2/2010

Datenschutz Nachrichten

33. Jahrgang
ISSN 0137-7767
9,00 Euro

Verbraucherdatenschutz

■ Datenschutzrechtliche Neuordnung des Hinweis- und Informationssystems der Versicherungswirtschaft ■ Sozialdatenschutz in der privaten Krankenversicherung ■ Wie man sich gegen Telefon-Abzocke wehren kann ■ Demo „Freiheit statt Angst“ in Berlin ■ Datenschutznachrichten ■ Rechtsprechung ■

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

Inhalt

Termine

Montag, 21. Juli 2010
ELENA – Auswirkungen auf Betriebs- und Dienstvereinbarungen zu personendatenverabeitenden Systeme
BTQ Kassel, InterCity Hotel, Kassel
Weitere Informationen unter:; www.btq-kassel.de/

Samstag, 11. September 2010
Freiheit statt Angst, Demonstration Berlin, Potsdamer Platz, 13 Uhr
Weitere Informationen unter: www.vorratsdatenspeicherung.de

Sonntag, 12. September 2010
DVD-Vorstandssitzung in Berlin
(Interessierte DVD-Mitglieder mögen sich bitte bei der Geschäftsstelle melden.)

Samstag, 9. Oktober 2010
DVD-Vorstandssitzung in Bonn
(Interessierte DVD-Mitglieder mögen sich bitte bei der Geschäftsstelle melden.)

Freitag - Sonntag, 5. - 7. November 2010
DVD & FIfF – Jahrestagung 2010 - transparenz.arbeit.kontrolle
Gemeinsam werden das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) und die Deutsche Vereinigung für Datenschutz (DVD) ihre Jahrestagung 2010 in Köln abhalten. Nach den fortgesetzten Datenskandalen wird sich die Tagung mit unterschiedlichsten Aspekten des Beschäftigtendatenschutzes befassen. Weitere Informationen und Anmeldung unter: www.fiff.de/veranstaltungen/fiff-jahrestagungen/JT2010

Sonntag, 7. November 2010
DVD-Mitgliederversammlung in Köln (im Anschluss an Tagung)
Weitere Informationen unter: www.datenschutzverein.de

Dienstag – Donnerstag, 9. - 11. November 2010
Technologieforum 2010 – Arbeitnehmerdatenschutz“
Ramada Hotel Kassel City
Weitere Informationen unter: www.dtb-kassel.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
33. Jahrgang, Heft 2

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)
Roland Schäfer
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
Titelbild, 65, 70, 71, 73: Frans Jozef Valenta, 4: LDI NRW, 67: Hajo Köppen

Datenschutz – do it yourself

Persönliche Daten sind bares Geld wert. Wer sich davon überzeugen will, muss nur auf der Homepage der Schober Information Group Deutschland GmbH (www.schober.de) in einer Abfragemaske einige Merkmale eingeben um 813 Anschriften zum Gesamtpreis von 919,10 € angeboten zu bekommen. Und wer bereits durch telefonische Werbung oder Gewinnankündigungen belästigt worden ist, ahnt, dass schon eine Telefonnummer eine geldbringende Information sein kann. Adressenhandel ist erlaubt, Werbeanrufe ohne vorherige Einwilligung der Betroffenen nicht. Gegen beides kann man sich aber schützen. Dem Handeln mit seinen Adressdaten kann man widersprechen. Und bei unerwünschter Werbung und Gewinnversprechungen via Telefon hilft eine Meldung über www.bundesnetzagentur.de, um den Belästigern das Leben zumindest schwerer zu machen. Und natürlich kann jeder von Behörden und Unternehmen Auskunft über die zu seiner Person gespeicherten Daten verlangen. Also warum nicht mal zum Beispiel bei seiner Versicherung, seinem Telekommuniaktionsanbieter, der Schufa etc. nachfragen, welche Daten über einen dort gespeichert sind.

Das Datenschutzrecht hält eine Reihe von hilfreichen Werkzeugen bereit, mit denen sich nach dem Grundsatz des „Do it yourself" erfolgreich Datenschutz praktizieren lässt. Allein auf die Datenschutzgesetzgebung und unternehmerische Compliance ist nicht unbedingt Verlass, wie dieses Heft am Beispiel der Versicherungsbranche zeigt.

Persönliche Daten sind bares Geld wert. Wer also seine Geldkonten pflegt, wird auch mit seinen Daten sorgsam umgehen – aktiver Datenschutz, jetzt erst recht.

Hajo Köppen Roland Schäfer

Autorinnen und Autoren dieser Ausgabe:

Harald Gall
Geschäftsführer, CPC The Profiling Company GmbH, Hamburg
gall@profiling-company.de

Hajo Köppen
Assessor jur., Planungsreferent, Datenschutzbeauftragter und Lehrbeauftragter für Datenschutzrecht an der Fachhochschule Gießen-Friedberg,
hajo.koeppen@verw.fh-giessen.de

Ulrich Lepper
Landesbeauftragter für den Datenschutz und Informationsfreiheit in Nordrhein Westfalen, Düsseldorf
poststelle@ldi.nrw.de

Dr. Birgit Schröder
Rechtsanwältin, Fachanwältin für Medizinrecht, Hamburg
www.dr-schroeder.com, kanzlei@dr-schroeder.com

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

Ulrich Lepper

Moderner Datenschutz – Was ist das?

Ulrich Lepper wurde am 21. Januar 2010 zum neuen Landesbeauftragten für den Datenschutz und Informationsfreiheit in Nordrhein Westfalen gewählt.

Im folgenden Text skizziert er den Schwerpunkt seiner zukünftigen Arbeit.

Wir leben in einer hoch technisierten Welt. Unsere digitalen Spuren hinterlassen wir etwa am Computer, im Netz, auf dem Handy, im Bordcomputer des Autos und auf Videoaufzeichnungen der Kameras, die unseren Alltag begleiten. Wie leicht heimliche Überwachung heute möglich ist, zeigten jüngst einige spektakuläre Fälle der Beschäftigtenüberwachung und legen auch Angebote von Tracking Services und Spy-Software für Handys und Computer nahe. Wie wichtig Sicherheit im Unternehmen heute ist, führten uns Fälle vor Augen, in denen ein nachlässiger Umgang mit Daten der Kundinnen und Kunden zum unzulässigen Verkauf und Missbrauch von Kontodaten führte. Wie schwierig der Schutz der Privatsphäre in einer vernetzten Welt ist, lernen wir zum Beispiel bei Facebook. Das wird untermauert durch eine aktuelle Studie der Stiftung Warntest[1] über soziale Netzwerke.

Die technische Entwicklung fordert uns heraus, das Recht muss damit Schritt halten, damit auch in Zukunft die Privatsphäre in einer digitalisierten Welt noch einen Wert hat. Einige wichtige und im Wesentlichen richtige Schritte wurden mit drei Gesetzesnovellen des Bundesdatenschutzgesetzes im letzten Jahr unternommen. Ein modernes Datenschutzrecht muss aber darüber hinausgehen und zukunftsfähige Grundlagen setzen. Deswegen hat die Konferenz der Datenschutzbeauftragten es Bundes und der Länder Eckpunkte für ein modernes Datenschutzrecht des 21. Jahrhunderts[2] vorgelegt. Wir wollen damit die Diskussion über eine grundlegende Datenschutzrechtsnovelle eröffnen.

Für mich ist dabei ganz wesentlich, dass die Rollen aller Akteure bei der Datenverarbeitung klar und den Verantwortungen entsprechend definiert sind. Neben starken Aufsichtsbehörden sind vor allem die verantwortlichen Stellen und die interne Datenschutzkontrolle von entscheidender Bedeutung für einen guten Datenschutz. Sie können Ihre Aufgaben nur verantwortlich wahrnehmen, wenn es klare Regeln gibt, die eindeutig umgesetzt werden können. Sie müssen eine zeitgemäße an Schutzzielen orientierte Vorgabe für die Datensicherheit erhalten. Datenschutzaudits oder -benchmarking können darüber hinaus zusätzlicher Ansporn für einen guten Datenschutz sein.

Die betriebliche Datenschutzkontrolle muss gestärkt werden, um Defizite vor Ort schnell in den Griff zu bekommen. Dazu gehört für mich auch, dass die Kontrollfunktionen von staatlicher und betrieblicher Aufsicht besser verzahnt werden. Nur so kann Datenschutz in der Fläche gewährleistet werden. Dass dies funktioniert ist in einem Lande von der Größe Nordrhein-Westfalens sehr wichtig. Ich will deshalb in meiner Amtszeit aktiv den Kontakt zu den Datenschutzbeauftragten in den Betrieben und Behörden suchen und ihre Expertise auch bei meinen Prüfungen einbeziehen.

Die größte Herausforderung für den Schutz der Privatsphäre ist das Internet, weil es keine nationalen Grenzen kennt. Die Eckpunkte enthalten konkrete Vorschläge für technische und rechtliche Instrumente, die den Schutz der Verbraucherinnen und Verbraucher im Netz verbessern können. Dennoch werden auch die Nutzerinnen und Nutzer selbst gefordert sein. Sie müssen sich nicht zuletzt durch den bewussten Umgang mit den eigenen Daten selbst schützen und können ihre kollektive Verbrauchermacht einsetzen, um den Respekt vor ihrer Privatsphäre einzufordern. Deswegen ist Medienkompetenz für mich ein entscheidender Faktor. Ohne medienkompetente Bürgerinnen und Bürger, die den Schutz ihrer Daten auch wollen und aktiv betreiben, wird jeder staatliche Schutzansatz im Netz scheitern. Der Stärkung von Medienkompetenz will ich meine Arbeit gemeinsam mit anderen Akteuren in Nordrhein-Westfalen ganz besonders widmen.

1 http://www.test.de/themen/computer-telefon/test/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-1855785/

2 siehe hierzu: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutz/Inhalt/79__Konferenz/modernes_Datenschutzrecht/Ein_modernes_Datenschutzrecht_fuer_das_21__Jahrhundert.php

Harald Gall

Datenschutzstudie in der Versicherungsbranche zeigt eklatante Lücken auf

Datenschutz ist als Aspekt der informationellen Selbstbestimmung im Grundgesetz verankert. Das Recht auf informationelle Selbstbestimmung geht auf ein Urteil des Bundesverfassungsgerichtes zurück und basiert auf den Artikeln (1) (Menschenwürde) und (2) (allgemeine Handlungsfreiheit) des Grundgesetzes.

Jede Bürgerin und jeder Bürger hat das Recht, selbst zu entscheiden, wer über ihre, bzw. seine Daten verfügen darf. Das Datenschutzgesetz soll sie bzw. ihn in diesem Recht bestärken. Allerdings zeigten die Datenskandale der jüngsten Zeit, dass Unternehmen Schwierigkeiten haben, ihren Verpflichtungen im Datenschutz nachzukommen. In der Diskussion um den Datenschutz wird immer wieder darauf verwiesen, dass es sich um Extremfälle handelte und ein Rückschluss auf die gesamte Wirtschaft oder einzelne Branchen nicht zulässig sei.

Dass dies so nicht richtig ist, zeigt eine Studie, die The Profiling Company durchgeführt hat. Zielgruppe der Studie ist die Versicherungsbranche.

Die Versicherungsbranche wurde ausgewählt, da sie mit besonders umfangreichen und sensiblen Daten umgeht. So muss ein Kunde schon beim Abschluss einer Versicherung umfassende Angaben zu seinen persönlichen Verhältnissen machen. In einigen Fällen werden auch Daten von früheren Versicherungsverträgen und sogar Daten von Ärzten und Krankenhäusern bezogen. Dazu kommen Daten, die sich während des Vertragsverlaufs ansammeln, wie Inkasso- oder Schadensdaten. Außerdem werden bei den meisten Versicherungen Daten für Marketingzwecke sowie Daten von Dritten, die in Schadensfällen mit einem Kunden verwickelt waren, gespeichert. Einige dieser Daten werden bei Prüfungen von Anträgen oder bei Schadensfällen beim zuständigen Fachverband oder bei anderen Versicherern abgefragt oder an diese weitergegeben. Diese Vielzahl und die Sensibilität der Daten stellen besonders hohe Anforderungen an die Versicherungen, zumal der Schaden bei fahrlässigem oder verantwortungslosem Umgang mit diesen Daten besonders hoch ist.

Die Ergebnisse der Studie sind bemerkenswert.

Eines der Kernelemente der Studie basiert auf einer Datenschutzauskunft nach § 34 Bundesdatenschutzgesetz. Nahezu 40% der Versicherungsunternehmen haben diese Anfrage überhaupt nicht beantwortet. 10 % haben zwar geantwortet, aber keine Auskunft über die gespeicherten Daten zu einer Testperson gegeben. Somit ist fast jedes zweite Unternehmen seiner gesetzlichen Verpflichtung zur Datenschutzauskunft nicht nachgekommen. Aber auch die Versicherungen, die geantwortet haben, geben Grund zu großer Besorgnis. In einem besonders gravierenden Fall wurden von der Gothaer Krankenversicherung sehr sensible Krankheitsdaten einer dritten/fremden Person übermittelt. Als der entsprechende Versicherer - der auch anderweitig aufgefallen war - damit konfrontiert wurde, zeigte er keinerlei Interesse an der Aufklärung des Sachverhaltes. Der Datenschutzbeauftragte der Gothaer schloss einfach kategorisch aus, dass seine Versicherungsgruppe einen Verstoß gegen das Datenschutzgesetz begangen haben könnte.

Bei allen Datenschutzauskünften wurden einige Datenbereiche beinahe durchgängig ignoriert. Schadens- und Inkassodaten wurden ebenso wenig übermittelt wie Scoring-Informationen, obwohl diese Datengruppen für die betroffenen Personen besonders wichtig sind. Gerade auf Basis dieser Daten werden Versicherungsanträge entschieden und Tarife berechnet. Erhält eine betroffene Person keinen Einblick in diese Daten, besteht für diese Person keine Möglichkeit, Fehler, die bei der Erhebung oder Ermittlung dieser Daten entstanden sind, zu korrigieren.

Sehr schwer tun sich Versicherungen auch beim Umgang mit Marketing- und Vertriebsdaten. Im Vorfeld der Studie wurden bei einigen Versicherungen Daten „hinterlassen“. Anschließend war kaum ein Unternehmen in der Lage, diese in der Datenschutzauskunft mitzuteilen, obwohl Versicherungsmitarbeiter auf Basis der Daten Kontakt mit der Testperson aufgenommen hatten.

Auch der Umgang mit Sicherheitsverfahren bei der Erhebung von personenbezogenen Daten ist erschreckend unprofessionell. Verfahren wie Opt-in oder Doppel-Opt-in sowie der Einsatz von HTTPS oder Capture-Methoden wurden von vielen Versicherungen nicht oder nicht an allen relevanten Stellen, an denen Daten erhoben wurden, verwendet.

Selbst gesetzliche Notwendigkeiten wie das Vorhandensein einer Datenschutzerklärung oder eines Verfahrensverzeichnisses werden von den Versicherungen nicht durchgängig beachtet. Besonders auffällig ist, dass die Verfahrensverzeichnisse, sofern sie überhaupt vorhanden waren, in keinem einzigen Fall den gesetzlichen Anforderungen gerecht werden konnten.

Die Größe oder die Reputation von Versicherungen spielt bei den Ergebnissen keine Rolle. Die Probleme ziehen sich durch alle Strukturen und Größenordnungen.

Die Mehrheit der Versicherungsunternehmen geht mit dem Thema Datenschutz fahrlässig um.

Prozesse, die den Datenschutz sicherstellen könnten, sind nicht oder nur in Ansätzen zu erkennen. Die Versicherungen ignorieren und brechen nicht nur Gesetze, sie signalisieren auch, welchen Stellenwert das Vertrauensverhältnis mit ihren Kunden jenseits von Werbeversprechen besitzt.

Der Versuch, mit den Versicherungsunternehmen ins Gespräch zu kommen, wurde mit Ausnahme von zwei Fällen mit zum Teil aggressiven Antworten abgeschmettert.

Der Handlungsbedarf in der Versicherungsbranche bezüglich Datenschutz ist enorm.

Dr. Thilo Weichert

Datenschutzrechtliche Neuordnung des Hinweis- und Informationssystems der Versicherungswirtschaft

1. Datenschutz in der Versicherungswirtschaft

Die Datenschutz-Baustellen in der Versicherungswirtschaft sind kaum zu überschauen. Demgemäß vielfältig sind auch die Themen, die das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) gemeinsam mit den Aufsichtsbehörden in der Arbeitsgruppe (AG) Versicherungswirtschaft des Düsseldorfer Kreises (DK), dem bundesweiten Zusammenschluss der Datenschutzaufsichtsbehörden nach § 38 BDSG, mit dem Gesamtverband der deutschen Versicherungswirtschaft GDV und den Versicherungsunternehmen (VU) erörtert. Weitgehend abgeschlossen sind die Verhandlungen über eine völlig überarbeitete Einwilligungsklausel für die gesetzlich nicht geregelten Verarbeitungsprozesse bzgl. Gesundheitsdaten und die Formulierung einer Schweigepflichtentbindung. Dies war nötig geworden, nachdem die AG Versicherungswirtschaft festgestellt hatte, dass die bisherigen sehr allgemein gehaltenen Einwilligungs- und Entbindungsklauseln unwirksam sind und das Bundesverfassungsgericht dies im Hinblick auf die Schweigepflichtentbindung bestätigte. Die AG und die Versicherungswirtschaft verständigten sich darauf, die Datenverarbeitung nicht mehr auf diese (unwirksamen) Klauseln zu stützen, sondern, so weit dies möglich ist, auf die gesetzlichen Erlaubnisnormen im BDSG, also insbesondere des § 28 BDSG.

Dies führte dazu, dass es erforderlich ist, die gesetzlichen Regelungen branchenspezifisch zu konkretisieren. Zu diesem Zweck verabredeten die AG mit dem GDV, Verhaltensregeln nach § 38a BDSG zu erarbeiten, die sowohl den VU wie auch den Versicherungsnehmern (VN) auf einem möglichst hohen Niveau Rechtssicherheit verschaffen. Auch die Erarbeitung dieser Verhaltensregeln (Codes of Conduct) sind weit vorangekommen. Nach den Novellierungen des BDSG bedürfen sie einer Anpassung an die nunmehr geltenden Vorschriften. In den Verhaltensregeln sollen möglichst viele in der Branche auftretende Datenschutzfragen beantwortet werden. Dies gilt u.a. auch für die äußerst kontroversen Themen der Verarbeitung von Gesundheitsdaten, die Nutzung für Werbezwecke, die Bonitätsprüfung und den Einsatz von Scoringverfahren oder die Einbeziehung von Versicherungsmaklern und Strukturvertrieben oder von Rückversicherungen. Von Sprengkraft ist auch der Datenaustausch im Versicherungskonzern: Einerseits besteht die gesetzliche Pflicht zur Spartentrennung; andererseits gibt es nicht zu ignorierende Notwendigkeiten des konzerninternen Datenaustauschs zu VN, z.B. bei spartenübergreifenden Vertragsgestaltungen und der gegenseitigen Auftragsdatenverarbeitung bzw. Funktionsübertragung. Auch bzgl. des Hinweis- und Informationssystems (HIS) der Versicherungswirtschaft besteht zwischen AG und GDV Einigkeit, dass die unwirksamen Einwilligungen durch eine tragfähige Lösung auf gesetzlicher Basis abgelöst werden sollen.

2. Hinweis- und Informationssystem - Uniwagnis

In den öffentlichen Diskussion über das Warnsystem der Versicherungswirtschaft wird oft der Begriff „Uniwagnis“ verwendet. Diese bezeichnet aber bei ganz korrekter Namensverwendung nicht das Warnsystem, sondern die hierfür eingesetze Software. Uniwagnis I heißt das Programm zur Verschlüsselung der Namensangaben in einen Strukturcode; Uniwagnis II dient der Dechiffrierung und Nutzung dieses Codes. Dennoch hat sich über die Zeit für die Bezeichnung des Gesamtsystems Uniwagnis eingebürgert. Von den VU und dem GDV selbst ist dagegen vom Hinweis- und Informationssystem, abgekürzt HIS, die Rede.

Das HIS wird derzeit vom GDV betrieben. Es entstand aus spezifischen Warndateien der Kfz-Sparte und anderen Sparten im Jahr 1993. Das neu eingerichtete Verfahren enthielt und enthält immer noch spartenspezifisch Informationen über besondere Risiken bzw. mögliche Betrugshinweise. Bei den Sparten handelt es sich um Kraftfahrtzeug (Kfz), Unfall, Rechtsschutz, Sachversicherung, Leben einschließlich Berufsunfähigkeit, Rente und Pflege, sowie Transport, einschließlich Reiseversicherung, und schließlich Haftpflicht. Die Privaten Krankenversicherungen (PKV) werden nicht vom GDV vertreten, auch wenn sie in den gleichen Versicherungskonzernen angeboten werden, sondern vom PKV-Verband. Der PKV-Verband beteiligt sich nicht am HIS, sondern betreibt ein eigenes Warnsystem mit der unverdächtigen Bezeichnung „Versichertenumfrage“. Dahinter verbirgt sich ein datenschutzrechtlich nicht minder unzulässiges, aber technisch eher überholtes und weniger umfangreiches Verfahren, bei dem VU Verdachtsfälle auf Kärtchen eintragen und in fernkopierter Form an die anderen PKV-Unternehmen weitergeben. Die Versichertenumfrage soll in der Folge hier nicht weiter erörtert werden, wenngleich auch dieses Verfahren gegen den Datenschutz verstößt, dies dem PKV-Verband und den VU bekannt ist und insofern eine Änderung erfolgen muss. Als rechtliche Grundlage für das HIS wurde bisher auf eine sehr allgemein gehal-

tene Einwilligungserklärung zurückgegriffen, mit der zugleich die VN auf eine wenig transparente Weise über die Existenz dieses Systems hingewiesen wurden. Ein weiterer Hinweis auf das System erfolgte in einem Merkblatt, das den VN bei Vertragsschluss überreicht werden sollte.

Ziel des HIS ist es, Hinweise zu geben auf besondere Risiken im Fall des Vertragsschlusses sowie auf möglichen Versicherungsbetrug im Leistungsfall. Es geht also nicht darum, Versicherungsvertragsschlüsse im Fall einer Meldung zwingend auszuschließen, sondern lediglich eine Warnung zu geben, die eine besondere Prüfung zur Folge hat. Daher werden auch nicht nur objektivierte Risiken gemeldet, sondern v.a. betrugsgeneigte Auffälligkeiten. Soweit derartige Auffälligkeiten in Rede stehen, erfolgt eine Bewertung anhand spartenspezifischer Checklisten in den Sparten Kfz, Unfall, Sach, Transport und Haftpflicht der VU. Wird nach der Systematik der Checklisten eine Gesamtpunktzahl von 60 überschritten, erfolgt eine Einmeldung in das HIS. Die Punktevergabe ergibt sich ausschließlich aus Auffälligkeiten bei der Schadenregulierung. Die Bewertung erfolgt auf Grund der in der Schadenbearbeitung gewonnenen Erkenntnisse des jeweiligen Sachbearbeiters auf der Basis seines Erfahrungswissens unter Heranziehung der Punkteliste. Die Checklisten liegen den Datenschutzaufsichtsbehörden vor, werden ansonsten aber nicht veröffentlicht. Durch die Geheimhaltung sollen Hinweise vermieden werden, die Versicherungsbetrügern nutzen könnten. Der GDV gibt an, dass die Punktevergabe auf der Auswertung von Gerichtsurteilen erfolgte, die besondere Verdachtsmomente für betrügerisches Verhalten anerkannt hätten. Derartige mit Punktwerten versehene Sachverhalte können in einer Verbindung von VN und Geschädigten liegen, in unwahrscheinlichen Schadenabläufen, in typischen Vorgehensweisen bei Betrügen und Ähnlichem. Gemeldet wird nicht nur ein verdächtiger VN; gemeldet werden können auch Anspruchsteller, Zeugen, Fahrer und Halter oder sachbezogen z.B. auch Kfz. 60 Punkte und damit zwangsläufig eine Meldung hat ein nachgewiesener Versicherungsbetrug zur Folge.

In den Sparten Rechtsschutz und Leben gab und gibt es Besonderheiten. So wurde bei Rechtsschutz nicht nur im Fall des Betrugsverdachtes eine Meldung bei Kündigung vorgenommen, sondern auch, wenn innerhalb von zwölf Monaten zwei bzw. innerhalb von drei Jahren drei Versicherungsfälle anfielen. Diese Regelung knüpfte an die in den Allgemeinen Rechtsschutzversicherungsbedingung generell vorgesehene Kündigungsmöglichkeit des Versicherers im Schadenfall an. Als Schadenfall wurde und wird gemäß der Systematik der Versicherungsbedingungen nicht die tatsächliche Leistung gewertet, sondern schon eine verbindliche Deckungsanfrage, die zu einer Entscheidung des VU führt. Grundsätzlich. nicht relevant war und ist, dass ein geführtes Klageverfahren erfolgreich war, auch nicht, dass eine besondere Situation vorlag oder vorliegt, z.B. ein streitsüchtiger Nachbar, der zu einer verstärkten Inanspruchnahme von Versicherungsleistungen zwingt. Im Bereich Leben, bei dem eine anders gelagerte Ausgangssituation gegeben ist, zielt die Meldung in HIS darauf ab, besondere Risiken festzustellen, die mit einem Versicherungsvertrag nicht oder nicht in der üblichen Weise abgesichert werden können. Derartige Risiken können im Vorliegen einer Erschwernis aus medizinischen Gründen liegen, also im Vorliegen einer – möglicherweise bei Vertragsabschluss verschwiegenen – Vorerkrankung oder der Ausübung eines risikoreichen Berufs. Ein Meldegrund liegt auch im Überschreiten bestimmter Versicherungssummen bzw. Jahresrenten im Versicherungsfall, also z.B. von Pflegebedürftigkeit oder Berufsunfähigkeit. Gemeldet werden sowohl der VN wie auch die zu versichernde Person.

Der Ablauf des bisherigen HIS-Meldeverfahren ist wie folgt: Stellt ein Sachbearbeiter ein besonderes Risiko bzw. einen Verdachtsfall fest, so meldet er dies per File-Transfer, Post oder Fax an den GDV. Dies sollte zudem in der Fallakte dokumentiert werden. Der GDV wandelt dann mit Hilfe der Uniwagnis-Software I die Namens- und Identifizierungsdaten in einen sog. phonetischen Strukturcode um. Dieser Strukturcode erlaubt es nicht, ohne eine elektronische Auflösung auf die Einzelperson zurückzuschließen. Mit ihm führen unterschiedlich geschriebene aber gleich ausgesprochene Namen zu einer gleichen Codierung. Für die Dechiffrierung des Codes wird die Software Uniwagnis II verwendet. Erfolgt eine Anfrage zu einem besonderen VN, so kann über den Strukturcode ein einziger Treffer gemeldet werden. Regelmäßig wird aber eine Liste von Treffern angezeigt mit abnehmender Wahrscheinlichkeit, dass die Treffer mit der gesuchten Person identisch sind. Dieses Verfahren wurde in der Vergangenheit gewählt, um dem Datenschutzrecht Rechnung zu tragen: Man ging davon aus, dass durch die Codierung eine Anonymisierung erfolge, was aus Datenschutzsicht erwünscht sei. Tatsächlich aber diente und dient aber das Verfahren ausschließlich dazu, eindeutige eingemeldete VN mit solchen Menschen abzugleichen, zu denen eine Anfrage gestartet wird. Es geht also nicht um eine anonyme, sondern um eine personenbezogene bzw. personenbeziehbare Datenverarbeitung.

Die Meldungen werden monatlich vom GDV zusammengefasst und mit dem bisherigen Bestand auf eine CD gebrannt bzw. auf einem Datenträgerband aufgezeichnet und an sämtliche in der jeweiligen Sparte tätigen VU versandt. Ein Datensatz wird nach fünf Jahren nicht mehr auf die CD übernommen. Erweist sich eine Meldung als unberechtigt, so erfolgt keine weitere Aufnahme auf den Datenträger. In den Bereichen Rechtsschutz und Kfz erfolgt die Auslieferung im Zweiwochenrhytmus. Die VU spielen die Datenträger in ihre Unternehmens-Informationstechnik (IT) ein und stellen sie so den Sachbearbeitenden zum Abruf bereit. Genutzt werden jeweils die aktuellen Datensätze. Der Zugriff auf diese Datensätze erfolgt getrennt nach Sparten. Besteht eine Zuständigkeit eines Sachbearbeiters für mehrere Sparten, so kann ein Abruf auf all diese Spartendaten erfolgen. Die Abfrage soll vom Sachbearbeiter insbesondere im Leistungsfall erfolgen. Beim Rechtsschutz und bei Leben steht

dem gegenüber die Risikoprüfung beim Vertragsabschluss im Vordergrund. Über eine Warnmeldung soll eine versicherungstechnisch für notwendig angesehene Risikoprüfung ermöglicht werden. Konsequenz kann dabei durchaus auch sein, dass kein Versicherungsschutz angeboten werden kann oder aber nur unter risikoangemessenen, veränderten Rahmenbedingungen (z.B. Zuschlag, Selbstbehalt). Stellt der Sachbearbeiter bei einer Abfrage einen Treffer fest, so nimmt er mit dem einmeldenden VU händisch, i.d.R. telefonisch, Kontakt auf, um abzugleichen, ob es sich bei dem Strukturcode-Treffer tatsächlich um die identische Person handelt. Ist dies nicht der Fall, so soll ein weiterer Datenaustausch unterbleiben. Sind weitere Treffer auf der Liste, so wird bei diesen entspechend vorgegangen. Erweist sich, dass die gemeldete Person mit der identisch ist, zu der die Anfrage erfolgt, so tauschen sich die VU über die weiteren Einzelheiten des Falles aus, insbesondere über die Gründe der Einmeldung, um dem anfragenden Sachbearbeiter Hinweise zu vermitteln, ob für den Vertragsantrag bzw. den Leistungsantrag relevante Tatsache vorliegen. Eine revisionssichere Dokumentation des Austauschs, also des Identifikationsverfahrens und der Fallabklärung, war bisher nicht gewährleistet.

3. Erfahrungen und Kritik

Die Praxis des HIS hatte sich innerhalb der VU über die Jahre etabliert. Die Versicherten, der Verbraucherschutz und die öffentliche Meinung nahmen von HIS kaum Kenntnis. Allenfalls war etwas von der Existenz einer „schwarzen Liste“ bekannt, die aber bzgl. der tatsächlichen Funktionsweise eine Black Box blieb und über deren Auswirkungen nur spektuliert werden konnte. Erlebten Betroffene unerklärliche Vorgehensweisen der VU, so blieben diese ungeklärt.

Betroffen waren vom HIS in den Blütezeiten knapp 10 Mio. Fallmeldungen, also insgesamt mehrere Millionen Menschen. Im Folgenden werden die Zahl der Meldungen im Jahr 2006 dokumentiert. In den Folgejahren gingen die Fallzahlen wieder zurück, nicht zuletzt wegen der öffentlichen Kritik und der gesteigerten Transparenz des Verfahrens und dem bewussteren Umgang mit HIS in den VU:

Sparte	Zahl der Verträge insg.	Zahl der Versicherten (Meldeaufkommen pro Jahr)
Kfz	ca. 100 Mio.	ca. 1 Mio.
Unfall	ca. 30 Mio.	ca. 500
Rechtsschutz	ca. 20 Mio.	ca. 36.000
Sach	ca. 70 Mio.	ca. 2.000
Leben	ca. 90 Mio.	ca. 750.000
Transport	ca. 300.000	ca. 50
Haftpflicht	ca. 40 Mio.	ca. 15.000
Insgesamt		ca. 9,5 Mio.*

* Die Zahl der jährlichen Meldungen ist je nach Sparte sehr unterschiedlich. Der Gesamtumfang des HIS-Datenbestands pro Sparte ergibt sich durch die Summierung der jährlichen Meldungen aus den letzten fünf Jahren.

Nachdem die Datenschutzaufsichtsbehörden das Verfahren über mehr als 10 Jahre akzeptiert hatten, wurde die datenschutzrechtliche Kritik seit Beginn des 21. Jahrhunderts lauter. So wurde klargestellt, dass es sich bei dem phonetischen Strukturcodeverfahren natürlich um ein personenbezogenes Verfahren handelt, mit der Konsequenz, dass sämtliche Datenschutzvorschriften beachtet werden müssen. In Frage gestellt wurde weiterhin die Annahme einer Datenverarbeitung im Auftrag durch den GDV für die einmeldenden VU (§ 11 BDSG): Die Fiktion, der GDV nehme die Meldungen der VU im Auftrag der VU entgegen und leite die Datenbestände an die anderen VU weiter, entspricht insofern nicht der Wirklichkeit, als das Verfahren vom GDV dominiert wird. Zwar nimmt dieser keinen bzw. nur geringen inhaltlichen Einfluss auf die tatsächlich verarbeiteten Daten, doch liegt die Herrschaft hierüber nach erfolgter Einmeldung beim GDV. Gegen die Auftragsdatenverarbeitung spricht weiter die Vermischung sämtlicher Meldungen einer Sparte aller VU bundesweit auf einem Datenträger. Dies ist als Auftragsdatenverarbeitung nicht zulässig. Unzulässig ist auch die Übermittlung des Gesamtdatenbestands an die und die Speicherung bei den jeweiligen VU, ohne dass insofern dort eine Erforderlichkeit besteht. Es handelt sich insofern um eine typische Vorratserhebung und -speicherung.

Die bisher eingeholten Einwilligungen bei den VN erfüllen nicht die rechtlichen Voraussetzungen des § 4a BDSG: Sie sind nicht hinreichend bestimmt im Hinblick auf die Art der Daten, der verarbeitenden Stellen und der konkreten Zwecke. Es erfolgt keine hinreichende Transparenz über den Erklärungsinhalt. Die Erklärungen sind nicht freiwillig, da es im Fall einer Einwilligungsverweigerung i.d.R. keine Möglichkeit gibt, einen Versicherungsvertrag zu erhalten. Die Erklärung ist auch nicht hinreichend hervorgehoben und explizit. Auch in sonstiger Hinsicht bestanden Transparenzdefizite. So erfolgte zunächst überhaupt keine Benachrichtigung nach § 33 BDSG über die Einmeldung und die damit einhergehende Datenübermittlung an die anderen VU. Auch die Auskunftserteilung an die Betroffenen war nicht gewährleistet: Wendete sich ein Betroffener an den GDV, so sah sich dieser als Auftragsdatenverarbeiter nicht für zuständig an; wurde ein VU konkret angesprochen, so gab es - im besten Fall - nur Auskunft über die selbst eingespeicherten Daten, nicht über die per Strukturcode darüber hinausgehend vor Ort verfügbaren Datensätze.

Die Konstruktion von Auftragsverhältnissen hatte weiter zur Folge, dass kein einheitliches Vorgehen bei den VU gesichert war. Dies gilt für die Einmeldung, vor allem aber für den weiteren Umgang mit den per Datenträger vom GDV erhaltenen Datensätzen. Deren Speicherung, deren Abruf, die Weiterverarbeitung und schließlich die Einzelfallabklärung waren weder geregelt noch wurden diese Vorgänge re-

visionssicher dokumentiert. Nicht einmal eine für den Betroffenen negative Entscheidung auf der Basis der HIS-Daten wurde so dokumentiert, dass eine Rechtmäßigkeitskontrolle möglich gewesen wäre. Dies betrifft sowohl die Rechtskontrolle und Fachaufsicht innerhalb der VU; besonders gravierend ist die dadurch bestehende faktische Unmöglichkeit einer Kontrolle durch die Datenschutzaufsicht und durch die Betroffenen in gerichtlichen Verfahren.

Die Aufsichtsbehörden im DK erhoben zunächst die Fakten und stellten diese in Kooperation mit dem GDV und den VU in einem Text zusammen, der 2007 im Internet veröffentlicht wurde, so dass für die Betroffenen und den Verbraucherschutz ein Mindestmaß an Transparenz geschaffen wurde:

https://www.datenschutzzentrum.de/wirtschaft/20070703-his.htm

Schon zuvor - im Jahr 2005 - verständigten sich die AG und der DK darauf, dass das HIS als nicht mehr mit dem Datenschutzrecht in Einklang stehend angesehen wird und dass von der Branche grundlegende Änderungen vorgenommen werden müssen. Dies wurde nach einem gewissen Zögern vom GDV und einzelnen in die Diskussion einbezogenen VU akzeptiert. Für eine Übergangszeit wurde - zwecks Behebung der größten Missstände - verabredet, eine Benachrichtigung der in HIS eingemeldeten Dritten (2007) sowie aller neu Eingemeldeten (ab April 2009) vorzunehmen. Ebenfalls ab April 2009 erklärte sich der GDV bereit, Auskunftsersuchen von Betroffenen entgegen zu nehmen und dafür zu sorgen, dass den Betroffenen durch die VU eine umfassende Antwort erteilt wird. Auskünfte für die Einmeldungsgründe sowie Berichtigungs- und Löschungsansprüche müssen mit dem VU geklärt werden; der GDV wird insofern vermittelnd tätig. Geändert wurden außerdem die engen Voraussetzungen für eine Einmeldung in der Sparte Rechtsschutz.

4. Neukonzeption von HIS

Die Diskussionen mit den Aufsichtsbehörden führten dazu, dass sich der GDV und die ihm angeschlossenen VU daran machten, das HIS neu zu konzipieren. Es wurde Einvernehmen darüber hergestellt, dass eine Warndatei im Versicherungsbereich auf gesetzlicher Grundlage gemäß § 29 BDSG betrieben werden kann und soll. Dies bedeutet, dass ein Rückgriff auf fragwürdige Einwilligungen nicht nötig ist. Einvernehmen besteht auch darüber, dass die künftig als Online-Auskunftei zu betreibende Warndatei nicht mehr mit phonetischen Strukturcodes arbeiten soll, sondern mit Klarnamen und einer eindeutigen Identifizierung der Betroffenen. Die bisherige Spartentrennung soll beibehalten werden. Bei sog. harten Negativdaten, etwa bei der Verurteilung wegen Versicherungsbetrug, soll eine Einspeicherung unabhängig von der Sparte vorgenommen werden. Auch die Löschfrist von fünf Jahren soll im Grunde beibehalten werden, wobei jedoch im Bereich Leben an eine Verlängerung der Speicherfrist auf bis zu zehn Jahren gedacht wird.

Das bisherige HIS wird vom GDV betrieben. Der GDV meint, den zusätzlichen Anforderungen an eine Online-Auskunftei mit dem eigenen technischen und rechtlichen Know-how nicht gerecht werden zu können. Daher wurde eine Ausschreibung vorgenommen, an der sich die größeren Bonitäts-Auskunfteien beteiligten. Den Zuschlag erhielt schließlich die informa Unternehmensberatung GmbH, die ohnehin bisher das umfangreichste Angebot für Bonitätsprüfungen in der Versicherungswirtschaft realisiert. Informa soll als eigenständige verantwortliche Stelle agieren, die vom GDV lizensiert wird. Der GDV wird allerdings weiterhin eine zentrale Ordnungsfunktion für die Versicherungswirtschaft wahrnehmen. Auch wegen möglicher Interessenkonflikte ist die Lizenzvergabe an eine Auskunftei zu kritisieren: Da das informa-Unternehmen nicht nur als HIS-Betreiber, sondern auch in anderen Branchen tätig ist, besteht das Risiko einer zweckübergreifenden Datennutzung. Es ist allerdings festzuhalten, dass informa vertraglich zu einer strikten Datentrennung verpflichtet ist und zudem mit der informa Risk and Fraud Prevention GmbH eine eigenständige Gesellschaft gegründet hat, deren ausschließlicher Geschäftszweck der Betrieb des HIS sein wird.

Wegen kartellrechtlicher Vorgaben soll künftig zwischen Datenabfragen bei der Antrags- und der Leistungsprüfung zwischen einem A-Verfahren und einem B-Verfahren unterschieden werden. Bei der Antragsprüfung soll der direkte Kontakt zwischen zwei Versicherern vermieden werden. In den mit dem 60-Punkte-System arbeitenden Sparten sollen die Meldekriterien im Wesentlichen beibehalten werden. Der DK hat die Meldekriterien am 16. Oktober 2010 eingehend mit dem GDV diskutiert und diese im Grundsatz akzeptiert. Einzelne Nacharbeiten werden seitens des GDV aktuell noch vorgenommen.

Unstreitig ist, dass die Betroffenen gemäß § 33 BDSG von einer Einmeldung benachrichtigt werden müssen. Dadurch, dass die Auskunftei als verantwortliche Stelle i.S.d. BDSG handeln wird, ist auch klar, dass auf Anfrage an die Betroffenen eine direkte Auskunft erteilt werden muss. Das Grundkonzept von HIS soll sich insofern nicht ändern, dass ein Treffer in HIS nur als Warnhinweis gewertet werden soll. Während bei der Nutzung des HIS in der Antragsbearbeitung der Versicherer ein Austausch zwischen den Unternehmen nicht möglich ist, sondern dem System sämtliche verfügbaren Informationen entnommen werden sollen, kann in den Fällen der Schadenbearbeitung über die Auskunftei vermittelt, der Kontakt zum Vorversicherer aufgenommen werden. Dies wird als erforderlich angesehen, um bei Betrugsverdacht weitergehende Hintergrundinformationen zu vergleichbaren Tatmustern, Vorgehensweisen o.ä zu erhalten. Durch die dokumentierte Vermittlung der Kontaktaufnahme durch die Auskunftei soll der Gefahr eines unkontrollierbaren und übermäßigen Informationsaustauschs begegnet werden. Zudem haben DK und GDV vereinbart, dass ein Compliance-Leitfaden erstellt wird, der hier einen Rahmen setzt.

Noch nicht völlig geklärt ist, ob und inwieweit Gesundheitsdaten, die datenschutzrechtlich einem besonderen Regime unterworfen sind (§§ 3 Abs. 9, 28 Abs. 6-9 BDSG; § 203 StGB), im Bereich Leben gespeichert und beaus-

kunftet werden. Da insofern erneut auf eine Einwilligung zurückgegriffen werden müsste, soll davon möglichst Abstand genommen werden. Festgelegt werden muss schließlich, unter welchen Voraussetzungen ein berechtigtes Interesse für eine Auskunfteianfrage anerkannt wird, ob z.B. vor sämtlichen Vertragsschlüssen ein Abgleich zugelassen werden kann und unter welchen Voraussetzungen eine Anfrage im Leistungsfall als berechtigt anzusehen ist. Klärungsbedürftig ist schließlich, wie und mit welchen Inhalten Detailanfragen auf der Basis von HIS-Auskünften zwischen den VUs weiterhin akzeptiert werden können.

5. Perspektiven

Derzeit wird die technische Realisierung des neuen HIS vorbereitet. Gemäß den Angaben des GDV befindet man sich im Zeitplan, der Wirkbetrieb des neuen HIS soll danach im Frühjahr 2011 beginnen. Hierzu muss nicht nur die Auskunftei etabliert werden. Die Schnittstellen zu den VU müssen eingerichtet und die sich neu ergebenden Abläufe in den VUs müssen etabliert werden. Der Auskunfteibetreiber erarbeitet aktuell ein Feinkonzept, das mit der AG Versicherungswirtschaft des DK und am Besten zusätzlich auch mit den Verbraucherschutzverbänden abgestimmt werden sollte. In einem detaillierten Compliance-Leitfaden wird den Sachbearbeitenden in den VU eine Handhabe für den regelgerechten Einsatz des neuen HIS gegeben werden. Voraussichtlich sind weitere normative allgemeine Regelungen nötig, die in einer Verhaltensregel nach § 38a BDSG festgehalten werden kann. Dies gilt insbesondere für Abläufe, Dokumentationspflichten und die Qualität der Auskünfte für die VU.

Risikobewertung und Betrugsabwehr im Versicherungsbereich sind eine wirtschaftlich, datenschutzrechtlich und vertraglich bedeutsame Angelegenheit sowohl für das VU wie für den VN. Die Gefahr von Fehleinschätzungen ist hoch. Ebenso besteht die Gefahr unkalkulierbarer Risiken und hoher Zahlungsansprüche, die auch zu Lasten der Versichertengemeinschaft gehen. Die bisherige Wegstrecke weg vom alten HIS und hin zu einem geregelten Auskunfteiverfahren wurde bisher in einem weitgehend kooperativen Verfahren zwischen AG und GDV zurückgelegt. Die offenen Fragen sowie die weiteren Schritte werden absehbar zu weiteren Meinungsverschiedenheiten und Konflikten führen. Es ist zu hoffen, dass auch diese dialogisch gelöst werden können.

Dr. Birgit Schröder

Sozialdatenschutz in der privaten Krankenversicherung

Praktische Auswirkungen der Neuregelung am Beispiel des § 194 VVG aus anwaltlicher Sicht

Die Kombination von steigender Nachfrage nach medizinischen Leistungen infolge des demographischen Wandels und einem sich dynamisch entwickelnden medizinischen Fortschritt stellt auch das System der privaten Krankenversicherungen vor große Herausforderungen.

Die Versicherungsgesellschaften haben verschiedene Instrumente entwickelt, um die Ausgabenseite in den Griff zu bekommen und vermeintlich „unberechtigte“ Forderungen abzuwehren. Dabei wird zunehmend auch ein Preisdruck auf die Ärzte ausgeübt.

Die Neuregelung im Versicherungsvertragsgesetz (VVG) hat weitreichende Auswirkungen, nicht nur auf das Erstattungsverhalten privater Krankenversicherungen und wirft eine Vielzahl von Fragen auf.

Das Problem

Die Vergütung ambulanter ärztlicher Leistungen erfolgt nach dem Kostendeckungsprinzip. Das hat zur Folge, dass der Vertrag direkt zwischen Arzt und Patient zustande kommt. Der Arzt stellt seine Leistungen dem Patienten gegenüber in Rechung, die dieser begleicht und an seine private Krankenversicherung zur Erstattung einreicht. Kostenschuldner ist der Patient, d.h. eine fehlende und inkomplette Erstattung durch seine Versicherung befreit ihn nicht von seiner Zahlungsverpflichtung gegenüber dem Arzt[1].

Erfahrungen aus der anwaltlichen Praxis

Privat krankenversicherte Patienten erleben es immer häufiger, dass die Erstattung von Arztrechnungen nicht problemlos vonstatten geht.

Immer häufiger wird die medizinische Indikation einzelner Leistungen In Frage gestellt oder gebührenrechtliche „Nebenkriegsschauplätze“ eröffnet.

Patienten müssen trotz umfangreicher Begründung seitens des behandelnden Arztes immer häufiger klagen, um ihre Rechte durchzusetzen.

Dazu kommt, dass viele Gesellschaften von ihren Versicherten umfangreiche Schweigepflichtsentbindungserklärungen einfordern, die diese häufig bedenkenlos abgeben – befinden sie sich doch in dem Dilemma, dass sie aus dem Versicherungsvertrag auch Mitwirkungspflichten treffen.

Es werden immer weitergehende Schweigepflichtentbindungserklärungen seitens der Versicherer verlangt. Neu ist dabei vor allem, dass diese bereits vor Beginn einer Behandlung eingefordert werden. Dabei steht nicht mehr die Frage im Vordergrund, retrospektiv festzustellen, ob eine Behandlung den Vorschriften der Gebührenordnung der Ärzte/Zahnärzte entsprechend in Rechnung gestellt wurde. Ansatz der Versicherungsgesellschaften ist vielmehr, bereits zu Beginn einer geplanten Behandlung auch Einfluss auf die Art der Behandlung zu nehmen.

§ 194 VVG i.V.m. § 86 VVG

Die Novellierung des Versicherungsvertragsgesetzes sollte dem Versicherungskunden mehr Rechte einräumen und Verbraucherschutzgesichtspunkte umsetzen[2].

Als wesentliche Inhalte gelten: Gesamtreform des Versicherungsvertragsrechts: Verbesserung des Verbraucherschutzes, Stärkung des Versicherungsnehmers, Neuregelung der Beratungs-, Aufklärungs- und Informationspflichten der Versicherer, Neuregelung von Vertragslaufzeiten, Widerrufs-, Rücktritts- und Kündigungsrecht, Mindeststandards für Berufsunfähigkeitsversicherungen, Modernisierung des Rechts der Lebensversicherung unter Einbeziehung der Rechtsprechung des Bundesverfassungsgerichts und des Bundesgerichtshofs[3].

§ 194 VVG

Mit der Neuregelung des Versicherungsvertragsgesetzes (VVG), ursprünglich als verbraucherfreundlich gepriesen, werden die Rechte des privat krankenversicherten Patienten in einem Punkt massiv beschränkt[4]:

Die Regelung des § 194 VVG „Anzuwendende Vorschriften“ bestimmt wörtlich:

(2) Steht dem Versicherungsnehmer oder einer versicherten Person ein Anspruch auf Rückzahlung ohne rechtlichen Grund gezahlter Entgelte gegen den Erbringer von Leistungen zu, für die der Versicherer auf Grund des Versicherungsvertrags Erstattungsleistungen erbracht hat, ist § 86 Abs. 1 und 2 entsprechend anzuwenden.

In § 86 VVG „Übergang von Ersatzansprüchen“ heißt es:

(1) Steht dem Versicherungsnehmer ein Ersatzanspruch gegen einen Dritten zu, geht dieser Anspruch auf den Versicherer über, soweit der Versicherer den Schaden ersetzt. Der Übergang kann nicht zum Nachteil des Versicherungsnehmers geltend gemacht werden.

(2) Der Versicherungsnehmer hat seinen Ersatzanspruch oder ein zur Sicherung dieses Anspruchs dienendes Recht unter Beachtung der geltenden Form- und Fristvorschriften zu wahren und bei dessen Durchsetzung durch den Versicherer soweit erforderlich mitzuwirken. Verletzt der Versicherungsnehmer diese Obliegenheit vorsätzlich, ist der Versicherer zur Leistung insoweit nicht verpflichtet, als er infolgedessen keinen Ersatz von dem Dritten erlangen kann. Im Fall einer grob fahrlässigen Verletzung der Obliegenheit ist der Versicherer berechtigt, seine Leistung in einem der Schwere des Verschuldens des Versicherungsnehmers entsprechenden Verhältnis zu kürzen; die Beweislast für das Nichtvorliegen einer groben Fahrlässigkeit trägt der Versicherungsnehmer.

Bislang musste sich der private Krankenversicherer etwaige Rückforderungsansprüche seines Versicherungsnehmers abtreten lassen, wollte er vermeintlich zu viel gezahlte Beträge vom Arzt zurück verlangen[5]. Bei diesem Vorgehen hatte der Patient stets die Kontrolle. Es gab eine schriftliche Abtretungserklärung, die die notwendige Transparenz gewährleisten konnte.

Das bedeutet, dass die Abtretung im Belieben des Versicherten lag. Nach der Neufassung ist eine solche Abtretung zukünftig nicht mehr erforderlich; ein vermeintlicher Rückforderungsanspruch geht kraft Gesetzes auf den Versicherer über und zwar sobald der Versicherer an den Patienten erstattet. Anstelle des Vertrages ist nunmehr die cessio legis, also ein gesetzlicher Forderungsübergang, getreten.

Dadurch erübrigt sich auch das Vorgehen einiger Praxen, sich von den Patienten Abtretungsverbote unterzeichnen zu lassen, um Streitigkeiten bei liquidationsrechtlichen Fragen möglichst im Arzt-Patienten-Verhältnis klären zu können.

Letztlich wird durch diese neue Möglichkeit der Versicherungsgesellschaften das Gleichgewicht in der Beziehung zwischen Arzt und Patient empfindlich gestört[6]. In dem neu eingefügten § 192 Abs. 3 VVG räumt der Gesetzgeber den privaten Krankenversicherern weiterhin die Möglichkeit zusätzlicher Dienstleistungen ein, insbesondere die Beratung über Leistungen sowie über die Anbieter solcher Leistungen, die Beratung über die Berechtigung von Entgeltansprüchen der Erbringer von Leistungen, Abwehr unberechtigter Entgeltansprüche, die Unterstützung der versicherten Personen bei der Durchsetzung von Ansprüchen wegen fehlerhafter Erbringung der Leistungen und der sich hieraus ergebenden Folgen, die unmittelbare Abrechnung der Leistungen. Der Begriff „insbesondere“ legt dabei nahe, dass gerade keine abschließende Aufzählung gewollt war.

In der Stellungnahme der Bundesärztekammer, Stand 17.01.2007, zum Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Reform des Versicherungsvertragsrechts (VVR)[7], heißt es dazu wörtlich: „*Durch die in dieser Regelung beispielhaft aufgeführten „zusätzlichen Dienstleistungen“ des Versicherers wird der Eindruck erweckt, dass die private Krankenversicherung den Service für ihre Versicherten verbessern oder sogar zum Fürsprecher des privat Versicherten werde, um ihn bei der Auswahl der ärztlichen Behandlung und der Leistungserbringer vorgeblich uneigennützig zu unterstützen. Aus Sicht der Bundesärztekammer wird diese Vermengung von Interessen den heutigen, durch Kostendruck geprägten Rahmenbedingungen für die*

Privaten Krankenversicherungen nicht gerecht. Der vom Gesetzgeber intendierte Servicecharakter wird – aufgrund der mit diesen Leistungen beabsichtigten Kostensteuerung – mit hoher Wahrscheinlichkeit zu einer Gängelung und Drangsalierung des Privatpatienten führen. Der Gesetzesentwurf ist keinesfalls ein Beitrag zum Schutz des Versicherten."

Damit wird sehr deutlich, dass gerade kein Service für den Versicherten zu erwarten ist, sondern vielmehr nach Möglichkeiten gesucht werden wird, die neuen Instrumente unter Kostenaspekten auszunutzen. Im Vordergrund wird dabei immer das Bestreben der Versicherungsgesellschaft, also einem Wirtschaftsunternehmen, nach Gewinnmaximierung stehen. Die Einführung der Managed-Care-Systeme[8] werden dabei ebenfalls unter dem Aspekt der Kostenreduktion erörtert werden.

Um diesen „Service" bieten zu können, müssen dem Versicherer wiederum umfangreiche, höchst sensible medizinische Daten zur Verfügung gestellt werden. Mehr und mehr wird der Versicherungsnehmer so zum gläsernen Patienten.

Für den Arzt bedeutet dieses Vorgehen einen Eingriff in seine grundgesetzlich durch Artikel 12 geschützte Berufsfreiheit und für den Patienten einen solchen in sein allgemeines Persönlichkeitsrecht aus Artikel 2 in Verbindung mit Artikel 1 Grundgesetz.

Die Frage, welche sensiblen medizinischen Daten nunmehr bei dem Versicherer ankommen, kann der Patient nicht mehr beantworten und schon gar nicht beeinflussen. Dass die Versicherer zur erweiterten „Rechungsprüfung" diese Daten anfordern, erscheint logisch und nachvollziehbar. Ebenso wenig wie eine Versicherungsgesellschaft ihre Versicherten objektiv, also wertfrei, beraten kann, will und wird, ebenso wenig wird sie sensibel mit den neuen Möglichkeiten umgehen.

Weitreichende Folgen vor dem Hintergrund einer massiven Entwertung der ärztlichen Schweigepflicht sind die Konsequenz. Diese hat eine lange Tradition, Verstöße sind nach § 203 Strafgesetzbuch strafbewehrt, und stellen damit die Grundlage für die Arzt-Patientenbeziehung dar.

Hinsichtlich der Reichweite der ärztlichen Schweigepflicht ist anerkannt, dass Tatsachen und Umstände umfasst sind, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung der Patient ein bei Berücksichtigung seiner persönlichen Situation sachlich begründetes Interesse geltend machen kann[9] kann. Die Regelung ist im Übrigen auch unverhältnismäßig, da sie einseitig zu Gunsten der Versicherer ausgestaltet wurde.

Konkret bedeutet dieses, dass die Versicherer Fälle über Jahre sammeln können, um dann gegen einzelne Ärzte gerichtlich vorzugehen. Das bedeutet für den Arzt massive Rechtsunsicherheit, weil er immer damit rechnen muss, mit Klagen überzogen zu werden. Der Arzt ist diesem Vorgehen relativ schutzlos ausgesetzt, zumal er – gerade bei einer langen rechtlichen Auseinandersetzung – der wirtschaftlich schwächere ist.

Dazu kommt die anwaltliche Erfahrung, dass die – stets mit Hilfe von Sachverständigengutachten – zu klärenden gebührenrechtlichen oder dem zugrundeliegenden medizinischen Fragen in der Regel zu Gunsten der Ärzteschaft entschieden werden.

In der Praxis gibt es bereits eine Vielzahl von Fällen, in denen von dieser Regelung Gebrauch gemacht wurde. Die Folgen sind derzeit noch nicht absehbar, dürften aber vor allem das Verhältnis des Patienten zu seinem Arzt betreffen. Die weiteren Dienstleistungen des Versicherers werden ihr übriges dazu beitragen, dass die klare Trennung von Versicherungs- und Vertragsrecht schleichend aufgehoben werden wird. Damit ist durchaus zu befürchten, dass sich das System der privaten Krankenversicherung dem der gesetzlichen annähern wird. Dass dieses im Interesse der Versicherungsgesellschaften, geschweige denn ihrer Versicherungsnehmer ist, darf bezweifelt werden.

Ausblick

Damit bleibt festzuhalten, dass eine Vielzahl von Fragen aktuell noch offen ist: So ist beispielsweise unklar, wie es rechtlich zu würdigen ist, wenn die Versicherung eine Position für nicht oder nicht in der angegebenen Höhe für berechnungsfähig halte, der Patient aber dennoch in Kenntnis dieser Auffassung in voller Höhe an den Arzt zahlt.

Denkbar wäre, dieses als Anerkenntnis des Patienten zu werten. Ob die Versicherung sich dieses gegen sich geltend lassen muss, ist derzeit noch ungeklärt. Da Folge ein Ausschluss des Rückforderungsrechts wäre, dürfte die Versicherung an dieser Auslegung kein Interesse haben. Der zahlende Patient würde aber letztlich ein Anerkenntnis zu Lasten seines Versicherers abgeben.

Es könnte sich der Einwand treuwidrigen Verhaltens stellen, wenn ein Versicherer in Kenntnis der Nichtschuld leistet und später den geleisteten Betrag von dem Arzt wieder zurückfordert. § 242 BGB sieht vor, dass sich die Vertragspartner vor, während und nach Abwicklung eines Schuldverhältnisses an die Gebote der Verlässlichkeit, Rücksichtnahme und Loyalität halten[10]. Gegen diese Grundsätze würde dann aber verstoßen.

Es ist nachvollziehbar, dass nach Möglichkeiten gesucht wird, die Ausgabenseite auch in der privaten Krankenversicherung in den Griff zu bekommen. Der Ansatz, der gewählt wurde, unterstellt allerdings den Leistungserbringern stets eine fehlerhafte Abrechnung. Dieser „Generalverdacht" dürfte selbst dann nicht angemessen sein, wenn konstatiert wird, dass sich viele Praxen nur und allein über einen bestimmten Prozentsatz an Privatpatienten rechnen.

Es bleibt also festzuhalten, dass sich die als verbraucherfreundlich gepriesenen Vorschriften für die private Krankenversicherung als einseitig zu Gunsten der Versicherungsgesellschaften erweisen – und dieses auf Kosten der Versicherungsnehmer, der Leistungserbringer und zu Lasten einer effektiven Sozialdatenschutzes.

1 Zu daraus folgenden Problemen der Honorarausfälle für die Ärzteschaft, die entstehen, wenn Patienten nur den geminderten Betrag weiterreichen, sind nicht Gegenstand. Sie führen aber zu Überlegungen, ob der sich verschlechternden Zahlungsmoral nicht auch mit einer Behandlung nur

gegen Vorschuss zu begegnen ist, vgl. dazu Kern, GesR 2007, 241ff.

2 Zu Materialien vgl. Schimikowski/Höra. Das neue Versicherungsvertragsgesetz 2007; als Gegenüberstellung alter und neuer Rechtslage Staudinger/Kassing, Das neue VVG- Eine synoptische Gegenüberstellung mit der alten Gesetzeslage 2008.

3 DIP, Dokumentations- und Informationssystem für Parlamentarische Vorgänge, http://dipbt.bundestag.de/extrakt/ba/WP16/90/9011.html (Zugriff 13.01.2010).

4 Dieser Punkt wurde auf Anfrage der Verfasserin weder von dem Ombudsmann private Kranken- und Pflegeversiche-rung noch dem Ombuds-mann für Versicherungen auf Nach-frage der Verfasserin aufgegriffen.

5 Vgl. dazu Marlow/Spuhl, Das neue VVG kompakt 3.Auflage 2008 S.783.

6 Arnold, kfo.info 03/08 – Seite 60ff.

7 http://www.bundesaerztekammer.de/downloads/VVR.pdf, Zugriff 13.01.2009.

8 Zu grundsätzlichen Bedenken vgl. BÄK, http://www.bundes-aerztekammer.de/downloads/VVR.pdf, Zugriff 13.01.2009.

9 Zum schutzwürdigen Geheimhaltungsinteresse vgl. nur OLG Karlsruhe v. 11.08.2006, 14 U 45/04; zum generellen Umgang mit Anfragen aus dem Bereich der Versicherungswirtschaft vgl. Landesärztekammer Baden-Württemberg, Merkblatt Zusammenarbeit zwischen Arzt und Privatversicherungen. http://www.aerztekammer-bw.de/20/merkblaetter/umgangPV.pdf, Zugriff 13.01.2010.

10 Vgl. zu Einzelheiten Kern/Wadle/Schroeder/Katzenmeier, Die Generalklausel des § 242 BGB, 2006.

Spendenaufruf

Die DVD will in diesem Jahr die Demonstration „Freiheit statt Angst“ finanziell unterstützen. Dazu wird Ihre Hilfe gebraucht.

Seit einigen Jahren findet in Berlin Anfang September eine zentrale Kundgebung zur Unterstützung der Bürgerrechte, insbesondere der Freiheit auf Privatsphäre und gegen den Überwachungswahn statt. Wie alle Veranstaltungen kostet das Geld.

Jeder gespendete Euro wird von der DVD verdoppelt. Also bitte zögern Sie nicht und geben Sie Ihren Beitrag.

Es ist ganz einfach:

Überweisen Sie Ihren Betrag auf das Konto 59 4 59 5 02 bei der Postbank Köln (BLZ 370 100 50) bis spätestens zum 11. September 2010. Geben Sie als Verwendungszweck „Freiheit statt Angst 2010“ an. Wir garantieren, dass alle Spenden vollständig und ohne Abzug dieser Veranstaltung zugute kommen. Verspätete Zweckspenden werden natürlich auch noch ordnungsgemäß weitergegeben.

Helfen Sie mit!

Flagge zeigen gegen die Einschränkung von Freiheitsrechten.

Hajo Köppen

Wie man sich gegen Telefon-Abzocke wehren kann

„Sie haben ein Mercedes Benz Cabrio gewonnen….."

Am 26. März 2009 verabschiedete der Deutsche Bundestag das „Gesetz zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen“[1], das am 4. August 2009 in Kraft trat. Dieses sog. Artikelgesetz[2] hat bezüglich unerlaubter Telefonanrufe[3] zu folgenden Änderungen und Verschärfungen geführt:

• Verstöße gegen das sich aus dem „Gesetz gegen unlauteren Wettbewerb (UWG)“ bestehende Verbot der unerlaubten Telefonwerbung[4] können mit einem Geldbuße bis zu 50.000 Euro geahndet werden (§ 20 UWG)[5]. Durch die Gesetzesänderung wird eindeutig klargestellt, dass ein Werbeanruf nur zulässig ist, wenn der Angerufene vorher ausdrücklich erklärt hat, Werbeanrufe erhalten zu wollen. So ist dem Anrufer die Möglichkeit genommen, sich auf Zustimmungserklärungen zu berufen, die der Verbraucher in einem völlig anderen Zusammenhang oder nachträglich erteilt hat.

• Bei Werbeanrufen darf der Anrufer seine Rufnummer nicht mehr unterdrücken, um seine Identität zu verschleiern (§ 102 Abs. 2 TKG). Dadurch soll sichergestellt werden, dass unerwünschte Werbeanrufe zukünftig besser verfolgt werden können. Bei einem Verstoß gegen das Verbot der Rufnummernunterdrückung droht eine Geldbuße bis zu 10.000 Euro (§ 149 Abs. 1 Nr. 17c TKG).

Verbot von „cold calls“

Mit diesen Gesetzesänderungen hat der Gesetzgeber auf eine Reihe von Datenschutzskandalen im Zusammenhang mit dem Handel mit Telefonnummern reagiert und der Tatsache Rechnung getragen, dass Verbraucherinnen und Verbraucher sich zunehmend durch unerwünschte Werbeanrufe (auch als „cold calling“ oder „Kaltakquise“[6] bezeichnet) belästigt und in ihrer Privatsphäre gestört fühlen.[7] So ergab eine Umfrage der Gesellschaft für Sozialforschung und statistische Analysen mbH (forsa) 2007, dass 64 % der Befragten in den letzten Monaten vor der Befragung ohne Einwilligung von einem Unternehmen angerufen worden waren. 86 % fühlten sich durch unaufgeforderte Werbeanrufe belästigt und 49 % waren der Meinung, dass die Anzahl der Werbeanrufe in den letzten beiden Jahren zugenommen hat. Eine repräsentative Umfrage der Gesellschaft für Konsumforschung (GfK) kam zu dem Ergebnis, dass sich die Zahl unerbetener Werbeanrufe in den ersten drei Quartalen 2006 im Vergleich zum Vorjahr um 31,3 Prozent erhöhte. Allein im ersten Quartal 2006 erfasste die GfK 82,6 Millionen unaufgeforderte telefonische Werbekontakte, rund 900.000 Anrufe pro Tag. In der Statistik der GfK belegen Lotterien und Gewinnspiele den Spitzenplatz, gefolgt von der Telekommunikationsbranche. Die Verbraucherzentrale (vzbv) nannte in ihrem Jahresbericht 2006/2007 sogar eine Zahl von 300 Millionen unaufgeforderten Werbeanrufen.[8]

Im Oktober 2006 befasste sich der Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz des Deutschen Bundestages auf Antrag der Koalitionsfraktionen mit der Belästigung der Bürger durch cold calls[9] und sprach die Empfehlung an das Bundesministerium für Justiz aus, einen schriftlichen Bericht zu dem Thema zu erstellen.

Am 26. Juni 2007 legte das Bundesministerium für Justiz den „Bericht zum Thema ‚unerwünschte Werbeanrufe‘ – cold calling“ vor, in dem die Problemlage einführend wie folgt beschrieben wird: „Unerwünschte Telefonwerbung hat sich in der letzten Zeit zu einem für die Verbraucher erheblich belästigendem Problem entwickelt, bei dem in einigen Fällen sogar Grenzen zu strafrechtlich relevanten Verhalten (z.B. Betrug, Nötigung) überschritten werden dürften. Gesicherte Erkenntnisse über das genaue Ausmaß der Belästigung bestehen allerdings nicht. Eine von der Verbraucherzentrale Bundesverband (vzbv) im Januar vorgelegte Umfrage der Gesellschaft für Konsumforschung (GfK) über die Entwicklung der Werbeanrufe in Deutschland besagt, dass es in den ersten drei Quartalen 2006 generell zu einem Anstieg von Werbeanrufen um 31,3 % gekommen sei. Allerdings wurde bei dieser Umfrage nicht zwischen erlaubten und unerlaubten Werbeanrufen differenziert, so dass die Zahl nur begrenzt aussagefähig ist.“[10] In dem 27 Seiten umfassenden Bericht wird abschließend empfohlen: „Die Bundesregierung hält es unter Berücksichtigung der dargestellten Sach- und Rechtslage für geboten, einen Gesetzentwurf vorzulegen, der ein bußgeldbewehrtes Verbot der Rufnummernunterdrückung sowie eine Bußgeldbewehrung des bestehnden Verbots des § 7 Abs. 2. Nr. 2 UWG enthält. Die Regelung soll zunächst befristet eingeführt und innerhalb von zwei Jahren nach ihrem In-Kraft-Treten auf ihre generalpräventive Wirkung und tatsächliche Durchsetzbarkeit sowie etwaigen weitergehenden gewerbe- und zivilrechtlichen Handlungsbedarf hin evaluiert werden. Weiterhin wird sich die Bundesregierung an der notwendigen Verbraucherinformation beteiligen.“

Was tun gegen „cold calls“?

Es ist selten genug, dass die Rechtslage so eindeutig ist wie bei einem Werbeanruf, zu dem der Umworbene nicht vorher ausdrücklich seine Einwilligung gegeben hat. Wie aber stoppt man Unternehmen, die sich an die gesetzlichen Vorgaben nicht halten wollen? Das schnelle Auflegen des Telefonhörers bei lästigen Werbeanrufen mag kurzfristig Ruhe schaffen, vor zukünftigen Anrufen schützt das allerdings nicht. Und auch der Hinweis an dem Gesprächspartner irgendwo in einem Callcenter, er möge solche Anrufe zukünftig unterlassen, verhindert nicht zwingend einen weiteren Anruf. Was also tun als Verbraucher? Als Antwort auf diese Frage im folgenden die Schilderung eines „Selbstversuches“ am Beispiel von Anrufen mit Gewinnversprechungen.

„… Sie haben ein Mercedes Benz Cabrio gewonnen.“

Mir geht es zumindest so: abends um 21:45 h möchte ich nach einem Arbeitstag doch etwas Ruhe haben. Zumindest will ich nicht durch telefonische Werbe- und Gewinnversprechungen belästigt werden. Eigentlich möchte ich solche Anrufe überhaupt nicht erhalten. So auch am 12. Mai, als zu besagter Uhrzeit das Telefon klingelte und mir eine weibliche Stimme vom Band den „Gewinn eines Mercedes Benz Cabrio im Wert von 45.000,- € oder eines Geldpreises in vergleichbarer Höhe“ mitteilte. Und damit der Gewinnanspruch nicht verfällt, sollte ich unverzüglich unter 09005 673 400 in einem Call-Center anrufen und zur „Sicherung des Gewinns“ einen mitgeteilten „Veranstaltungscode“, bestehend aus einer vierstelligen Zahl, mitteilen. Dann wäre der Gewinn meiner. 3 Minuten und 27 Sekunden redete „Ihre Laura Stern“, so die Abschiedsworte, auf mich ein und legte mir mehrmals nahe, unverzüglich unter angegebener Telefonnummer anzurufen; sonst wäre der Gewinn futsch.

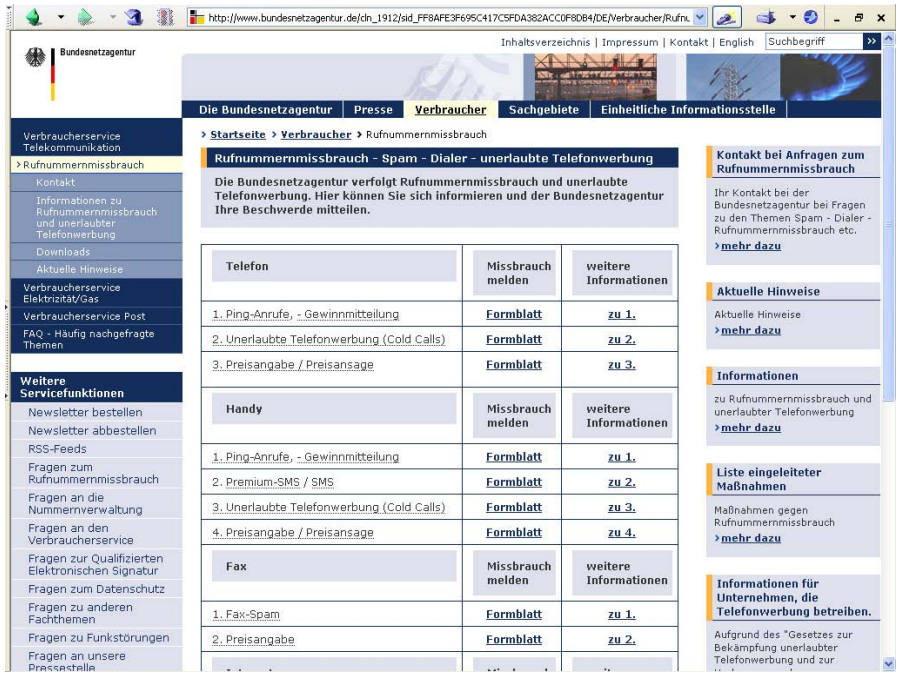
Es kann nur gehofft werden, dass die Zahl der Zurückrufenden möglichst klein ist. Denn zu gewinnen gibt es nichts; der Anrufende findet auf seiner Telefonrechnung für den Rückruf stattdessen die Gebühren für eine hochpreisige Telefonnummer.[11] Bei den Veranstaltern handelt es sich schlichtweg um Betrüger, die mit dieser Telefon-Abzocke das schnelle Geld machen wollen. Ich habe Laura Stern also nicht zurückgerufen. Stattdessen habe ich zwei Tage später am PC die Seite www.bundesnetzagentur.de aufgerufen. Dort finden sich unter der Rubrik >Rufnummernmissbrauch< mehrere Formulare im pdf-Format, mit denen man Ping-Anrufe[12], Gewinnmitteilungen und Cold-Calls melden kann. Es sind nur wenige Informationen in das Formular einzutragen. Dazu sollte man sich beim Anruf schon die wichtigsten Daten der Bandansage notieren: Tag, Uhrzeit und Dauer des Anrufs, die Rückrufnummer und die Kernpunkte der Telefonansage wie Gegenstand des Gewinns sowie den Namen des Anrufers. Zu dem Anruf von „Laura Stern“ füllte ich am 14. Mai das zweiseitige Formular „Mitteilung über den Erhalt unverlangter Werbung über Fax, Telefon und E-Mail“ aus und verschickte den unterschriebenen Ausdruck per Fax um 9:39 h an die Bundesnetzagentur. Ich war offensichtlich nicht der einzige „Gewinner“ eines Mercedes Benz Cabrio, der statt Laura Stern zurückzurufen sich direkt an die Bundesnetzagentur gewandt hatte.

Hilfe von der Bundesnetzagentur

Bereits am Nachmittag des gleichen Tages veröffentlichte die Bundesnetzagentur unter der Überschrift „Bundesnetzagentur greift bei neuer Welle unerlaubter Telefongewinnversprechungen durch[13]“ eine Pressemitteilung mit folgendem Wortlaut: „Die Bundesnetzagentur hat heute wegen unerlaubter telefonischer Gewinnversprechen die Abschaltung der Rufnummer (0)9005 673 400 eines Diensteanbieters aus Turin angeordnet. Damit hat sie umgehend auf Beschwerden von Verbrauchern reagiert, die ihr heute Vormittag bekannt wurden. In den unerlaubten Anrufen wurde den Betroffenen der Gewinn eines Mercedes Cabriolets bzw. von bis zu 45.000 Euro versprochen. Zum Abruf des vermeintlichen Gewinns forderte eine Frau Laura Stern die betroffenen Verbraucher auf, die hochpreisige Rufnummer zurückzurufen.

Zusätzlich hat die Bundesnetzagentur zu der missbräuchlich eingesetzten Rufnummer (0)9005 673 400 ein Rechnungslegungs- und Inkassierungsverbot für die Zeit ab dem 12. Mai 2010 erlassen. Den Netzbetreibern ist es danach untersagt, Entgelte für Anrufe auf diese Rufnummer ab dem 12. Mai 2010 in Rechnung zu stellen bzw. nach bereits erfolgter Rechnungslegung die Inkassierung dieser Forderungen zu betreiben.

Neben der bereits zum Einsatz gekommenen Rufnummer (0)9005 673 400 hat die Bundesnetzagentur



auch die Abschaltung aller weiteren (0)900er Rufnummern des Turiner Diensteanbieters verfügt. Durch die präventive Abschaltung dieser neun Rufnummern schiebt die Bundesnetzagentur bereits jetzt möglichen künftigen Wellen von Gewinnanrufen über diese Rufnummern einen Riegel vor. (…)“

Diese Pressemitteilung wurde am Tag darauf von der Presse unter Überschriften wie „Telefon-Abzocke gestoppt“[14] verarbeitet.

Die Bundesnetzagentur verfolgte die Angelegenheit weiter und reichte am 18.05.2010 in der Pressemitteilung „Bundesnetzagentur verhängt weitere Rechnungslegungs- und Inkassierungsverbote zu bereits abgeschalteten 0900er Rufnummern (Ergänzung zum Aktuellen Hinweis vom 14.05.2010)“ folgenden ergänzenden Hinweis nach: „Die Bundesnetzagentur hat heute ergänzend zu bereits am 14.05.2010 verhängten Maßnahmen zu neun weiteren 0900er Rufnummern die Rechnungslegung- und Inkassierung für die Zeit ab dem 12.05.2010 untersagt. Wie schon am 14.05.2010 berichtet, hatte die Bundesnetzagentur bereits zum vergangenen Wochenende die Abschaltung von zehn 0900er Rufnummern eines Turiner Diensteanbieters wegen unerlaubter telefonischer Versprechen des Gewinns eines Mercedes Cabriolets angeordnet. Dabei hatte die Bundesnetzagentur zu der Rufnummer (0)9005 673 400 zusätzlich ein Rechnungslegungs- und Inkassierungsverbot ausgesprochen. Mit der Untersagung der Rechnungslegung und Inkassierung auch für die verbleibenden neun 0900er Rufnummern des Turiner Unternehmens reagierte die Bundesnetzagentur umgehend auf neuerliche Verbraucherbeschwerden. Sie untersagt damit den Netzbetreibern, ab dem 12. Mai 2010 Entgelte für Anrufe auf diese Rufnummern in Rechnung zu stellen, entgegenzunehmen oder beizutreiben. Das Verbot gilt für folgende Rufnummern: (0)9005 673 100, (0)9005 673 200, (0)9005 673 500, (0)9005 673 510, (0)9005 673 678, (0)9005 890 940, (0)9005 890 955, (0)9005 890 960, (0)9005 890 970.“

Bereits im Februar war ich durch eine telefonische Gewinnversprechung belästigt worden. Auch in diesem Fall hatte die Bundesnetzagentur nach Meldungen von Verbrauchern schnell reagiert[15] und die Nummer (0)9005 080 400 und sechs weitere Nummern der Firma Y2M Media Ltd., Great Hampton Street 69, B186EW Birmingham, GB, gesperrt. Die hatte einen „neuwertigen BMW im Wert von 30.000 € oder Bargeld“ versprochen. Natürlich ist aus dem BMW nichts geworden. Und wenn mir demnächst ein Porsche angeboten wird, auch aus dem wird nichts werden. Aber ich will auch überhaupt keinen Porsche haben, genauso wenig wie betrügerische Telefon-Abzock-Versuche.

1 BGBl. I 2009, Seite 2413.

2 Als Artikelgesetz wird ein Gesetz bezeichnet, das gleichzeitig Vorschriften z.B. zu einer bestimmte Thematik in einer ganzen Reihe von Gesetzen ändert. Im vorliegenden Fall wurden Bestimmungen des Gesetzes gegen den unlauteren Wettbewerb (UWG), des Telekommunikationsgesetzes (TKG) und des Bürgerlichen Gesetzbuches (BGB) geändert.

3 Durch das Gesetz wurden darüber hinaus die Widerrufsrechte von Verbraucherinnen und Verbrauchern bei telefonischen Vertragsschlüssen erweitert, die hier aber nicht Gegenstand der Erörterung sind.

4 Gem. § 7 Abs. 2 Nr. 2 UWG liegt eine „unzumutbare Belästigung“ immer vor bei einer „Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung“. Fairerweise sollte man die im Gesetzestext folgende Einschränkung also zumindest erwähnen.

5 Zuständig für die Verhängung von Bußgeldern ist gem. § 20 Abs. 3 UWG i.V.m. 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn.

6 Unter „Kaltakquise“ wird die Erstansprache eines potenziellen Kunden verstanden, zu dem bisher keine Geschäftsbeziehung bestanden.

7 Nur am Rande hier der Hinweis, dass der Bundesgerichtshof bereits in seinem Urteil vom 19. Juni 1970, Aktz. I ZR 115/68 (abgedruckt in BGHZ 54, Seiten 188-193) festhielt: „Es verstößt gegen die guten Sitten des lauteren Wettbewerbs, unaufgefordert Inhaber von Fernsprechanschlüssen, zu denen bislang keine Beziehungen bestehen, in ihrem privaten Bereich anzurufen, um Geschäftsabschlüsse anzubahnen oder vorzubereiten, insbesondere um Waren oder sonstige Leistungen anzubieten.“

8 Siehe Verbraucherzentrale Bundesverband (vzbv) „Die Stimme der Verbraucher - Jahresbericht 2006/2007“, Seite 45, abrufbar unter: www.vzbv.de/mediapics/jahresbericht_2006_07_vzbv.pdf.

9 Vgl. Ausschussprotokoll Nr. 16/27, Seite 38-40.

10 Siehe „Bericht zum Thema unerwünschte Werbeanrufe – cold calling“, abrufbar unter: www.bmj.bund.de/enid/Verbraucherschutz/Unerwuenschte_Telefonwerbung_1cj.html.

11 Wenn eine (0)900er-Rufnummer angerufen wird, müssen die Brutto-Preise pro Minute bzw. je Nutzung angesagt werden. Die Preisansage muss kostenlos sein und spätestens drei Sekunden vor Beginn der Entgeltpflicht beendet sein. Mit der Preisansagepflicht wird sichergestellt, dass der Anrufer Zeit hat zu entscheiden, ob er den Dienst oder die Weiterleitung zu dem genannten Preis in Anspruch nehmen will. Die Verpflichtung erstreckt sich auch auf etwaige Tarifänderungen während der Verbindung, wobei die Ansage der Tarifänderung auch während der Inanspruchnahme des Dienstes erfolgen kann.

12 Um Ping-Anrufe handelt es sich, wenn das Telefon oder Handy nur einmal klingelt. Es erscheint eine Rufnummer im Display oder in der Anruferliste des Angerufenen, die den Verbraucher animieren soll, diese meist hochpreisige Rufnummer zurückzurufen; (gebräuchliche Rufnummernbereiche: 0137..., 0900..., 0180..., oder auch 5-stellige Kurzwahlrufnummern).

13 Vgl. Pressemitteilung „Bundesnetzagentur greift bei neuer Welle unerlaubter Telefongewinnversprechen durch“ vom 14.05.2010; abrufbar unter www.Bundesnetzagentur.de in der Rubrik „Presse“.

14 Vgl. Gießener Allgemeine vom 15.05.2010.

15 Vgl. Pressemitteilung „Bundesnetzagentur hat bei `Friedrich von Haber´ und `Carmen Götz´ durchgegriffen“ vom 25.02.2010; abrufbar unter www.Bundesnetzagentur.de in der Rubrik „Presse“.

transparenz . arbeit . kontrolle

FIfF DVD Deutsche Vereinigung für Datenschutz e. V.

Vom 5.–7.11.2010 werden FIfF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung) und DVD (Deutsche Vereinigung für Datenschutz) eine gemeinsame Jahrestagung mit dem Titel „transparenz.arbeit.kontrolle“ im Bürgerzentrum Alte Feuerwache in Köln veranstalten.

Die Datenschutzdiskussionen der letzten zwei Jahre haben gezeigt, dass es nicht nur den Datenhunger staatlicher Stellen zu begrenzen gilt. Auch die Begehrlichkeiten der Privatwirtschaft haben ein teilweise erschreckendes Ausmaß angenommen. In wirtschaftlich schwierigen Zeiten scheinen sich viele Unternehmen der Loyalität ihrer Beschäftigten durch besonders intensive Kontrolle versichern zu wollen. Dabei werden zunehmend Schamgrenzen überschritten – oft ohne jegliches Unrechtsbewusstsein. Automatisierte Kontrolle der Arbeitsleistung findet nicht nur durch eigens zu diesem Zweck gesammelte Daten statt. Bei Bedarf werden auch „Nebenprodukte“ wie Systemprotokolle und private E-Mails zweckentfremdet zur Leistungs- und Verhaltenskontrolle genutzt. Datenschutz wird in solcher Atmosphäre oft nur noch als lästige Behinderung empfunden. Wer es als normal ansieht, Krankenakten über seine Beschäftigten anzulegen, Umkleideräume mit Videokameras zu überwachen oder systematisch und in großem Stil E-Mails zu durchsuchen, hat ganz offensichtlich ein Problem mit seinem Grundrechtsverständnis. Dass derartige Ignoranz leider nicht nur seltene Einzelfälle betrifft, zeigen die Nominierungen für die BigBrotherAwards, die seit einigen Jahren immer dreistere Formen der Ausforschung durch Arbeitgeber offenbaren.

Wir wollen im Rahmen der Jahrestagung den Fragen nachgehen, welche Auswirkungen Überwachung auf Beschäftigte hat und wie sie das Arbeiten beeinflusst, welche technischen Unanständigkeiten heute zur Beschäftigtenüberwachung auf dem Markt angeboten werden, welche Zulässigkeitsgrenzen bei der Überwachung von Beschäftigten eingehalten werden müssen und wie man sich als Einzelner oder als Betriebs- oder Personalrat vor dem Einsatz unzulässiger Spionageprogramme schützen kann. Außerdem soll die aktuelle politische Lage in Bezug auf ein Arbeitnehmerdatenschutzgesetz erörtert werden.

Die Tagung beginnt am Freitag nachmittags mit zwei Hauptvorträgen und wird am Samstag nach einem weiteren Hauptvortrag mit vier parallelen Workshop-Sessions fortgesetzt. Eine Plenumsveranstaltung beendet die Tagung am Samstagnachmittag. Sonntags werden die Mitgliederversammlungen von FifF und DVD stattfinden.

Großdemonstration „Freiheit statt Angst“ 2010 in Berlin

Für Samstag, den 11.09.2010 ruft ein breites Bündnis im Rahmen eines internationalen Aktionstages dazu auf, für Bürgerrechte, Datenschutz und ein freies Internet auf die Straße zu gehen.

Der Erfolg der Massenverfassungsbeschwerde gegen die Vorratsdatenspeicherung in Deutschland setzte ein deutliches Zeichen für die Freiheit. Die Richtlinie zur Vorratsdatenspeicherung muss aber auch auf europäischer Ebene gekippt werden, um eine Neuauflage oder Wiedereinführung hierzulande zu verhindern.

Auch die Internetsperren konnten in Deutschland vorerst verhindert werden. Jedoch stieß die EU-Kommissarin Cecilia Malmström diese Debatte erneut an.

Aber auch am Arbeitsplatz, in Bildungsinstitutionen und im Privaten nimmt Überwachung weiter zu, wodurch die informationelle Selbstbestimmung zunehmend eingeschränkt wird. Beschäftigte werden in ihrem Arbeitsumfeld, teilweise auch bis in ihr Privatleben hinein überwacht. Zugleich registrieren, überwachen und kontrollieren uns staatliche Stellen bei immer mehr Gelegenheiten. Egal was wir tun, mit wem wir sprechen oder telefonieren, wohin wir uns bewegen oder fahren, mit wem wir befreundet sind, wofür wir uns interessieren, in welchen Gruppen wir uns engagieren - der „große Bruder“ Staat und die „kleinen Brüder und Schwestern“ aus der Wirtschaft wissen es immer genauer. Der Abbau an Privatsphäre und Vertraulichkeit gefährdet unsere demokratische Gesellschaft. Menschen, die sich ständig beobachtet und überwacht fühlen, können sich nicht unbefangen und mutig für ihre Rechte und eine gerechte Gesellschaft einsetzen, in Deutschland und weltweit.

Die zunehmende Vermischung der Kompetenzen von Polizei, Geheimdiensten und Militär sowie die Auslagerung hoheitlich staatlicher Gewalt an private Unternehmen baut Bürgerrechte kontinuierlich ab.

Vertrauliche Daten werden aber nicht nur im Namen der Bundesrepublik, sondern auch im Namen der Europäischen Union gesammelt. Im Aktionsplan zum sogenannten „Stockholmer Programm“ ist beispielsweise der massive Ausbau europäischer Sicherheitsarchitekturen, die Aufrüstung an den Außengrenzen Europas und eine äußerst bedenkliche Zusammenführung von EU-Datenbanken vorgesehen. Damit wird nicht nur das Recht auf informationelle Selbstbestimmung gefährdet, auch die Menschenrechte von Migrantinnen und Migranten werden beschnitten. Diese zweifelhafte Sicherheitsdoktrin lehnen wir ab und setzen uns daher für ein freies und lebenswertes Europa ein.

Eine freie und offene Gesellschaft kann nur durch die Gewährleistung von Privatsphäre, vertraulicher Kommunikation und einem zensurfreien Informationszugang Bestand haben. Privatsphäre ist ein wichtiger Teil unserer menschlichen Würde – und zwar in allen Lebensbereichen. Deshalb rufen wir dazu auf, sich an der Großdemonstration am 11. September 2010 in Berlin zu beteiligen.

Treffpunkt für die diesjährige Demonstration „Freiheit statt Angst 2010“ ist am Samstag, dem 11. September um 13.00 Uhr am Potsdamer Platz.

Gleichzeitig rufen wir weltweit alle Menschen dazu auf, sich am internationalen Aktionstag „Freedom not Fear“ zu beteiligen.

Informationen zur Demonstration, Organisation und Informationen und Möglichkeiten der Beteiligung unter www.FreiheitStattAngst.de

Unsere Forderungen:

1. Überwachung abbauen

- Keine Vorratsdatenspeicherung - weder auf nationaler, noch auf europäischer Ebene
- Abschaffung der verpflichtenden flächendeckenden Erhebung biometrischer Daten
- Keine RFID-Ausweisdokumente
- Schutz vor unnötiger Datensammlung und Bespitzelung am Arbeitsplatz
- Einführung eines Arbeitnehmerdatenschutzgesetzes
- Zeitgemäße Datenschutzgesetze
- Berücksichtigung des Datenschutzes bereits in der Konzeptionsphase aller öffentlichen eGovernment-Projekte
- Ersatzlose Abschaffung des Personenkennzeichens „Steuer-ID“
- Keine einheitliche Schülernummer (Schüler-ID/Schülerdatei)
- Konkrete Datenschutzrichtlinien für Hochschulen und andere Bildungseinrichtungen die den neuen Anforderungen gerecht werden

- Keine massenhafte zentrale Speicherung von persönlichen Arbeitnehmerdaten (ELENA)
- Keine systematische Überwachung des Zahlungsverkehrs oder sonstige Massendatenanalysen in der EU (z.B. SWIFT)
- Keinen Informationsaustausch sensibler Daten mit den USA und anderen Staaten ohne wirksamen Grundrechtsschutz
- Keine pauschale und ausufernde Registrierung aller Flug- und Schiffsreisenden (PNR-Daten)
- Keine automatisierte Kfz-Kennzeichenüberwachung und Standorterfassung oder Nutzung darauf aufbauender Technologien (z.B. Toll Collect)
- Abbau und stärkere Regulierung von Videoüberwachung und Verbot des Einsatzes von Verhaltenserkennungssystemen
- Keine heimliche Durchsuchung von Privatcomputern, weder online noch offline (z.B. Bundestrojaner)
- Keine Einführung der elektronischen Gesundheitskarte (eGK)
- Schaffung von Transparenz bezüglich des Austausches sensibler Daten durch europäische Polizeibehörden

2. Evaluierung der bestehenden Überwachungsbefugnisse

Wir fordern eine unabhängige Überprüfung aller bestehenden Überwachungsbefugnisse im Hinblick auf ihre Wirksamkeit, Verhältnismäßigkeit, Kosten, schädliche Nebenwirkungen und Alternativen. Insbesondere fordern wir das EU-Parlament dazu auf, bestehende und geplante europäischer Projekte zur inneren Sicherheit, welche die Grundrechte der Menschen in Europa einschränken, sofort zu überprüfen.

3. Moratorium für neue Überwachungsbefugnisse

Nach der inneren Aufrüstung der letzten Jahre fordern wir einen sofortigen Stopp neuer Gesetzesvorhaben auf dem Gebiet der inneren Sicherheit, wenn sie mit weiteren Grundrechtseingriffen verbunden sind.

4. Gewährleistung der Meinungsfreiheit und des freien Meinungs- und Informationsaustauschs über das Internet

- Verpflichtende gesetzliche Festschreibung von Netzneutralität
- Freies, ungefiltertes und unzensiertes Internet, in Deutschland und weltweit, ohne Sperrlisten oder Vorkontrollen - sei es von staatlicher Seite oder durch Internetprovider
- Keine Sperrungen von Internetanschlüssen („Three Strikes“)
- Verbot der Installation von Filterinfrastrukturen in die Infrastruktur des Internets
- Entfernung von Internet-Inhalten nur auf Anordnung unabhängiger und unparteiischer Richter mit Rechtsweggarantie
- Festschreibung eines globalen digitalen Grundrechtsschutzes als digitale Menschenrechts-Charta des 21. Jahrhunderts
- Einführung eines uneingeschränkten Zitierrechts für Multimedia-Inhalte, da dies unverzichtbar ist für öffentliche Debatten in Demokratien
- Schutz von Plattformen zur freien Meinungsäußerung im Internet (partizipatorische Websites, Foren, Kommentare in Blogs), die heute durch unzureichende Gesetze bedroht werden, welche Selbstzensur begünstigen

Weitere Informationen auf unseren Wikiseiten:

- Ablaufplan für den Demo-Tag
- Eine Liste der Rednerinnen und Redner sowie das Bühnenprogramm
- Pressemappe (PDF)
- Live-Streams
- Möglichkeiten, mitzuhelfen und zu bewerben (Infomaterial, Banner)
- Anreise und Übernachtung, Sonderzüge
- Updates zur Vorbereitung über Twitter
- Demo-Song und Demo-Videos

Es wird ein Demo-Büro in Berlin geben, das Presseanfragen bearbeitet und als Anlaufstelle für Aktivistinnen und Aktivisten fungiert:
Hessische Straße 10, 10115 Berlin
Tel: 030 / 577 09 151

Siehe auch: Kontaktformular, Pressekontakte

Spendenkonto: Humanistische Union, Kontonummer: 30 74 250, Bankleitzahl: 100 205 00 (Bank für Sozialwirtschaft), Verwendungszweck: „Demo Freiheit statt Angst“

Direkter Link zu dieser Seite:
http://www.FreiheitStattAngst.de
http://www.vorratsdatenspeicherung.de
http://www.bigbrotherawards.de

Gemeinsame Presseerklärung:

Eckpunkte eines Beschäftigtendatenschutzgesetzes

Bonn, 20.5.2010

Ende März hat Bundesinnenminister de Maizière Eckpunkte zur Neuregelung des Beschäftigtendatenschutzes im Bundesdatenschutzgesetz (BDSG) vorgelegt. Zudem kursieren verschiedene „inoffizielle“ Zwischenversionen eines bisher nicht veröffentlichten Referentenentwurfs. Angeblich soll der Entwurf noch vor der Sommerpause vom Kabinett verabschiedet werden. Der geplante Ablauf legt den Schluss nahe, dass die Bundesregierung eine öffentliche Diskussion über das geplante Gesetz vermeiden möchte.

Im Zentrum der Überlegungen des Bundesministeriums des Inneren (BMI) steht ganz offensichtlich nicht die Sicherung des allgemeinen Persönlichkeitsrechts von Beschäftigten, sondern das Ziel, Unternehmen eine Erlaubnis zur Nutzung von Beschäftigtendaten zu Korruptionsbekämpfung und Compliance-Überwachung zu verschaffen.

Dieser Ansatz ist falsch.

Zweck des Beschäftigtendatenschutzes muss es vielmehr sein, Beschäftigte vor der Verletzung ihres verfassungsmäßig garantierten informationellen Selbstbestimmungsrechts zu schützen. Die Vorfälle bei Lidl, Schlecker, Siemens, der Deutschen Bahn und der Telekom machen deutlich, dass es einer gesetzlichen Regelung dringend bedarf.

Ziel einer eigenständigen gesetzlichen Regelung muss es sein, für Arbeitgeber und Beschäftigte klare und möglichst verständliche Regelungen zu schaffen. Davon profitieren Beschäftigte und Arbeitgeber gleichermaßen: Ein eindeutiger Rechtsrahmen schafft Sicherheit bei der praktischen Umsetzung und für die Betroffenen.

Insbesondere sind folgende Vorgaben und Regelungen in einem modernen Beschäftigtendatenschutz unverzichtbar:

- Einwilligungen im Arbeitsverhältnis dürfen nur dann als Zulässigkeitsgrundlage gelten, wenn die Erteilung nachweisbar freiwillig und ohne Druck erfolgen kann und erfolgt ist.
- Datenerhebungen müssen immer beim Beschäftigten erfolgen. Unrechtmäßig erworbene Daten müssen einem Beweisverwertungsverbot unterliegen.
- Das Fragerecht des Arbeitgebers bei der Einstellung muss streng an der Bedeutung und Erforderlichkeit für die angestrebte Beschäftigung orientiert sein.
- Die „berechtigten Interessen“ des Arbeitgebers müssen in Bezug auf Vorhaben konzernweiter Verarbeitung von Beschäftigtendaten (z. B. Personaldatenverarbeitung in einer Konzernzentrale) gem. § 28 Abs. 1 Nr. 2 bzw. § 28 Abs. 2 Nr. 1 BDSG präzisiert und konkretisiert werden.
- Wenn der Arbeitgeber Beschäftigtendaten im Rahmen einer Auftragsdatenverarbeitung durch einen Dienstleister verarbeiten lässt, von dem er wirtschaftlich abhängt (z. B. die Konzernmutter), muss die gem. § 11 BDSG vorgesehene Kontrolle des Auftragnehmers mangels realer Durchsetzbarkeit durch eine externe, unabhängige Instanz ausgeübt werden.
- Es ist klarzustellen, dass der Arbeitgeber gegenüber seinen Beschäftigten kein Diensteanbieter im Sinne der Telekommunikationsgesetzgebung ist. Zum Schutz privater E-Mails müssen klare, dem Schutzniveau des Telekommunikationsgeheimnisses entsprechende Regeln definiert werden, die eine Einsichtnahme und Verwendung durch den Arbeitgeber ausschließen.
- Die Beobachtung und Überwachung von Beschäftigten mittels Video- oder Tonaufnahmen ist grundsätzlich zu untersagen. Der Schutz gilt am Arbeitsplatz und im privaten Umfeld gleichermaßen. Ausnahmen sind nur in streng begrenzten Gefährdungslagen zuzulassen.
- Verbote und Informationspflichten beim Umgang mit Beschäftigtendaten, die für den Arbeitgeber gelten, sind auch beim Einsatz externer Dienstleister einzuhalten.
- Die Auskunftspflicht des Arbeitgebers gegenüber den Beschäftigten bzgl. der über sie automatisiert verarbeiteten Daten ist so zu konkretisieren, dass eine wirksame Umsetzung garantiert ist.
- Ärztliche Untersuchungen dürfen nur angeordnet werden, wenn sie gesetzlich vorgeschrieben sind. Die ärztliche Schweigepflicht für Betriebsärzte darf nicht aufgeweicht werden.
- Die Arbeitnehmervertretung muss das Recht erhalten, im Namen von Beschäftigten in Datenschutzfragen zu klagen.
- Die Arbeitnehmervertretung ist an der Auswahl des betrieblichen oder behördlichen Datenschutzbeauftragten zu beteiligen.
- Die verbindlich bereitzustellende Arbeitskapazität und Ressourcen des betrieblichen oder behördlichen Datenschutzbeauftragten müssen systematisch an der Zahl der Beschäftigten orientiert sein.
- Die gesetzlichen Schutzvorgaben dürfen durch Betriebs- oder Dienstvereinbarungen nicht unterschritten werden.

Anmerkung:

Der Entwurf des BMI ist am 28.05.2010 erstmals veröffentlicht worden. Die DVD hat hierzu eine ausführliche Stellungnahme abgegeben,

erhältlich unter www. datenschutzverein.de/materialien.html (vgl. auch im Folgenden ausgedruckte PE).

Unterzeichner:

Klaus-Dieter Jansen und Friedrich Wicke-Gehrke, AOT Consulting GmbH, Dortmund

Beratung und Schulung über Informationstechnologie e.V. (BESIT e.V.), Nürnberg

BIT e.V. - Berufsforschungs- und Beratungsinstitut für interdisziplinäre Technikgestaltung, Bochum

Karl-Hermann Böker, Böker-Beratung, Bielefeld

Lothar Bräutigam, sovt, Darmstadt

Deutsche Vereinigung für Datenschutz e.V., Bonn

Reinhardt Diehl • Beratung, Kassel

Werner Alten, EFOB - Entwicklungsforschung und Beratung, München

FIfF - Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Bremen

Rena Tangens und padelun, FoeBuD e.V., Bielefeld

Forba Partnerschaft, Berlin

FORBIT - Forschungs- und Beratungsgesellschaft Informationstechnologie mbH

Alvar C. H. Freude, Stuttgart, FITUG e. V.

P. Herholtz, Berater, Hamburg

Werner Hülsmann, Konstanz

Bernd Zimmermann, NIM - Netzwerk Innovative Mitbestimmung, Gelsenkirchen

Rolf-Christian Otto, Fachanwalt für Arbeitsrecht, Kassel

Sylvia Wetke und Marianne Djavadi, tbo-Beratung, Hannover

Technik und Leben e.V., Bonn

TEMPI GmbH, Bielefeld

Dr.-Ing. K. Meyer-Degenhardt, Fachbereich Mathematik und Informatik, Universität Bremen

WSO – WickeSchwitalla-Organisationsberatung, Dortmund

Redaktion „Die ZeitSchrift“, Bielefeld

Friedrich-Karl Beckmann für den Konzernbetriebsrat der Philips Deutschland GmbH

Presseerklärung:

Harsche Kritik am Gesetzentwurf für Arbeitnehmerdatenschutzgesetz

Bonn, 22.06.2010

Das Bundesministerium des Innern hat am 28.05.2010 einen Entwurf für ein Gesetz zur Regelung des Beschäftigtendatenschutzes vorgelegt. Zwölf neue Paragrafen im Bundesdatenschutzgesetz sollen die Verarbeitung der Daten von Angestellten, Arbeitern und sonstigen Beschäftigten durch die Arbeitgeber regeln. Zu dem Gesetzesentwurf erklärt die Deutsche Vereinigung für Datenschutz e.V. Bonn:

Die Forderung nach einem Arbeitnehmerdatenschutzgesetz wird seit Jahren von Fachleuten und von Gewerkschaften erhoben. Dieser Gesetzentwurf aber schadet mehr als er nützt. Einem großen Regulierungsaufwand mit langen und verschachtelten Vorschriften steht kein Zugewinn für den Arbeitnehmerdatenschutz gegenüber. So besteht kein Bedürfnis nach den Gesetzesbestimmungen über das Fragerecht des Arbeitgebers gegenüber Stellenbewerbern, weil dieses in einer jahrzehntelangen Rechtsprechung zufrieden stellend und praxisnah geregelt worden ist. Sensible Fragen, wie etwa die Überwachung und Auswertung von dienstlichen Telefongesprächen, werden einseitig zu Lasten des Datenschutzes der Arbeitnehmer gelöst. So sollen beispielsweise auch das heimliche Mithören von Telefongesprächen und sogar die Auswertung privater E-Mails von Arbeitnehmern erlaubt werden. Damit würde der Datenschutz im Beschäftigungsverhältnis nicht gestärkt, sondern im Gegenteil deutlich beschnitten werden. Dass Datenschutzverstöße spürbare Folgen für die Arbeitgeber haben sollen, sieht auch der nun vorgelegt Gesetzentwurf nicht vor.

Zusammenfassend bemerkt Sönke Hilbrans, Vorsitzender der Deutschen Vereinigung für Datenschutz:

„Der Gesetzesentwurf aus dem Bundesinnenministerium ist kein Gesetzesentwurf zum Schutz von Beschäftigtendaten, sondern ähnelt eher einem Polizeigesetz. Datenschutzskandale lassen sich so nicht verhindern, sondern allenfalls legalisieren.“

„Der Gesetzentwurf enttäuscht auf ganzer Linie“, bedauert auch das DVD-Vorstandsmitglied Sören Jungjohann. „Das Bundesinnenministerium hatte die Möglichkeit, den Beschäftigtendatenschutz in Deutschland praktikabel und zukunftsorientiert zu regeln. Leider wurde diese Chance vertan.“

Die Deutsche Vereinigung für Datenschutz hat sich zu dem Gesetzentwurf in einer ausführlichen Stellungnahme geäußert. Diese Stellungnahme und den Referentenentwurf vom 28.05.2010 finden Sie auf der Website der DVD unter

http://www.datenschutzverein.de/materialien.html

Cartoon

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund

Bundesratsinitiative gegen Internet-Straßenansichten

Die schwarz-grün (-gelb) regierten Bundesländer Hamburg und Saarland haben im Streit um Googles Straßenansichtsdienst Street View eine Bundesratsinitiative für eine Änderung des Bundesdatenschutzgesetzes (BDSG) eingebracht (Bundesrats-Drucksache 259/10 vom 28.04.2010). Der Gesetzentwurf sieht vor, Gesichter und Kfz-Kennzeichen unkenntlich zu machen, bevor Daten ins Netz gestellt werden. Abgebildete Menschen sollen ein uneingeschränktes Widerspruchsrecht erhalten. Gleiches soll für Hausbesitzer und deren Mieter gelten, die gegen die Abbildung ihrer Wohnhäuser im Netz sind. Damit würden die Kriterien der deutschen Datenschutzaufsichtsbehörden, des sog. Düsseldorfer Kreises, für gesetzlich verbindlich erklärt. Der Gesetzesantrag wurde zur Beratung in die Ausschüsse des Bundesrates verwiesen.

Das Vorhaben stößt beim Branchenverband Bitkom, so bei dessen Präsident August-Wilhelm Scheer, auf Kritik. „Der Entwurf ist vor allem eines: politischer Aktionismus." Das Vorhaben richte sich auch gegen Anbieter von Navigationsdaten für Autos, Satellitenbildern oder Luftaufnahmen. Der Gesetzentwurf sei unnötig. Schon heute mache Google Street View Gesichter und Nummernschilder unkenntlich. Jeder könne auch der Abbildung seines Wohnhauses widersprechen. Hamburgs Justizsenator Till Steffen (GAL) meinte dagegen, die Selbstverpflichtung, die Google sich auferlegt habe, reiche nicht aus. Es sei offen, ob Google sie in allen Punkten beachten werde. Zudem beziehe sich der Entwurf auf alle Anbieter mit ähnlichen Angeboten. „Wir brauchen hier eine faire Regelung, gleiche Regeln für alle Wettbewerber in diesem heiß umkämpften Markt." Der Bürger müsse selbst entscheiden können, ob er an Diensten wie Google Street View teilnehmen wolle oder nicht. Google filmt seit mehr als einem Jahr für Google Street View bundesweit Häuser und Straßen ab (DANA 2/2008, 121). Ursprünglich wollte Justizsenator Steffen nach eigenen Angaben warten, bis Bundesverbraucherministerin Ilse Aigner (CSU) ihren versprochenen Gesetzentwurf zu dem Thema vorlegt. Weil sich dann aber nichts getan habe, ergreife Hamburg die Initiative (www.heise.de 07.05.2010; PM Justizbehörde Hamburg 24.04.2010).

Bund

ZKA warnt vor Sofortüberweisung.de

Der Zentrale Kreditausschuss (ZKA), eine Einrichtigung der deutschen Kreditinstitute, warnte vor dem Online-Bezahldienst sofortüberweisung.de. Er wies darauf hin, dass die KundInnen einer Bank mit der Nutzung des Dienstes gegen die Geschäftsbedingungen ihrer Bank verstoßen. Bei Bezahlung mit sofortüberweisung.de werden die vertraulichen Bezahldaten (PIN und TAN) nicht auf den Seiten der eigenen Bank eingegeben, sondern in ein Formular des Bezahldienstes, der sie zur Bank weiterleitet. Derart können die Daten über den Bezahldienst ausgespäht werden. Zwar seien bei dem seit drei Jahren arbeitenden Dienst bisher keine Missbrauchsfälle bekannt geworden. Gemäß Eigenangaben kann damit bei ca. 10.000 Unternehmen bezahlt werden, u.a. bei Dell, Conrad und der Fluglinie KLM. Der kostenlose Dienst funktioniert mit Konten fast jeder Bank. Riskant für die KundInnen, die immer mehr diesen Dienst nutzen, ist aber die Haftung. Diesen droht im Missbrauchsfall, auf den Schäden sitzen zu bleiben. Nach einem ähnlichen Prinzip funktioniert seit Jahren auch der Bezahldienst der Telekom „t-pay online Überweisung" (Finanztest 3/2010, S. 8).

Bund

Datenpanne bei Arcor

Rund 200.000 vertrauliche Kundendatensätze des inzwischen mit Vodafone verschmolzenen Telekommunikations-(TK-) Unternehmens Arcor und weiterer Firmen sollen über Callcenter-Betreiber auf dem Schwarzmarkt gelandet sein. Entsprechende Ermittlungen gibt es offenbar bei der Staatsanwaltschaft Bonn. Datenlecks gab es demnach auch beim Kabelnetz-Betreiber Unitymedia. Ein Sprecher von Vodafone teilte mit, die Daten stammten aus dem Jahr 2000 und seien somit allein von KundInnen der damals selbständigen Arcor (SZ 16.03.2010, 19).

Bund

Anstieg bei Privatauskünften an Geheimdienste

Die deutschen Geheimdienste haben 2008 insgesamt 64 Mal bei Banken, Fluglinien und Telekommunikations-(TK-) Unternehmen Auskunft über Verbindungsdaten oder Kontoinhabende verlangt. Dies ist im Vergleich zum Vorjahr eine deutliche Steigerung. 2007 hatte es insgesamt 43 Fälle gegeben. Bei 52 Maßnahmen und 150 Betroffenen im Jahr 2008 wurden TK-Verbindungen abgefragt. Die meisten Abfragen kamen - wie im Vorjahr - vom Bundesamt für Verfassungsschutz (SZ 19.02.2010, 6).

Bund

BND aktiv gegen Enthüllungen über Stasi

Der Bundesnachrichtendienst (BND) hatte offensichtlich das Bonner Kanzleramt 1990 aufgefordert, die Bürgerkomitees und Runden Tische in der Noch-DDR aufzulösen bzw. auflösen zu lassen und weitere Stasi-Enthüllungen zu verhindern. Die neuen, stark basisdemokratisch geprägten Gremien der vor der Wiedervereinigung stehenden DDR mit KirchenleutenBürgerrechtlerInnen und ehemals politisch Verfolgten wurden vom BND als „Störfaktor“ bezeichnet. Am 02.04.1990, also zwei Wochen nach der ersten freien Volkskammerwahl der DDR, wurde der Vizepräsident des BND Paul Münstermann von der Regierung Kohl um eine Einschätzung der Lage gebeten. Münstermann soll dazu geraten haben, die allzu eigenwillig agierenden Bürgergremien aufzulösen, da sie den geordneten Prozess der Wiedervereinigung störten - auch indem sie auf Stasi-Aufklärung in Parlamenten und Parteien drängten: „Sie sind die Hauptinitiatoren für Beschuldigungen hinsichtlich MfS-Kontakten von Volkskammerabgeordneten. Wenn die neue (DDR-) Regierung handlungsfähig bleiben will, muss sie unverzüglich die Aktivitäten dieser Gremien beenden.“ Der DDR-Innenminister Peter-Michael Distel (CDU) wickelte dann unter den Augen der Bonner Regierung, der die schnelle Vereinigung wichtiger war als die Aufarbeitung, mit Hunderten von Ex-Stasi-Offizieren den Geheimdienst der DDR ab (SZ 16.04.2010, 5).

Bund

Mit dem Ein-Cent-Trick an Kontodaten

Betrüger machen sich - gemäß einer Warnung des Verbraucherschutzministeriums des Bundes - die Neuregelung vom Oktober 2009 zunutze, wonach Banken nicht mehr verpflichtet sind zu prüfen, ob Kontonummern und Name eines Empfängers übereinstimmen. Sie tragen in Überweisungsformularen beliebige Zahlenreihen ein und denken sich Phantasienamen aus. Die Neuregelung basiert auf einer EU-Richtlinie, die den Geldverkehr in der EU beschleunigen soll. Banken sollen nicht mehr davon profitieren, dass sie sich Zeit lassen beim Ausführen von Aufträgen. Ab 2012 müssen alle Zahlungen grds. bis zum Ende des folgenden Geschäftstages abgewikkelt sein. Dies ist angeblich nur möglich, indem das Überweisungsverfahren vollautomatisiert abgewickelt wird. Dabei wird die Kontonummer maschinell gelesen, egal, ob der Name passt oder nicht. Wird eine 1-Cent-Überweisung nicht als Fehlbuchung zurückgewiesen, so wissen die Betrüger, dass das Konto besteht. Sie behaupten dann gegenüber der Bank, das Recht zu haben, per Lastschrift Beträge von dem fremden Konto einzuziehen. Ob sie das tatsächlich dürfen, prüft die Bank nicht. In der Folge buchen sie von dem fremden Konto einen Betrag ab, der nicht so groß ist, dass es auffällt, aber auch nicht zu wenig, damit es sich „lohnt“. Die KundInnen müssen innerhalb von sechs Wochen Widerspruch einlegen, sonst laufen sie Gefahr, das abgebuchte Geld nicht zurückzubekommen. Gemäß den Angaben des Verbraucherministeriums können im Fall von Betrug Widersprüche innerhalb von 13 Monaten durchgesetzt werden. Die parlamentarische Staatssekretärin Julia Klöckner empfiehlt den Kontobesitzenden dringend, regelmäßig ihre Kontoauszüge zu prüfen. Allerdings hat nicht jede 1-Cent-Überweisung einen kriminellen Hintergrund: Hilfsorganisationen und Online-Zahldienste nutzen die Methode auch, um die Identität eines Spenders oder Kunden zu prüfen (Kuhr SZ 01.03.2010, 1; Der Spiegel 9/2010, 16).

Bund

Bahn beruft neuen Datenschutz-Beirat

Ein prominent besetzter Datenschutz-Beirat soll der Deutschen Bahn AG helfen, die Einhaltung des Datenschutzes im Staatskonzern zu verwirklichen. Der Beirat wird nun vom Vorsitzenden der Bahngewerkschaft GDBA Klaus-Dieter Hommel geleitet. Der Beirat trifft sich etwa viermal im Jahr und berät über den korrekten Umgang mit KundInnen- und MitarbeiterInnendaten. 1/3 der zwölf Mitglieder vertreten die Arbeitnehmerschaft, darunter Betriebsratschef Günter Kirchheim und die Vorstände der Gewerkschaften Transnet und GDL, Reiner Bieck und Norbert Quitter. Weiterhin sitzen darin die Professoren Peter Wedde, Peter Gola und Jürgen Taeger sowie der Vorsitzende des Fahrgastverbands Karl-Peter Naumann, die Vorsitzende von Transparency International Deutschland Sylvia Schenk und die ehemalige Bundesjustizministerin Herta Däubler-Gmelin (SPD). Letztere war als Anwältin an der Aufklärung des Datenskandals bei der Bahn 2008/2009 maßgeblich beteiligt, der zur Demission des langjährigen Bahnchefs Hartmut Mehdorn und des halben Vorstandes führte (vgl. DANA 1/2009, 20; 3/2009, 109; 4/2009, 153). Bahnvorstand Gerd Becht erklärte die Datenaffäre für aufgeklärt: „Die Konsequenzen wurden gezogen“. Zahlreiche Verantwortliche hätten den Konzern verlassen müssen. Es gebe neue, strengere Vorgaben für den Schutz von Mitarbeiter- und Kundendaten. Damit habe die neue Bahnspitze „ihr Versprechen zur Aufklärung erfüllt“. Der Ablauf interner Ermittlungen bei Korruptionsverdacht sei völlig neu geregelt worden. Es gebe keine Grauzonen mehr. Die Datenschutzabteilung sei stark ausgebaut worden. Im zentralen Datenschutz hat der Konzern die MitarbeiterInnenzahl auf 50 verzehnfacht; hinzu kommen 80 DatenschutzkoordinatorInnen in den Tochtergesellschaften. Es gebe eine wegweisende Vereinbarung zum Arbeitnehmer-Datenschutz. (FR 04.05.2010, 16).

Bund

US-Schnellrestaurants spionieren Franchisenehmer aus

Zahlreiche Betreiber von McDonalds-Restaurants fühlen sich, so der Münchner Rechtsanwalt Horst Beck, von der Geschäftsleitung ausspioniert und unter Druck gesetzt und „systematisch herausgedrängt“. Allein Becker

hat in den vergangen Jahren zwei Dutzend solcher McDonalds-Partner vertreten. Die Vorwürfe gehen von der Manipulation von Restaurantkontrollen über Schikanen bis zum gezieltem Bespitzeln. Auf missliebige Filialisten wurden vom Konzern Detektive angesetzt; die Staatsanwaltschaft München ermittelt. Hintergrund scheint eine Strategie der Marktbereinigung durch McDonalds zu sein, die über außerordentliche Kündigungen durchgesetzt werden soll. Als Marktleiter Süd des McDonalds-Konzern ist in Bayern ein Mann eingesetzt, der schon als Koch bei der Nationalen Volksarmee ab 1980 Kameraden für die DDR-Stasi ausspioniert haben soll unter dem Pseudonym „Goulaschkanone“ bzw. als IM „Roland“. McDonalds, das von der Spitzeltätigkeit seines Mitarbeiters Kenntnis hatte, prüfte die Akten und stellte fest, dass die Stasi-Tätigkeit für die neue Beschäftigung kein Problem sei. Dieser schickt Kontrolleure, intern „Field Consultants“ genannt in die McDonalds-Filialen, um zu prüfen, ob Konzernvorgaben beachtet würden. Auf den Restaurantbetreiber Ulrich Enzinger in Lindau am Bodensee wurde als Spitzel eine Mitarbeiterin Enzingers auf einer McDonalds-Kreuzfahrt angeheuert, die Material sammelte, das später in der Auseinandersetzung um die Vertragsauflösung genutzt wurde. In einem anderen Fall hatte ein Field Consultant eine Mitarbeiterin in ein Café geladen, um über Karrierechancen zu reden und sie dann aufzufordern, ihren Chef auszuspionieren. Nach manipulierten Kontrollen prüfte der ins Visier geratene Restaurant-Betreiber die Kontrolleure bei Kontrollen mit der Videokamera, was dann aber McDonalds „wegen der „Verletzung der Persönlichkeitsrechte“ gerichtlich verbieten lassen wollte. Inzwischen hat dieser Betreiber eine außerordentliche Kündigung erhalten. Angesprochen durch die Presse räumte McDonalds-Deutschland-Chef Bane Knezevic Fehler ein. Dass Detektive auf einen Franchise-Nehmer angesetzt wurden, sei ein „absoluter Einzelfall“ gewesen, „von dem ich erst im Nachhinein erfahren habe“. Den Vorwurf der Manipulation von Prüfergebnissen wies Knezevic mit dem Hinweis zurück, es habe sich bei diesen Beschwerden „um Probleme bei der Kommunikation und nicht um vorsätzliche Manipulation“ gehandelt.

Parallel dazu wurde bekannt, dass McDonalds und auch die Schnellrestaurantkette Subway von ihren Franchise-Nehmern tiefe Einblicke in die Intimsphäre und die politische Gesinnung verlangen. Wer Partner bei Subway werden möchte, muss der Erstellung eines Prüfberichts „im Einklang mit den Anti-Terror-Gesetzen“ zustimmen. Dieser Report soll Informationen über „Charakter“, „Lebensweise“ und „Beziehungen“ enthalten. Die Bewerbenden sollen Auskunft erteilen, ob sie „jemals direkt oder indirekt an terroristischen Aktivitäten beteiligt“ gewesen seien. McDonalds forderte von potenziellen Franchise-Nehmenden Angaben über nichteheliche Beziehungen, „körperliche Leiden“ sowie über „Datum und Anlass der letzten ärztlichen Untersuchung“. Moritz Karg vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein hält die Praxis der amerikanischen Konzerne für unzulässig. McDonalds teilte mit, die Erfassung diene „der grundlegenden Beurteilung und Dokumentation, ob ein Bewerber für so eine weitreichende Geschäftsbeziehung wie einen Franchisevertrag in Betracht kommt“. Auf weitere Nachfrage teilte McDonalds mit: „Uns ist bewusst, dass wir durch die Präzisierung einzelner Formulierungen dem Geist der datenschutzrechtlichen Bestimmungen noch besser gerecht werden können: So meint die Formulierung ´körperliche Leiden` lediglich jene gesundheitlichen Einschränkungen, die das Absolvieren einer Ausbildung unmöglich machen, die auch die aktive Mitarbeit in einem McDonalds Restaurant umfasst. Gegenwärtig überprüfen wir unsere Fragen im Franchise-Antrag nochmals kritisch dahingehend, ob wir deren Formulierungen zum besseren Verständnis optimieren können“. Subway wollte zu der Datenerhebung keine Stellung nehmen (Goetz/Wassermann/Wensierski, Der Spiegel 12/2010, 112 f.; Der Spiegel 10/2010, 17)

Bayern

Seehofer-Büroleiter schnüffelte in CSU-Zentrale

Markus Zorzi, von 2004 an Landesgeschäftsführer der CSU und seit Dezember 2009 Büroleiter des bayerischen Ministerpräsidenten Horst Seehofer gab zu, den Computer des neuen CSU-Landesgeschäftsführers Bernhard Schwab ausspioniert zu haben. Am 09.03.2010 teilte die Staatskanzlei dann mit, dass dies Konsequenzen hat: „Der Leiter des Büros des Ministerpräsidenten wurde wegen eines Dienstvergehens von seinen Aufgaben entbunden. Ein Disziplinarverfahren wurde eingeleitet.“ Ein Motiv nannte Zorzi zunächst nicht; wohl aber entschuldigte er sich umgehend. Er galt bis dahin als „hochkorrekt“, als umgänglich und geradlienig. Von Personen aus dem Umfeld wird vermutet, Zorzi habe offenbar nicht auf das Herrschaftswissen verzichten wollen, das er als Leiter der CSU-Landesleitung gehabt hatte. Außerdem soll es Spannungen zwischen Zorzi, einem Vertrauten Seehofers, und Schwab, dem letzten in der Landeszentrale verbliebenen Stoiber-Mann, gegeben haben. Die Entlassung begründete Seehofer damit, er könne ein solches Vorgehen nicht dulden, schon allein deshalb nicht, um sich nicht dem Vorwurf auszusetzen, eine Bespitzelung der CSU-Landesleitung gar selbst angeordnet zu haben. Über einen derartigen Vorwurf war zuvor letztlich der frühere Ministerpräsident Edmund Stoiber gestrauchelt, dem die damalige Fürther Landrätin Gabriele Pauli vorgeworfen hatte, sein Büroleiter Michael Höhenberger habe ihr Privatleben ausspionieren wollen. Der 44jährige Zorzi ist studierter Jurist und hatte vor seiner politischen Karriere im bayerischen Sozialministerium gearbeitet (Stroh/Ramelsberger SZ 10.03.2010, 30).

Bayern

Justizministerin fordert Missbrauchsmeldepflicht an Schulen

Bayerns Justizministerin Beate Merk (CSU) fordert eine Meldepflicht für Missbrauchsvorwürfe an Schulen: „Diese Debatte muss jetzt geführt werden." Wie genau eine gesetzliche Regelung aussehen könnte, dafür gäbe es noch keine Pläne. Sie forderte aber, dass die Verantwortlichen an schulischen Einrichtungen künftig mitteilen, wenn es bei ihnen Vorwürfe gibt. „Ich werde ernsthaft prüfen, ob und in welchem Umfang verbindliche Meldepflichten eingeführt werden müssen." Für eine Verankerung im Strafrecht wäre allerdings der Bund zuständig. Und wenn eine Meldepflicht im Schulgesetz oder über die Gesundheitsvorsorge geregelt werden soll, fiele das nicht in Merks Ressort. Derweil wurden in Bayern immer neue Missbrauchsvorwürfe bekannt, so aus den 60er Jahren bis in die 90er hinein z.B. im Internat der Benedektinerabtei Plankstetten, am Ingolstädter Canisiuskonvikt oder bei den Regensburger Domspatzen (SZ 15.03.2010, 31).

Bayern

Sensoren kontrollieren LKW

Die oberbayerische Polizei testet ein neues Verfahren zur elektronischen Kontrolle des Schwerverkehrs. In der Teerdecke eingebaute Sensoren und eine Infrarotkamera sollen bei fahrenden Lastkraftwagen (LKW) feststellen, ob sie überladen, ihre Reifen abgefahren sind oder die Bremsen nicht einwandfrei funktionieren. Die Teststrecke liegt an der Autobahn A8 bei Bad Aibling im Kreis Rosenheim Fahrtrichtung München, wo besonders viele LKWs unterwegs sind. Bisher werden die Fahrzeuge durch die Polizei oder das Bundesamt für Güterverkehr von der Autobahn gelotst und kontrolliert. Das von der Europäischen Union mit 6 Mio. Euro geförderte Projekt soll die Voraussetzungen schaffen, dass Verstöße automatisch mit einem Bescheid geahndet werden, ohne dass der LKW angehalten wird (SZ 07.05.2010, 29).

Berlin

Verfassungsschutz-Informant im Bundestag

Der Berliner Verfassungsschutz hatte zeitweilig mit dem Referenten eines früheren SPD-Bundestagsabgeordneten zusammengearbeitet. Der wissenschaftliche Mitarbeiter des sächsischen SPD-Politikers Andreas Weigel hatte nach Presseberichten parallel zu seiner Tätigkeit im Bundestag einen unbefristeten Arbeitsvertrag mit dem Geheimdienst. Der Mann war demnach von 2003 bis 2005 für den Verfassungsschutz tätig. Der inzwischen aus dem Bundestag ausgeschiedene Abgeordnete Weigel wusste angeblich von der äußerst ungewöhnlichen Zusammenarbeit (SZ 24.03.2010, 6).

Niedersachsen

Verfassungsschutz bremst Einbürgerung von Linken-Politikerin

Der niedersächsische Innenminister Uwe Schünemann (CDU) hatte alles in seiner Macht Stehende unternommen, dass Jannine Menger-Hamilton nicht eingebürgert und damit deutsche Staatsangehörige wird. Menger-Hamilton ist in Celle geboren, hat europäische Eltern (aus Italien und England), deutsches Abi und deutschen Hochschulabschluss, ist mit einem Niedersachsen verheiratet, ist in der Linkspartei, dort stellvertretende Kreisgeschäftsführerin und arbeitet in einem festen Job bei der neuen Landtagsfraktion der Linken in Kiel. Dass sie seit zweieinhalb Jahren auf die Einbürgerung wartete, war dem Landesamt für Verfassungsschutz (LfV) in Hannover zuzuschreiben. Sie hat einen Rechtsanspruch auf Einbürgerung, wenn sie nicht „aktiv etwas gegen die freiheitliche demokratische Grundordnung unternommen hätte", so der frühere Bundesjustizminister Edzard Schmidt-Jortzig (FDP). Der behördliche Verfassungsschutzes legte „Erkenntnisse" der kommunalen Ausländerbehörde vor, verbunden mit der Erläuterung, dass „kein Interesse bestehen" könne, „eine Person einzubürgern, die Mitglied einer Partei ist, zu deren Grundlage der Marxismus" gehöre. Schünemann war über den Einbürgerungsantrag vom Oktober 2007 im Mai 2008 vom LfV-Präsidenten informiert worden. Auf einem Schreiben in der Einbürgerungsakte von Menger-Hamilton ist nach Presseangaben der Vermerk zu lesen: „...ist mit der Hausleitung des MI abgestimmt" (MI = Ministerium des Innern). Hauke Jagau (SPD), Präsident der Region Hannover, verstand dies als Weisung. Diese hätte zwar übergangen werden können. Bloß „jeder Sachbearbeiter weiß dann, dass seine Entscheidung aufgehoben würde", so Jagau. Dies sieht Schmidt-Jortzig rechtlich anders: „Der Hinweis auf die Mitgliedschaft in einer Partei genügt nicht, auch wenn es bei der Person Zweifel an der Verfassungstreue gibt. Wenn die Partei verboten wäre, dann gäbe es einen Automatismus, dass ihre Anhänger nicht eingebürgert werden. Aber das ist hier ja offenkundig nicht der Fall. Und deswegen müssten die Einwände direkt auf die Antragstellerin bezogen sein."

Die Angelegenheit wurde am 17.03.2010 im Niedersächsischen Landtag erörtert, wo FDP und Union von einem Versagen der Einbürgerungsbehörde redeten, so Heinz Rolfes (CDU): „Die Entscheidungsschwäche von Herrn Jagau ist erschreckend". Bei ihm zu Hause im Emsland würde sich „jeder kleine Bürgermeister trauen, solche Angelegenheiten im eigenen Ermessen zu entscheiden". Die Opposition sah dagegen die Schuld bei Innenminister Schünemann, der die Überwachung der Linkspartei verteidigte. Frank Briese (Grüne) nannte ihn deshalb einen „Gesinnungsethiker", der sich „schweißgebadet" in einem veralteten „Albtraum von Moskau" und kommunistischer Weltherrschaft wälze. Linken-Chefin Tina Flauger sprach von „Hexenjagd" und fragte, welche Rolle bei dieser Posse der Innenminister gespielt habe

und fragte in der Tradition von Armee-Rat Joseph N. Welsh, der 1954 damit das Ende der Kommunisten-Jagd von US-Senator Joe McCarthy vorbereitet hatte: „Have You no sense of decency, Sir? - Haben Sie keinen Sinn für Anstand, Herr Schünemann?“ SPD-Fraktionschef Wolfgang Jüttner reagierte auch empört: „Ein Verfassungsminister, der den Verfassungsschutz missbraucht, einen politischen Kampfauftrag zu erledigen, hat sich moralisch selbst erledigt.“

Die Region Hannover kündigte an, nun unabhängig vom Votum des Verfassungsschutzes „in absehbarer Zeit“ zu entscheiden; inzwischen ist Menger-Hamilton Deutsche. Nach dem Eklat um ihre Person sah sich die Landeshauptstadt Hannover in einem anderen Fall veranlasst, dem 20jährigen Syrer Aram A. die Einbürgerung auszusprechen, obwohl das Ministerium hierfür noch kein grünes Licht gegeben hatte. Dem Antragsteller wirft das LfV vor, sich in der DKP-nahen Sozialistischen Deutschen Arbeiterjugend engagiert zu haben. Ordnungsdezernent Marc Hansmann sicherte zu, dass „die Stadt selbst über den Fall entscheiden“ werde. Zuvor, 2007, war der niedersächsische Landtagsabgeordnete der Linken Victor Perli eingebürgert worden. Die zuständige Einbürgerungsbehörde Wolfenbüttel hatte angeblich vergessen, die bundesweit vorgeschriebene Regelanfrage beim Verfassungsschutz zu stellen, „obwohl Anhaltspunkte, die im Rahmen einer Regelanfrage zutage getreten wären, vorlagen“, so Ministeriumssprecher Klaus Engemann (Schirrmeister www.taz.de 17.03.2010; Schirrmeister www.taz.de 10.03.2010).

Nordrhein-Westfalen

120.000 Euro-Bußgeld gegen Postbank

Der nordrhein-westfälische Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI NRW) Ulrich Lepper hat ein Bußgeld in Höhe von 120.000 Euro gegen die Postbank verhängt, weil diese bis Herbst 2009 freiberuflichen HandelsvertreterInnen für Vertriebszwecke den Zugriff auf Kontobewegungsdaten von Kunden ermöglicht hatte (vgl. DANA 4/2009, 151). „Die Postbank ist eindeutig zu weit gegangen. Ich frage mich, was das Bankgeheimnis noch wert sein soll, wenn rund 4.000 freiberufliche Außendienstmitarbeiter weit über eine Million Kontodatensätze von Kundinnen und Kunden abrufen können“, erläuterte Lepper am 07.05.2010. Kontodaten seien hochsensibel, etwa, wenn es um das Einkommen vom Sozialamt, um Zeitungsabos oder die Bezahlung einer Rechnung einer auf Herzkrankheiten spezialisierten Klink gehe. Die Stiftung Warentest hatte Oktober 2009 öffentlich gemacht, dass die Postbank den freien Handelsvertretern jahrelang Einsicht in alle Kontobewegungen ihrer KundInnen gewährt hatte. Sei etwa ein höherer Geldbetrag auf dem Konto eines Kunden eingegangen, hätten die freien MitarbeiterInnen umgehend Kontakt zu den KundInnen aufnehmen können, um ihnen Geldanlagen zu verkaufen. Gemäß Lepper fanden sich bei einer Prüfung Arbeitsanweisungen, in denen die selbstständigen HandelsvertreterInnen explizit aufgefordert wurden, Kontodaten vor einer Kontaktaufnahme auszuwerten.

Zuvor hatte schon der Verbraucherzentrale Bundesverband (vzbv) die Postbank abgemahnt (DANA 1/2010, 24). Die Postbank erklärte zunächst, es sei notwendig, dass die freien FinanzberaterInnen, die in der Postbank Finanzberatungs AG organisiert sind, „anlassbezogen Zugriff auf Kontodaten haben sollen, um eine fundierte Kundenberatung durchführen zu können“. Dafür habe man Regeln „rechtlicher und technischer Art“ aufgestellt, die die FinanzberaterInnen einhalten müssten. Seit November 2009 wurde der Zugriff auf Girobewegungsdaten durch HandelsvertreterInnen dann aber doch technisch unterbunden. Kontobewegungen seien sehr sensible Daten, die viel über unsere Lebensweise aussagen, meinte Lepper. Diese dürften weder von Banken und erst recht nicht von Handelsvertretern für Werbezwecke ausgewertet werden (www.heise.de 07.05.2010; PM LDI NRW 07.05.2010).

Nordrhein-Westfalen

Ausspähung von E-Mails bei der CDU

Die Staatsanwaltschaft Düsseldorf ermittelt seit Februar 2010 „gegen unbekannt“ wegen des Verdachts der „Ausspähung von Daten“ in der Parteizentrale der nordrhein-westfälischen CDU. Zuvor hatte der Personalchef der NRW-CDU Strafanzeige erstattet. In den vorangegangenen Monaten waren durch vertrauliche Unterlagen aus der CDU-Zentrale in Düsseldorf etliche Affären aufgedeckt worden. So war im September 2009 ein E-Mail-Verkehr bekannt geworden, wonach maßgebliche Strategen der CDU und die Staatskanzlei in umstrittene Video-Beobachtungen der SPD-Herausforderin bei den Landtagswahlen, Hannelore Kraft, von Anfang an eingebunden waren. Wenig später wurde enthüllt, dass der inzwischen zurückgetretene CDU-Generalsekretär Hendrik Wüst doppelte Krankenkassenzuschläge von der Landes-CDU und dem Landtag kassiert hatte. Schließlich wurden CDU-Werbebriefe an Journalisten lanciert, in denen spendablen Sponsoren Gespräche mit Ministerpräsident Rüttgers für etwa 6.000 Euro offeriert wurden. Danach bemühte sich die CDU, den Maulwurf mit Hilfe der Staatsanwaltschaft aufzuspüren.

Der Generalsekretär der Landes-CDU Andreas Krautscheid warf den Internet-Blogs „Wir in NRW“ und „Ruhrbarone“ vor, seit Monaten mit „geklauten E-Mails“ zu arbeiten und den bevorstehenden NRW-Wahlkampf „zu einer Schlammschlacht“ zu machen. Der „Ruhrbarone“-Blog habe mit weiteren Enthüllungen gedroht. Der Sprecher des NRW-Blogs Alfons Pieper wies die Vorwürfe zurück: „Wir haben keine Papiere geklaut. Wir haben Papiere aus dem Inner-Circle der CDU - und die veröffentlichen wir“. David Schraven, Mitinitiator des „Ruhrbarone“-Blogs, warf der Landesregierung vor, investigative Journalisten „zu kriminalisieren“ und „mitten im Wahlkampf die Strafverfolgung als Staatswaffe einzusetzen, um die eigene Position abzusichern“. Der Rüttgers-Berater Boris Berger entschuldigte sich in einem vertraulichen Schreiben bei der SPD-Spitzenkandidatin Hannelore Kraft für abfällige Äußerungen in seinem E-Mail-Verkehr. Krautscheid er-

klärte, die der CDU entwendeten Berger-Mails enthielten einen „gelegentlich derben Tonfall“ und „Unhöflichkeiten“, die er zwischenzeitlich für ausgeräumt halte. Nach Presseberichten soll Berger u.a. über Kraft geschrieben haben „Das geschieht der Alten recht. Immer auf die Omme“.

Zuvor musste die CDU vor dem Düsseldorfer Arbeitsgericht auf Anraten der Richter die Kündigung einer Ex-Betriebsrätin zurücknehmen, die fristlos gekündigt worden war, weil sie von Hendrik Wüst der Illoyalität verdächtigt wurde. Die 48jährige Sachbearbeiterin war 28 Jahre lang Parteimitglied und 22 Jahre bei der Landespartei angestellt. Hintergrund waren Fehler in Computerdateien, für welche die Sachbearbeiterin verantwortlich gemacht wurde. Deren Anwalt sieht die Kündigung im Zusammenhang mit den E-Mail-Indiskretionen (Nitschmann SZ 04.03.2010, 6; Nitschmann 25.02.2010, 5).

Saarland

Judith Thieser wird neue Datenschutzbeauftragte

Der Ministerpräsident des Saarlands Peter Müller hat am 21.04.2010 dem schwarz-gelb-grünen Kabinett die bisherige Mettlacher Bürgermeisterin Judith Thieser als neue Datenschutzbeauftragte vorgeschlagen. Müller betonte, dass mit dieser Entscheidung zum ersten Mal eine Frau für dieses Amt nominiert wird. Es handele sich um „eine qualifizierte Juristin mit langjähriger Verwaltungserfahrung“. Dies erfolge in einer Situation, in der das Amt des Datenschutzbeauftragten durch die Zusammenführung des öffentlichen und des nicht-öffentlichen Datenschutzes an Bedeutung gewänne. Zwei Tage später kürte die Landespressekonferenz (LPK) Saar den bisherigen 60jährigen Landesbeauftragten für Datenschutz und Informationsfreiheit Roland Lorenz mit der „Goldenen Ente“. Mit dem Preis zeichnet die LPK Saar seit 1973 alljährlich Persönlichkeiten des öffentlichen Lebens für ihren offenen Umgang mit der Presse aus. Sie begründeten die Vergabe des Medienpreises an Lorenz mit dessen öffentlichkeitswirksamen und pressefreundlichen Amtsausübung. Bei der Ausgestaltung des Polizeigesetzes habe er sich erfolgreich dafür eingesetzt, dass die Journalisten einen besonderen Schutz vor dem „Großen Lauschangriff“ und der Telekommunikationsüberwachung erhielten. Lorenz habe bereitwillig die Journalisten beraten, wie sie die entsprechenden Gesetze nutzen können. Die LPK äußerte die Hoffnung, dass Thieser die selbstbewusste und unabhängige Linie von Lorenz fortführt. Lorenz hatte zuvor öffentlich geäußert, für eine weitere sechsjährige Amtszeit zur Verfügung zu stehen.

Die 54jährige Thieser, die bisher durch Äußerungen zum Datenschutz nicht in Erscheinung getreten war, ist CDU-Mitglied und war vor ihrem Bürgermeisteramt als Rechtsanwältin tätig. Die Personalentscheidung Müllers wurde von der Opposition scharf kritisiert: Die SPD meinte, Thieser sei in der eigenen Partei in Mettlach umstritten. Die Regierungsfraktionen von FDP und Grünen unterstützen dagegen den Personalvorschlag, wenngleich es ein offenes Geheimnis ist, dass beide Fraktionen bereit gewesen wären, Lorenz´ Wiederwahl zu unterstützen. Die Widerstände gegen Lorenz kamen aus dessen eigener Partei, der CDU, mit der er sich offenbar zu oft angelegt hatte. Dies war bei der Reform des Polizeigesetzes 2007, aber auch in Personalfragen und bzgl. der Kompetenzen seiner Behörde. In der Presse wurde darauf hingewiesen, dass die Wahl Thiesers für das Land kostenträchtig wäre, da Lorenz vorzeitig in den Ruhestand mit entsprechenden Vorsorgungsbezügen geschickt werde. Die Wahl Thiesers wurde möglich, nachdem Ende März 2010 der 58jährige FDP-Vize und ehemalige Landtagsabgeordnete Manfred Baldauf mitgeteilt hatte, er stehe für das Amt eines Datenschutzbeauftragten nicht zur Verfügung. Er zog damit die Konsequenzen aus dem wochenlangen öffentlichen Streit zwischen FDP und der Landtagsopposition aus SPD und Linkspartei, „um weiteren Schaden von dem Amt abzuwenden“. Der FDP wurde vorgeworfen, mit der Berufung von Baldauf diesen versorgen zu wollen (vgl. DANA 1/2010, 32; Freund Saarbr.Ztg. 22.04.2010, 13.04.2010, 23.03.2010; PM LfDI Saarland 23.04.2010, 21.04.2010).

Schleswig-Holstein

Über Schüler-VZ aufgelauert und zusammengeschlagen

Einem 15jährigen Schüler aus Lübeck, der sich mit einer 23jährigen Frau gestritten hatte, wurden seine privaten Angaben im Internetnetzwerk Schüler-VZ zum Verhängnis: Die Frau machte über das Portal dessen Schule ausfindig, lauerte ihn mit einem 17jährigen gemeinsam auf und ließ ihn mit einem Nietenhandschutz verprügeln. Der 15jährige konnte leicht verletzt ins Schulgebäude flüchten (SH-Z 01.03.2010, 3).

Jahrelange Überwachung durch Bundeskriminalamt rechtswidrig

Mit erst im Juni veröffentlichten Beschlüssen vom 11. März 2010 hat der 3. Strafsenat des Bundesgerichtshofs die Überwachung von drei mutmaßlichen Mitgliedern der „militanten gruppe“ in den Jahren 2001 – 2006 für rechtswidrig erklärt. Betroffen davon sind allein bei einem Betroffenen 39 (!) Anordnungen des Ermittlungsrichters beim Bundesgerichtshof, der unter häufig wörtlicher Übernahme von Anträgen des Generalbundesanwalts Telefonüberwachungen und längerfristige Observationen genehmigt hatte. Nach Feststellung des Bundesgerichtshofs haben die Ermittlungen, welche durch linguistische Gutachten des Bundesamts für Verfassungschutz ausgelöst worden waren, von Anfang an nicht auf einem tragfähigen Tatverdacht beruht. Entlastende Unterlagen, etwa ein entlastendes Gutachten des Bundeskriminalamts, wurden zudem in den Überwachungsanträgen des Generalbundesanwalts nicht erwähnt und blieben auch vom Ermittlungsrichter unberücksichigt. Der Bundesgerichtshof rügte ferner, dass einige der aufgehobenen Überwachungsmaßnahmen nicht zur Strafverfolgung durchgeführt wurden, sondern der Gefahrenabwehr dienen sollten. Dazu hätten, wenn überhaupt, andere Behörden auf anderer Rechtsgrundlage vorgehen müssen. (FR v. 19.6.2010; taz v. 19.6.2010; BGH, Beschluss v. 11.03.2010, Geschäftszeichen: StB 16/09 u.a.; www.bundesgerichtshof.de).

Datenschutznachrichten aus dem Ausland

Österreich

Marathonläuferin beendet wegen Doping-Test ihre Karriere

Die österreichische Läuferin Eva-Maria Gradwohl, die kurz zuvor am 11.04.2010 mit einer Weltklassezeit den Linz-Marathon gewonnen hatte, verweigerte einen Dopingtest und beendete damit ihre sportliche Karriere. Die 37jährige war im Urlaub, wie sie auf ihrer Homepage erklärte: „Ich wollte nicht die geplante Bootsfahrt mit Freunden verschieben. Ich wollte einfach meinen Urlaub ... genießen, aber das ist als Leistungssportler nicht möglich. Ich habe die Dopingkontrollen abgebrochen, was ein klarer Regelverstoß ist und somit muss ich die Konsequenzen tragen.“ Das vorzeitige Ende ihrer Profikarriere, die sie erst 2007 begonnen hatte, begründete Gradwohl mit den verschärften Regeln des Anti-Doping-Kampfes: „Ich bin es leid, jeden Tag anzugeben, wo ich bin, was ich mache und eine Stunde meines Tages zu warten, ob die Dopingkontrolle kommt oder nicht.“ David Müller, Manager für Prävention und Öffentlichkeit der österreichischen Nationalen Anti-Doping-Agentur (NADA) bestätigte: „Grundsätzlich ist ein verweigerter Test zu handhaben wie ein positiver Test“. Gradwohls Lebenspartner, der 53jährige ehemalige Langlauftrainer im Österreichischen Skiverband Walter Mayer ist seit der sog. Blutbeutel-Affäre bei Olympia Salt Lake City 2002 vom Internationalen Olympischen Komitee gesperrt. Er gilt auch als Auslöser der Doping-Affäre bei Olympia 2006 in Turin und saß wegen des Verdachts des Handels mit Dopingmitteln einige Zeit in Untersuchungshaft (SZ 05.05.2010, 28).

Frankreich

Loppsi 2: umfassende Internetkontrolle und mehr Sicherheitsbefugnisse

Frankreichs Präsident Nicolas Sarkozy hat ein Gesetzespaket mit dem niedlichen Namen „Loppsi 2“ eingebracht, in dem Behörden mit umfassenden Überwachungsrechten ausgestattet werden sollen: Internetsperren, Spähaktionen auf Privatrechnern, Video-Überwachung. Loppsi steht für „loi d‘orientation et de programmation pour la performance de la sécurité intérieure“. Für die Vertreter der französischen Regierungspartei ist es der Riegel gegen digitale Kriminalität. Die Rede ist vom „Gesetz für die Orientierung und Programmierung des Erfolgs der Inneren Sicherheit“. Dem Parlament mit seiner konservativen Mehrheit lag das Werk am 16.02.2010 vor. Wenn dann auch noch der Senat zustimmt, kann das Gesetz im Sommer 2010 in Kraft treten. Die Vorlage enthält Regelungen, die Frankreich zu dem Land in Europa machen werden, in dem das Internet am stärksten reglementiert, kontrolliert, überwacht und zensiert wird. Ein Netzsperrengesetz soll künftig Provider zwingen, auf Anordnung der Behörden den Zugang zu inkriminierten Seiten zu sperren. „Der vorliegende Entwurf“, so heißt es im Artikel 4, „macht es jedem, der den Zugang zum Internet anbietet, zur Aufgabe, dass Nutzer keinen Zugriff auf unziemliche Inhalte bekommen.“ Die Liste der Seiten wird den Providern per Erlass vom Innenministerium zugestellt. Das Vorgehen ist vergleichbar mit dem in Deutschland mittlerweile gekippten Zugangserschwerungsgesetz gegen Kinderpornografie. Überdies können Polizei und Sicherheitsdienste mit heimlich installierter Software künftig private Computer ausspähen. Der Fernzugriff der Verfolgungsbehörden auf den heimischen Computer würde damit erlaubt - unter Kontrolle eines Ermittlungsrichters, so der Vorschlag. In Deutschland wurde ein vergleichbarer Passus im neuen BKA-Gesetz unter dem Stichwort „Bundestrojaner“ eingeführt.

Die Web-Kontrollen sind nur ein Teil des Konvoluts „Loppsi 2“. Bei dem Paragrafenwerk handelt es sich um ein buntes Maßnahmenbündel aus dem Haus von Innenminister Brice Hortefeux - einem engen Vertrauten von Präsident Sarkozy, der 2002 die erste Version des Sicherheitskatalogs angeschoben hatte. Loppsi 1 habe, so die Regierung, die Sicherheitslage verbessert. Die Neuauflage diene nun, der Cyberkriminalität und anderen neuen Herausforderungen zu begegnen. Der Entwurf, in Arbeit seit Oktober 2007 und laut Hortefeux zuletzt um 13 Klauseln „wie beim Bodybuilding“ verstärkt, berührt nicht nur die Strafprozessordnung, Verkehrsregeln, Verteidigung, Sport und Ausländerrecht, sondern auch Fragen wie die Bestattung in Neukaledonien oder am Nordpol. Die Zeitung „Le Monde“ spricht konsequenterweise von einem „Kasten mit vielen Schubladen“. Darin liegen Werkzeuge für die städtische Polizei oder private Wachdienste. Es findet sich ein Hinweis auf die Ausweitung der Video-Überwachung - von 20.000 auf 60.000 Kameras bis Ende 2011 - die als „Videoschutz“ verharmlost wird. Vernehmungen sollen künftig am besten per TV-Schalte abgewickelt werden, damit den Beamten erspart bleibt, die Verdächtigen auf dem Weg vor den Richter zu eskortieren. Zugleich drohen schärfere Strafen bei Einbrüchen, Überfällen oder betrunkenem Fahren. Die Präfekten sollen die Erlaubnis bekommen, für Minderjährige unter 13 Jahren eine nächtliche Ausgangssperre zu verhängen. Loppsi 2 sieht weiterhin die leichtere Vernetzung von elektronischen Polizeikarteien und gespeicherten Privatdaten etwa bei Banken vor. In Zukunft soll bestraft werden, wer die Identität von Geheimagenten enthüllt. Auf den Flughäfen werden bald Körperscanner getestet, um leichter Terroristen zu finden. Dies alles erfolgt - so Innenminister Hortefeux - in der hehren Absicht, die „alltägliche Sicherheit der Franzosen zu verbessern,

um das Niveau und die Qualität der Dienstleistungen der Sicherheitskräfte des Inneren zu erhalten".

Präsident Nicolas Sarkozy bleibt damit seiner harten Linie treu. Erst im Jahr 2009 hatte seine Regierung das „Hadopi"-Gesetz durchgedrückt, das es erlaubt, unbelehrbaren Nutzern illegaler Internettauschbörsen nach dem dritten Verstoß den Netzzugang zu kappen. Mit dem neuen Gesetz wird nun die nächste Stufe rabiater Netzregulierung eingeleitet. Die Vorlage des Gesetzes erfolgte wenige Wochen vor den französischen Regionalwahlen, einer Abstimmung mit Signalcharakter, bei denen der Präsident laut Umfragen einen Misserfolg zu befürchten hatte, was ihn angesichts der grassierenden Wirtschaftskrise, steigender Arbeitslosigkeit, katastrophal wachsender Staatsverschuldung und innenpolitischer Pannen dazu veranlasste, die Furcht vor dem Bösen im Internet zu schüren, um die BürgerInnen an die Urnen zu bringen.

BürgerrechtlerInnen und Opposition sind angesichts dieses Überwachungskatalogs entsetzt. Sie beschwören die Angst vor dem totalen Überwachungsstaat, so etwa Jean-Pierre Dubois, Präsident der französischen Liga für Menschenrechte: „Wir sehen eine ganze Serie von Entgleisungen und Einschränkungen von Rechten." Die Grünen-Europaabgeordnete Sandrine Bélier beklagt „eine echte Bedrohung" für die Neutralität des Internets. „Filterung und Blockierungen des Webs sind heute gängige Ausdrucksformen im legislativen Arsenal einer Regierung, die sich beim Umgang mit öffentlichen Freiheiten besonders schamlos darstellt." Bélier rügt vor allem die polizeiliche Kontrollaufgabe, die an die Provider weitergereicht wird, obwohl sie eigentlich „gerichtlichen und rechtlichen Autoritäten vorbehalten" sei. Dies ist einer der Gründe, weswegen das von der damaligen Familienministerin Ursula von der Leyen (CDU) eingebrachte Netzsperrengesetz in Deutschland von Union und FDP gekippt werden soll (Simons www.spiegel.de 16.02.2010; Ulrich SZ 11.02.2010, 8; www.netzpolitik.org 10.02.2010; www.unwatched.org 30.01.2010; www.datenschutz.de 20.05.2009).

Großbritannien

Parlament beschließt mit Digital Economy Bill Netzsperren und Überwachung

Britische Netzanbieter müssen bald überwachen, was ihre KundInnen im Netz so ansehen - und ihnen im Zweifel den Zugang sperren. Auf Initiative des Wirtschaftsministers Lord Mandelson wurde in der Nacht des 07.04.2010 das „Digital Economy Bill" mit 189 Stimmen, in der Mehrheit von der Konservativen Partei, von 236 der anwesenden Parlamentsmitgliedern beschlossen. Die weiteren 414 der 650 Mitglieder des Unterhauses (House of Commons) nahmen an der Abstimmung nicht teil. Das Gesetz über die digitale Wirtschaft regelt faktisch eine inhaltliche Überwachung des britischen Netzes. Am 15.04.2010 gab das Oberhaus dem Gesetz seinen Segen, so dass dieses von der Königin unterschrieben werden konnte, um wirksam zu werden. Damit droht jedem, der verdächtigt wird, über das Internet illegale Inhalte zu nutzen, dass sein Zugang verlangsamt oder gesperrt wird. Danach kann das Netz auch abgeklemmt werden, wenn jemand in dem Haushalt verdächtigt wird, Urheberrechte zu verletzen. Eine gerichtliche Untersuchung ist nicht vorgesehen. Bei einem Einspruch des Betroffenen liegt die Beweislast bei ihm. Die Internetanbieter müssen dafür sorgen, dass über ihre Leitungen nichts Illegales läuft. Im Zweifel also haben sie zu überwachen, was sich ihre Kunden so ansehen. Tun die Netzanbieter das nicht, können sie mit Strafen bis zu 250.000 Pfund belegt werden. Dies gilt auch für Anbieter offener WLAN-Zugänge, wie beispielsweise die Kaffeekette Starbucks in ihren Filialen.

Firmen, bei denen über Internet Filme, Dokumente oder Mails gespeichert werden können, bekommen ebenfalls ein Problem, da, so die Gesetzesbegründung, der Speicherplatz genutzt werden kann, illegale Inhalte zu hinterlegen. Die Now Show, eine satirische Radiosendung auf BBC, kommentierte das mit den Worten, der menschliche Hintern sei geeignet, Drogen zu schmuggeln, doch sei das noch kein Grund, den Inhalt eines jeden danach zu untersuchen. Eine Regelung im Gesetz ermöglicht die Sperrung von Internetseiten mit illegalen Inhalten. Dies ist auf Anordnung eines Gerichtes möglich, wenn die Seiten „schwere schädliche Auswirkungen auf Unternehmen oder Verbraucher" haben. Das könne beispielsweise auch Wikileaks treffen, so der Liberaldemokrat John Hemming bei der ersten Lesung: „Sehen Sie sich Wikileaks an. Dort steht Material, das der Regierung gehört. Die würde das sicher gerne anwenden, um Wikileaks in Großbritannien zu sperren." Sein Parteikollege Don Foster ergänzte, Entsprechendes könne auch mit YouTube oder Google passieren. BürgerrechtlerInnen und Unternehmen hatten das Gesetz bekämpft, z.B. mit dem Slogan „Kreativität ist der Feind". Für sie ist besonders schmerzlich, dass der damalige Noch-Premier Gordon Brown am Tag vor der Abstimmung den Termin für Neuwahlen verkündete und bei der Queen um die Auflösung des Parlaments nachsuchte. Dieses kann, um einige letzte Dinge zu beraten, eine so genannte Aufräumperiode (wash-up) von einigen Tagen beschließen. Das hat es auch getan, unter anderem, um das schwer umstrittene Gesetz noch durchzubringen. Denn den Konservativen war eine Mehrheit nach den Wahlen am 06.05.2010 längst nicht sicher (Biermann www.zeit.de 08.04.2010).

Finnland

Mann ohne Hose klagt gegen Google Street View

Ein Finne klagt gegen Google Street View, weil der Straßenbilderdienst im Internet (Street View) ihn ohne Hose in seinem Garten „erwischt" hat. Er sei auf den Aufnahmen, die weltweit abrufbar sind, zu identifizieren, wird von ihm moniert. Damit habe das Internetunternehmen seine Privatsphäre verletzt und ihn der Lächerlichkeit preisgegeben (Kieler Nachrichten 13.02.2010 S. 12).

Rußland

Kompromittierungskampagnen durch Sicherheitsdienst

Immer wieder wird berichtet, dass der russische Sicherheitsdienst gezielt schöne Frauen einsetzt, um Menschen zu erpressen oder zu kompromittieren. Im Jahr 2009 tauchten im Internet Fotos des stellv. britischen Konsuls in Jekaterinburg auf, die ihn mit der Unterschrift „Die Abenteuer des Mr. Hudson in Russland“ in einer kompromittierenden Situation mit zwei Frauen zeigten. Ähnlich undiplomatisch war der Umgang mit einem Angehörigen der US-amerikanischen Botschaft, der 2009 mit einer Prostituierten gefilmt wurde und über den russische Zeitungen kolportierten, er sei womöglich ein CIA-Agent gewesen. Nun wurde bekannt, dass offensichtlich eine im Dienste des Sicherheitsdienstes tätige Blondine auf die Zahlungsbereitschaft der indischen Regierung eingewirkt haben könnte, statt der ursprünglich angesetzten 800 Mio. Dollar für den gebrauchten Flugzeugträger Admiral Gorschkow 2,3, Mrd. Dollar zu zahlen. Das indische Militär hat gegen den Kommandeur Sukhjunder Singh Ermittlungen eingeleitet, nachdem eine pikante CD an das Hauptquartier der Marine geschickt worden war. Die Bettfotos werden auf die Zeit zwischen 2005 und 2007 datiert, in der Singh als Chef der Technik-Kommission in der russischen Werftstadt Sewerodwinsk die Reparatur und Umrüstung des Flugzeugträgers beobachtete. Die Ermittler haben noch keinen Beweis dafür, dass die Dame aus Russland den Kaufpreis des Flugzeugträgers tatsächlich beeinflusst hat. Öffentliche Personen werden immer öfter mit Videos und Fotos verunglimpft, egal, ob die Bilder echt sind oder nicht. Der regierungskritische Satiriker und Radiomoderator Viktor Schwenderowitsch, gerade erst bei einem Seitensprung erwischt, beschuldigte in satirischer Form die Behörden, ihn reingelegt zu haben. In seinem Blog wendet er sich an die „Genossen Tschekisten“ des russischen Geheimdienstes: „Das ist eine Diskriminierung des Alters. Jungen Oppositionellen bietet ihr kostenlos zwei Frauen an und auch noch eine Portion Kokain. Und uns Fünfzigjährigen nur eine, und kein Spielzeug mehr dazu“ (Nienhuysen SZ 24./25.04.2010, 12).

USA

Republikaner veranlassen PC-Pornokontrolle bei Mitarbeitern der Börsenaufsicht

Gemäß Statistiken vertreiben sich ca. 16% der amerikanischen Männer auch an Büroarbeitsplätzen ihre Zeit mit dem Betrachten von Pornos auf ihrem Computer. Dazu gehörten auch etliche Mitarbeiter der US-Börsenaufsicht (SEC) in Washington. Während das amerikanische Finanzsystem in den Kollaps schlitterte, befassten sich viele SEC-Bedienstete mit Sexbildern. Dies berichtet ein auf Druck eines US-Senators erstellter Bericht, der 33 Fälle aus den Jahren 2007 und 2008 auflistet. Ein Jurist hatte in der Washingtoner Zentrale bis zu acht Stunden täglich Pornos angesehen und heruntergeladen. Als seine Festplatte voll war, brannte er die Bilder auf DVDs. Der Mann ist inzwischen entlassen. Ein anderer wurde innerhalb eines Monats in 16.000 Fällen von internen Filtern daran gehindert, auf Pornoseiten zuzugreifen. Via Google gelang es ihm dennoch, seinen Computer mit „sehr explizitem Material zu füllen“. Er wurde für zwei Wochen vom Dienst suspendiert. Ein Beschuldigter rechtfertigte sich damit, es habe täglich nicht mehr als eineinhalb Stunden mit Pornos verbracht. Ein anderer, der an einem einzigen Nachmittag 385 Mal versucht hatte, auf eine Pornoseite zu gelangen, bezeichnete seine Ausflüge als „generelle Ablenkung“. Je höher der Stress im Job, desto öfter habe er sich virtuell entspannen müssen. In mindestens einem Fall wurde auf den Festplatten auch Kinderpornografie gefunden. Der Pornovorwurf trifft v.a. Beschäftigte der oberen Gehaltsklassen: 17 der beschuldigten Mitarbeiter saßen auf hohen Posten mit Jahresgehältern von mehr als 200.000 Dollar. Ziel des von den Republikanern angeforderten Berichtes war es vor allem, die SEC zu diskreditieren, um Präsident Barack Obamas Pläne für eine verschärfte staatliche Aufsicht über Amerikas Finanzsysteme zum Scheitern zu bringen (SZ 24./25.04.2010, 14).

USA

Super-Hacker zu 20 Jahren Gefängnis verurteilt

Der 28jährige Albert Gonzalez wurde in Bosten für einen der größten Datenklaus der US-amerikanischen Geschichte in Boston zu einer Freiheitsstrafe von 20 Jahren verurteilt. In einem weiteren Verfahren droht ihm eine Verurteilung zu weiteren 5 Jahren. Er hatte die Kreditkartendaten von 130 Mio. Betroffenen gehackt. Der Schaden für die betroffenen Kaufhausketten, Banken und Versicherer wird mit fast 200 Mio. Dollar angegeben. Gonzalez bereute vor Gericht: „Ich mache niemanden als mich selbst für alles verantwortlich.“ Er habe nicht wirklich aus Habsucht gehandelt, sondern vielmehr so etwas wie eine „Internetsucht“ gehabt und vom Reiz nicht lassen können, das System zu schlagen. An den Schaden bei den Kontobesitzenden habe er eigentlich nie gedacht: „Ich bin immer davon ausgegangen, dass sie von den Finanzinstitutionen entschädigt werden. Der Täter fuhr mit zwei Komplizen jeweils mit einem Laptop an Geschäften vorbei und suchte nach ungeschützten oder ungenügend gesicherten Computernetzwerken. Dort installierten sie Spezialprogramme, die ihnen die in den Geschäften benutzten Kreditkartennummern automatisch übermittelten. Die derart erbeuteten Daten verhökerte Gonzalez im Internet unter dem Pseudonym „Soupnazi“ oder „Segvec“ auf dem Schwarzmarkt, v.a. in die Ukraine oder nach Russland. Nach seiner Festnahme fanden die Behörden allein auf zwei Servern des Hackers noch die Daten von 40 Mio. Kreditkarten. Gonzalez kam nach Einschätzungen der Behörden selbst zu 2,8 Mio. Dollar, die er in ein Appartement in Miami, ein Auto, Rolex-Uhren anlegte - und in ei-

nen Tiffany-Ring für seine Freundin. 1,1 Mio. Dollar hatte er im Garten seiner Eltern vergraben. Nach seiner Festnahme 2008 hatte er die Polizei zu dem Versteck geführt.

Besondere Brisanz hat der Fall dadurch, dass Gonzalez vermutlich zur selben Zeit, in der er die Kreditkartendaten klaute, Informant eines US-Geheimdienstes war. Er versorgte offensichtlich den Secret Service mit Daten über andere Hacker. Gonzalez war bereits 2003 ein erstes Mal festgenommen worden. Das Verfahren war eingestellt worden, nachdem er in den Dienst des Secret Service getreten war. Die Staatsanwaltschaft hatte auf die Höchststrafe von 25 Jahren plädiert. Sie warf Gonzalez vor, der Rädelsführer eines internationalen Hacker- und Betrügerrings gewesen zu sein. Neben der Haftstrafe belegte die Richterin den Verurteilten zu drei Jahren Computerverbot nach seiner Haftentlassung (Klüver SZ 27./28.03.2010, 1, 11).

USA

Gericht stoppt Gen-Patentierung

Ein Gericht in New York hat die Patentierung von Genen grundsätzlich für unzulässig erklärt. In dem Verfahren ging es um Patente des US-amerikanischen Unternehmens Myriad Genetics auf die Gene BRCA1 und BRCA2. Frauen mit bestimmten Veränderungen (Mutationen) in diesen beiden Erbgutabschnitten haben ein erhöhtes Risiko bzgl. Brust- und Eierstockkrebs. In der 152 Seiten langen Urteilsbegründung führt Richter Robert Sweet aus, dass man Gene grds. nicht patentieren könne. Sie seien keine Erfindung, sondern eine Entdeckung. Wegen ihrer Patente auf die beiden Gene hat die Fa. Myriad in den USA das Monopol für den Verkauf von Tests auf ein erblich bedingtes Krebsrisiko durch BRCA1 und BRCA2. Die Untersuchung kostet mehr als 3.000 Dollar. Mangels Alternative zahlen viele Frauen diesen hohen Preis. Eine Bestätigung durch ein anderes Labor war bisher nicht möglich, da nur Myriad die Untersuchung anbieten durfte.

Auch in Deutschland besitzt Myriad Genetics Patente auf Abschnitte der Gene BRCA1 und BRCA2. Diese wurden aber nach Protesten von ÄrztInnen, WissenschaftlerInnen, Greenpeace und Frauenorganisationen schon vor Jahren so stark eingeschränkt, dass die Firma keinen Monopolanspruch auf den Test hat. Das Europäische Patentamt erteilt aber nach wie vor Patente auf Gene, weil es die Entdeckung eines Erbgut-Abschnitts als Erfindung gelten lässt, so Christoph Then, Gentechnikberater von Greenpeace. Etwa 20% der menschlichen Gene, u.a. für verschiedene Erbkrankheiten, sind patentiert. Für die PatientInnen hat dies meist negative Konsequenzen. Gemäß US-amerikanischen Untersuchungen haben mehr als die Hälfte aller Diagnoselabors schon einmal die Entwicklung besserer Testverfahren eingestellt, weil ihre Arbeit durch ein Patent auf ein bestimmtes Gen blockiert wurde (Baier SZ 31.03.2010, 18).

USA

WADA will Bluttests beim Baseball

Die Welt-Anti-Doping-Agentur (WADA) fordert von der US-amerikanischen Baseball-Liga (MLB) den Einsatz von Bluttests, um Doping mit dem Wachstumshormon HGH nachzuweisen. WADA-Präsident John Fahey verlangte von Liga und Spielervereinigung umfangreiche Testreihen und die Meldung der Ergebnisse für eine Datenbank. Bislang setzt die MLB nur Urintests ein; Bluttests werden abgelehnt. Fahey betonte, das Wachstumshormon sei gegenwärtig nur im Blut nachweisbar, wie z.B. beim britischen Rugby-Spieler Terry Newton, der November 2009 als erster Sportler überführt wurde. Doping ist ein großes Problem im US-Sport. Schon 2003 wurde der Home-Run-König Barry Bonds verdächtigt, mit Steroiden gedopt zu haben. Vier Jahre später präsentierte Ex-Senator George Mitchell Belege für systematisches Doping in der MLB, beschuldigte über 80 Profis, darunter nationale Helden wie den Pitcher Roger Clemens. Im Februar 2009 bekannte Superstar Alex Rodriguez, er habe zwei Jahre lang Steroide genommen (Der Spiegel 13/2010, 115).

USA

Mit Schulcomputern Kinder privat ausspioniert

Mit Mini-Kameras in Schul-Computern des Schuldistrikts von Lower Meriton, einem wohlhabenden Vorort im Speckgürtel von Philadelphia, wurden über 56.000 teilweise sehr private Fotos erstellt, gespeichert und offenbar genau ausgewertet. Dies wurde bekannt, als der 15jährige Blake Robbins ins Direktorium seiner High School zitiert und von der Lehrerin mit einem Foto konfrontiert wurde, das ihn daheim vor seinem Mac-Computer zeigte. Eine Handvoll Drops am Bildrand hatten bei der Lehrerin den Verdacht geschürt, Blake handele mit Drogen. Dieser gibt jedoch an: „Es waren nur normale Bonbons“. Nun ermittelt das FBI - gegen die Schulbehörde wegen des Verdachtes illegaler Spähangriffe. In den an die SchülerInnen von der Harriton High School und einer weiteren Schule verteilten 2.300 Lernlaptops sind Webcams installiert. Die Ermittlungen ergaben, dass viele SchülerInnen, so der Anwalt der Robbins-Eltern Mark Haltzmann „regelrecht ausspioniert“ wurden, wobei „reihenweise Menschen erfasst wurden, die mit der Schule überhaupt nichts zu tun haben“. Der Lower Merion School District (LMSD) gibt inzwischen zu, in 146 Fällen per Fernsteuerung eine sog. Spyware auf den Macs aktiviert zu haben, um so gestohlen geglaubte oder verschollene Schulcomputer wieder aufzufinden. Der Computer machte dann alle 15 Minuten ein Foto seiner Umgebung und dazu noch jeweils einen Screenshot. Anschließend übersandte das Macbook die Daten über das Internet an den Rechner der Schulbehörde, der alles zentral archivierte.

Im Hause der Familie Robbins produzierte der Schul-Mac auf diese Weise mindestens 400 Fotos innerhalb von zwei Wochen. Mal schläft Blake, mal macht er Hausaufgaben, meist ist er allein, mal im Kreis seiner Familie. Weil Blake im Internet gern chattet, wurden per Screenshots gleich auch Blakes Freunde

samt des Cousins in Connecticut mitregistriert. 2009 witzelte eine Angestellte in einer E-Mail an ihre Chefin Carol Cafiero, die offizielle Verwalterin aller 2300 Schulcomputer, das Programm entwickele sich zu „einer kleinen LMSD-Seifenoper". Cafiero wurde vom Dienst suspendiert; die Schulbehörde hat ihr Überwachungsprogramm eingestellt. Cafiero wehrt sich gegen Anwalt Haltzman, der öffentlich mutmaßte, die Verantwortliche für die Spähangriffe habe „vielleicht wie eine Voyeurin" auch Bilder von pubertären Jungs auf ihrem Privat-PC daheim gespeichert und betrachtet. Cafiero rechtfertigt ihre Aktion damit, Blake Robbins habe früher „mindestens zwei Schul-Computer" zerstört und obendrein nicht jene Versicherungsgebühr von 55 Dollar bezahlt, ohne die niemand einen Schul-Mac mit nach Hause nehmen darf. Wer öffentliches Eigentum derart behandele, der dürfe „keine legitimen Erwartungen von Privatsphäre" hegen. Die Lokalpresse kürte die Affäre bereits in Anspielung auf die Watergate-Affäre zum „Webcam-Gate". Hinweise, wonach 2/3 der 56.000 Aufnahmen von 6 Computern stammten, die 2008 aus einem Schulschrank geklaut worden waren, wurden weitgehend ignoriert. Allerdings wusste der Schuldistrikt keine Antwort auf die Frage, weshalb die fehlenden Computer nicht schlicht mittels IP-Adresse im Internet nachverfolgt wurden. Derweil erinnerten sich immer mehr SchulkameradInnen von Blake Robbins, wie bei ihnen im Schlafzimmer „regelmäßig dieses kleine grüne Lämpchen am Mac aufflackerte", also das Signal, dass die Kamera aktiviert ist. Auf Nachfrage hatte die Behörde abgewiegelt, es handele sich um „eine Panne am Gerät". Inzwischen befasst sich der US-amerikanische Kongress mit dem Thema (Wernicke SZ 27.04.2010, 12; Zips SZ 24.02.2010, 9).

China

Hacker attackieren Dalai Lama und die UNO

In einer über acht Monate erarbeiteten Studie des Information Warefare Monitor und der Shadow Server Foundation in den USA und Kanada wird beschrieben, wie mutmaßlich in China beheimatete Hacker Zugriff auf geheime Dokumente u.a. von Regierungen, Behörden, Botschaften und Verteidigungsexperten nahmen. Sie untersuchten eine Attacke auf den Computer im Büro des Dalai Lama und entdeckten eine groß angelegte Spionageaktion, die sich v.a. gegen Indien richtet, aber auch gegen Botschaften anderer Länder und die UNO. Als Besonderheit erwies sich, dass die Angreifer kostenlos verfügbare Internetdienste wie Twitter, Google und Yahoo benutzten, um Computer aus der Ferne zu steuern. Genutzt wurden Sicherheitslücken bei populären Programmen, mit denen präparierte Dateien untergeschoben wurden, die durch installierte Virensuchprogramme nicht entdeckt wurden. Die Forschenden: „Was dann kommt, wird nur von der Phantasie und den Fähigkeiten der Angreifer begrenzt." Sie konnten einige der Angriffe zurückverfolgen und erlangten so sogar Zugriff auf einen Rechner mit einem Spionageprogramm, das u.a. eine ganze Reihe von als „vertraulich" und „geheim" eingestuften Dokumenten aus dem indischen Verteidigungssektor enthielt. Gefunden wurde weiterhin der E-Mail-Verkehr eines ganzen Jahres des Dalai Lama mit 1.500 Dateien. Die Forschenden meinen, nur einen kleinen Einblick in das „beunruhigende Ökosystem der Cyber-Spionage" genommen zu haben. Obwohl nur die Attacke auf tibetische Organisationen untersucht wurde, sei man so auf eine große Zahl anderer Opfer gestoßen. China wies den Vorwurf zurück, systematisch Spionage zu betreiben. Die Forschenden fanden jedoch deutliche Hinweise darauf, dass die Angriffe ihren Ausgang in der Stadt Chengdu nahmen. Dort gibt es nicht nur eine technische Universität mit Netzwerksicherheit als Schwerpunkt, sondern auch eine entsprechende Spezialeinheit der Armee (Martin-Jung SZ 07.04.2010, 1, 4, 8).

Technik-Nachrichten

Divas-Suchmaschine findet eindeutige Datei-Fingerprints

Digitale Fingerprints sollen u.a. helfen, illegal genutzte Video- und Audiodateien im Internet aufzuspüren. Das Party-Video, der Werbespot, ein langer Originalbeitrag oder ein kurzer Filmschnipsel oder eine Musikdatei - mit Hilfe von Fingerprints kann Auskunft gegeben werden über Tempo, Genre, Rhythmik, Szenenwechsel, Kamerabewegungen oder Bildhelligkeit. Im Gegensatz zu manuell eingegebenen Metadaten sind die automatisch generierten Fingerprints immer eindeutig. In vielen Archiven werden sie beim Einstellen erzeugt. Bei Verfügbarkeit im Internet müssen sie bei jedem Suchvorgang neu erstellt werden. Dazu war es bislang nötig, komprimierte Dateien zu dekomprimieren. Mit der Multimedia-Suchmaschine Divas, kurz für Direct Video&Audio Content Search Engine, ist das nicht mehr nötig. Sie findet die gesuchte Datei, ohne den gesamten Medienbestand vorher zu entpacken. Divas eignet sich zur Suche im Internet und in Archiven ebenso wie zum Monitoring von TV-Programmen, um etwa die vertragsgemäße Ausstrahlung eines Werbespots zu überprüfen. Weil die Software von komprimierten Dateien Fingerprints nehmen kann, arbeitet sie schneller als vergleichbare Suchmaschinen. Gerald Schuller vom Fraunhofer-Institut für Digitale Medientechnologie IDMT in Ilmenau: „Bei unseren Testreihen mit MP3-Dateien hat sich die Suchdauer fast halbiert" (SZ 15.04.2010, 29).

Google-Mail weitet Werbedatennutzung aus

Google-Mail-Nutzende müssen künftig damit rechnen, dass die kontextgebundene Werbung nicht mehr nur an die jeweils geöffnete Nachricht angepasst wird, sondern auch an ältere Mails. Das Unternehmen gab dies in einem Blog-Posting bekannt. Für einige Nachrichten, etwa Geburtstagswünsche, gäbe es keine „guten" Anzeigen, die Google einblenden könne. In solchen Fällen wolle man zukünftig auf andere Nachrichten zurückgreifen. Google speichere keine zusätzlichen Informationen für die Neuerung. Die Zuordnung von Werbung laufe völlig automatisch ab; MitarbeiterInnen seien bei der Auswahl von Anzeigen nicht involviert, weder Nachrichten noch andere persönliche Informationen würden Anzeigekunden zugänglich gemacht (www.heise.de 21.01.2010).

iPhone unsicher

Gemäß einer Untersuchung der Tübinger Sicherheitsfirma Syss sind die eleganten iPhones riskanter als andere Smartphones. Wenn ein iPhone verbummelt oder geklaut wird, können selbst Amateure den angeblich sicheren Passcode des Geräts leicht knacken und vertrauliche Daten auslesen, inklusive verschlüsselter Passwörter für E-Mail-Accounts, so Sebastian Schreiber von Syss: „Ein Angreifer kann mit Software, die im Internet frei verfügbar ist, in kurzer Zeit an die vertraulichen Daten gelangen." Wichtigstes Hilfsmittel für seinen Testangriff war eine weit verbreitete Jailbreak-Software, die eigentlich dazu gedacht war, das Installieren von Programmen zu ermöglichen, die der Hersteller offiziell nicht zulässt. Das Knacken des iPhones dauert damit nur wenige Minuten. Es gebe nur einen sicheren Schutz: keine vertraulichen Daten und Passwörter auf dem iPhone speichern (Der Spiegel 6/2010, 141).

Rechtsprechung

EuGH

Deutsche Datenschutzaufsicht ist nicht genug unabhängig

Der Europäische Gerichtshof (EuGH) verurteilte die Bundesrepublik Deutschland mit Urteil vom 09.03.2010 dazu, die Organisation der Datenschutzaufsicht über private Firmen unabhängiger zu gestalten (Az. C-518/07). Im Folgenden werden wesentliche Ausführungen des EuGH dokumentiert:

Zur Tragweite des Erfordernisses der Unabhängigkeit der Kontrollstellen

[17] Die Beurteilung der Begründetheit der vorliegenden Klage hängt davon ab, welche Tragweite das Unabhängigkeitserfordernis des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 hat, und somit von der Auslegung dieser Bestimmung. In diesem Zusammenhang sind deren Wortlaut sowie die Ziele und die Systematik der Richtlinie 95/46 heranzuziehen.

[18] Was erstens den Wortlaut von Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 angeht, ist angesichts des Fehlens einer Definition in der Richtlinie auf den gewöhnlichen Sinn der Wendung „in völliger Unabhängigkeit" abzustellen. In Bezug auf öffentliche Stellen bezeichnet der Begriff „Unabhängigkeit" in der Regel eine Stellung, in der gewährleistet ist, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln kann.

[19] Entgegen dem Standpunkt der Bundesrepublik Deutschland deutet nichts darauf hin, dass das Unabhängigkeitserfordernis allein das Verhältnis zwischen den Kontrollstellen und den ihrer Kontrolle unterstellten Einrichtungen beträfe. Im Gegenteil wird der Begriff „Unabhängigkeit" durch das Adjektiv „völlig" verstärkt, was eine Entscheidungsgewalt impliziert, die jeglicher Einflussnahme von außerhalb der Kontrollstelle, sei sie unmittelbar oder mittelbar, entzogen ist.

[20] Zweitens geht in Bezug auf die Ziele der Richtlinie 95/46 insbesondere aus deren Erwägungsgründen 3, 7 und 8 hervor, dass sie durch die Harmonisierung der nationalen Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in erster Linie den freien Verkehr dieser Daten zwischen Mitgliedstaaten gewährleisten soll (vgl. in diesem Sinne Urteil vom 20. Mai 2003, Österreichischer Rundfunk u. a., C-465/00, C-138/01 und C-139/01, Slg. 2003, I-4989, Randnrn. 39 und 70), der für die Errichtung und das Funktionieren des Binnenmarkts nach Art. 14 Abs. 2 EG erforderlich ist.

[21] Der freie Verkehr personenbezogener Daten kann jedoch das Recht auf Privatsphäre beeinträchtigen, wie es u. a. in Art. 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (vgl. in diesem Sinne Urteile des EGMR vom 16. Februar 2000, Amann/Schweiz, Recueil des arrêts et décisions 2000-II, §§ 69 und 80, und vom 4. Mai 2000, Rotaru/Rumänien, Recueil des arrêts et décisions 2000-V, §§ 43 und 46) und durch die allgemeinen Grundsätze des Gemeinschaftsrechts anerkannt ist.

[22] Deshalb und wie insbesondere aus ihrem zehnten Erwägungsgrund und Art. 1 hervorgeht, hat die Richtlinie 95/46 außerdem zum Ziel, den durch die bestehenden nationalen Rechtsvorschriften garantierten Schutz nicht zu verringern, sondern vielmehr in der Gemeinschaft bei der Verarbeitung personenbezogener Daten ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten zu gewährleisten (vgl. in diesem Sinne Urteile Österreichischer Rundfunk u. a., Randnr. 70, sowie vom 16. Dezember 2008, Satakunnan Markkinapörssi und Satamedia, C-73/07, Slg. 2008, I-9831, Randnr. 52).

[23] Die in Art. 28 der Richtlinie 95/46 vorgesehenen Kontrollstellen sind somit die Hüter dieser Grundrechte und Grundfreiheiten, und ihre Einrichtung in den Mitgliedstaaten gilt, wie es im 62. Erwägungsgrund der Richtlinie heißt, als ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten.

[24] Um diesen Schutz zu gewährleisten, müssen die Kontrollstellen zum einen die Achtung des Grundrechts auf Privatsphäre und zum anderen die Interessen, die den freien Verkehr personenbezogener Daten verlangen, miteinander ins Gleichgewicht bringen. Im Übrigen sind die verschiedenen nationalen Kontrollstellen nach Art. 28 Abs. 6 der Richtlinie 95/46 zu gegenseitiger Zusammenarbeit aufgerufen und können gegebenenfalls von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden.

[25] Die Gewährleistung der Unabhängigkeit der nationalen Kontrollstellen soll die wirksame und zuverlässige Kontrolle der Einhaltung der Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherstellen und ist im Licht dieses Zwecks auszulegen. Sie wurde eingeführt, um die von ihren Entscheidungen betroffenen Personen und Einrichtungen stärker zu schützen, und nicht, um diesen Kontrollstellen selbst oder ihren Bevollmächtigten eine besondere Stellung zu verleihen. Folglich müssen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen. Hierzu müssen sie vor jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein und nicht nur vor der Einflussnahme seitens der kontrollierten Einrichtungen.

[26] Drittens ist die Richtlinie 95/46 hinsichtlich ihrer Systematik als Gegenstück zu Art. 286 EG und der Verordnung Nr. 45/2001 zu sehen. Diese betreffen die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft sowie den freien Verkehr dieser Daten. Die Richtlinie verfolgt diese Ziele ebenfalls, aber in Bezug auf die Verarbeitung solcher Daten in den Mitgliedstaaten.

[27] So wie Kontrollstellen auf nationaler Ebene bestehen, ist auch auf der Ebene der Union eine Kontrollstelle damit beauftragt, die Anwendung der Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu überwachen, nämlich der EDSB. Nach Art. 44 Abs. 1 der Verordnung Nr. 45/2001 übt dieser sein Amt in völliger Unabhängigkeit aus. In Abs. 2 desselben Artikels wird zur Erläuterung dieses Begriffs der Unabhängigkeit hinzugefügt, dass der EDSB in Ausübung seines Amtes niemanden um Weisung ersucht und keine Weisungen entgegennimmt.

[28] Angesichts dessen, dass Art. 44 der Verordnung Nr. 45/2001 und Art. 28 der Richtlinie 95/46 dasselbe allgemeine Konzept zugrunde liegt, sind beide Bestimmungen homogen auszulegen, so dass nicht nur die Unabhängigkeit des EDSB, sondern auch die der nationalen Stellen impliziert, dass sie bei der Wahrnehmung ihrer Aufgaben keinerlei Weisungen unterliegen.

[29] Ausgehend vom Wortlaut von Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 sowie von den Zielen und der Systematik dieser Richtlinie ist eine klare Auslegung der genannten Bestimmung möglich. Folglich ist es nicht erforderlich, die Entstehungsgeschichte dieser Richtlinie heranzuziehen oder auf die einander widersprechenden Ausführungen der Kommission und der Bundesrepublik Deutschland dazu einzugehen.

[30] Nach alledem ist Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 dahin auszulegen, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen. Abs. 56

Zur staatlichen Aufsicht

[31] Sodann ist zu prüfen, ob die staatliche Aufsicht, der in Deutschland die Kontrollstellen unterworfen sind, die die Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich überwachen, mit dem so beschriebenen Unabhängigkeitserfordernis vereinbar ist.

[32] Hierzu ist festzustellen, dass die staatliche Aufsicht gleich welcher Art es der Regierung des betroffenen Landes oder einer Stelle der ihr untergeordneten Verwaltung grundsätzlich ermöglicht, auf Entscheidungen der Kontrollstellen unmittelbar oder mittelbar Einfluss zu nehmen bzw. diese Entscheidungen aufzuheben und zu ersetzen.

[33] Es trifft zwar, wie die Bundesrepublik Deutschland geltend macht, a priori zu, dass die staatliche Aufsicht nur sicherstellen soll, dass das Handeln der Kontrollstellen den geltenden nationalen und gemeinschaftsrechtlichen Bestimmungen entspricht, und demnach nicht darauf abzielt, diese Stellen dazu zu zwingen, politische Zielsetzungen zu verfolgen, die dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den Grundrechten zuwiderlaufen.

[34] Es lässt sich aber nicht ausschließen, dass die Aufsichtsstellen, die Teil der allgemeinen Staatsverwaltung und damit der Regierung des jeweiligen Landes unterstellt sind, nicht zu objektivem Vorgehen in der Lage sind, wenn sie die Vorschriften über die Verarbeitung personenbezogener Daten auslegen und anwenden.

[35] Die Regierung des betroffenen Landes hat nämlich, wie der EDSB in seinen Erklärungen hervorhebt, möglicherweise ein Interesse an der Nichteinhaltung der Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, wenn es um die Verarbeitung solcher Daten im nichtöffentlichen Bereich geht. Sie kann selbst involvierte Partei dieser Verarbeitung sein, wenn sie davon betroffen ist oder sein könnte, z. B. im Fall einer Kooperation von öffentlichen und privaten Stellen oder im Rahmen öffentlicher Aufträge an den privaten Bereich. Außerdem könnte sie ein besonderes Interesse haben, wenn sie für

bestimmte ihrer Aufgaben, insbesondere zu Zwecken der Finanzverwaltung oder der Strafverfolgung, Zugang zu Datenbanken benötigt oder ein solcher Zugang einfach nur sachdienlich ist. Im Übrigen könnte diese Regierung auch geneigt sein, wirtschaftlichen Interessen den Vorrang zu geben, wenn es um die Anwendung der genannten Vorschriften durch bestimmte Unternehmen geht, die für das Land oder die Region wirtschaftlich von Bedeutung sind.

[36] Hinzu kommt, dass bereits die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen. Zum einen könnte es, wie die Kommission ausführt, einen „vorauseilenden Gehorsam" der Kontrollstellen im Hinblick auf die Entscheidungspraxis der Aufsichtsstellen geben. Zum anderen erfordert die Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre, dass ihre Entscheidungen, also sie selbst, über jeglichen Verdacht der Parteilichkeit erhaben sind.

[37] Nach alledem ist festzustellen, dass die staatliche Aufsicht, der die für die Überwachung der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zuständigen Kontrollstellen in Deutschland unterworfen sind, nicht mit dem Unabhängigkeitserfordernis, wie es in Randnr. 30 des vorliegenden Urteils beschrieben ist, vereinbar ist.

Zu den von der Bundesrepublik Deutschland angeführten Grundsätzen des Gemeinschaftsrechts

[38] Nach Auffassung der Bundesrepublik Deutschland würde es gegen mehrere Grundsätze des Gemeinschaftsrechts verstoßen, das Unabhängigkeitserfordernis des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 so auszulegen, dass der Mitgliedstaat gezwungen wäre, sein bewährtes und effektives System der Aufsicht über die Kontrollstellen hinsichtlich der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich aufzugeben.

[39] Erstens stehe insbesondere das Demokratieprinzip einer weiten Auslegung dieses Unabhängigkeitserfordernisses entgegen.

[40] Dieses Prinzip, das nicht nur in der deutschen Verfassung, sondern auch in Art. 6 Abs. 1 EU verankert sei, verlange eine Weisungsgebundenheit der Verwaltung gegenüber der Regierung, die ihrerseits dem Parlament verantwortlich sei. So müssten Eingriffe in die Rechte der Bürger und Unternehmen der Rechtsaufsicht des zuständigen Ministers unterliegen. Da die Kontrollstellen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gemäß Art. 28 Abs. 3 der Richtlinie 95/46 über bestimmte Eingriffsbefugnisse gegenüber Bürgern und dem nichtöffentlichen Bereich verfügten, sei eine erweiterte Rechtmäßigkeitskontrolle ihres Handelns über Rechts- oder Fachaufsichtsinstrumente dringend geboten.

[41] Hierzu ist festzustellen, dass der Grundsatz der Demokratie zur Gemeinschaftsrechtsordnung gehört und in Art. 6 Abs. 1 EU ausdrücklich als Grundlage der Europäischen Union niedergelegt ist. Als den Mitgliedstaaten gemeinsamer Grundsatz ist er daher bei der Auslegung eines sekundärrechtlichen Aktes wie Art. 28 der Richtlinie 95/46 zu berücksichtigen.

[42] Dieser Grundsatz bedeutet nicht, dass es außerhalb des klassischen hierarchischen Verwaltungsaufbaus keine öffentlichen Stellen geben kann, die von der Regierung mehr oder weniger unabhängig sind. Das Bestehen und die Bedingungen für das Funktionieren solcher Stellen sind in den Mitgliedstaaten durch Gesetz und in einigen Mitgliedstaaten sogar in der Verfassung geregelt, und diese Stellen sind an das Gesetz gebunden und unterliegen der Kontrolle durch die zuständigen Gerichte. Solche unabhängigen öffentlichen Stellen, wie es sie im Übrigen auch im deutschen Rechtssystem gibt, haben häufig Regulierungsfunktion oder nehmen Aufgaben wahr, die der politischen Einflussnahme entzogen sein müssen, bleiben dabei aber an das Gesetz gebunden und der Kontrolle durch die zuständigen Gerichte unterworfen. Eben dies ist bei den Aufgaben der Kontrollstellen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten der Fall.

[43] Gewiss kommt ein Fehlen jeglichen parlamentarischen Einflusses auf diese Stellen nicht in Betracht. Die Richtlinie 95/46 schreibt jedoch den Mitgliedstaaten keineswegs vor, dem Parlament jede Einflussmöglichkeit vorzuenthalten.

[44] So kann zum einen das Leitungspersonal der Kontrollstellen vom Parlament oder der Regierung bestellt werden. Zum anderen kann der Gesetzgeber die Kompetenzen der Kontrollstellen festlegen.

[45] Außerdem kann der Gesetzgeber die Kontrollstellen verpflichten, dem Parlament Rechenschaft über ihre Tätigkeiten abzulegen. Insoweit lässt sich eine Parallele zu Art. 28 Abs. 5 der Richtlinie 95/46 ziehen, wonach jede Kontrollstelle regelmäßig einen Bericht über ihre Tätigkeit vorlegt, der veröffentlicht wird.

[46] Nach alledem ist der Umstand, dass den Kontrollstellen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich eine von der allgemeinen Staatsverwaltung unabhängige Stellung zukommt, für sich allein noch nicht geeignet, diesen Stellen die demokratische Legitimation zu nehmen.

[47] Zweitens verpflichtet der von der Bundesrepublik Deutschland ebenfalls angeführte, in Art. 5 Abs. 1 EG verankerte Grundsatz der begrenzten Einzelermächtigung die Gemeinschaft, nur innerhalb der Grenzen der ihr im EG-Vertrag zugewiesenen Befugnisse und gesetzten Ziele tätig zu werden.

[48] Die Bundesrepublik Deutschland macht insoweit geltend, die Unabhängigkeit der Kontrollstellen von den übergeordneten Verwaltungsstellen könne nicht auf der Grundlage von Art. 100a EG-Vertrag, auf den die Richtlinie 95/46 gestützt sei, verlangt werden.

[49] Diese Bestimmung ermächtigt den Gemeinschaftsgesetzgeber zum Erlass von Maßnahmen zur Verbesserung der Bedingungen für die Errichtung und das Funktionieren des Binnenmarkts, wobei die entsprechenden Maßnahmen tatsächlich dieses Ziel verfolgen und dazu beitragen müssen, Hemmnisse für die mit dem EG-Vertrag garantierten wirtschaftlichen Freiheiten zu beseitigen (vgl. in diesem Sinne u. a. Urteile vom 5. Oktober 2000, Deutschland/Parlament und Rat,

C-376/98, Slg. 2000, I-8419, Randnrn. 83, 84 und 95, vom 10. Dezember 2002, British American Tobacco [Investments] und Imperial Tobacco, C-491/01, Slg. 2002, I-11453, Randnr. 60, sowie vom 2. Mai 2006, Parlament/Rat, C-436/03, Slg. 2006, I-3733, Randnr. 38).

[50] Wie bereits dargelegt, ist die Unabhängigkeit der Kontrollstellen in dem Sinne, dass sie jeglicher äußeren Einflussnahme entzogen sein müssen, die ihre Entscheidungen steuern könnte, ein im Hinblick auf die Ziele der Richtlinie 95/46 wesentliches Element. Sie ist erforderlich, um in allen Mitgliedstaaten ein gleich hohes Niveau des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten zu schaffen, und trägt so zum freien Datenverkehr bei, der für die Errichtung und das Funktionieren des Binnenmarkts erforderlich ist.

[51] Nach alledem geht eine weite Auslegung des Erfordernisses der Unabhängigkeit der Kontrollstellen nicht über die Grenzen der Befugnisse hinaus, die der Gemeinschaft nach Art. 100a EG-Vertrag, der die Rechtsgrundlage der Richtlinie 95/46 bildet, zugewiesen werden.

[52] Drittens beruft sich die Bundesrepublik Deutschland auf die in Art. 5 Abs. 2 und 3 EG verankerten Grundsätze der Subsidiarität und der Verhältnismäßigkeit sowie auf den Grundsatz der loyalen Zusammenarbeit zwischen den Mitgliedstaaten und den Gemeinschaftsorganen nach Art. 10 EG.

[53] Sie verweist insbesondere auf Nr. 7 des durch den Vertrag von Amsterdam dem EU-Vertrag und dem EG-Vertrag beigefügten Protokolls über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit, wonach bewährte nationale Regelungen sowie Struktur und Funktionsweise der Rechtssysteme der Mitgliedstaaten unter Einhaltung der gemeinschaftlichen Rechtsvorschriften geachtet werden sollten.

[54] Es verstoße gegen dieses Erfordernis, wenn die Bundesrepublik Deutschland gezwungen werde, ein ihrer Rechtsordnung fremdes System zu übernehmen und damit ein effektives, seit fast 30 Jahren bewährtes Kontrollsystem aufzugeben, das weit über den nationalen Bereich hinaus richtungsweisend für die Datenschutzgesetzgebung gewesen sei.

[55] Diesem Vorbringen ist nicht zu folgen. Wie in den Randnrn. 21 bis 25 sowie 50 des vorliegenden Urteils ausgeführt, geht die Auslegung des Unabhängigkeitserfordernisses des Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 in dem Sinne, dass dieses Erfordernis einer staatlichen Aufsicht entgegensteht, nicht über das hinaus, was zur Erreichung der Ziele des EG-Vertrags erforderlich ist.

[56] In Anbetracht aller vorstehenden Erwägungen ist festzustellen, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben "in völliger Unabhängigkeit" wahrnehmen, falsch umgesetzt hat.

Das oben in den wichtigsten Passagen abgedruckte Urteil wird Auswirkungen im Bund wie in allen Bundesländern haben. Am stärksten trifft es die Länder, bei denen die Datenschutzaufsicht im nicht-öffentlichen Bereich noch in der Innenverwaltung stattfindet, also in Baden-Württemberg, Bayern, Brandenburg, Hessen, Saarland, Sachsen-Anhalt und Thüringen. Die Musik beim Datenschutz spielt genau in diesem Bereich. So konstatierte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) Johannes Caspar in seinem Tätigkeitsbericht, dass inzwischen 80% aller Eingaben den Wirtschaftsbereich betreffen. Das Urteil legt nahe, die Datenschutzbehörden als oberste Bundes- bzw. Landesbehörden, gleichgestellt den Ministerien oder den Rechnungshöfen auszugestalten. Dagegen gibt es Widerstand, z.B. in Bayern. So meinte der zuständige Regierungspräsident Thomas Bauer, man würde am liebsten alles lassen wie bisher. Die Landesregierung habe doch noch nie Einfluss genommen und die Datenschutzbehörde habe auch jetzt schon (seit kurzem, vgl. DANA 2/2009, 71) eine sichtbare Sonderstellung. Der Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein Thilo Weichert, beschreibt dagegen, dass Firmen immer wieder versucht hätten, über die Regierung bzw. das als Rechtsaufsicht eingesetzte Innenministerium Einfluss zu nehmen, z.B. Google oder die Schufa, doch hätten sie hiermit keinen Erfolg gehabt.

Wie weit die Sonderstellung der Datenschutzaufsicht gehen wird, ist noch nicht absehbar, insbesondere inwieweit die Sonderstellung auch die Dienstaufsicht einschränkt, wie die Haushalte aufgestellt werden, wie die Verwaltung und v.a. das Personalmanagement geordnet wird. Der HmbBfDI Johannes Caspar meinte: "Wenn wir überall frei agieren müssten, beispielsweise beim Personalmanagement, wäre das eine zusätzliche Aufgabe, für die wir gar nicht die Kapazität haben." Daher könne man die neue Stärke gar nicht nutzen. Freiheit bekomme man nur, "wenn man die Freiräume auch besetzen kann". Kaum Änderungen wird es in Schleswig-Holstein und in Berlin geben. Das ULD ist eine Anstalt des öffentlichen Rechts; der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist schon oberste Landesbehörde. Einen weiteren "positiven Nebeneffekt" des Urteils sieht der ULD-Leiter Weichert außerdem darin, "dass wir nun gezwungen sind, eine einheitliche nationale Struktur der Datenschutzbehörden aufzubauen". Bisher war der öffentliche Bereich in der Datenschutzkonferenz und der nicht-öffentliche Bereich im sog. "Düsseldorfer Kreis" organisiert (Biermann www.zeit.de 09.03.2010).

VG Berlin

Kein Anspruch auf Einschreiten der Datenschutzaufsicht bei Internetpresse

Das Verwaltungsgericht (VG) Berlin wies mit Gerichtsbescheid vom 23.03.2010 die Klage eines Petenten des Berliner Datenschutzbeauftragten (BlnBDI) zurück, der von diesem ein

Einschreiten gegen Veröffentlichungen im Internet zu seiner Person forderte (Az. VG 1 K 285.09). Die Beschwerde richtete sich gegen im Internet abrufbare Zeitungsartikel, die Bezug nahmen auf eine datenschutzrechtlich zulässige Presseerklärung des Kammergerichts zu einer strafrechtlichen Verurteilung des Klägers und Petenten. Dieser trug vor, dass der Verbleib dieser Artikel im Internet gegen den Resozialisierungsgedanken verstoße. Er hatte zunächst erfolglos von den Presseorganen eine Löschung der Beiträge gefordert. Dann verlangte er erfolglos vom BlnBDI, gegen die Presseorgane vorzugehen. Der BlnBDI machte geltend, die Verarbeitung personenbezogener Daten zu journalistischen Zwecken dürfe von ihm aufgrund des in § 41 Abs. 1 Bundesdatenschutzgesetz (BDSG) geregelten „Medienprivilegs" für Presseerzeugnisse nicht kontrolliert werden. Das VG wies die Klage mit folgenden Gründen ab:

„Der Kläger hat nach den Grundsätzen über das Petitionsrecht einen Anspruch darauf, dass der Berliner Datenschutzbeauftragte Eingaben von Bürgern prüft und darauf antwortet (vgl. BVerfG NJW 1977, 118). Diesen Anspruch hat der Beklagte mit seinem Schreiben erfüllt. Der Kläger hat aber keinen Anspruch auf ein aufsichtsrechtliches Einschreiten des Datenschutzbeauftragten gegen die vom Kläger genannten Zeitungen und den Rundfunk Berlin-Brandenburg. § 38 BDSG, der die Befugnisse des Datenschutzbeauftragten als Aufsichtsbehörde auch über nicht-öffentliche Stellen regelt, gilt gem. § 41 Abs. 1 BDSG nicht für Presseveröffentlichungen zu journalistisch-redaktionellen Zwecken („Medienprivileg"). Davon sind auch Presseartikel erfasst, die über das Internet abrufbar sind (vgl. BGHZ 181, 328; juris Rn. 20, 21). Dem Beklagten fehlt die Möglichkeit, im Sinne des Klägers u.a. auf die Berliner Zeitung, die Berliner Morgenpost und den Tagesspiegel und den Rundfunk Berlin-Brandenburg wegen eines Beitrags in der Abendschau vom 30.10.12007 einzuwirken."

VG Bremen

Keine Auskunft aus Datenschutzkontrolle an geprüfte Stelle

Mit Urteil vom 25.03.2010 entschied das Verwaltungsgericht (VG) der Freien Hansestadt Bremen, dass ein zu Recht von einem Petenten, einem früheren Beschäftigten, angeschwärztes Unternehmen keinen Anspruch auf Akteneinsicht bzw. Auskunft über den Informanten hat (Az.):

„4. Den Klägern ... stehen auch keine verfahrensunabhängigen Akteneinsichts- und Auskunftsrechte nach § 21 BremDSG zu. ...

Die Information des Petenten war sachlich und enthielt keine strafbaren Inhalte. ... Im Ergebnis stellt sich seine E-Mail vom 10.01.2009 als ein nachgerade typischer Fall einer Mitteilung an die Aufsichtsbehörde nach § 38 Abs. 1 Satz 8 i.V.m. § 21 Satz 1 BDSG dar. ... Da der Petent mit seiner Mitteilung keine Straftat begangen hat, ist seine Identität von der Beklagten zu schützen. Das Begehren der Kläger ..., seinen Namen zu offenbaren, würde darauf hinauslaufen, ihn Pressionen der Kläger auszusetzen. Dies gilt, ohne dass dieses einer näheren Darlegung bedarf - ohne weiteres, wenn es sich bei dem Petenten nach wie vor um einen Beschäftigten der Klägerin ... handeln sollte. Aber auch dann, wenn der Petent aus dem Betrieb der Klägerin ... inzwischen ausgeschieden wäre, müsste er angesichts des bisherigen Vorgehens der Kläger damit rechnen, dass ihm in verschiedener Weise zugesetzt würde. Angesichts der Bewertung seines Handelns durch die Kläger als geschäftsschädigende Denunziation lassen sich vielfältige Möglichkeiten zu Pressionen denken, die auf ihn mit anwaltlicher Hilfe und bei der bestehenden wirtschaftlichen Übermacht der Klägerseite ausgeübt werden könnte.

Dieses ist aber angesichts der Inanspruchnahme eines gesetzmäßigen Rechts durch den Petenten auf Mitteilung an die Aufsichtsbehörde nach § 38 Abs. 1 Satz 8 i.V.m. § 21 Satz 1 BDSG nicht als berechtigtes Interesse der Kläger .... anzusehen. Hinzu kommt, dass die Hinweise des Petenten in der Sache berechtigt waren. ...

5. Auf verfahrensunabhängige Akteneinsichts- und Auskunftsansprüche nach dem Bremer Informationsfreiheitsgesetz (BremIFG) können sich die Kläger ... auch nicht berufen. Soweit es um die Verarbeitung personenbezogener Daten zum Zwecke der Datenschutzkontrolle durch die Aufsichtsbehörde geht, ist das Bremische Datenschutzgesetz das speziellere Gesetz. Es hat damit Anwendungsvorrang vor dem BremIFG. Dementsprechend bestimmt auch § 1 Abs. 3 BremIFG, dass Regelungen in anderen Rechtsvorschriften über den Zugang zu amtlichen Informationen mit Ausnahme von § 29 BremVwVfG vorgehen ...

Stellt die Aufsichtsbehörde einen Verstoß gegen datenschutzrechtliche Vorschriften fest, ist sie danach befugt, die Betroffenen hierüber zu unterrichten. ...

Dass die Verletzung des Datenschutzes durch die Klägerin .... kein Betriebsgeheimnis darstellen kann, folgt schon aus dem Umstand, dass die Aufsichtsbehörde gesetzlich befugt ist, diesen Umstand nach Maßgabe des § 38 Abs. 1 Satz 6 bekannt zu geben. Das schließt das Vorliegen eines gesetzlich geschützten Geheimnisses aus."

VG Schleswig

Informant über Raucherschutzverbotsverstoß bleibt geheim

Das Verwaltungsgericht (VG) Schleswig hat mit Urteil vom 03.12.2009 die Klage einer Inhaberin einer Kieler Gaststätte zurückgewiesen, die mehrfach gegen das Rauchverbot in Lokalen verstoßen hatte, mit der sie Name und Adresse des Informanten erfahren wollte, der die zuständige Ordnungsbehörde auf diese Verstöße hingewiesen hatte. Weder das allgemeine Verwaltungsrecht, noch das Informationsfreiheitsgesetz Schleswig-Holstein gewähren danach einer WirtIn einen Anspruch auf uneingeschränkte Akteneinsicht. Die Stadt Kiel hatte die Einsicht aus grundsätzlichen Erwägungen abgelehnt: BürgerInnen, die sich an Ordnungsbehörden wendeten, um zu ihrem Recht zu kommen,

sollen deswegen keine negative Folgen befürchten müssen (SH-Z 17.02.2010, 3).

BGH

Schwerkriminelle bleiben langfristig im Netz

Namen, Fotos und weitere Angaben über den Kriminalfall früherer Straftäter dürfen nach Urteilen des Bundesgerichtshofs (BGH) in Karlsruhe vom 09.02.2010 im Internet sichtbar bleiben (Az: VI ZR 243/08 und 244/08). Die Täter, es handelte sich um die Mörder des Schauspielers Walter Sedlmayr, hätten auch nach ihrer Haftentlassung keinen generellen Anspruch darauf, dass Online-Archive entsprechend bereinigt würden. Die Täter hatten gegen Spiegel Online geklagt. Sie waren 1993 wegen des Mordes an Sedlmayr zu lebenslangen Haftstrafen verurteilt und 2007 beziehungsweise 2008 entlassen worden. Ihre Tat hatte großes öffentliches Aufsehen erregt. Spiegel Online bot nach der Haftentlassung der beiden ein kostenpflichtiges Internet-Dossier mit Hintergründen und alten Artikeln über den Mord zum Herunterladen an. In den Originalberichten waren auch Namen, Fotos und weitere Angaben zu den Verurteilten enthalten. Das Duo bestreitet die Tat bis heute. Es hatte im Jahr 2004 Anträge auf Wiederaufnahme des Verfahrens gestellt; vor deren Zurückweisung hatten sie sich an die Presse gewandt. Die Kläger machten nun geltend, die Angaben im Internet behinderten ihre Wiedereingliederung in die Gesellschaft. Die Klage hatte in den Vorinstanzen Erfolg. Auf die Revision des Spiegels hob der BGH die Urteile der Vorinstanzen auf und wies die Klagen ab.

Die Verurteilten waren schon im Dezember 2009 in einem ganz ähnlichen Verfahren gegen das Deutschlandradio gescheitert. Weitere Klagen sind beim BGH, beim Europäischen Gerichtshof (EuGH) in Luxemburg sowie den Justizbehörden in den USA anhängig. Die Karlsruher BGH-Richter erkannten zwar in dem Internetangebot einen Eingriff in das Persönlichkeitsrecht der Kläger, jedoch sei dieser nicht rechtswidrig. Im besonderen Fall müsse das Schutzinteresse der Kläger hinter dem Informationsinteresse der Öffentlichkeit und dem Recht auf freie Meinungsäußerung zurückstehen. Das veröffentlichte Dossier sei nicht geeignet, die Kläger „ewig an den Pranger“ zu stellen oder in einer Weise „an das Licht der Öffentlichkeit zu zerren“, die sie als Straftäter (wieder) neu stigmatisieren könnte. Die zusammengefassten Meldungen enthielten sachbezogene, wahrheitsgemäße Aussagen über ein Kapitalverbrechen an einem bekannten Schauspieler, das erhebliches öffentliches Aufsehen erregt hatte. Angesichts der Schwere des Verbrechens, der Bekanntheit des Opfers, des erheblichen Aufsehens, das die Tat in der Öffentlichkeit erregt hatte, und des Umstands, dass sich die Verurteilten noch im Jahr 2004 um die Aufhebung ihrer Verurteilung bemüht hatten, seien die Meldungen zum Zeitpunkt der erstmaligen Veröffentlichung zulässig gewesen.

Hieran habe sich trotz der zwischenzeitlich erfolgten Entlassung der Kläger aus der Haft nichts geändert. Dem Dossier käme nur eine geringe Breitenwirkung zu. Es enthalte nur eindeutig als solche erkennbare Altmeldungen und sei nur durch gezielte Suche auffindbar. Darüber hinaus setze die Kenntnisnahme von den die Kläger identifizierenden Inhalten den kostenpflichtigen Abruf des Dossiers voraus, wodurch der Zugang zu den beanstandeten Inhalten zusätzlich erschwert werde. Zu berücksichtigen sei weiterhin, dass ein anerkennenswertes Interesse der Öffentlichkeit nicht nur an der Information über das aktuelle Zeitgeschehen, sondern auch an der Möglichkeit besteht, vergangene zeitgeschichtliche Ereignisse zu recherchieren. Würde das weitere Bereithalten eindeutig als Altmeldung erkennbar und sei diese im Zeitpunkt der erstmaligen Veröffentlichung zulässig, so würde nach Ablauf einer gewissen Zeit oder nach Veränderung der zugrunde liegenden Umstände die Veröffentlichung nicht ohne weiteres unzulässig. Anderenfalls wäre die Beklagte verpflichtet, von sich aus sämtliche archivierten Meldungen immer wieder auf ihre Rechtmäßigkeit zu kontrollieren. Hierdurch würde die Meinungs- und Medienfreiheit nach Art. 5 Grundgesetz in unzulässiger Weise eingeschränkt. Angesichts des mit einer derartigen Kontrolle verbundenen personellen und zeitlichen Aufwands bestünde die Gefahr, dass die Beklagte entweder ganz von einer der Öffentlichkeit zugänglichen Archivierung absehen oder bereits bei der erstmaligen Veröffentlichung die Umstände ausklammern würde, die – wie vorliegend der Name des Straftäters – die Meldung später rechtswidrig werden lassen könnten, an deren Mitteilung die Öffentlichkeit aber im Zeitpunkt der erstmaligen Berichterstattung ein schützenswertes Interesse hat.

Den Klägern steht demnach auch kein Anspruch auf Unterlassung erneuter Verbreitung der in den Meldungen enthaltenen Bilder zu. Bei den beanstandeten Abbildungen handele es sich um Bildnisse aus dem Bereich der Zeitgeschichte gemäß § 23 Abs. 1 Nr. 1 KUG, die auch ohne Einwilligung der Kläger als Teil des beanstandeten Dossiers zum Abruf im Internet bereitgehalten werden durften. Die Fotos illustrieren die Meldungen, in denen wahrheitsgemäß, sachbezogen und objektiv über die Anklageerhebung gegen die Kläger wegen Mordes an einem bekannten Schauspieler bzw. den Beginn der Hauptverhandlung berichtet wird und die damit an ein zeitgeschichtliches Ereignis anknüpfen. Die Aufnahmen seien somit kontextbezogen (www.spiegel.de 09.02.2010; Bundesgerichtshof PM Nr. 30/2010 09.02.2010).

OLG Düsseldorf

Pressefreiheit erlaubt versteckte Kamera

Das Oberlandesgericht (OLG) Düsseldorf hat nach Verhandlung am 25.01.2010 am 08.03.2010 eine einstweilige Verfügung des Landgerichts (LG) Düsseldorf aufgehoben, wonach dem Fernsehsender RTL bescheinigt wurde, dass ein heimliches Filmen in der Praxis eines klagenden Arztes unzulässig war, weil der Mediziner dadurch in seinem allgemeinen Persönlichkeitsrecht verletzt wurde. RTL hatte gegen diese Entscheidung Beschwerde eingelegt und argumentiert, ein Anfertigungsverbot

von Aufnahmen mit versteckter Kamera schränke die gesamt Branche in ihrem journalistischen Handlungsspielraum ein, und erhielt vom OLG Recht (SZ 09.03.2010, 15; OLG Düsseldorf PM 22.01.2010).

OLG Frankfurt/Main

Kein DNA-Vaterschaftstest bei sozial-familiärer Beziehung

Behörden haben nach § 1600 Abs. 3 BGB das Recht, Vaterschaftsanerkennungen mit aufenhaltsrechtlichen Konsequenzen anzufechten. Voraussetzung ist der Verdacht, dass es sich nicht um den biologischen Vater handelt und, dass zwischen dem Anerkennenden und dem Kind keine sozial-familiäre Beziehung besteht. Das Amtsgericht lud im konkreten Fall den Anerkennenden unter Androhung einer zwangsweisen Vorführung zu einem DNA-Test. Dieser wehrte sich hiergegen beim Oberlandesgericht (OLG) Frankfurt/Main mit dem Argument, dass es auf eine derartige Untersuchung gar nicht ankomme. Das OLG gab dem Anerkennenden mit Beschluss vom 16.02.2010 Recht (Az. 1 W 36/10). Der Einwand, dieser habe eine sozial-familiäre Beziehung zum Kind, sei erheblich. Das Tatsachengericht müsse gemäß § 387 ZPO prüfen und gegebenenfalls durch Zwischenurteil entscheiden, ob die Entnahme einer DNA-Probe zu Recht verweigert wurde. Ist diese nicht nötig, so muss der DNA-Abgleich dem Anerkennenden auch nicht zugemutet werden (ANA-ZAR 2/2010, 15).

LG Köln

Internet-Straßenansichten seien zulässig

Das Landgericht Köln wies mit Urteil vom 13.01.2010 die Klage einer Klägerin ab, die die Ansicht vertrat, die Abbildung von Gebäuden und Häuser der Stadt Köln im Internetportal „Bilderbuch-Köln“ sei unzulässig (28 O 578/09). Die Klägerin ist Eigentümerin eines Hauses in Köln. Die beklagte Betreiberin der Internetportals verfolgt das erklärte Ziel, in absehbarer Zeit im Internet jedes Gebäude in Köln abzubilden. Zur Erschließung der Bilder wird Google Maps eingesetzt; die Fotos stammen von diversen Nutzern. Die Gebäude können bei der Beklagten auch über eine Adresssuche gefunden werden. Die Klägerin meinte, dass dies eine unzulässige Veröffentlichung personenbezogener Daten sei und im übrigen ihr allgemeines Persönlichkeitsrecht verletzt wird. Das Gericht ging davon aus, dass ein Eingriff in das allgemeine Persönlichkeitsrecht ausscheidet, weil die veröffentlichten Fotos nur das abbilden, was jedermann von der Straße aus ohnehin sehen kann. Mit Blick auf den geltend gemachten Verstoß gegen Datenschutzrecht meinte es, dass sich die Beklagte auf das Medienprivileg des § 41 BDSG berufen kann, weil sie u.a. auch Informationen zur Architektur und Stadtgeschichte anbietet. Abgesehen davon sei eine Verwendung des Bildmaterials nach § 29 Abs. 2 BDSG zulässig, insbesondere wegen der Bedeutung der Meinungs- und Informationsfreiheit (www.jurablog.com 08.02.2010; www.internet-law.de 08.02.2010).

LG Münster

Mitgliederdatenherausgabeanspruch an einzelnes Mitglied

Das Landgericht (LG) Münster gewährte in Beschlüssen vom 02.02., 22.02.und 25.02.2010 im Rahmen eines einstweiligen Rechtsschutzverfahrens einem einfachen Mitglied des Vereins Slow Food den Zugriff auf die E-Mail-Adressen aller 9.600 Vereinsmitglieder - unter der Voraussetzung allerdings, dass diese von einem Treuhänder verwaltet werden (Az. 014 O 60/10). Diesen aber dürfe sich der Kläger Jörn Frühauf, ein pensionierter Psychologe aus Berlin, selbst aussuchen. Jederzeit könnten also „Kläger und Treuhänder Daten austauschen, und niemand kontrolliert das“, fürchtet Ulrich Rosenbaum, der Leiter der Berliner Sektion des Vereins. Der Kläger hatte zuvor an Slow Food geschrieben, er wolle bald für den Vorstand kandidieren, weshalb er sich allen Mitgliedern per Newsletter vorstellen müsse. Der Verein, der für mehr Genuss beim Essen und gegen die Verbreitung von Fast Food kämpft, weigerte sich. Die Klage hiergegen beim LG Münster war erfolgreich.

„Der Verfügungsanspruch folgt aus einem mitgliedschaftlichen Informationsanspruch, der sich aus den allgemeinen vereinsrechtlichen Grundsätzen ableiten lässt. Das privatrechtliche Vereinsrecht gibt den Mitgliedern von Vereinen einen durchsetzbaren Anspruch auf Einsicht in die Mitgliederlisten und Herausgabe einer Abschrift mit deren Anschriften (vgl. Saarländisches Oberlandesgericht, Urteil vom 02.04.2008 1 U 450/07 m.w.N.). Der Anspruch beruht darauf, dass sich der Einzelne bei privatrechtlichen Vereinen freiwillig dem Verein angeschlossen hat und damit mit den anderen Mitgliedern in eine gewollte Rechtsgemeinschaft eingetreten ist, die von ihm auch fordert, dass er den anderen Mitgliedern bei berechtigtem Interesse derselben den Kontakt mit ihm durch Angabe seiner Personalien ermöglicht, ganz im Gegenteil zu dem Zwangsmitglied in einer Zwangskörperschaft, das den anderen Mitgliedern nicht die Preisgabe persönlicher Daten schuldet (vgl. Saarländisches Oberlandesgericht a.a.O.).

In der Person des Klägers ist ein berechtigtes Interesse an der Aushändigung einer Mitgliederliste zu bejahen. Er beabsichtigt, in der Mitgliederversammlung in Würzburg am 27.02.2010 für ein Vorstandsamt zu kandidieren. Darin ist zugleich der Verfügungsgrund für den Erlass der einstweiligen Verfügung zu sehen. Dem berechtigten Anliegen des Verfügungsklägers stehen auch nicht sonstige Gründe entgegen, insbesondere nicht die Interessen der übrigen Vereinsmitglieder. Diese werden durch den Treuhänder gewahrt. Dieser wird vor Verbreitung von Informationen des Verfügungsklägers zur bevorstehenden Wahl die Mitglieder informieren müssen, so dass diese die Wahl haben, ihrerseits dem Treuhänder mitzuteilen, ob ihnen Informationen des Antragstellers zugeleitet werden oder nicht. So hat jedes Mitglied selbst die Möglichkeit zu entscheiden, ob es E-Mail-Post des

Verfügungsklägers entgegen nehmen möchte oder nicht. Die Gefahr von `aufgezwungenen Newsletter´ - wie vom Verfügungsbeklagten dargestellt - besteht somit überhaupt nicht."

Kein Rolle bei der Entscheidung spielte, dass es auf der Internetseite von Slow Food einen geschützten Bereich gibt, in dem jeder seine Kandidatur publik machen kann. Der Landesbeauftragte für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen (LDI NRW) kritisierte die Entscheidung. Die Erforderlichkeit der begehrten Datenübermittlung erschließe sich nicht, weil „Diskussionspapiere und Kandidatenvorstellungen auf der Homepage für alle Mitglieder präsentiert werden können", heißt es in einem Gutachten. Die Herausgabe einer Liste aller Vereinsmitglieder an ein Einzelmitglied sei vor diesem Hintergrund als „datenschutzrechtlich unzulässig" anzusehen. Die Entscheidung des Gerichts sei deshalb „heikel", so Behördensprecherin Bettina Gayk.

„Das Gericht hat hier ganz klar gegen geltendes Recht verstoßen", ärgert sich auch Ulrich Rosenbaum. Es käme bei dezentral geführten Vereinen wie Slow Food mit Tausenden Mitgliedern gerade nicht darauf an, dass sich die Mitglieder untereinander kennen. Wer einem solchen Verein beitrete, habe nicht zwingend Interesse am Kontakt mit anderen Mitgliedern. „Wenn der Beschluss generell gelten würde, könnte sich bald jedes einfache Vereinsmitglied die Daten anderer Mitglieder beschaffen", befürchtet die Berliner Datenschutzanwältin Christine Wehr. Das gelte auch für Vereine wie den Automobilklub ADAC oder Amnesty International. Für Datenmissbrauch gibt es zwar im konkreten Fall kein Indiz, allerdings soll der beauftragte Treuhänder die Daten inzwischen an vier Personen weitergegeben haben, weil er sich selbst überfordert fühlte.

Slow Food hat gegen den Beschluss Beschwerde eingelegt. Es habe an die hundert Austritte gegeben, sagt Ulrich Rosenbaum, schon jetzt sei ein hoher finanzieller Schaden entstanden. Viele Mitglieder hätten sich schriftlich gegen die Datenweitergabe gewehrt, zum Beispiel der ehemalige Bundesverkehrsminister Volker Hauff (SPD). „Ich fordere Sie auf, mir die Streichung meiner privaten E-Mail-Adresse und des vorhandenen Datenbestands zu bestätigen. Einzig für diese Bestätigung gestatte ich Ihnen die Nutzung meiner privaten E-Mail-Adresse." Bei den Vorstandswahlen in Würzburg hat der Kläger Frühauf die Quittung für seinen Newsletter bekommen: Nur neun von 330 Delegierten stimmten für ihn. Inzwischen scheint ihm die Sache selbst peinlich zu sein. Er wolle die Adressen zurückgeben, ließ Frühauf den Verein wissen. Die Aktion sei ein Riesenfehler gewesen (Kuhn www.morgenpost.de 12.03.2010; Kuhn www.welt.de 16.03.2010).

AG Halle

Schufa darf umstrittene Forderungen nicht speichern

Das Amtsgericht (AG) Halle hat mit Beschluss vom 09.12.2009 entschieden, dass umstrittene Forderungen bei der Schufa nicht eingetragen werden dürfen (Az. 105 C 4636/09). Betroffen war eine Person, die auf eine Abofalle im Internet hereingefallen war und dann die Zahlung verweigerte. Ihm war mit einem Schufaeintrag gedroht worden, wovon er sich - nach Ansicht des AG zu Recht - nicht beeindrucken ließ (Finanztest 3/2010, 8).

BFH

Neugierde von Finanzämtern gebremst

Der Bundesfinanzhof (BFH) hat mit Urteil von 24.02.2010 entschieden, dass ein Finanzamt im Besteuerungsverfahren eines Bankkunden von der Bank im Regelfall erst dann die Vorlage von Kontoauszügen verlangen kann, wenn die Bank eine zuvor geforderte Auskunft über das Konto nach § 93 Abgabenordnung nicht erteilt hat, wenn die Auskunft unzureichend ist oder Bedenken gegen ihre Richtigkeit bestehen (Az. II R 57/08). In dem Fall hatte das Finanzamt zunächst von einer Bankkundin persönlich die Kontoauszüge verlangt, um ihre Angaben überprüfen zu können. Die Kundin hatte diese jedoch vernichtet. Daraufhin wandte sich die Behörde an die Bank und verlangte die Herausgabe der Kontoauszüge. Diese weigerte sich nach Ansicht des BFH zu Recht. Zuerst hätte das Finanzamt die Bank um Auskunft über die Höhe der Umsätze bitten müssen. Wäre dies erfolglos geblieben, hätte es die Original-Kontoauszüge verlangen können (SZ 08.04.2010, 24; BFH PM Nr. 28 07.04.2010).

Europäischer Gerichtshof

Verstoß gegen „Terrorliste" nicht strafbar.

Mit Urteil vom 29.6.2010 hat der Europäische Gerichtshof (EuGH) in Luxemburg die Anwendung von § 34 Aussenwirtschaftsgesetzes stark beschnitten. Die Vorschrift stellt u.a. die Sammlung von Finanzmitteln für eine Organisation, die auf den sog. Terrorlisten der Europäischen Union steht, unter Strafe. Auf Vorlage des Oberlandesgerichts (OLG) Düsseldorf hatte sich der EuGH damit zu befassen, ob die Strafvorschrift gemeinschaftsrechtskonform ist. Am Beispiel der als Terrororganisation gelisteten türkischen DHKP-C erklärt der EuGH zum wiederholten Mal, dass die Aufnahme auf die Terrorliste durch den Rat der EU bis zum Juni 2007 ohne Begründung erfolgt und damit nichtig ist. Sie durfte den Angeklagten in dem Verfahren vor dem OLG Düsseldorf nicht entgegengehalten werden. Dass die fortdauernde Listung der DHKP-C von Rat der EU seit Juni 2007 begründet wurde, konnte daran wegen des strafrechtlichen Rückwirkungsverbots für die Tatvorwürfe aus der Zeit vor Juni 2007 nicht ändern. Über Tatvorwürfe aus der Zeit nach Juni 2007 hatte der EuGH, dem die Begründung der Listung nicht vorlag, nicht zu entscheiden. Pressemitteilung des Europäischen Gerichtshofs Nr. 64/2010 vom 29.6.2010; EuGH, Urteil v. 29.6.2010, Geschäftszeichen: C-550/10; Presseerklärung des Republikanischen Anwältinnen- und Anwältevereins (RAV) v. 1.7.2010.

Buchbesprechung

Detlef Tiegel
Achtung Abzocke!
Wie ich den Datenskandal der Call-Center ins Rollen brachte,
Wilhelm Heyne Verlag München, 2010,
207 S., ISBN 978-3-453-60125-3,
8,95 Euro

(tw) Nachdem der Datenschutz die Schlagzeilen der Presse erreicht hat, ist er im Bereich der Alltagsliteratur angekommen. Das Taschenbuch beschreibt sich selbst mit den Schlagworten „Das Schwarzbuch zum Datenklau“ und „Was Sie wissen müssen, um sich zu schützen“. Beides ist nicht zu viel versprochen. Der Autor Detlef Tiegel ist der Call-Center-Mitarbeiter aus Lübeck, der im Jahr 2008 der Verbraucherzentrale Sehleswig-Holstein eine CD mit 17.000 illegal beschafften Adressdaten incl. Kontoverbindungen übergeben hat, was eine heftige öffentliche Debatte über illegalen Datenhandel, Missbrauch von Kontodaten und Direktmarketing auslöste, was letztlich zur Novellierung des Bundesdatenschutzgesetzes im Bereich Adresshandel und Werbung führte. Dabei koppelt der Autor geschickt seine Geschichte mit allgemeinen Informationen zum Daten- und Verbraucherschutz, woraus ein einerseits lebendiges, ja sogar spannendes und andererseits ein informatives lehrreiches Buch wurde. Er beschreibt zunächst, wie er zum Call-Center-Agenten wurde, dann wie er bei einer billigen Call-Center-Klitsche mit dessen illegalen Praktiken konfrontiert wurde und schließlich, wie der Skandal öffentlich aufbereitet wurde. Zwischendrin beschreibt er kurz die wichtigsten Grundsätze des Datenschutzrechtes und dessen zentrale Schwerpunkte, also das Entstehen von Datenspuren, deren Nutzung durch Sicherheitsbehörden, durch die Wirtschaft, durch Arbeitgeber und insbesondere über das Internet und durch Electronic Cash und Kundenkarten.

Der Aufhänger wie der Schwerpunkt ist aber der Datenklau und die Abzocke durch die unheilige Allianz von Call-Centern und Aboverkäufern im undurchsichtigen Geflecht anonymer Firmen. Tiegel beschreibt aus eigener Erfahrung wie auch mit einem objektivierten Überblick, wie Daten abgezogen, aufbereitet, zu Cold Calls, fingierten Verträgen und zu unzulässigen Kontoabbuchungen missbraucht und weiterverkauft werden. Insofern wird im leicht verständlichen und lesbaren Plauderstil ein Sittengemälde einer Branche geboten, von der die Öffentlichkeit bis 2008 nur ganz wenig wusste. Der Autor schildert eindringlich die Abhängigkeiten in dieser Branche, bei der aus Opfern von Abhängigkeiten aus Blauäugigkeit und Arbeitslosigkeit Täter werden, die durch die Anonymität des Vorgehens oft wenige Skrupel kennen und die einen gewaltigen Schaden bei vielen Menschen auslösen. Dabei beschreibt er seine eigene ursprüngliche Unbedarftheit, die auf der Basis der gemachten Erfahrungen langsam aber sicher dahin reifte, dass er die erlebten Machenschaften im Fernsehen und anderen Medien anprangerte, und nun in einem Buch bekannt macht, bei dessen Erstellung ihm Carsten Görig zur Seite stand.

Das Buch ist also keine Trittbrettpublikation, mit der eine abgestandene Suppe zum xten Mal wieder aufgewärmt wird, sondern eine konsistente originäre Darstellung der Call-Center-Branche mit pädagogischer Datenschutz- und Verbraucherschutzaufklärung. Die LeserInnen werden darüber informiert, mit welchen Tricks sie konfrontiert werden, was dahinter steckt und wie man sich dagegen wehren kann, um nicht mit Telefonwerbung belästigt und unberechtigten Kontoabbuchungen geschröpft zu werden. Es informiert über die Arbeit der Verbraucherzentralen und der Datenschutzaufsichtsbehörden. Es zeigt aber auch die noch weit verbreitete Hilflosigkeit unserer Gesellschaft, mit dem Datenklau und der Abzocke umzugehen, da die handelnden Firmen und die kriminellen Vorgehensweisen fast so schnell wechseln, wie das Wetter.

Ilija Trojanow/Juli Zeh
Angriff auf die Freiheit
Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte,
Hanser München 2009

(tw) Erfrischenderweise nicht die hunderste Beschreibung der Überwachungstechnologie und der Kontrollgesetze von Fachleuten, sondern eine belebende ideologische und zugleich moderne Abrechnung von zwei SchriftstellerInnen mit der herrschenden Überwachungspolitik. Aber herrscht sie überhaupt? Das Bundesverfassungsgericht, eine kritische Öffentlichkeit, liberale Kräfte im Apparat, nicht zu vergessen die offiziellen Datenschutzbeauftragten stehen für einen Gegenentwurf zu der die bisherige Politik dominierenden Überwachungsideologie! Und nicht nur das: Derzeit lassen Äußerungen aus der EU-Kommission oder aus der Bundesregierung zweifeln, ob diese überhaupt noch dominiert. Aber sie lebt

und gedeiht weiter. Damit setzen sich Trojanow und Zeh auseinander: Mit der Kontrolldenke in unseren Köpfen, mit dem Nachbeten der öffentlich gepredigten Meinung, mit den ideologischen und den politischen Protagonisten unserer Freiheitsbeschränkung. Die AutorInnen beschränken sich nicht auf Datenschutz und informationelle Selbstbestimmung, sondern benennen den größeren Zusammenhang: unsere grundrechtlichen Freiheiten und unsere Demokratie. Diese sind äußerst lebendig, aber auch äußerst bedroht - eben von den ideologischen und politischen Protagonisten, die mit Namen genannt werden: Der in diesem Bereich nicht mehr aktive Schäuble wird ebenso entlarvt wie ein Staatsrechtler namens Deppenheuer und dessen historisches Vorbild Carl Schmitt.

Als Freund von sauberen Fakten ist ein gut informierter Datenschützer bei der Lektüre eingangs noch etwa skeptisch angesichts der wenig präzisen Beschreibung mancher Überwachungspraktiken. Es wird die Relativität vieler Maßnahmen eher ausgeblendet, um einen umso besseren und analytischeren Blick auf das Wesentliche zu erlangen: Was bedroht unsere Freiheit im Informationszeitalter; sind es die Terroristen, die zur Rechtfertigung so vieler Überwachungs- und Unterdrückungsmaßnahmen herangezogen wurden und werden, oder sind es doch die staatlichen Sicherheitsfundamantalisten, die unsere Freiheiten zu Tode schützen? Die Antwort von Trojanow und Zeh ist klar und umfassend gut begründet. Terroristische Kriminelle hat es immer gegeben; diesen kann mit rechtsstaatlichen Methoden Einhalt geboten werden. Sie bedrohen unsere Freiheit vor allem dadurch, dass sie den hoheitliche Überwachungsfanatiker die Stichworte liefern. Diese Fanatiker hat es zwar auch schon immer gegeben, doch diese bedrohten und bedrohen weiterhin direkt unsere Freiheit.

Das Taschenbuch ist didaktisch gut aufgebaut: es holt die NormalbürgerIn bei dem ab, was sie bewegt: die Bilder in den Medien, die Erklärungen der Presse und der Politik und die Schlüsse, die sie selbst zieht. Dann wird von den beiden AutorInnen eine andere Sicht präsentiert, die überzeugt. Eine Minigeschichte unserer Freiheitsrechte vorangeschickt, werden die Argumente der Angstmacher vorgetragen, die Frage nach der wirklichen Sicherheit gestellt, die „Gesetze ohne Sinn und Verstand“ beschrieben, um deren spekulative Herangehensweise zu entlarven und, warum wir uns das gefallen lassen. Mit Angst lässt sich journalistisch Kasse machen. Mit Blick auf die Politik wird richtig - in Abwandelung eines bekannten Spruchs - festgestellt: „Denn sie wissen nicht, was sie tun.“ Das Buch ist eine Kampfschrift gegen Feinderklärungen und gegen die Angst und macht dadurch Mut.

Dass dessen Sicht überzeugt, davon sind die AutorInnen überzeugt. Ein Problem bleibt, dass nach getaner Überzeugungsarbeit des Buches so manche BürgerIn im Leben mit Grautönen konfrontiert wird, die das klare Bild und die Schlussfolgerungen verdunkeln. Das ist aber wohl unvermeidbar, wollten die AutorInnen ja nicht eine wissenschaftliche Untersuchung über aktuelle Bedrohungen unserer Freiheiten schreiben, sondern ein politisches Traktat, bei dem die Schwarz-Weiß-Kontraste den besonderen Reiz ausmachen. Das ist ihnen argumentativ und sprachlich vorzüglich gelungen. Und in einem 30seitigen Anhang wird dann sogar die Wissenschaftlichkeit durch umfangreiche Quellenangaben und Hintergründe hergestellt. So ist das Buch nicht nur der NormalbürgerIn zu empfehlen, sondern auch dem schon überzeugten politischen Praktiker, der im Tagesgeschäft immer mit den Grautönen zu tun hat, wobei die Kontraste manchmal schnell verwischen. Insofern hat das Buch selbst dem langjährigen Datenschutzaktivisten und Rezensenten Erkenntnis, Freude und Ermutigung gegeben.

SoliServ.de DGB ibbs Seminare für Betriebsräte dtb

5. dtb-Forum für Arbeitnehmervertreter 2010

Daten ohne Schutz: Gläserne Belegschaften? Gläserne Betriebe!

Neue Technik, neues Recht – der Aufbruch in eine neue Dimension jetzt auch im Arbeitnehmerdatenschutz?

9.–11. November 2010 in Kassel

MITARBEITER AUSGESPÄHT

Deutsche Telekom räumt neue Spitzelangriffe ein. Drogeriemarktkette überwacht Kunden und Mitarbeiter. Deutsche Bahn: Spitzelaffäre weitet sich aus. Kontrolle im Job – jeder vierte Angestellte fühlt sich überwacht. Die Bespitzelung im Arbeitsleben nimmt kein Ende und glaubt man den Herstellern, so steht uns mit neuer IT-Technik „der Aufbruch in eine neue Dimension" bevor. Kommt es damit zu mehr „gläsernen Belegschaften und Betrieben" als je zuvor, nicht nur bei Lidl, der Deutschen Telekom oder der Deutschen Bahn?

Auf dem 5. dtb-Forum in Kassel gehen wir der Frage nach, ob mit den jüngsten Novellierungen im Datenschutzrecht nun auch der Aufbruch in eine neue Dimension im Arbeitnehmerdatenschutz gelungen ist. Haben die Beschäftigten mit den Neuerungen bessere Handlungsmöglichkeiten und Instrumente, um sich auch im Arbeitsleben gegen unangemessene Kontrollen, betriebliche Rasterfahndungen und Datenmissbrauch zu wehren?

Ziel des Technologieforums ist zu zeigen, wie

- die aktuelle Rechtslage für Arbeitnehmer und Betriebsräte aussieht,
- die Arbeitnehmervertretung für neue IT-Systeme praktikable Regelungen findet und
- in der Praxis die Einhaltung von Betriebsvereinbarungen zu IT-Systemen überprüft werden kann.

Wir werden dazu

- gemeinsam mit namhaften Experten aus Wirtschaft, Politik, Wissenschaft und Praxis diskutieren,
- neue Methoden wie biometrische Identifikation und „Spitzelsoftware" live demonstrieren und
- in speziellen Fachforen praxisbezogene Handlungsmöglichkeiten erarbeiten.


Gerhart Baum


Wolfgang Däubler


Thilo Weichert

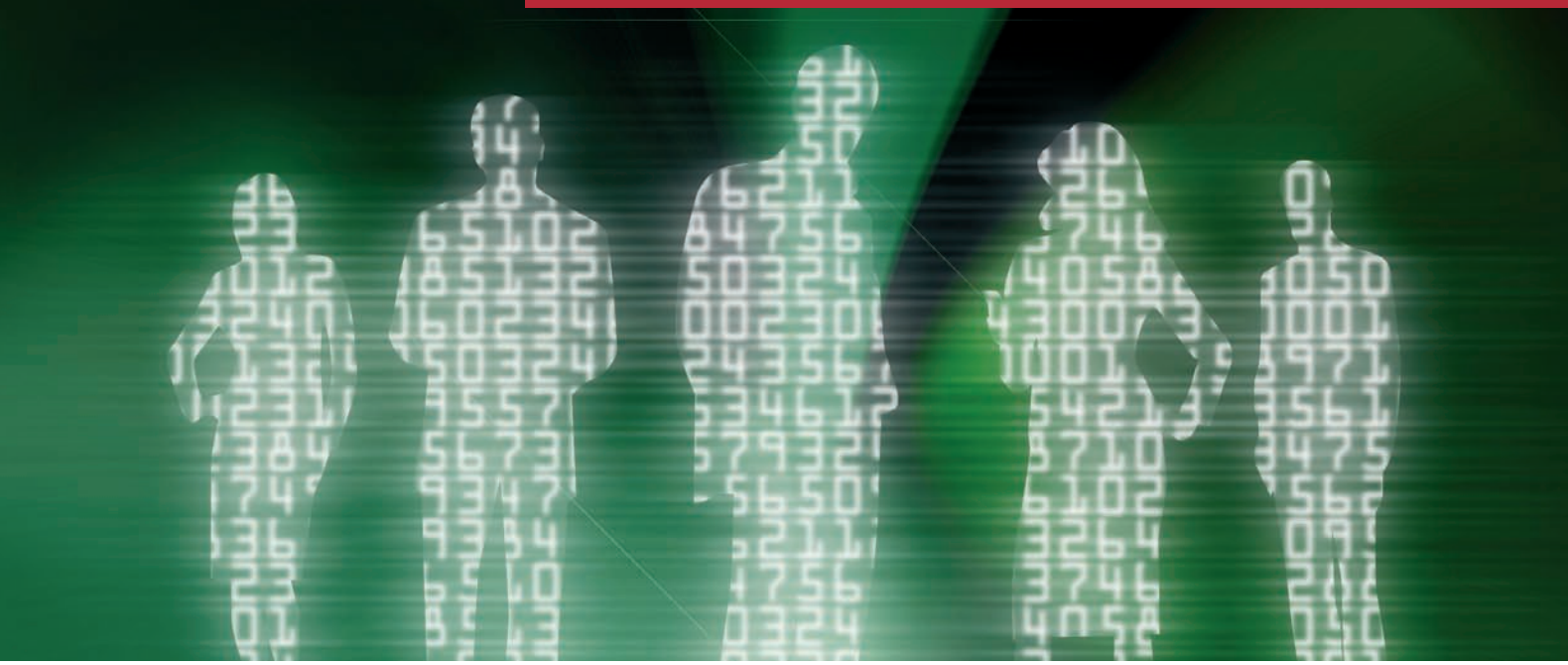

Ulrike Schramm-de Robertis


Thomas Hoeren


Thomas Leif

Weitere Informationen: www.dtb-kassel.de oder Tel. (05 61) 70 575 70

Vertrauen ist gut. Anwalt ist besser.



27. Oktober 2010 in Berlin

DAV-FORUM DATENSCHUTZ

Privatsphäre in der globalen Informationsgesellschaft
Ist der Datenschutz noch zu retten?

Programm

09.30 Uhr	Begrüßungskaffee
10.00 Uhr	**Grußworte** Rechtsanwalt Prof. Dr. Wolfgang EWER, Präsident des Deutschen Anwaltvereins, Kiel Staatssekretärin im Bundesministerium des Innern und Beauftragte der Bundesregierung für Informationstechnik Cornelia ROGALL-GROTHE, Berlin
10.30 Uhr	**Fällt der Datenschutz durch die sozialen Netzwerke?** Philippe GRÖSCHEL, Jugendschutzbeauftragter bei schülerVZ, Vorstandsmitglied der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter e.V., Berlin Prof. Dr. Indra SPIECKER gen. DÖHMANN LL.M., KIT – Karlsruher Institut für Technologie, Karlsruhe
11.15 Uhr	**Datenschutz und Meinungsfreiheit: Regulierung von Medieninhalten über das BDSG?** Rechtsanwalt Thorsten FELDMANN, LL.M., JBB, Berlin Dr. Thilo WEICHERT, Landesdatenschutzbeauftragter Schleswig-Holstein, Kiel
12.00 Uhr	Mittagessen
13.00 Uhr	**Stiftung Datenschutz** Bundesministerin der Justiz Sabine LEUTHEUSSER-SCHNARRENBERGER, Berlin Rechtsanwalt Dr. Peter BRÄUTIGAM, Noerr LLP, München Hubertus PRIMUS, Chefredakteur test, Stiftung Warentest, Berlin
14.15 Uhr	**Ist das Verbotsprinzip noch zeitgemäß? – Überlegungen zur Novellierung des BDSG** Rechtsanwalt Prof. Dr. Jochen SCHNEIDER, SSW, München
14.45 Uhr	**Online-Durchsuchung und Vorratsdatenspeicherung – Konsequenzen für den Datenschutz?** Rechtsanwalt Niko HÄRTING, Berlin
15.15 Uhr	**Kernanforderungen an ein neues europäisches Datenschutzrecht** N.N. **Vorstellung von Privatheit und Datenschutz außerhalb der EU** Rechtsanwältin Dr. Ursula WIDMER, Immediate Past President der ITECHLAW International Technology Law Association, Bern, Schweiz
16.00 Uhr	Kaffeepause
16.30 Uhr	**Podiumsdiskussion: Datenschutz 2020** Holger BLEICH, Heise Newsticker, Journalist, Hannover Rechtsanwalt Prof. Dr. Dr. h.c. mult. Winfried HASSEMER, Vizepräsident des Bundesverfassungsgerichts a.D., Frankfurt/Main Constanze KURZ, Chaos Computer Club, sachverständiges Mitglied der Enquete-Kommission Internet und digitale Gesellschaft, Berlin Rechtsanwalt Dr. Helmut REDEKER, Vorsitzender des Ausschusses Informationsrecht des DAV, Bonn Dr. Thilo WEICHERT, Landesdatenschutzbeauftragter Schleswig-Holstein, Kiel Lutz WILDE, Redakteur Finanztest, Stiftung Warentest, Berlin Moderation: Rechtsanwalt und Notar Ulrich SCHELLENBERG, DAV-Vizepräsident, Berlin
18.00 Uhr	Ende der Veranstaltung
Gesamtmoderation:	Rechtsanwältin Dr. Astrid AUER-REINSDORFF, Berlin Rechtsanwalt Dr. Peter BRÄUTIGAM, Noerr LLP, München
Anschließend:	Gemeinsamer Empfang mit den Gästen und Teilnehmern der ITECHLAW International Technology Law Association im Foyer des Maritim proArte. Begrüßung durch die Justizsenatorin Gisela VON DER AUE, Berlin

Tagungsort: Maritim proArte Hotel Berlin, Friedrichstraße 151, 10117 Berlin
Teilnehmergebühren: Die Teilnahme an der Veranstaltung ist kostenfrei.
Hotelzimmer: Für die Teilnehmer haben wir im Tagungshotel bis zum 31.08.2010 ein Zimmerkontingent (EZ/DZ ab 139,00/ab 154,00 EUR zzgl. 22,00 EUR Frühstück pro Person) auf Abruf reservieren lassen. Die Zimmerreservierung bitten wir telefonisch (Tel.: 030 / 2033-4410) unter dem Stichwort „DAV-Forum“ selbst vorzunehmen.
Anmeldungen (schriftlich erbeten) bitte an: Deutsche**Anwalt**Akademie, Veranstaltungsorganisation, Mareen Uhl, Littenstraße 11, 10179 Berlin
(Tel.: 030 / 72 61 53 182, Fax: 030 / 72 61 53 188, uhl@anwaltakademie.de). Ein Fortbildungsnachweis nach § 15 FAO wird auf Wunsch erteilt.

DeutscherAnwaltVerein

Anwalt der Anwälte