.06.2010).

AG Herford

Radarkontrollen ohne ausreichende Rechtsgrundlage

Ein Richter des Amtsgerichts (AG) Herford hat 42 geblitzte Autofahrer freigesprochen, weil es keine genauen Regelungen gebe, „wie und wo fotografiert werden darf“. Die Staatsanwaltschaft Bielefeld will den Massenfreispruch nun prüfen. Der 62jährige Richter Helmut Knöner erläuterte, dass es bei Verkehrskontrollen um den Schutz der Bevölkerung gehe und nicht ums „Geldverdienen“. Er forderte eindeutige gesetzliche Regelungen zur Tempoüberwachung und betonte: „Es geht nicht primär darum, Raser freizusprechen.“ Knöner kritisierte die rechtlichen Grundlagen der Verkehrsüberwachung. Foto- und Videoaufnahmen von Autofahrern würden etwa auf Grundlage eines Terrorabwehrgesetzes gemacht. Auch gebe es keine genauen Regelungen und Vorschriften dafür, an welchen Orten die Geschwindigkeit der Autofahrer überprüft werde. „Wir brauchen eine Regelung, wie und wo fotografiert werden darf und dass Starenkästen dort aufgebaut werden, wo es Sinn und Zweck hat“ (www.faz.net 10.11.2010; www.handelsblatt.com 10.11.2010).

BAG

Informationelle Selbstbestimmung sichert Einsicht in Personalakte

Das Bundesarbeitsgericht (BAG) in Erfurt urteilte am 16.11.2010, dass ArbeitnehmerInnen auch noch nach Ausscheiden aus ihrer Firma ein Einblicksrecht in deren dortige Personalakte haben. Dies wird aus dem Recht auf informationelle Selbstbestimmung abgeleitet. Die Vorinstanzen hatten die Klage abgewiesen. Der Kläger war Leiter eines Schadensbüros einer Versicherungsgesellschaft, die er Mitte 2007 verließ. Über das Abschlusszeugnis mussten sich Arbeitgeber und Arbeitnehmer in einem gerichtlichen Vergleich einigen. Dabei erfuhr

der Arbeitnehmer, dass das Unternehmen ihm offenbar mangelnde Loyalität vorwarf. Seinen Antrag auf Einsicht in die Personalakte lehnte der Versicherer ab, was nach Ansicht des BAG unzulässig war. Dem Arbeitgeber käme eine „vertragliche Rücksichtnahmepflicht" zu. Der Arbeitnehmer hat auch nach Beendigung des Arbeitsverhältnisses ein berechtigtes Interesse daran, den Inhalt seiner fortgeführten Personalakte auf ihren Wahrheitsgehalt zu überprüfen. Der Anspruch folgt allerdings nicht aus § 34 BDSG. Die dort geregelten Ansprüche auf Auskunft und Einsicht gälten noch nicht für nur in Papierform dokumentierte personenbezogene Daten. Dies soll sich aber mit dem neuen Beschäftigtendatenschutzrecht ändern, das sich in der parlamentarischen Beratung befindet (SZ 17.11.2010, 19; BAG PM 84/2010).

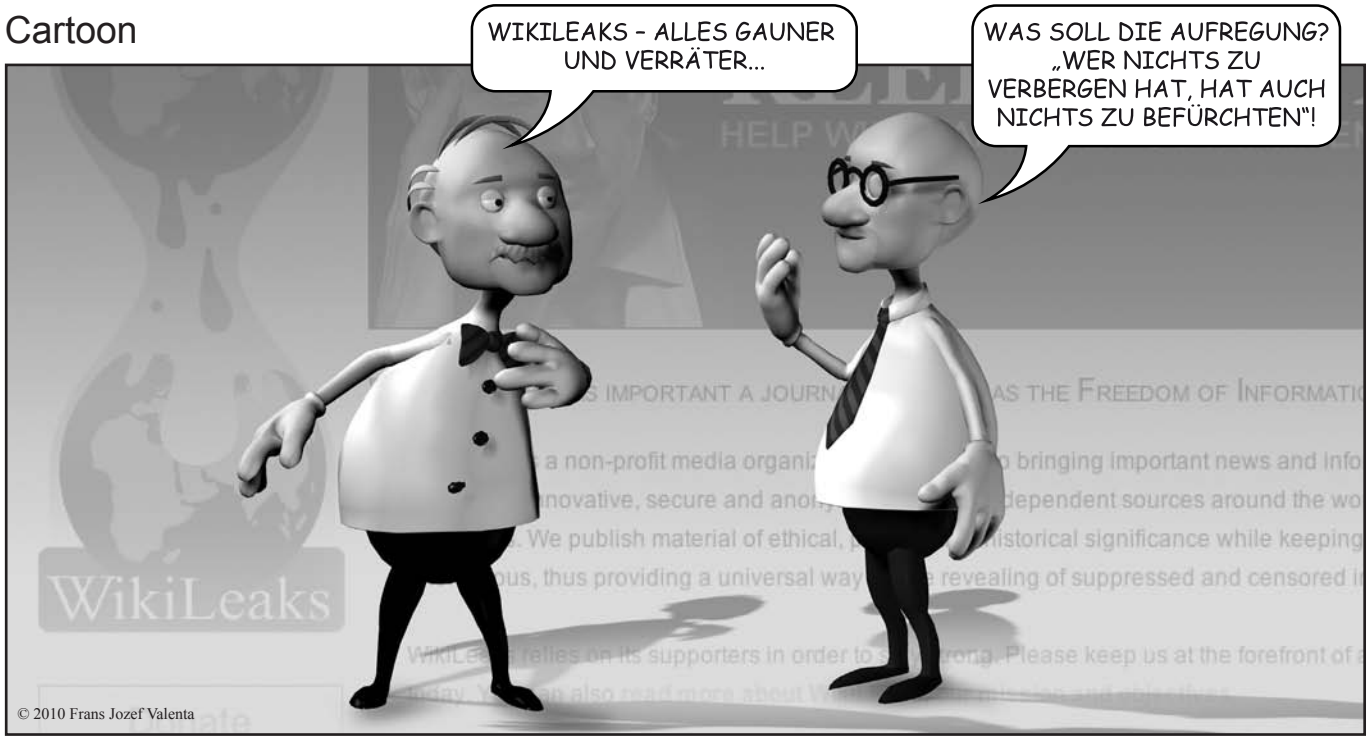
FG Köln

Nur Zweifel an Verfassungsgemäßheit der Steuer-ID

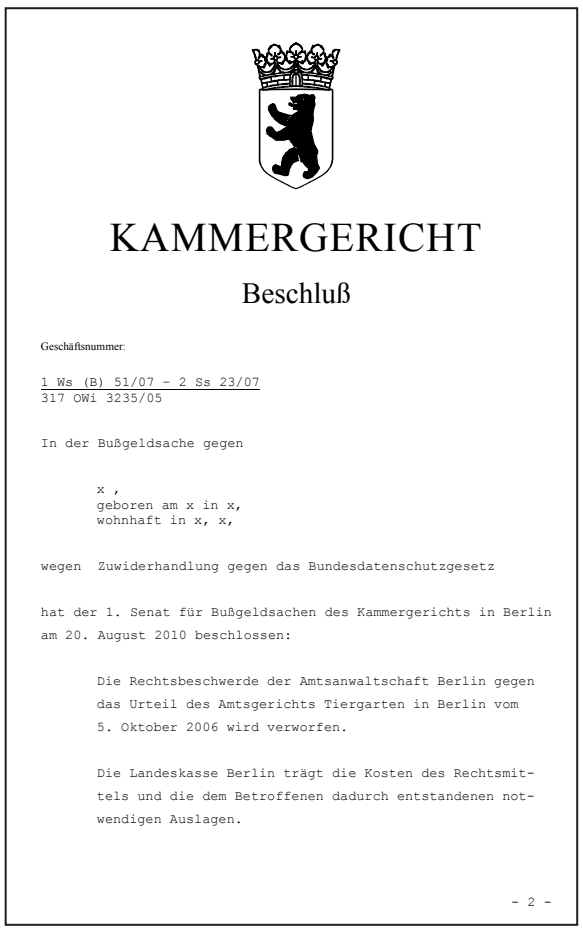
Das Finanzgericht (FG) Köln hat mit Urteilen vom 07.07.2010 in sieben Musterverfahren Klagen gegen die Steueridentifikationsnummer (Steuer-ID) abgewiesen (Az. u.a. 2 K 3093/08, 2 K 3986/08, 2 K 3265/08). Der 2. Senat äußerte, er habe „erhebliche Zweifel" an der Verfassungsmäßigkeit der Steuernummer; doch wiege das Recht des einzelnen Bürgers auf informationelle Selbstbestimmung weniger schwer als das Interesse der Allgemeinheit an einer gleichmäßigen Besteuerung. Da das in Deutschland allein zuständige FG Köln nicht völlig davon überzeugt war, dass die Steuer-ID verfassungswidrig ist, legte es die Verfahren nicht dem Bundesverfassungsgericht vor, ließ aber gegen die Urteile die Revision beim Bundesfinanzhof (BFH) in München zu. Seine verfassungsrechtlichen Zweifel begründet das FG damit, dass durch die Steuernummer alle in der Bundesrepublik Deutschland ansässigen BürgerInnen zentral durch den Staat erfasst würden. Durch Erweiterungen und durch Vernetzung verschiedener Datenpools könne ein großer zentraler Datenbestand geschaffen werden, mit dem Persönlichkeitsprofile möglich würden. Es sei fragwürdig, die Steuer-ID „flächendeckend" zuzuteilen und „flächendeckend" Daten zu speichern, unabhängig davon, ob die betreffenden Personen schon einen Besteuerungstatbestand erfüllt hätten. Es komme zu einer Art „Vorratsdatenspeicherung".

Die 11stellige Steuer-ID wurde vom Bundeszentralamt für Steuern inzwischen an 82 Mio. Menschen vergeben. Das beklagte Bundesamt in Bonn-Beuel erklärte, die Ziffer lasse keine Rückschlüsse auf bestimmte Personen zu. Hinter den Musterverfahren stehen über 170 Klagen, zu denen BürgerrechtlerInnen aufgerufen hatten. Rechtsanwalt Martin Heufelder meinte zum Verhandlungsbeginn, die im Oktober 2008 eingeführte Steuernummer verletzte das Grundrecht auf informationelle Selbstbestimmung, sei ein Schritt hin zum „gläsernen Bürger" und setze eine „gigantische Kontrollmaschine" in Gang. Dies zeige sich auch daran, dass selbst Babys unmittelbar nach der Geburt mit Post vom Bundeszentralamt für Steuern (BZSt) eine Steuer-ID erhalten. Einzelne KlägerInnen hatten die „Nummerierung" der Menschen als „Personenkennzeichen" aus religiösen Gründen abgelehnt. Hierzu argumentierte das Gericht, die Steuer-ID stelle lediglich ein behördeninternes Ordnungsmerkmal dar. Den KlägerInnen werde nicht ihr christlicher Name abgesprochen. Er bleibe erhalten und werde auch wie bisher verwendet (www.heise.de 09.09.2010; SZ 10.09.2010, 6).

Cartoon



Urteil zum Datenschutz und anwaltlicher Verschwiegenheitspflicht



KAMMERGERICHT

Beschluß

Geschäftsnummer:

1 Ws (B) 51/07 – 2 Ss 23/07
317 OWi 3235/05

In der Bußgeldsache gegen

x ,
geboren am x in x,
wohnhaft in x, x,

wegen Zuwiderhandlung gegen das Bundesdatenschutzgesetz

hat der 1. Senat für Bußgeldsachen des Kammergerichts in Berlin am 20. August 2010 beschlossen:

Die Rechtsbeschwerde der Amtsanwaltschaft Berlin gegen das Urteil des Amtsgerichts Tiergarten in Berlin vom 5. Oktober 2006 wird verworfen.

Die Landeskasse Berlin trägt die Kosten des Rechtsmittels und die dem Betroffenen dadurch entstandenen notwendigen Auslagen.

- 2 -

Gründe:

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat gegen den Betroffenen einen Bußgeldbescheid mit einer Geldbuße von 3.000 EUR wegen einer – wie sich aus dem Gesamtzusammenhang des Bescheides ergibt – vorsätzlichen Zuwiderhandlung nach den §§ 43 Abs. 1 Nr. 10, 38 Abs. 3 Satz 1 BDSG erlassen. Auf seinen Einspruch hat ihn das Amtsgericht durch Urteil vom 5. Oktober 2006 von diesem Vorwurf aus rechtlichen Gründen freigesprochen. Die Rechtsbeschwerde der Amtsanwaltschaft, mit der sie die Verletzung materiellen Rechts rügt, bleibt ohne Erfolg.

Das Amtsgericht hat festgestellt: Der Betroffene, ein Rechtsanwalt, hatte als Verteidiger in einem Strafverfahren vor dem Amtsgericht Potsdam am 23. August 2004 zwei Briefe zum Gegenstand der Hauptverhandlung gemacht, die ein Zeuge, der mit dem Angeklagten in einem Nachbarschaftsstreit lag, an seine Hausverwaltung geschrieben hatte. Trotz mehrfacher Aufforderung durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit verweigerte der Betroffene unter Berufung auf seine anwaltliche Verschwiegenheitspflicht die Auskunft, wie er in den Besitz der Briefe gekommen war.

Der Senat entscheidet über die Rechtsbeschwerde nach § 80a Abs. 3 Satz 1 OWiG in der Besetzung mit drei Richtern.

Das angefochtene Urteil ist nicht zu beanstanden. Das Amtsgericht hat den Betroffenen zu Recht freigesprochen. Die festgestellte Auskunftsverweigerung des Betroffenen ist nicht bußgeldbewehrt.

Nach § 43 Abs. 1 Nr. 10 BDSG handelt (in der hier in Betracht kommenden Alternative) ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 38 Abs. 3 Satz 1 BDSG eine von der Aufsichtsbehörde verlangte Auskunft nicht erteilt. Die Frage, ob der Datenschutzbeauftragte Auskunft über die Herkunft von Informationen verlangen darf, die der Rechtsanwalt im Zusammenhang mit einer Strafverteidigung erlangt und verwendet hat, ist obergerichtlich – soweit ersichtlich – noch nicht entschieden.

Den Bestimmungen des BDSG sind auch Rechtsanwälte als nicht-öffentliche Stellen (§§ 1 Abs. 2 Nr. 3, 2 Abs. 4 Satz 1 BDSG) unterworfen, wenn sie – wie hier der Betroffene – personenbezogene Daten (§ 3 Abs. 1 BDSG) erheben (§ 3 Abs. 3 BDSG) und nutzen (§ 3 Abs. 5 BDSG). Allerdings sieht § 1 Abs. 3 BDSG Einschränkungen vor, die den Anwendungsbereich des BDSG als Auffanggesetz begrenzen (vgl. Gola/Schomerus, BDSG 9. Aufl., Rdn. 23 zu § 1).

Nach Satz 1 dieser Bestimmung gehen dem BDSG andere Rechtsvorschriften des Bundes vor, die auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind. Soweit das Amtsgericht in den Bestimmungen der BRAO eine „bereichsspezifische Sonderregelung“ im Sinne des § 1 Abs. 3 Satz 1 BDSG sieht, teilt der Senat diese Auffassung nicht. Inwieweit die Subsidiaritätsklausel greift, bestimmt sich allein nach Ziel und Inhalt der mit dem BDSG konkurrierenden Vorschrift (vgl. Walz in Simitis (Hrsg.), BDSG 6. Aufl., Rdn. 170 zu § 1). Die berufsrechtlichen Bestimmungen der BRAO betreffen überwiegend den Schutz des Mandanten und das öffentliche Interesse an einer funktionierenden Strafrechtspflege, deren selbständiges Organ der Rechtsanwalt ist (§ 1 BRAO). Der Schutz von Gegnern des Mandanten oder sonstigen Dritten ist nicht Normzweck der BRAO (Redeker in Abel (Hrsg.), NJW-Schriften 63, 2. Aufl., S. 45). Das BDSG hingegen schützt sämtliche Personen, die durch den Umgang des Rechtsanwalts mit personenbezogenen Daten beeinträchtigt werden (§ 1 Abs. 1 BDSG). Die Rechtsbeschwerde weist zutreffend darauf hin, daß die Subsidiaritätsklausel des § 1 Abs. 3 Satz 1 BDSG schon nach ihrem Wortlaut die Verdrängung des BDSG lediglich in dem Umfang normiert, „soweit“ für deckungsgleiche Sachverhalte in anderen Rechtsvorschriften abweichende Regelungen vorliegen (vgl. Walz aaO; Gola/Schomerus aaO, Rdn. 24 zu § 1). Von der erforderlichen Tatbestandskongruenz (vgl. Schmidt in Taeger/Gabel, BSDG, Rdn. 33 zu § 1) mit dem BDSG kann bei den durch das Amtsgericht zitierten §§ 43a Abs. 2, 56 Abs. 1, 73 Abs. 2 Nr. 4, 74, 113 ff. BRAO keine Rede sein. Sie bestimmen die anwaltlichen Pflichten im Umgang mit Daten, die Kontroll- und Aufsichtspflichten sowie die Sanktionsmöglichkeiten (der Rechtsanwaltskammer) nur rudimentär, haben keinen mit dem Schutzzweck des BDSG vollständig übereinstimmenden Regelungsgehalt und schließen somit die Anwendbarkeit des BDSG nicht aus.

Hingegen ist hier § 1 Abs. 3 Satz 2 BDSG einschlägig. Nach dieser Bestimmung bleibt unter anderem die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten „unberührt“. Danach schließen andere gesetzliche Vorschriften die Anwendung des BDSG aus, wenn sie derartige Geheimhaltungspflichten zum Gegenstand haben und den davon betroffenen Personenkreis weitergehend als im BDSG schützen (vgl. Gola/Schomerus aaO, Rdn. 25 zu § 1). Eine solche Verschwiegenheitsverpflichtung des Rechtsanwalts, die sich auf alles bezieht, was ihm in Ausübung seines Berufes bekannt geworden ist, ergibt sich aus § 43a Abs. 2 Satz 1 und 2 BRAO. Sie gehört, wie die Gesetzesüberschrift zeigt, zu den anwaltlichen Grundpflichten, die nicht nur den individuellen Belangen des Rechtsanwalts und seines Mandanten dienen, sondern auch dem öffentlichen Interesse an einer wirksamen und geordneten Rechtspflege Rechnung tragen (vgl. BVerfGE 110, 226, 252). Die Institution Strafverteidigung genießt durch Art. 19 Abs. 4 GG verfassungsrechtlichen Schutz. Das steht im Einklang mit der Rechtsprechung des EGMR, wonach der Schutz der Vertraulichkeit der zwischen Rechtsanwalt und Mandant ausgetauschten Informationen eine wesentliche Garantie des Rechts auf Verteidigung darstellt (vgl. EGMR NJW 2007, 3409 (3411); EuGRZ 2003, 472 (478); König in: Festschrift für Rainer Hamm zum 65. Geburtstag, S. 325 (335)). Danach ist der Strafverteidiger weder berechtigt noch verpflichtet, die im Rahmen des Mandatsverhältnisses erhaltenen Informationen an Dritte weiterzugeben.

Die Verschwiegenheitspflicht wird nicht durch § 24 Abs. 2 Satz 1 Nr. 2 BDSG außer Kraft gesetzt. Die Vorschrift stellt zwar klar, daß der in § 1 Abs. 3 BDSG festgeschriebene Vorrang von Spezialvorschriften nicht eingreift und auch alle personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, der Kontrolle des Datenschutzbeauftragten zugänglich sind. Die Regelung betrifft aber nur den Bereich der öffentlichen Stellen (§ 24 Abs. 1 BDSG).

Für private Stellen gelten die §§ 27 bis 38a BDSG, allerdings nicht, wie § 27 Abs. 1 BDSG und im Umkehrschluß auch § 27 Abs. 2 BDSG zeigen, beim Umgang mit personenbezogenen Daten außerhalb von nicht automatisierten Dateien (§ 2 Abs. 2 Satz 2 BDSG), soweit sie nicht aus einer automatisierten Datei entnommen worden sind. Dazu hat das Amtsgericht, aus seiner Sicht folgerichtig, keine näheren Feststellungen getroffen. Soweit die Generalstaatsanwaltschaft es in ihrer Zuschrift als „naheliegend“ bezeichnet, daß die verfahrensgegenständlichen Briefe beim Adressaten (der Hausverwaltung) jedenfalls in einer strukturierten Akte (vgl. Simitis in Simitis aaO Rdn. 73 zu § 1; Art. 2c EG-Datenschutzrichtlinie vom 25. Oktober 1995) gesammelt und damit einer (automatisierten) Datei entnommen und durch die Aufnahme in die Handakten des Betroffenen und Verwendung im Strafprozeß verarbeitet und genutzt worden seien, handelt es sich um reine Mutmaßungen, die weder im Bußgeldbescheid noch im Urteil eine Stütze finden. Der Senat kann aber offen lassen, ob die Voraussetzungen des § 27 Abs. 2 BDSG hier vorliegen. Denn nach § 38 Abs. 3 Satz 1 BDSG, auf den sich die Bußgeldbehörde beruft, haben die der Aufsicht unterliegenden Stellen dem Datenschutzbeauftragten zwar auf Verlangen die zur Erfüllung seiner Aufgaben erforderlichen Auskünfte zu erteilen. Nach Satz 2 dieser Vorschrift kann der Auskunftspflichtige jedoch die Beantwortung solcher Fragen verweigern, mit der er sich der Gefahr einer strafrechtlichen Verfolgung aussetzt. Das ist hier der Fall.

Denn § 203 Abs. 1 Nr. 3 StGB stellt für den Rechtsanwalt die Verletzung von Privatgeheimnissen seines Mandanten unter Strafe. Er handelt bei der Weitergabe von derartigen Informationen „unbefugt“ im Sinne des § 203 StGB, also rechtswidrig. Entgegen der Ansicht der Beschwerdeführerin ergibt sich aus dem Urteil des Bundesgerichtshofs vom 9. Dezember 2002 (BGHSt 48, 126) keine Offenbarungspflicht des Rechtsanwalts. Die Entscheidung verhält sich dazu nicht. Sie betraf einen Datenschutzbeauftragten, bei dem der Bundesgerichtshof zur Befugnis der Preisgabe von (Amts-)Geheimnissen keine Aussage getroffen und eine Strafbarkeit nach § 353b StGB deshalb ausgeschlossen hatte, weil das Tatbestandsmerkmal der Gefährdung wichtiger öffentlicher Interessen nicht vorgelegen habe. Aus der Kontrollpflicht der Datenschutzbehörde ergibt sich keine gesetzliche Befugnis (oder gar Verpflichtung) des Rechtsanwalts zur Weitergabe mandatsbezogener Informationen an den Datenschutzbeauftragten (vgl. Fischer, StGB 57. Aufl., Rdn. 37 zu § 203; Lenckner/Eisele, in: Schönke/Schröder, StGB 28. Aufl., Rdn. 29 zu § 203). Die Vorschrift des § 38 Abs. 3 Satz 1 BDSG, deren Verletzung § 43 Abs. 1 Nr. 10 BDSG sanktioniert, enthält keine dem § 24 Abs. 2 Satz 1 Nr. 2 BDSG entsprechende Bestimmung, nach der sich auch bei nicht-öffentlichen Stellen die Kontrolle des Datenschutzbeauftragten auf diejenigen personenbezogenen Daten erstreckt, die der beruflichen Geheimhaltung unterliegen (vgl. Redeker NJW 2009, 554; König, a.a.O. S. 333). Die Beschwerdeführerin beruft sich hier, wie auch Weichert (NJW 2009, 550), zu Unrecht auf § 38 Abs. 4 Satz 3 BDSG. Nach dieser Vorschrift findet zwar (über § 24 Abs. 6 BDSG) die Rege-lung des § 24 Abs. 2 Satz 1 Nr. 2 BDSG Anwendung. Sie ist aber schon nach der Gesetzessystematik auf § 38 Abs. 4 BDSG beschränkt und betrifft nicht die Auskunftspflicht des Betroffenen, sondern seine Pflicht zur Duldung der in § 38 Abs. 4 Satz 1 BDSG bestimmten Maßnahmen, um die es hier nicht geht. Abgesehen davon bestehen auch die Duldungs- und daraus abgeleiteten Mitwirkungspflichten des § 38 Abs. 4 BDSG nur in den Grenzen, in denen der Betroffene zur Auskunft nach § 38 Abs. 3 BDSG verpflichtet ist (vgl. Petri in Simitis aaO, Rdn. 59 zu § 38). Hinzu kommt, daß eine Verletzung des mit der Auskunftspflicht korrespondierenden Einsichtsrechts des Datenschutzbeauftragten (§ 38 Abs. 4 Satz 2 BDSG) nicht bußgeldbewehrt ist, da § 43 Abs. 1 Nr. 10 BDSG insoweit nur auf § 38 Abs. 4 Satz 1 BDSG verweist.

Der Rechtsbeschwerde der Amtsanwaltschaft muß danach der Erfolg versagt bleiben.

Die Kosten- und Auslagenentscheidung beruht auf den §§ 473 Abs. 1 Satz 1, Abs. 2 Satz 1 StPO, 46 Abs. 1 OWiG.

Buchbesprechung

Peter Gola
Datenschutz und Multimedia am Arbeitsplatz – Rechtsfragen und Handlungshilfen für die betriebliche Praxis.
3. Aufl. 2010, Datakontext-Verlag, 39,95 €.

Wer die sieben Zeilen Vorwort zur 3. Auflage gelesen hat, erwartet zunächst kein ambitioniertes Werk. Und nach der Lektüre des Inhaltsverzeichnisses erscheint Multimedia für so ausgefeilte Technologien wie die Festnetztelefonie auch ein etwas hochgestochenes Wort. Aber der erste Eindruck täuscht: Auch in der dritten Auflage ist es die LeserInnenfreundlichkeit, die für den Autor oberste Priorität hat. Vor uns liegt ein Buch, das den Akteuren in der betrieblichen Praxis wirklich Handlungshilfe sein will. Wer sich zügig mit den datenschutzrechtlichen Konsequenzen und typischen Fehlerquellen beim Einsatz von Kommunikationstechnik in der Arbeitswelt befassen will, findet mit dem Buch den passenden Steigbügel. Dafür schärft der Autor das Problembewusstsein seiner LeserInnen und gibt vor allem ArbeitnehmervertreterInnen ein ganzes Arsenal kritischer Fragen und datenschutzfreundlicher Lösungen an die Hand, aus denen in der betrieblichen Praxis wertvolle Argumente werden können. Einem Durchmarsch der Arbeitgeberinteressen beim Einsatz von Kommunikationstechnik hat die Leserschaft des Buches vieles entgegenzusetzen. Dieser Wille zu praktischen Antworten und NutzerInnenfreundlichkeit geht leider auf Kosten des juristischen Tiefgangs, so zum Beispiel bei der Erörterung der Rechtsprechung zu Verwertungsverboten nach Persönlichkeitsrechtsverletzung oder zur Abweichung vom gesetzlichen Datenschutzstandart durch Betriebsvereinbarungen. Auch findet sich als „jüngst" verzeichnete Rechtsprechung aus dem Jahre 2005. Das mag verzeihlich erscheinen, da die betrieblichen Akteure die Auseinandersetzungen um die aufgeworfenen Rechtsfragen wohl im Wesentlichen ohnehin unter Einschaltung von Rechtsbeiständen und professionellen BeraterInnen führen müssen. Die nun vorgelegte Auflage wird womöglich auch nur eine bescheidene Halbwertszeit haben und das Sprungbrett für die Fortsetzung des Werkes nach der Regelung des Beschäftigtendatenschutzes im BDSG sein. Der Bedarf an einem anwendungsorientierten Praxishandbuch wie diesem wird eher zu- als abnehmen.

Gola/Schomerus
BDSG, Kommentar
10. Aufl. 2010, Verlag CH. Beck, 617 Seiten, € 54,00

(SH) Er ist dünner geworden, der Gola/Schomerus, aber nicht leichter. Das drucktechnisch etwas geliftete und nun enger gesetzte Werk ist inhaltlich gewachsen. Das mag das Verdienst des umtriebigen Gesetzgebers sein, aber die AutorInnen sind ihm hart auf den Fersen. Dabei geht es ihnen wie vielen fleißigen KommentatorInnen: Kaum ist das Werk erschienen, stellt der Gesetzgeber mit dem Entwurf für ein Beschäftigtendatenschutzgesetz gleich alles wieder in Frage. Die Kommentierung des § 32 BDSG fällt gleichwohl engagiert und vollständig aus und zeigt für alle praktisch bedeutenden Fragestellungen Lösungswege und weiterführende Hinweise auf. Gelungen ist auch die Bestimmung des Verhältnisses zu den weiterhin auf Beschäftigtendaten anwendbaren Passagen von § 28 BDSG. Die kritische Begutachtung der Gesetzgebung zu § 32 BDSG sah sich dabei vor allem vor einer Aufgabe: zu zeigen, dass sich in der Rechtswirklichkeit mit der Gesetzesnovelle nicht viel ändern sollte. So ist es das Verdienst der Neuauflage, die bekannten Positionen der Fachwelt im neuen Gesetzestext zu verankern.

Dem verstorbenen Kommentarmitbegründer Rudolf Schomerus ist Barbara Körffler, Mitarbeiterin beim ULD, in das AutorInnenteam nachgefolgt. Sie führt nun bei der Kommentierung des 2. Abschnitts des Gesetzes – öffentlicher Bereich – die Feder. Ihr Einstieg hat an dem bis in die Randnummern hinein fast unverändert gebliebenen Kommentierung des 2. Abschnitts bislang keine strukturellen Spuren hinterlassen. Gegenüber der 9. Auflage (2007) hat das Werk im Wesentlichen eine genaue Durchsicht und Aktualisierung um erfreulich junge Literatur und Rechtsprechung erfahren. Dies und einige noch behutsam eingebrachte neue Akzente lassen erwarten, dass das Kapitel zum öffentlichen Bereich in Zukunft einen noch höheren Gebrauchswert erhalten wird.

Der Gola/Schomerus ist in der 10. Auflage eine kundige und sichere Handreichung in aller Kürze. Auch die Neuauflage referenziert aber leider weiterhin zentrale Gerichtsentscheidungen nur in der Datenschutzfachpresse, welche vielen Praktikerinnen und Praktikern im Arbeits- oder Verwaltungsrecht schlichtweg nicht zur Hand ist. Wer die Argumente es Kommentars nachvollziehen will, wird trotzdem einen Bibliothekszugang oder eine kommerzielle Datenbank brauchen.

Presseerklärung:

GI stellt zehn Thesen zu Sicherheit und Datenschutz in Cloud Computing vor

Die Gesellschaft für Informatik e.V. (GI) hat zehn Thesen zu Sicherheit und Datenschutz in Cloud Computing vorgestellt. Im „Cloud Computing" werden viele vernetzte Rechner gemeinsam genutzt.

„Cloud Computing ist in aller Munde und wird heute in vielfältigen Umgebungen eingesetzt. Deshalb ist es sehr wichtig, Risiken zu kennen und Handreichungen für einen verantwortungsvollen Einsatz von Clouds zu definieren", sagte GI-Präsident Stefan Jähnichen. Die GI habe deshalb folgende zehn Thesen aufgestellt, die die Herausforderungen Identity Management, Access Control und Integrity Control, Logging und Auditing, Risk Management und rechtliche Compliance aus technischer und juristischer Sicht beschreiben:

Cloud Computing (früher: Grid-Computing und Utility Computing) bezeichnet preiswerte zentral und dynamisch organisierte große (verteilte und virtualisierte) Cluster von IT-Systemen (shared infrastructures, Server-Farmen): Hardware, Speicher- und Netzkapazitäten, Plattformen (Datenbanken und Run-Time-Environment) und Anwendungen (verteilte Nutzung von Software: Hosted Applications). Öffentliche Clouds sind in Deutschland und/oder im Ausland oder an nicht (näher) spezifizierten Orten und auch off-shore angesiedelt; jedenfalls kann der Anwender nicht erkennen, an welchem Ort des weltweiten Internets seine Daten gespeichert oder verarbeitet werden. Die Cloud ist intransparent und damit unkontrollierbar. Öffentliche Clouds werden von Outsourcingnehmern auch ohne ausdrückliche Information des Auftraggebers eingesetzt. Wir alle benutzen Clouds, wenn wir z.B. mit Suchmaschinen, Software as a Service, webbasierten Maildiensten, Social Communities und Kalendern im Internet arbeiten.

Die folgenden Herausforderungen hinsichtlich Identity Management, Access Control und Integrity Control, Logging und Auditing, Risk Management und rechtlicher Compliance müssen also gelöst werden:

1. Clouds können ein Sicherheitsrisiko darstellen wegen der außerhalb des Unternehmens fehlenden Durchsetzungsmöglichkeit unternehmenseigener Sicherheitspolitiken, -strategien und -verfahren sowie Sicherheitsmaßnahmen und ihrer Kontrollierbarkeit. Das Gesamt-Sicherheitsniveau bei Cloud Computing kann naturgemäß nicht höher sein, als das Sicherheitsniveau innerhalb des Unternehmens – durch die unverzichtbare Vor- und Nach-Verarbeitung im Unternehmen.

2. Daher lassen bereits heute Unternehmen nur ausgewählte Daten in öffentlichen Clouds verarbeiten und verarbeiten wertvolle Daten ausschließlich in privaten Clouds (in-house).

3. Private Clouds unterscheiden sich unter Sicherheitsaspekten nicht von den herkömmlichen unternehmenseigenen IT-Systemen, weil sie der unternehmenseigenen Sicherheitspolitik unterliegen und vollständig kontrolliert werden können. Entsprechendes gilt für rechtliche Vorgaben für die innerbetriebliche Informationsverarbeitung.

4. Bei der Nutzung öffentlicher Clouds (und auch hybrider) sind nationale Gesetze und branchenspezifische Selbstregulierungsmaßnahmen einzuhalten (Compliance); daraus folgt für einige Branchen, dass Clouds gar nicht genutzt werden dürfen. Risikomanagement (z. B. aus § 91 Abs. 2 AktG) und Sicherheitskonzepte sind bei der Nutzung von Clouds anzupassen. Einschränkungen ergeben sich insbesondere aus dem Datenschutzrecht, das die Übermittlung personenbezogener Daten in Staaten außerhalb der EU nur sehr eingeschränkt zulässt und auch innerhalb der EU Pflichten für die Auftragsdatenverarbeitung festsetzt, die nur eine eingeschränkte Nutzung öffentlicher Clouds erlauben.

5. Der Transport der zu verarbeitenden Daten zu öffentlichen Clouds erfolgt über das völlig unsichere Internet und kann nur äußerst aufwändig abgesichert werden.

6. Daten können zur Erhöhung der Vertraulichkeit in der Cloud verschlüsselt gespeichert werden; allerdings können Daten nicht verschlüsselt verarbeitet werden, dazu müssen sie in der Cloud erst wieder entschlüsselt werden – können dann allerdings in öffentlichen Clouds von Dritten ausgelesen werden. Alle eingesetzten Standard- und/oder Individualprogramme zum Transport zu Clouds und zur Verwaltung von Clouds (Virtualisierung, Lastausgleich, geografische Verteilung, Sicherungs- und Sicherheitsmaßnahmen etc.) und auch Verschlüsselungsprogramme und Protokolle sind nicht fehlerfrei; sie können vielmehr kritische (aus dem Internet ausnutzbare) Sicherheitslücken enthalten, die (unbekannten) Dritten ein Auslesen oder Abhören der Daten erlauben.

7. Sicherheitsrelevante Vorfälle müssen sorgfältig untersucht werden können (Forensik). Dies wird allerdings durch die geografische Verteilung der sehr vielen genutzten IT-Systeme schwierig bis unmöglich. Die Beschlagnahme lokalisierter Daten(träger) durch Ermittlungsbehörden verursacht Probleme, weil entweder der auf Virtualisierung und Mehrmandantenfähigkeit basierende Cloud-Betrieb gestört wird oder die Alternative eines (potentiell manipulierten) Snapshots der Daten aus der Cloud nur verminderten Beweiswert vor Gericht hat.

8. Cloud-Betreiber können ihre Dienste einstellen – z.B. bei wirtschaftlichen Schwierigkeiten. Auch in solchen Fällen muss nicht nur vertraglich sondern auch technisch die volle Kontrolle durch den Anwender erhalten bleiben: Das so genannte „vendor-lock-in" könnte etwa durch branchenübergreifende Standards verhindert werden. Unentgeltliche Cloud-basierte Dienste werden häufig ohne jegliche Garantie angeboten, so dass die verarbeiten Daten besonders hohen Risiken ausgesetzt sind. Verträge bevorzugen zudem derzeit die Cloud-Anbieter und berücksichtigen nicht in angemessener Form die Interessen der Cloud-Nutzer.

9. Bei vertraglichen Vereinbarungen besteht häufig eine Diskrepanz zur technischen Durchsetzung (z.B. technische Unmöglichkeit der Datenlöschung bei Vertragsende oder besonderen Ereignissen wie Insolvenz).

10. Zur Beherrschung der Risiken durch gemeinsame Nutzung von Hard- und Software (Internet, Infrastruktur, Software und Verfahren) gleichzeitig mit unbekannten Dritten muss Cloud Computing dem Wert der verarbeiteten Daten entsprechend abgesichert werden. Öffentliche Clouds müssen wie Kritische Infrastrukturen behandelt werden, sofern sie allgemein und weitverbreitet genutzt werden sollen. Dabei sind auch kartellrechtliche Aspekte wie die „Essential-facilities-Doktrin" zu beachten.

Insgesamt ergeben sich stark erhöhte Anforderungen an die Absicherung unternehmenseigener und auch privater Datenverarbeitung bei Cloud Computing und zwar hinsichtlich Vertraulichkeit, Integrität, Verbindlichkeit (z.B. Authentifizierung Berechtigter) und Verfügbarkeit der verarbeiteten Daten und genutzten IT-Systeme, ferner auch stark erhöhte Anforderungen an die rechtliche Absicherung.

PRESSEMITTEILUNG

Brüssel, Freitag, den 3. Dezember 2010

"Moment der Wahrheit" für die Richtlinie über die Vorratsspeicherung von Daten: Der EDSB fordert eindeutige Beweise für die Notwendigkeit

In einer Rede heute bei der Konferenz der Europäischen Kommission in Brüssel zum Thema "*Taking on the Data Retention Directive*" hat Peter Hustinx, der Europäische Datenschutzbeauftragte (EDSB), sich stark dafür ausgesprochen, die Gelegenheit des laufenden Bewertungsprozesses zu nutzen, um die Notwendigkeit und Rechtfertigung der Richtlinie über die Vorratsspeicherung von Daten deutlich zu demonstrieren.

Der EDSB betonte erneut, dass die Vorratsspeicherung von Verkehrs- und Standortdaten aller Personen in der europäischen Union (EU), wann immer sie das Telefon oder das Internet benutzen, einen riesigen Eingriff in das Recht auf Privatsphäre aller Bürger bedeutet. Als solche bewertet der EDSB die Richtlinie als das am meisten **in die Privatsphäre eingreifende Instrument**, das jemals von der EU im Hinblick auf Umfang und Anzahl der Menschen, die davon betroffen werden, angenommen wurde.

Eine solch massive Verletzung der Privatsphäre muss solide gerechtfertigt werden. Der EDSB hat daher die Europäische Kommission dazu aufgefordert, die Bewertung zu verwenden, um tatsächlich **die Notwendigkeit der Richtlinie zu beweisen**. Konkrete Fakten und Zahlen sollten auch die Beurteilung ermöglichen, ob die bei der Bewertung vorgestellten Ergebnisse mit anderen weniger in die Privatsphäre eingreifenden Mitteln hätten erreicht werden können.

"*Die Bewertung, auf die wir derzeit warten, ist der Moment der Wahrheit für die Richtlinie über die Vorratsspeicherung von Daten*", erklärte Peter Hustinx. "*Beweise sind erforderlich, dass sie eine notwendige und verhältnismäßige Maßnahme darstellt. Ohne einen solchen Nachweis sollte die Richtlinie zurückgezogen oder durch ein weniger in die Privatsphäre eingreifendes Instrument ersetzt werden, das den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit entspricht.*"

Der EDSB bestand weiter auf der Tatsache, dass die Richtlinie über die Vorratsspeicherung von Daten offensichtlich die **Harmonisierung der nationalen Rechtsvorschriften verfehlt hat**. Signifikante Unterschiede zwischen den einzelstaatlichen Rechtsvorschriften zur Umsetzung haben zu einer Rechtsunsicherheit bei den Bürgern geführt. Es hat sich auch eine Situation ergeben, in der die Verwendung der auf Vorrat gespeicherten Daten **nicht strikt** auf die Bekämpfung von schweren Straftaten **begrenzt** ist.

Nach Ansicht des EDSB sollte ein neues oder geändertes EU-Instrument zur Vorratsdatenspeicherung **klar in seinem Umfang definiert** werden und **Rechtssicherheit für die Bürger** schaffen. Dies bedeutet, dass es auch die Möglichkeit für den Zugang und die Weiterverwendung durch Strafverfolgungsbehörden regeln und keinen Raum für die Mitgliedstaaten lassen sollte, die Daten für weitere Zwecke zu nutzen.

Hintergrund-Informationen

Die Richtlinie über die Vorratsspeicherung von Daten (Richtlinie 2006/24/EG (PDF)) erfordert von öffentlichen Anbietern elektronischer Kommunikationsdienste (Telefon- und Mobilfunkunternehmen, Internetanbieter) Verkehrs-, Standort- und Teilnehmerdaten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten auf Vorrat zu speichern.

Die Richtlinie unterliegt derzeit einem Bewertungsprozess, der darauf zielt, ihre Anwendung durch die Mitgliedstaaten und ihre Auswirkung auf Unternehmen und Verbraucher zu beurteilen. Das Ziel ist auch festzustellen, ob die Richtlinie in angemessenem Verhältnis mit den Vorteilen für die Strafverfolgung, den Marktkosten und den Auswirkungen auf die Grundrechte, insbesondere das Recht auf Privatsphäre und den Schutz personenbezogener Daten, steht. Das Ergebnis der Bewertung wird der Kommission bei ihrer Entscheidung helfen, ob eine Überarbeitung der Richtlinie erforderlich ist.
