3/2011

Datenschutz Nachrichten

34. Jahrgang
ISSN 0137-7767
9,00 Euro

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

Datenschutz in Online-Spielen

■ Datenschutzstudie des ULD zu Online-Spielen ■ Wie viel Realität verträgt eine virtuelle Welt? ■ Profil-Erstellung bei Online-Spielen ■ Erlebte Rechenschaftsverpflichtung: Zur Psychologie des Verantworten-Müssens ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechung ■

Inhalt

Termine

Mittwoch, 19. Oktober 2011
Infoveranstaltung zum Beschäftigtendatenschutz
Brüssel. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

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

Samstag, 29. Oktober 2011
DVD-Mitgliederversammlung
Bonn.

Dienstag, 1. November 2011
Redaktionsschluss DANA 4/11
Thema: Datenschutz in der Schule,
verantwortlich: Hajo Köppen
Fragen und Anregungen bitte an:
hajo.koeppen@verw.th-mittelhessen.de

Freitag, 11. November 2011 bis
Sonntag, 13. November 2011
FIfF-Jahrestagung
Thema: Dialektik der Informationssicherheit
Hochschule München, Lothstr. 64
fiff@fiff.de

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

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Frans Jozef Valenta
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

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

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

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Frans Jozef Valenta
Seite 106: pixelio.de, F. J. Valenta

Datenschutz in Online-Spielen

Liebe Leserinnen und Leser,

das Titelbild zu dieser Ausgabe wurde von den Fantasy-Inhalten vieler Online-Rollenspiele angeregt. Dort kämpft das Gute gegen das Böse. Das Gute ist selbstverständlich der Datenschutz und das Böse wird repräsentiert durch Datenschutzverstöße bei Online-Spielen. Zur Visualisierung sollte ein siebenköpfiger Drache die Rolle des Bösen übernehmen – im Verlauf des Gestaltungsprozesses zeigte sich jedoch, dass von sieben überall im Raum verteilten Ungeheuern eine erheblich größere Bedrohung ausgeht als die Konzentration der Drachenköpfe an einem Ort. Die dargestellten Ungeheuerlichkeiten sind NUTZUNGSBEDINGUNGEN, ARBEITSSPEICHERSCANNING, FREUNDESLISTEN, CHATAUFZEICHNUNG, ERFOLGSSTATISTIK, SPIELVERLAUFSPROTOKOLLIERUNG und PERSÖNLICHKEITSPROFILE. Die Kämpferinnen sind mit Schwert (Kraft, Durchhaltevermögen) und Zauberstab (Intelligenz, List) ausgerüstet.
Wenn Sie die nachfolgenden Artikel lesen, werden Sie feststellen, dass Datenschutz bei Online-Spielen nur ein nebensächliches Thema ist. Vielleicht liegt es daran, dass Politiker, Journalisten, Verbraucher- und Datenschützer nur sehr selten selbst online spielen und dass die betroffenen Spieler zwar verärgert über die Knebelungen sind, letzlich aber der Wille, am Spiel teilzunehmen, größer ist als der Drang, der Entrechtung etwas entgegen zu setzen.
Mit der Zunahme an Spielen in Sozialen Netzwerken wie Facebook wird das Problem, wo jeweils Bestandsdaten, Nutzungsdaten und Kommunikationsinhalte zu welchen Zwecken verarbeitet und von wem diese eingesehen werden können, immer größer und unüberschaubarer. Sehr viele dieser Spiele können „Gratis“ gespielt werden. Aber sie sind natürlich nicht kostenlos, denn der Nutzer bezahlt mit der Preisgabe seiner Daten, die als Basis für die Einblendung von zielgerichteten Werbebotschaften dienen.
Auf der Rückseite dieses Heftes finden Sie eine kleine Auswahl von Screenshots zu aktuellen Spielen im Internet. Jedes Spiel verlangt eine Registrierung und damit die Offenlegung der Identität des Spielers. Der Markt wächst stark. Es ist viel Geld zu verdienen und hohe Umsätze lassen sich durch möglichst viele Informationen über die Spieler generieren. Es gibt noch eine ganze Menge zu tun, um den Schutz der Konsumenten zu erreichen. Wir müssen uns dem Kampf gegen die Drachen stellen.

Frans Jozef Valenta

Autorinnen und Autoren dieser Ausgabe:

Henry Krasemann
Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Referat Datenschutz-Gütesiegel, Kiel. ULD71@datenschutzzentrum.de

Evelyn Miksch
Freie Autorin. evelyn.miksch@googlemail.com

Marc Solga
Wirtschaftspsychologe und systemischer Coach (dvct), leitet die Arbeitsgruppe Kompetenz- und Personalentwicklung an der Fakultät für Psychologie der Ruhr-Universität Bochum.
Kontakt: J.-Prof. Dr. Marc Solga, Ruhr-Universität Bochum, Fakultät für Psychologie, Universitätsstr. 150, 44780 Bochum, marc.solga@rub.de, www.ruhr-uni-bochum.de/personalpsychologie/

Frans Jozef Valenta
Selbständiger Grafik Designer und Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz. valenta@t-online.de

Henry Krasemann
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Datenschutz in Online-Spielen

Aktuelle Situation

Online-Spiele erfreuen sich wachsender Beliebtheit. Betreiber aus aller Welt bieten die Spiele auf ihren unterschiedlichen Plattformen an. Waren es zunächst vor allem die PCs mit ihren Online-Rollenspielen und Browsergames, die den Trend gesetzt haben, so ist heute in den aktuellen Spielkonsolen die Online-Funktionalität eines der größten Verkaufsargumente. Doch auch Handys und Handheld-Geräte wie das iPhone oder auch iPad erlauben inzwischen das Spielen allein oder gemeinsam mit anderen Spielern von allen Orten aus, an denen ein (Mobilfunk-)Netz vorhanden ist. Online-Spiele erlauben die Verwaltung von Spieler-Freunden, die Kommunikation mittels Text, Sprache und Bild sowie die Integration von Sozialen Netzwerken wie Facebook und Twitter. Im Gegenzug wächst rasant die Zahl der Spiele, die direkt in Sozialen Netzwerken wie Facebook oder StudiVZ gespielt werden.

Das Problem

Online-Spiele erheben in der Regel zahlreiche Informationen über die Menschen, die sie nutzen. Dies sind Angaben für die Vertragsgestaltung und die Bezahlung, aber auch Daten über das Nutzungsverhalten des einzelnen Spielers. Die Erfassung einiger dieser Informationen ist für den Spieler erkennbar, etwa wenn er ein Formular ausfüllen muss. Andere Daten jedoch werden ohne sein Zutun oder sein bewusstes Einverständnis erhoben und verwendet. Mit dem Ziel, Raubkopierer und Schummler zu bekämpfen, werden etwa bei einigen Spielen im Hintergrund Informationen über den Computer und über die darauf vorhandenen Dateien und Programme erfasst – Daten, die auch viel über den Nutzer des Rechners aussagen können.

Auch Informationen darüber, welche Spiele wann und wie gut gespielt werden, werden verarbeitet und teilweise sogar frei abrufbar ins Web gestellt. Dem Betreiber ermöglicht dies eine Nutzungsanalyse bzw. eine detaillierte Profilbildung all ihrer Kunden. Aber auch Werbetreibende können hieran Interesse haben, um Zielgruppenorientierte Werbung platzieren zu können. Eine Profilbildung ist zwar nach § 15 Abs. 3 Telemediengesetz (TMG) zur bedarfsgerechten Gestaltung des Dienstes, Werbung oder Marktforschung zulässig. Jedoch darf dieses nur unter Verwendung von Pseudonymen erfolgen, die mit den Identifikationsdaten des Trägers des Pseudonyms nicht zusammengebracht werden dürfen. Außerdem muss dem Betroffenen ein ausdrückliches Widerspruchsrecht eingeräumt werden. Kaum ein Anbieter setzt diese gesetzliche Vorgabe jedoch bisher um.

Eine Gefahr besteht insbesondere dann, wenn die öffentlichen oder auch geheimen bzw. internen Informationen des Spielers mit weiteren (externen) Daten in Verbindung gebracht werden. Dies betrifft z. B. die Integration von Spielen in Netzwerke wie Facebook, StudiVZ oder Google+. Ist jemand etwa in der Lage, über Soziale Netzwerke, Suchmaschinen oder auch persönliche Kontakte ein umfassendes Profil über den Spieler zu erstellen, dann ergeben sich hieraus Vermutungen und Rückschlüsse über einen Menschen, die zu spürbaren Auswirkungen auf das Leben des Einzelnen führen können.

Die Studie

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat 2010 eine Studie zu Datenschutz in Online-Spielen herausgegeben. Diese wurde vom Bundesministerium für Bildung und Forschung gefördert. Hierin wurden die wichtigsten Datenschutzprobleme bei Online-Spielen identifiziert und Lösungen aufgezeigt. Wir haben aktuelle Spiele für zahlreiche Spieleplattformen auf ihre Datenverarbeitung hin analysiert. Dies betraf die gängigen Konsolen mit den Diensten bzw. Spielsystemen Xbox Live, PlayStation Network und Wii Connect, tragbare (Spiel-)Geräte wie das iPhone, Nintendo DS und PSP, Computerprogramme wie World of Warcraft oder Herr der Ringe Online, Computerspielsysteme wie Valve Steam und auch plattformübergreifende Spiele wie Browsergames und Spiele in Sozialen Netzwerken wie FarmVille.

Besonderes Augenmerk wurde dabei auf die Transparenz der Datenverarbeitung und die Datenschutzerklärungen gelegt. Auch Meinungen und Diskussionen in Fachzeitschriften und Foren wurden untersucht. Von uns veranstaltete Workshops mit Herstellern und Betreibern von Online-Spielen lieferten weitere Informationen. Besonders wertvoll war eine Umfrage mit mehr als 1.000 Teilnehmern, die wir unter Spielern durchgeführt haben. Insbesondere einige offen gehaltene Fragen, die die Spieler einluden, eigene Gedanken zu dem Thema mitzuteilen, brachten wesentliche Ergebnisse und halfen dabei, Problembereiche zu identifizieren.

Die Ergebnisse wurden auf ihre Relevanz hinsichtlich des geltenden Datenschutzrechts betrachtet. Hierzu haben wir zunächst untersucht, welches (internationale) Recht in welchen Konstellationen zur Anwendung kommt. Im weiteren Verlauf der Studie haben wir dann den Schwerpunkt auf das europäische und das in Deutschland geltende Recht gelegt, das bei den meisten Spielen, die sich an den deutschen Markt richten, anwendbar ist.

Auf Basis dieser Ergebnisse haben wir 27 Einzelfunktionen von Online-Spielen identifiziert, die datenschutzrechtlich relevant sind. Für jede dieser Funktionen haben wir die einschlägigen Datenschutzgesetze identifiziert, deren Regelungsinhalt dargelegt und Hinweise für den praktischen Einsatz gegeben. Daraus entstand ein Datenschutz-Leitfaden für Online-Spiele. Dieser wurde dann mit Herstellern und Betreibern von Online-Spielen in einem Workshop

diskutiert, um Rückmeldungen aus der Praxis zu erhalten.

Neben der rechtlichen Einordnung waren für die Studie aber auch die Interessen der Spieler wichtig. Diese wurden frühzeitig mittels der o. g. Umfrage, einem Workshop, Vorträgen und Vorlesungen eingebunden.

Ein eigenes Kapitel der Studie beschäftigt sich mit den sozioökonomischen Aspekten von Datenschutz in Online-Spielen. Abschließend haben wir untersucht, welche Geschäftsmöglichkeiten sich aus dem praktizierten Datenschutz ergeben. Unter der Prämisse, dass Datenschutz in Online-Spielen auch ein Geschäftsmodell sein kann, gehen wir auf mögliche Dienstleistungen und Zertifizierungen ein.

Ergebnisse

a) Rechtsgrundlagen

Betreiber von Online-Spielen im außereuropäischen Ausland (z.B. USA oder auch Japan) müssen sich in der Regel an deutsches Datenschutzrecht halten, wenn sie ihre Angebote direkt (auch) an deutsche Spieler richten. Innerhalb der EU kann im Rahmen des Herkunftslandsprinzip bzw. Territorialprinzip auch nur das Recht des Landes relevant sein, in dem die Daten verarbeitende Stelle (meist der Betreiber der Spiele) ihre Niederlassung hat. Da jedoch das Datenschutzrecht in der EU durch entsprechende Richtlinien in vielen Lebensbereichen vereinheitlicht ist, ergeben sich für die meisten Fälle nur geringe Abweichungen gegenüber dem deutschen Datenschutzrecht.

Bei Online-Spielen handelt es sich um Telemedien, auf die in Deutschland das Telemediengesetz (TMG) Anwendung findet. Dies bezieht sich auf Bestandsdaten und Nutzungsdaten zur Erbringung des Spiels. Darüber hinaus gehende Datenverarbeitung richtet sich in der Regel nach dem Bundesdatenschutzgesetz (BDSG), teilweise auch bei bestimmten Diensten nach dem Telekommunikationsgesetz (TKG).

Grundsätzlich gilt, dass für die Verarbeitung von personenbezogenen Daten entweder eine Rechtsgrundlage oder die Einwilligung des Spielers vorliegen muss. Ist beides nicht gegeben, so ist die Verarbeitung der Daten rechtswidrig. Typischerweise zulässig ist die Verarbeitung von Informationen für die Vertragsgestaltung oder Abrechnung (§ 14 TMG). Auch die Nutzungsdaten dürfen verwendet werden, um das Spiel zu erbringen oder abzurechnen (§ 15 TMG). Darüber hinausgehende Erhebung und Nutzung von personenbezogenen Daten bedarf jedoch in der Regel der Einwilligung des Spielers. Diese muss informiert und freiwillig erfolgen. Somit ist ein besonderes Augenmerk darauf zu legen, den Spieler über die gewünschte Datenverarbeitung umfassend und verständlich aufzuklären. Dies umfasst auch den Hinweis darauf, dass Daten im außereuropäischen Ausland verarbeitet werden. Dabei ist zu beachten, dass Einwilligungen auch widerrufen werden können, protokolliert werden und abrufbar bleiben müssen (§ 13 Abs. 2 TMG).

Über das Setzen von Cookies muss inzwischen nicht mehr nur informiert werden. Art. 5 Abs. 3 der europäischen E-Privacy-Richtlinie fordert sogar, dass für das Setzen eines Cookies oder das Speichern anderer Informationen auf dem Endgerät eines Nutzers die ausdrückliche Einwilligung eingeholt werden muss. Nur wenn das Speichern dieser Informationen zur Erbringung des Dienstes unbedingt erforderlich ist, kann auf die Einholung der Einwilligung verzichtet werden. Bei den Spielkonsolen und PC-Spielen erfolgt das Speichern etwa von Spielständen etc. in der Regel transparent und mit Einwilligung des Spielers. Bei Browsergames jedoch kann es mit Umsetzung der Richtlinie notwendig werden, die ausdrückliche Einwilligung vor dem Setzen des Cookies beim Spieler einzuholen. Bisher steht die Umsetzung der Richtlinie in Deutschland trotz Ablauf der Umsetzungsfrist der EU im Mai 2011 noch aus.

Betreiber von Online-Spielen müssen ihre Datenverarbeitung auf die erforderlichen Daten beschränken. Grundsätzlich sollten sie sich somit bei jedem erhobenen Datum darüber Gedanken machen, ob dieses für die Diensterbringung wirklich notwendig ist. Hinzu kommt, dass sie für jede Datenerhebung vorab auch einen Zweck festlegen müssen. Eine Abfrage von Daten mit dem Hintergedanken, dass man diese eventuell eines Tages mal für einen unbestimmten Zweck benutzen könnte, ist nicht zulässig. Der Spieler ist bei der Datenerhebung in der Regel über den gewählten Zweck zu informieren. Auch nach der Erhebung bleibt der Spiele-Betreiber in der Pflicht, regelmäßig zu überprüfen, ob inzwischen die Erforderlichkeit für die Speicherung der Daten entfallen ist bzw. der angestrebte Zweck erreicht wurde. In diesem Fall muss er die Daten löschen, sofern kein sonstiges rechtlich geregeltes Aufbewahrungsrecht vorliegt. Eine generelle Pflicht zur Vorratsdatenspeicherung für Daten von Spielern gibt es nicht.

Hinzu kommen Anforderungen, die den Betreiber dazu verpflichten, mittels technisch-organisatorischer Vorkehrungen den unzulässigen Zugriff auf die Daten zu verhindern.

Ausdrücklich im Gesetz (§ 13 Abs. 6 TMG) festgelegt ist, dass die Anbieter auch die anonyme bzw. pseudonyme Nutzung des Spiels ermöglichen müssen. Hierüber müssen sie den Spieler informieren, und es müssen Maßnahmen ergriffen werden, dass Pseudonyme nicht unzulässigerweise aufgedeckt werden.

Die Übermittlung an Dritte bedarf ebenfalls der Einwilligung des Spielers oder einer gesonderten Rechtsgrundlage. Dabei kann kein Konzernprivileg geltend gemacht werden, das größeren Spiele-Betreibern den freien Datenverkehr zwischen Tochterunternehmen und Konzernmutter erlauben würde. Auch dort gelten die allgemeinen Grundsätze des Datenschutzrechts und es bedarf einer gesetzlichen Rechtfertigung bzw. Einwilligung des Betroffenen für die Übermittlung. Innerhalb der EU gibt es jedoch mit dem Instrument der Auftragsdatenverarbeitung eine Möglichkeit, Datenverarbeitungsdienstleistungen auszulagern. Notwendig sind hierfür jedoch insbesondere entsprechend gestaltete Verträge und die sorgfältige Auswahl und Kontrolle des Auftragnehmers durch den Auftraggeber. Sollen darüber hinaus Daten etwa an Werbedienstleister übermittelt werden, ist hierfür die ausdrückliche Einwilligung des Spielers erforderlich.

Besondere Probleme können sich dabei bei der Einbindung von Cloud-Dienstleistern ergeben. Werden Spielerdaten „in der Cloud“ gespeichert, so ist auch hierfür in der Regel ein Auftragsdatenverarbeitungsvertrag er-

forderlich. Probleme ergeben sich insbesondere dann, wenn nicht ausgeschlossen werden kann, dass personenbeziehbare Daten auch außerhalb der EU, insbesondere in den USA, verarbeitet werden. Zwar bieten einige amerikanische Cloud-Anbieter auch die ausschließliche Verwendung europäischer Rechnerfarmen an. Jedoch kann meist dennoch nicht ausgeschlossen werden, dass amerikanische Administratoren etwa auf Weisung von Sicherheitsbehörden auf die Daten in Europa zugreifen. In diesem Fall müssen ggf. zusätzliche Vorkehrungen wie der Einbau wirksamer Verschlüsselungstechniken ergriffen werden, um eine Auftragsdatenverarbeitung zu ermöglichen.

Bedient sich der Spiele-Betreiber eines Sozialen Netzwerkes wie Facebook oder Google+, um sein Spiel anzubieten, so tritt er in der Regel ebenfalls als Telemediendiensteanbieter im Sinne des TMG auf. Die Übermittlung von Spielerdaten an das Soziale Netzwerk muss deshalb ebenso rechtlich abgesichert sein, wie wenn er sich eines anderen Providers bedienen würde. Zwar käme auch hier wieder das rechtliche Konstrukt der Auftragsdatenverarbeitung in Frage. Diese scheitert jedoch in vielen Fällen daran, dass die Betreiber von Sozialen Netzwerken nicht bereit sind, einen solchen Vertrag zu schließen und sich den Weisungen des Auftraggebers zu unterwerfen. Außerdem haben Facebook und Co. meist ein Eigeninteresse an den gesammelten Daten, was sie als Auftragnehmer disqualifiziert – davon abgesehen, dass die Daten in der Regel außerhalb der EU verarbeitet werden. Und ein Widerspruchsrecht gegen die Profilbildung im Sinne des § 15 Abs. 3 TMG räumen sie auch nicht ein.

Zu beachten ist, dass nach deutschem Recht auch die IP-Adresse des Rechners des Spielers ein personenbeziehbares Datum ist und damit die Datenschutzgesetze hierauf anwendbar sind. Rechtlichen Problemen kann durch eine umgehende Anonymisierung der IP-Adresse nach Diensterbringung aus dem Weg gegangen werden.

Anonyme Statistiken unterfallen zwar nicht dem Datenschutzrecht. Sobald jedoch Profile unter Pseudonym erstellt werden, muss dem Spieler ein Widerspruchsrecht eingeräumt werden, worüber er aufzuklären ist (§ 15 Abs. 3 TMG).

Schließlich müssen die Betreiber von Online-Spielen die Rechte der Spieler auf Auskunft, Berichtigung, Löschung und Sperrung der über sie gespeicherten Daten umsetzen.

Die Kommunikation zwischen den Spielern unterliegt großteils dem Fernmeldegeheimnis und darf nicht überwacht werden. Ausnahmen können sich im Rahmen der Jugendschutzgesetze ergeben, sofern die Spieler über die entsprechenden Einschränkungen informiert wurden.

b) Untersuchung der Spiele

Die Untersuchung einer Auswahl der auf dem Markt befindlichen Spielsysteme und Spiele im Rahmen der Studie hat zahlreiche Verstöße gegen die Datenschutzgesetze aufgezeigt. Kaum eine Datenschutzerklärung war so verfasst, dass sie dem Grundsatz der sowohl umfassenden als auch verständlichen Aufklärung entsprach. Einige Betreiber lassen sich dabei weitgehende Rechte an der Verwendung der personenbezogenen Daten einräumen, die nicht im Einklang mit dem Erforderlichkeitsprinzip und Zweckbindungsprinzip stehen. Insbesondere Betreiber außerhalb der EU behandeln die IP-Adresse nicht als besonders schützenswertes Datum. Einwilligungen wurden großteils nur pauschal eingeholt, ohne dass die genauen Auswirkungen für den Spieler immer erkennbar waren. Die Löschung von Daten war teilweise gar nicht oder erst auf wiederholte Nachfrage möglich. Bei der Einbindung in Soziale Netzwerke war nicht immer differenzierbar, welche Daten zu welchem Zweck dem Spiele-Betreiber zur Verfügung gestellt werden.

Einige Spiele übermittelten schon bei der Einrichtung des Spiels Daten an den Betreiber, ohne dass dieses für den Spieler ersichtlich war. Werden im Hintergrund Systeme zur Rechnerüberwachung installiert, so ist oftmals kaum erkennbar, was genau diese Programme überwachen und übermitteln.

Die Verpflichtung zur Einräumung einer pseudonymen bzw. anonymen Bezahlung und Nutzung wird nur von wenigen Betreibern umfassend umgesetzt. Selbst wenn anonyme Bezahlsysteme (Prepaid-Karten) angeboten werden, werden teilweise weitere den Spieler identifizierende Daten erhoben, ohne dass hierfür eine Erforderlichkeit, etwa aus Jugendschutzgründen, erkennbar ist.

Auch Kommunikationsinhalte werden von einigen Betreibern analysiert, teilweise aus Sicherheitsgründen, teilweise zu Werbezwecken – ein klarer Verstoß gegen das Fernmeldegeheimnis.

c) Weitere Ergebnisse

Die Untersuchungen, Gespräche und die Umfrage haben gezeigt, dass viele Spieler an dem Thema Datenschutz interessiert sind. Sie haben das Gefühl, keine wirkliche Kontrolle über ihre Daten ausüben zu können und fühlen sich schlecht informiert. Aber auch die Betreiber sind verunsichert und sich teilweise nicht bewusst, welche Datenschutzvorgaben sie einzuhalten haben.

Die datenschutzgerechte Gestaltung von Online-Spielen kann den beteiligten Unternehmen helfen, Vertrauen bei Spielern aufzubauen und diese langfristig an sich zu binden. Audits und Gütesiegel können die Hersteller und Betreiber dabei unterstützen. Wo nicht die technischen und fachlichen Möglichkeiten beim Betreiber für eine datenschutzgerechte Abwicklung des Spielgeschehens gegeben sind, können externe Dienstleister helfen.

Ausblick

Während der Erstellung der Studie und auch danach haben sich zahlreiche neue Entwicklungen auf dem Markt der Online-Spiele ergeben, die neue Datenschutzprobleme mit sich bringen können. So nimmt die Integration von Spielen in Soziale Netzwerke sprunghaft zu. Im Bereich der sog. Casual Games werden auch Gesundheitsdaten wie das eigene Gewicht oder Jogging-Verhalten zu Spieldaten. Bei Online-Spielen auf Mobilgeräten kommen nunmehr auch Standortdaten hinzu, die besonderen rechtlichen Regelungen unterliegen.

Wir stehen in Deutschland immer noch am Anfang der Entwicklung von Online-Spielen zum Massenphänomen. Dies eröffnet aber auch die große Chance, Neuentwicklungen gleich datenschutzgerecht zu gestalten, um so die gleichen Fehler, wie bei vielen anderen Online-Dienstleistungen, zu vermeiden.

Evelyn Miksch

Wie viel Realität verträgt eine virtuelle Welt?

Der Text dieses Artikels erschien 2010 in der Oktober-Ausgabe
des GameStar MMO Magazins (IDG Entertainment Media GmbH)

Anonymität, ade! Blizzard kündigte Anfang Juli an, wer einen Beitrag im offiziellen WoW- oder Starcraft-Forum schreibe, müsse künftig seinen echten Namen angeben. Noch bevor der Plan in die Tat umgesetzt werden konnte, stoppten ihn die Spieler – vorerst. In aufklärerischer Mission haben wir uns ebenfalls in den Namenskrieg gestürzt.

Der Sinn eines Rollenspiels besteht darin, in die Haut eines fiktiven Helden zu schlüpfen und in einer erfundenen Welt großartige Abenteuer zu erleben. Doch was wäre diese Welt, wenn man als Ork namens Heinz-Rüdiger Müller durch die virtuellen Wälder ziehen würde? Keine Frage, heroische oder blumige Namen gehören in ein Rollenspiel wie Tomaten in den Ketchup. Solche Namen grenzen nicht nur Fantasie von Realität ab, sie bieten auch den Schutz der Anonymität – ein wichtiger Punkt für die zugehörigen Foren.

Doch hier macht Blizzard der Community einen Strich durch die Rechnung und holt sie unsanft auf den Boden der Realität: Ab Ende Juli sollten Spieler in den Foren von World of Warcraft, StarCraft II, Diablo II, Warcraft II sowie in allen Battle.net-Foren nur noch unter ihren richtigen Namen Beiträge verfassen können.

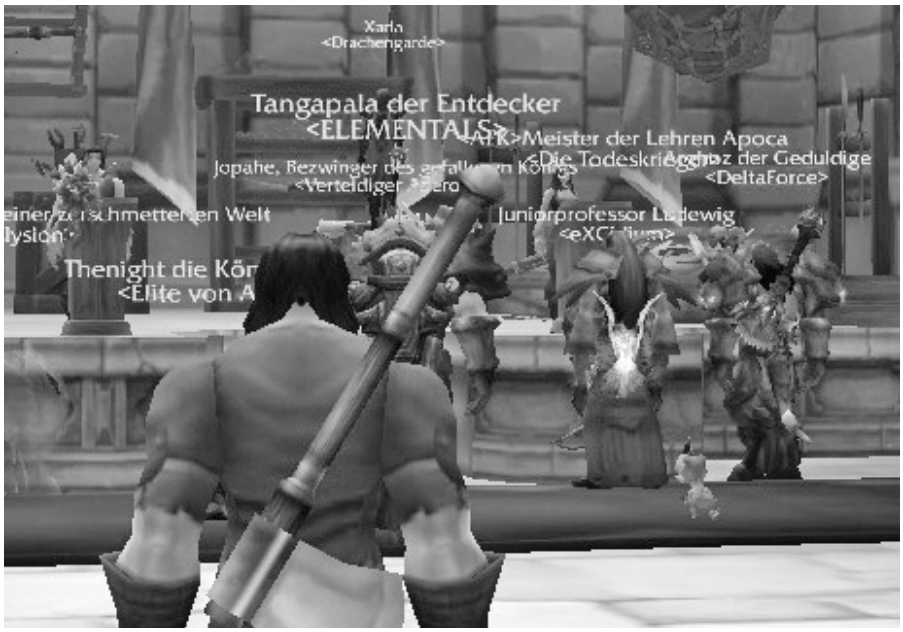
Mit dieser Ankündigung begann eine Geschichte, die nicht weniger spannend ist als ein guter Krimi. In den Hauptrollen glänzen Pseudonyme, Geschäfte, Geld sowie Kundenrechte. Fraglich ist allerdings, ob es überhaupt ein Happy End gibt. Zahlreiche Spieler und Datenschutz-Rechtsexperten haben sich dazu geäußert und fanden tagelang kein anderes Thema.

Was bisher geschah

Real ID heißt das neue Freundschaftssystem von Battle.net und markiert den Anfang des Online-Identitätsdilemmas. Blizzard selbst beschreibt Real ID als „eine neue, optionale Identitätsebene, die über die Ebene des Spielcharakters hinausgeht und Spieler untereinander über mehrere Blizzard-Entertainment-Spiele hinweg verbindet“. Ziel ist, den sozialen Aspekt der Spielerfahrung zu verbessern. Eines der wichtigsten Features sind die spiel-, realm- und fraktionsübergreifenden realen Namen. Hier können Sie – wenn Sie möchten – die richtigen Namen Ihrer Freunde und von deren Freunden inklusive aller Charaktere sehen. Selbiges geht natürlich auch bei Ihnen in den Freundeslisten ihrer Freunde. Zu Real ID gehört auch die sogenannte „Rich Presence“-Technologie. Sie ermöglicht es Ihnen, in Echtzeit herauszufinden, was Ihre Freunde gerade in welchem Spiel machen.

Inwiefern Real ID eine gute Idee ist oder kritisch betrachtet werden muss, werden wir später genauer unter die Lupe nehmen. Fakt ist, dass dieses System mit den offiziellen Blizzard-Foren verbunden werden sollte, in dem das Beiträgeverfassen nur mit realen Namen zulässig sein sollte. Blizzard-Mitbegründer Mike Morhaime begründete die Maßnahme mit folgenden Worten: „Wenn der für Onlineunterhaltungen typische Schleier der Anonymität gelüftet ist, wird dies zu einer besseren Umgebung in den Foren führen, konstruktive Unterhaltungen fördern und die Blizzard-Community auf eine Art und Weise zusammenbringen, wie sie bisher nicht verbunden war.“

Nicht ohne die Spieler. Letzteres funktionierte hervorragend, denn die Spielergemeinde war verbunden wie nie zuvor – in ihrer Empörung über Blizzard. Allein im deutschen WoW-Forum sammelten sich innerhalb kürzester Zeit über 12.000 Beschwerdebeiträge. Entsetzt und erschrocken lassen Spieler ihrem Unmut freien Lauf und drohen mit einem Boykott des Forums. „Teilnahme nur für Leute, die bereit sind, auf den Schutz ihrer personenbezogenen Daten zu verzichten? Ihr ekelt mich an!“, ist nur eine von vielen Meinungen.



In den USA nahm die Diskussion einen brisanteren Verlauf. Der Community-Manager und Autor des Forenbeitrags mit den neuen Regeln, Pseudonym Bashiok, wollte mit gutem Beispiel vorangehen und veröffentlichte seinen Klarnamen. Ein Fehler, wie er schnell feststellen musste. Seine privaten Daten wie Telefonnummer, Adresse, Alter, Vorlieben, Name seiner Frau, Schule seiner Kinder usw. fanden ihren Weg schneller ins Forum als er World of Warcraft sagen konnte. Einige User posteten sogar Bilder seines Wohnhauses – Google Street View sei Dank. Dieser unfreiwillige Daten-Striptease zeigt, wie fragwürdig Blizzards Vorhaben ist, und macht gleichzeitig deutlich, dass die Spieler einen Widerstand leisten, der sich unmöglich ignorieren lässt.

Nur zwei Tage nach der Ankündigung des geplanten Klarnamen-Zwangs in den Foren, lenkte Mike Morhaime ein: „Wir haben zu diesem Zeitpunkt entschieden, dass es nicht nötig sein wird, reale Namen für das Verfassen von Beiträgen in den offiziellen Blizzard-Foren zu nutzen." Die Community hat ihr Ziel erreicht und Spieler müssen sich so schnell nicht von ihrer Privatsphäre trennen. Allerdings ist es ein Etappensieg, denn Blizzard will nicht gänzlich von seinem Vorhaben Abstand nehmen.

Was wäre, wenn ...

Zum jetzigen Zeitpunkt können Sie also aufatmen. Doch das neue Battle.net inklusive optionaler Real ID existiert weiterhin, und das Problem ist nicht vom Tisch.

Über die Features des neuen Freundschaftssystems erfahren Sie nicht nur, dass die Blutelfe Neluwen gar keine Frau ist, sondern auch, was Ihre Freunde gerade machen oder welche Charaktere sie noch so steuern, und das spielübergreifend. Spinnt man den Faden weiter, können Sie also sehen, ob Ihr Freund mit einem seiner Helden Ihr Verbündeter ist, während er mit einer anderen Spielfigur Ihr ärgster Feind ist. Das gilt im Übrigen ebenfalls für Freundes-Freunde, wodurch vielleicht ganz schnell der eine oder andere Politiker, Lehrer et cetera als WoW-Liebhaber enttarnt werden kann. Doch glücklicherweise sind diese Funktionen kein Muss.

Dennoch ist eine Sensibilisierung im Umgang mit den eigenen Daten extrem wichtig. Stellen Sie sich nur einmal vor, der Klarnamen-Zwang für die Foren hätte sich durchgesetzt: Dann wäre jeder User eindeutig als World of Warcraft-Spieler identifizierbar. Für die berufliche Laufbahn könnte das erhebliche Konsequenzen haben, wenn der Arbeitgeber Ihren Namen googelt und feststellt, dass Sie leidenschaftlicher Fan eines Spiels sind, welches mit Begriffen wie „Suchtgefahr" in einem Atemzug genannt wird. Von weiteren Problemen wie im Fall Bashiok wollen wir gar nicht erst reden. Vielleicht denken Sie nun „Dann hätte ich auf die Nutzung des Forums verzichtet". Doch das könnte schwieriger sein, als gedacht. Haben Sie zum Beispiel ein technisches Problem, stehen Ihnen folgende Möglichkeiten zur Verfügung: der Ingame-Kundendienst, bei dem man häufig auf das Forum verwiesen wird, das Kontaktformular, mit dem erhebliche Wartezeiten einhergehen, die teure Telefonhotline oder – die nötige Auskunft im Forum suchen. Letzteres ist definitiv die effektivste Variante, wäre aber ohne realen Namen nicht mehr nutzbar gewesen.

Rechtliche Grundlagen

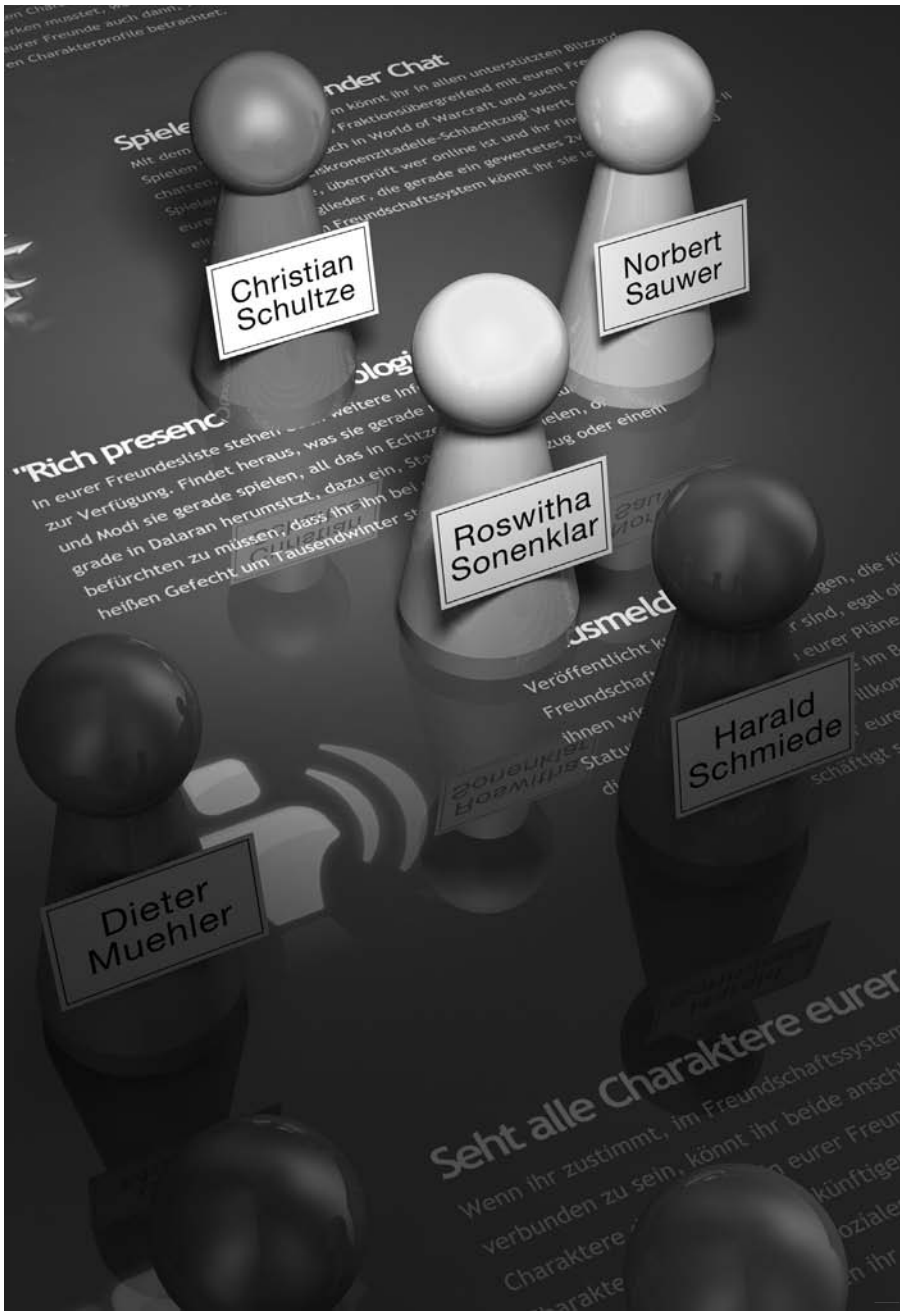
Selbstverständlich kann ein Unternehmen wie Blizzard in Sachen Datenschutz nicht einfach Entscheidungen treffen, ohne sich an gesetzliche Grundlagen zu halten. „Grundsätzlich lässt sich sagen, dass eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (§4 Absatz 1 des Bundesdatenschutzgesetzes)", bestätigt uns Juliane Heinrich, Pressesprecherin des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Problematisch ist jedoch, dass Blizzard Entertainment Vivendi Universal Games zwar einen Sitz in Deutschland hat, man dort aber nur für den Verkauf zuständig ist. Die veröffentlichten Daten hingegen verantwortet Blizzard Europe in Frankreich, und somit ist die Anwendung des deutschen Rechts schwierig. Geht es nach dem deutschen Gesetz, verstößt der Zwang zu realen Namen in den Foren etwa gegen §13 Absatz 6 des Teledienstedatenschutzgesetzes. Hier heißt es: „Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren." Darüber hinaus spielen aber auch die AGB von Blizzard eine Rolle. Schließlich holt sich die

Spieleschmiede damit die Erlaubnis für diverse Umstrukturierungen.

Wie man unschwer erkennen kann, ist neben der Zuständigkeit der Aufsichtsbehörden der komplette Sachverhalt kompliziert und eine eindeutige Lösung für dieses juristische Kuddelmuddel steht weiterhin aus. Nichtsdestotrotz müssen Sie das alles nicht ohne Widerworte über sich ergehen lassen. Nutzen Sie Ihr Recht auf freie Meinungsäußerung und schreiben Sie Blizzard oder der französischen Datenschutzbehörde, falls Sie mit geplanten Änderungen nicht zufrieden sind.

World of Facebook

Doch es bleibt eine weitere Frage im Raum stehen: Wozu das Ganze? Freundschaftssysteme, wie wir sie aus sozialen Netzwerken kennen, machen die Spieler nicht zu Unrecht stutzig. Fundament für diese neuen Features ist wohl unbestreitbar die Kooperation mit Facebook. Blizzard behält sich laut Geschäftsbedingungen vor, alle gesammelten Informationen über seine Nutzer mit den Daten von Drittanbietern – zum Beispiel Facebook – anzureichern. Real ID ist schlicht und ergreifend die technische Verbindung zwischen Facebook und Battle.net und ermöglicht das Abgleichen der Freundschaftslisten. Nennen Sie beispielsweise ein Facebook-Profil Ihr Eigen, ist dort sichtbar, wen Sie als Freunde in WoW geaddet haben, vorausgesetzt, Sie nutzen die Real ID-Funktionen. Schlussendlich steht die gegenseitige Kundenzuführung im Fokus einer solchen Zusammenarbeit. Speziell im Fall von Blizzard ist die personalisierte Ingame-Werbung für aktuelle oder zukünftige MMOs eine denkbare Erklärung, und dafür wären möglichst viele Informationen über die Spieler Gold wert.



Werbetext aus einer Battle.Net-Werbeseite zum Freundschaftssystem. Hier wird für einen Verzicht auf Spieler-Pseudonyme geworben. http://eu.battle.net/de/realid/

Fortsetzung folgt

Machen wir eine kleine Bestandsaufnahme: Die Spieler-Community hat sich erfolgreich gegen den Klarnamen-Zwang in Blizzard-Foren gewehrt. Allerdings nur vorerst. denn wie Mike Morhaime erklärt. sind die realen Namen zum Veröffentlichen von Forenbeiträgen „zu diesem Zeitpunkt“ nicht nötig. Ein Nachspiel ist also nicht ausgeschlossen. Was für den Moment bleibt. ist das Freundschaftssystem Real ID und dafür können wir keine Empfehlung aussprechen.

Natürlich ist es toll, serverunabhängig mit Freunden zu chatten. Doch momentan sind die Bedingungen dafür nicht annehmbar, weil es an Sicherheitseinstellungen mangelt. Selbst bei Facebook oder StudiVZ kann der User selbst entscheiden, wer welche Inhalte zu sehen bekommt. Real ID hingegen funktioniert momentan nur nach dem Motto „ganz oder gar nicht“. Stehen Sie etwa der „Freunde von Freunden“-Anzeige kritisch gegenüber. müssen Sie das komplette Real ID-System abschalten, da sich die Funktion nicht einzeln deaktivieren lässt.

Daher unser Tipp: Nutzen Sie bewährte Helfer wie TeamSpeak, um mit Freunden spiel- und serverunabhängig zu kommunizieren. Überlegen Sie also lieber zweimal, wem Sie welche Daten anvertrauen. Außerdem verlieren virtuelle Orte wie Azeroth, an dem wir ein anderes Ich sein können, ihren Zauber. wenn sie mit zu viel Realität verschmelzen.

„Ein weiter Schritt in Richtung gläserner Mensch“

Ein GameStar MMO-Interview mit Frans Jozef Valenta, Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e.V. (DVD)

▶ Im amerikanischen WoW-Forum veröffentlichte ein Blizzard-Mitarbeiter seinen Namen, um die Harmlosigkeit von Real ID zu demonstrieren. Wenige Minuten später posteten User seine Telefonnummer und andere private Daten. Ist eine solche Reaktion gerechtfertigt?

◀ F. J. Valenta: Diese (nicht extreme) Reaktion war richtig. Sie sollte zeigen, wie einfach es ist, auf der Basis von Klarnamen private, zum Teil sensible Daten zu recherchieren. Die Veröffentlichung von Adresse, Telefonnummer, Alter, Angaben zum sozialen Umfeld und persönlichen Vorlieben des Mitarbeiters sollte Blizzard dazu bringen, über die Folgen des Missbrauchs nachzudenken. Wer etwa über Mitspieler in World of Warcraft verärgert ist, hätte es viel einfacher, mit den ermittelbaren Informationen Rache zu üben. Das könnte ein Jux sein – aber auch eine kriminelle Handlung.

▶ Daraufhin führte Blizzard das System auf freiwilliger Basis ein. Waren die Folgen des Vorhabens den Entwicklern nicht bewusst?

◀ F. J. Valenta: Blizzard hat mit einem geringen Datenschutzbewusstsein, wie es in sozialen Netzwerken üblich ist, gerechnet und muss nun umdenken.

▶ Wie müssen Spieler informiert werden, was Blizzard mit persönlichen Daten anstellt?

◀ F. J. Valenta: Man kann Blizzard nicht vorwerfen, Spieler im Unklaren darüber zu lassen, dass Daten gesammelt werden. Das Unternehmen bemüht sich um eine transparente Darstellung der Gründe für die Erfassung: ein geregelter Spielablauf. Zumindest in den Datenschutzrichtlinien für die Internetseiten werden die Rechte des Nutzers in Bezug auf die Speicherung genannt.

▶ Ein weiterer entscheidender Punkt ist die Zusammenarbeit zwischen Blizzard und Facebook. Dafür werden etwa Freundeslisten abgeglichen, um „das soziale Unterhaltungserlebnis für die Spieler zu verbessern“. Welche Bedeutung hat das aus Datenschutzsicht?

◀ F. J. Valenta: Hier wird ein weiterer Schritt in Richtung »gläserner Mensch« gegangen. Bringt Google dann noch sein Patent zur Erstellung psychologischer Profile bei Onlinespielen ein, wird man über die Art der Werbung im Internet erfahren, ob man als Spieler vorsichtig, höflich, aggressiv, verletzend oder ruhig ist. Es ist nur eine Frage der Zeit, wann von staatlicher Seite Begehrlichkeiten geweckt werden, denn eine Auswertung der gesammelten Daten zur Vorratsdatenspeicherung (wenn sie wieder eingeführt wird) könnte zusammen mit den Facebook-lnformationen aufschlussreiche Persönlichkeitsbilder erzeugen.

▶ Grundsätzlich erfreuen sich Onlinespiele immer größerer Beliebtheit und sind untrennbar damit verbunden, dass die Spieler irgendwann irgendwo ihre Daten hinterlassen, sei es bei der Bezahlung, sie es beim Runterladen und so weiter. Worauf sollte man dabei achten, um seine Daten zu schützen?

◀ F. J. Valenta: Wer seine Daten schützen möchte, möge sich vergewissern, dass es sich um eine offizielle Blizzard-Seite handelt, und persönliche Daten sollten nur über eine sichere SSL-Verbindung (https) übermittelt werden. Oft fordern betrügerische E-Mails dazu auf, die eigenen Account-Daten zu verifizieren – dazu gibt Blizzard auf der Seite http://eu.battle.net/de/security/ Empfehlungen.

▶ Wir haben noch eine letzte Spielfrage: Viele Onlinespiele-Entwickler gehen mit spezieller Software gegen Schummler vor. So muss man häufig vor der Installation eines Spiels einer Anticheat-Software zustimmen. Diese sucht den Rechner nach Cheatprogrammen ab. Ist das aus Sicht des Datenschutzes kritisch zu betrachten? Gibt es rechtliche Grundlagen, die diese Situation für Entwickler und Spieler regeln?

◀ F. J. Valenta: Entweder man erlaubt Blizzard die Überwachung des Computers und kann spielen, oder man möchte nicht, dass der eigene Rechner durchsucht wird, und lässt sich ausschließen. Wer spielen will, muss auf die Redlichkeit von Blizzard vertrauen. Gesetzliche Regeln zu diesen Maßnahmen gibt es nicht. Blizzard legt die Regeln fest. Da die Methoden zur Verhinderung von Cheats sehr deutliche Parallelen zu Spyware aufweisen, hat Blizzard 2005 den österreichischen Big Brother Award, einen Negativpreis, erhalten.

Blizzard legt die Regeln fest. Hier ein Beispiel:

> **12.4 Nutzerinhalt.**
> Als „Nutzerinhalt“ gelten alle Mitteilungen, Bilder, Geräusche und sonstige Materialien und Informationen, die Sie über einen Spiel-Client oder den Service hochladen oder übertragen, oder die andere Nutzer hochladen oder übertragen, einschließlich, ohne jedoch darauf beschränkt zu sein, aller Chatnachrichten. Hiermit gewähren Sie Blizzard eine unbefristete, unwiderrufliche, weltweite, kostenlose, nicht exklusive Lizenz, einschließlich des Rechts zur Vergabe von Unterlizenzen an Dritte, sowie das Recht, derartige Nutzerinhalte, auch in abgeänderter Form, sowie daraus abgeleitete Arbeiten zu vervielfältigen, zu berichtigen, anzupassen, abzuändern, zu übersetzen, neu zu formatieren, davon abgeleitete Arbeiten anzufertigen, herzustellen, in Verkehr zu bringen, zu veröffentlichen, zu vertreiben, zu verkaufen, zu lizenzieren, dafür Unterlizenzen zu vergeben, zu übertragen, zu vermieten, zu verleasen, zu übermitteln, öffentlich zu zeigen oder aufzuführen, elektronischen Zugriff zu gewähren, zu senden, der Öffentlichkeit mittels Telekommunikation mitzuteilen, auszustellen, auszuführen oder sie in einen Computerspeicher einzugeben, und solchen Inhalt sowie alle geänderten oder davon abgeleiteten Arbeiten zu nutzen und zu betreiben. Soweit die anwendbaren Gesetze dies zulassen, verzichten Sie hiermit auf alle Persönlichkeitsrechte, die Sie ggf. in Bezug auf Nutzerinhalte haben.
>
> http://eu.blizzard.com/de-de/company/about/termsofuse.html

Frans Jozef Valenta

Persönlichkeits-Profile bei Online-Spielen

Vorratsdatenspeicherung bei Online-Spielen? Das ist tägliche Praxis. Und niemand regt sich darüber auf?

Das zur Zeit beliebteste Massen-Mehrspieler-Online-Rollenpiel ist World of Warcraft. Es kam im Jahre 2005 auf den Markt und zählte im August 2011 weltweit circa 11,1 Millionen Abonnenten.[1]

Im Spiel nehmen Spieler die Rollen fiktiver Charaktere bzw. Figuren ein und erleben selbst handelnd soziale Situationen bzw. Abenteuer in einer erdachten Welt. Durch das Absolvieren von Aufgaben (Quests) erhalten die Spieler Erfahrungspunkte, die für Verbesserungen dieser Charakterwerte eingesetzt werden.[2]

Der Spielehersteller Blizzard Entertainment hat mit dem Patch 3.0 am 15.10.2008 das „Erfolgssystem“[3] eingeführt. Es listet in Form einer Art Logbuch bereits erreichter und zu erreichende Ziele auf. Einträge gibt es zum Beispiel für die Erkundung durch das erstmalige Bereisen von Gebieten, für „Spieler gegen Spieler“, „Dungeon & Schlachtzug“, Berufe, Ruf und Weltevents.[4]

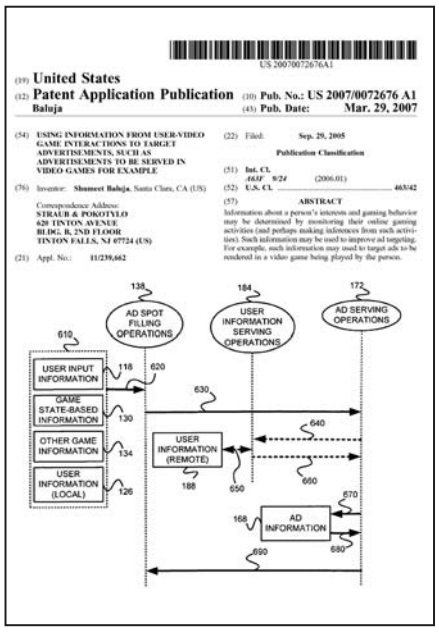
Dieses Erfolgssystem funktioniert nur deshalb, weil alle Spielschritte detailliert protokolliert werden. Blizzard weiß bei jeder Spielfigur, welche Aktionen sie wann ausgeführt hat.

Dies ist die ideale Basis zu dem 2005 eingereichten und 2007 veröffentlichten US-Patent 20070072676.[5] Es geht dabei um „Using information from user-video game interactions to target advertisements, such as advertisements to be served in video games for example“ – das Sammeln von Informationen über Spieler-Interaktionen für Onlinewerbevermarktung. Als Erfinder eingetragen ist Shumeet Baluja, ein wissenschaftlicher Mitarbeiter von Google.[6]

In dem Patent wird beschrieben, in welcher Weise die aufgezeichneten Spieleigenschaften, wie mit Chat verbrachte Zeit, das Verhalten beim Tauschhandel, die Erforschung von Gebieten, die Entscheidung bei Konfliktsituationen, eine ruhige oder aggressive Spielweise, sowie besonnene oder risikofreudige Aktionen, zu gezielter Werbung führen kann.

Wenn ein Spieler zum Beispiel zwei Stunden ununterbrochen spielt, sollten Anzeigen für Pizza, Cola, Kaffee und andere Waren eingeblendet werden. Wer im Spiel lieber die Zeit mit dem Austausch von Textbotschaften an andere Spieler verbringt, statt Abenteuer zu erleben, der erhält Anzeigen für Handys oder andere Kommunikationsmittel. Wer eine Vorliebe für das Entdecken von neuen Regionen hat, ist möglicherweise im Urlaub an Reisen interessiert und bekommt Werbeangebote aus dem Touristik-Bereich.

Im Februar 2007 hat Google passenderweise die in San Francisco ansässige Firma Adscape Media gekauft.[7] Dieses Unternehmen hat sich auf In-Game-Werbung spezialisiert.



Die von Blizzard gesammelten Informationen eignen sich allerdings nicht nur für eine an die Situation angepasste Werbung, sondern sie verraten eine ganze Menge über die Persönlichkeit der Spieler – auch wenn oft bewusst eine andere Identität vorgespielt wird.

Es ist nicht unerheblich, ob jemand lieber allein spielt oder kooperativ innerhalb einer Gilde Schlachtzüge meistert. Fühlt sich ein Spieler innerhalb einer Gruppe wohler in der Rolle des normalen Gruppenmitgliedes oder zeigen sich Ambitionen zum Anführer? Wird eine Spielweise bevorzugt, bei dem die Gegner vorwiegend computergesteuert und damit berechenbarer sind, oder reizt eher PvP (Player versus Player – Spieler gegen Spieler)?

Der Teamgeist hat bei Blizzard einen hohen Stellenwert in der Ausgestaltung des Spiels.[8] Das ging in der Anfangszeit allerdings so weit, dass die Einzelgänger unter den Spielern an bestimmten Stellen ohne fremde Mithilfe keine Chancen hatten, bestimmte Ziele zu erreichen. Inzwischen hat sich Blizzard den Wünschen seiner Abonnenten gebeugt und zahlreiche Gegner-Konstellationen für „Einzelkämpfer“ angepasst.

Bereits der Name „World of Warcraft“ verrät, dass es sich um ein Kampfspiel handelt, dennoch kann man im Prinzip auch (fast) ohne Blutvergießen in höhere Stufenbereiche aufsteigen, wenn man zum Beispiel Spaß am Handeln im Auktionshaus hat, gerne virtuell angelt oder kocht. Manche Charaktere können so eingesetzt werden, dass sie selbst keinen Schaden zufügen und statt dessen in Gruppen Heilfunktionen ausführen, wie Priester, Druiden, Schamanen und Paladine. Es gibt aber auch die Option, das aggressive Potential dieser Figuren zu nutzen.[9]

Aus der Summe zahlreicher Einzelentscheidungen lassen sich psychologische Tendezen erkennen – in vielen

Fällen sogar psychologische Profile erstellen. An Hand der über eine längere Zeit beobachteten Spielweise lässt sich durchaus erkennen, wer eine militärische Laufbahn einschlagen könnte, in der Bankbonität herabgestuft werden sollte, über Führungqualitäten verfügt, wegen seines rüpelhaften Verhaltens gemieden werden sollte, spielsüchtig oder arbeitslos ist.

Da Blizzard aber auch die kompletten Chats aufzeichnet[10], die oft sehr viele private Details enthalten, hat das Unternehmen wertvolle Informationen über die Persönlichkeit der mit Realnamen eingetragenen und unter Pseudonym agierenden Kunden.

Diese Informationen wecken natürlich Begehrlichkeiten. Was wäre, wenn Blizzard die Daten mit Facebook und anderen Sozialen Netzwerken abgleicht? Einen Versuch in dieser Richtung mit „Abgleich-Optimierung“ durch die Einführung von Klarnamen ist glücklicherweise gescheitert (DANA 3/11, Seite 99).

Diverse Geheimdienste und Behörden im Dienst der „Strafverfolgung und Terrorismusbekämpfung“ dürften diese Daten wohl ebenfalls interessant finden.

Bei manchen Quests entsteht sogar der Eindruck, als wären Sie speziell für das Casting von Rekruten in Spezialeinheiten vorgesehen. Für die Klasse der Todesritter gibt es zum Beispiel eine Aufgabe, die das Töten von Zivilisten vorschreibt: *„Doch was am aller wichtigsten ist: tötet die flüchtenden Dorfbewohner. Tote Soldaten nehmen sie in Kauf, doch einfache Bürger? Das erfüllt die Herzen der Menschen mit Furcht.“*[11] Die Erfüllung dieser Aufgabe wird mit 12250 Erfahrungspunkten belohnt.

Das World of Warcraft-Erfolgssystem soll für die Akzeptanz der umfangreichen Protokollierung des Spiels sorgen.

Auch der Umgang mit Geld – z. B. im Auktionshaus – wird statistisch erfasst.

Während es sich bei dem Spiel in den allermeisten Fällen um Gegner handelt, die selbst angreifen, die als Reaktion die eigene „Verteidigung“ erfordern, lösen flüchtende, um das Leben bettelnde Zivilpersonen, auch wenn sie nur virtuell existieren, eine Hemmung zur Aktion aus. Wie verhält man sich in dieser Situation? Augen zu und durch? Befehl ist Befehl? Oder den inneren Prinzipien gehorchend den weiteren Verlauf abbrechen? Das Feldversuchslabor von Blizzard zeichnet alles auf und fügt das Verhalten als weiteren Baustein zu den Erkenntnisen eines individuellen Profils hinzu.

Es kann durchaus sein, dass Spieler Entscheidungen treffen, die nur damit zu tun haben, ein möglichst gutes Abschneiden bei den „Erfolgen“ zu erzielen. Dies bedeutet auch für Einzelspieler letztlich eine Unterwefung zur Gruppenkonformität. Die wirkliche Identität wird überlagert. Dann ist allerdings wie im richtigen Leben eine umfassende psychische Analyse mit objektiver Bewertung aller Spielteilnehmer nur eingeschränkt möglich.

Schon allein die Tatsache, dass mehrere Spieler sich einen Account teilen können, verhindert eine klare Profilbildung. Denkbar wäre allerdings, das Blizzard aus der Verschiedenartigkeit der Spielhandlungen erkennt, dass es sich beispielsweise um drei Spieler handelt und über Filtertechniken automatisch eine Trennung in Spieler A, Spieler B und Spieler C ohne eindeutige Personenidentifikation vornimmt.

Wer World of Warcraft spielen möchte, muss ausdrücklich die Erlaubnis zum Scan des Arbeitsspeichers geben.[12] Blizzard begründet dies mit der Notwendigkeit zur Verhinderung von Cheats (Spielschummeleien). Der nächste Schritt könnte die Erlaubnis zur Online-Festplattendurchsuchung sein. Ein Bundestrojaner würde über die Accountanmeldung individualisiert per Patch

(automatisiertes Programm-Zwangsupdate) übermittelt werden.

Das Spiel überzeugt durch eine besondere Faszination, in der jeder seinen Leidenschaften als Jäger und Sammler nachgeht, wo alle gesellschaftlichen Schichten vertreten sind und wo man (noch) klassenlos das Böse oder das Gute bekämpfen kann, um dem Alltag zu entfliehen.

Und weil das Spiel so außergewöhnlich, interessant, amüsant, spannend und manchmal sogar suchterzeugend ist,[13] bleibt allen Liebhabern des Spiels nichts anderes übrig, als auf „Akzeptieren“ zu klicken und damit auf die Persönlichkeitsrechte zu verzichten.

Das Prinzip des Erfolgssystem mit perfekter Spielprotokollierung und hoher Duldungsbereitschaft durch die Nutzer wird sicher weitere Inspirationen für Google, Facebook und inzwischen auch Microsoft zur Aushöhlung des Datenschutzes liefern.

1 http://de.wikipedia.org/wiki/World_of_Warcraft

2 http://de.wikipedia.org/wiki/Rollenspiel_(Spiel)

3 http://de.wikipedia.org/wiki/World_of_Warcraft#Erfolgssystem

4 http://www.buffed.de/World-of-Warcraft-PC-16678/Guides/FAQ-zum-Erfolgssystem-791392/

5 http://arstechnica.com/old/content/2007/05/google-patent-for-game-ads-evaluates-user-actions-psychology.ars

6 http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%22200700726 76%22.PGNR.&OS=DN/20070072676&RS=DN/20070072676

7 http://www.gamestar.de/hardware/news/internet/1468926/google.html

8 http://eu.battle.net/wow/de/game/guide/playing-together

9 http://eu.battle.net/wow/de/game/class/

10 http://eu.blizzard.com/de-de/company/about/termsofuse.html

11 http://wowdata.buffed.de/?q=12678

12 http://eu.blizzard.com/de-de/company/about/termsofuse.html

13 http://www.rollenspielsucht.de/resources/Warum_WoW_suechtig_machen_kann_RPfeiffer.pdf

Marc Solga

Erlebte Rechenschaftsverpflichtung: zur Psychologie des Sich-Verantworten-Müssens

Erlebte Rechenschaftsverpflichtung ist die Erwartung, beurteilt zu werden und Rechenschaft geben – d. h. sich erklären und rechtfertigen – zu müssen. Wer Rechenschaftsverpflichtung empfindet weiß, dass er sich vor einer Instanz mit Sanktionsmacht verantworten muss.

In Wirtschaftsunternehmen wird Rechenschaftsverpflichtung durch Leistungsbeurteilungsprozesse, Management Audits, Überwachungssysteme, Codes of Ethics usw. erzeugt, um das Verhalten von Mitarbeitern und Führungskräften zu steuern. Datenscreenings und Videoüberwachung, Kündigung wegen kleinster Vergehen, die Pflicht zur Offenlegung von Einkünften – gemeinsames Ziel dieser Maßnahmen, über deren Angemessenheit vor wenigen Monaten öffentlich gestritten wurde, war und ist es, Rechenschaftsverpflichtung zu forcieren. Gelegentlich ist dabei von Compliance Management die Rede. Der Begriff Rechenschaftsverpflichtung (engl. accountability) soll das subjektive Erleben kennzeichnen, das durch Überwachungs- und Steuerungsmaßnahmen dieser Art entsteht, und so den Blick auf die psychologischen Aspekte von Compliance Management richten.

Obwohl der Begriff eine Grunderfahrung unseres Arbeitslebens beschreibt, wissen Arbeits- und Organisationspsychologen noch wenig über die Wirkungen von Rechenschaftsverpflichtung. Die systematische Untersuchung ihrer Effekte im Kontext von Arbeit und Beruf hat erst vor wenigen Jahren begonnen. Dabei spricht Vieles dafür, dass wir Rechenschaftsverpflichtung brauchen, weil sie wichtige psychologische und gesellschaftliche Funktionen erfüllt:

Rechenschaftsverpflichtung ermöglicht Selbstregulation. Wir sind erst dann in der Lage, uns selbst zu steuern, wenn wir eine Vorstellung davon haben, was andere von uns erwarten und welchen Spielregeln wir folgen müssen. Zweitens: Identitätsentwicklung (die Entwicklung unseres Selbstbilds) benötigt Rechenschaftsverpflichtung. Denn wir brauchen Bewertungsprozesse, um zu verstehen, wer wir sind und wo wir stehen. Es bedarf der Auseinandersetzung mit sozialen Erwartungen und Bewertungskriterien. Drittens: Rechenschaftsverpflichtung gilt vielen Autoren als zentrales Integrations- und Steuerungsprinzip sozialer Systeme. Menschen und folglich Gruppen, Organisationen und Gesellschaften wären nicht in der Lage, koordiniert zu handeln, wenn nicht Rechenschaftsverpflichtung dafür sorgen würde, dass Einzelne sich an die Erwartungen und Aufträge ihrer Partner gebunden und zur Kooperation verpflichtet fühlen.

Erlebte Rechenschaftsverpflichtung steht im Mittelpunkt mehrerer Forschungsprojekte, die wir seit etwa anderthalb Jahren an der Ruhr-Universität Bochum, Fakultät für Psychologie, durchführen. Sie leisten einen Beitrag zur Psychologie des Sich-Verantworten-Müssens in Organisationen. Dabei interessieren wir uns für drei Aspekte: Erstens, welchen Einfluss hat erlebte Rechenschaftsverpflichtung auf die berufliche Leistung von Mitarbeitern und Führungskräften? Zweitens, welche Auswirkungen hat Rechenschaftsverpflichtung auf unser Wohlbefinden? Und schließlich: Welchen Einfluss hat Rechenschaftsverpflichtung auf solche Aktivitäten, die den legitimen Interessen eines Arbeitgebers zuwider laufen? Anders formuliert: Ist Rechenschaftsverpflichtung geeignet, kontraproduktives Verhalten – Krankfeiern, Diebstahl, Geheimnisverrat, Mobbing etc. – zu reduzieren? Ich will im Folgenden kurz skizzieren, was unsere Studien bisher ergeben haben.

Rechenschaftsverpflichtung und berufliche Leistung

Es ist zunächst hilfreich, zwei Facetten von beruflicher Leistung zu unterscheiden, passive und proaktive. Passive Leistung erfolgt im Sinne eines Arbeitsauftrags. Proaktive Leistung wird eigenverantwortlich oder gar eigenmächtig erbracht. Sie folgt dem Ziel, Arbeitsbedingungen oder -prozesse zu verbessern; es fehlt aber der entsprechende Auftrag – die Proaktiven sind ihre eigenen Auftraggeber.

Erlebte Rechenschaftsverpflichtung kann beide Formen beruflicher Leistung fördern, die passive ebenso wie die proaktive. Der zugrunde liegende Wirkungsmechanismus ist aber jeweils ein anderer: Wir investieren unsere Arbeitskraft in passive Leistung, wenn wir die auferlegte Rechenschaftsverpflichtung als bedrohlich erleben (Furcht vor Misserfolg und Strafe). Wir investieren unsere Arbeitskraft proaktiv, wenn wir die auferlegte Rechenschaftsverpflichtung als Chance begreifen (Hoffnung auf Erfolg und Belohnung).

Ein sozialpsychologischer Ansatz – die Theorie des regulatorischen Fokus – geht davon aus, dass wir zwei handlungssteuernde Systeme in uns tragen. Sie werden als Promotions- und Vermeidungsfokus bezeichnet. Wenn wir im Promotionsfokus sind, so folgen wir dem Prinzip, Gewinne, Erfolge und Belohnungen zu maximieren. Wenn wir im Vermeidungsfokus sind, agieren wir nach der Maxime, Verluste, Misserfolge und Bestrafung zu vermeiden. Der regulatorische Fokus, so die besagte Theorie, wird durch Kontextbedingungen getriggert – Signale, die wir aus der Umgebung erhalten, aktivieren den Promotions- oder aber den Vermeidungsfokus.

Wir gehen mit Blick auf diese Theorie davon aus, dass Rechenschaftsverpflichtung über die Aktivierung des

regulatorischen Fokus auf berufliche Leistung wirkt. Mitarbeiter investieren in passive Leistung, wenn sie durch das Erleben von Rechenschaftsverpflichtung in den Vermeidungsfokus kommen. Sie investieren in proaktive Leistung, wenn im Erleben von Rechenschaftsverpflichtung zugleich der Promotionsfokus aktiviert wird.

Ob wir passive oder proaktive Aspekte in den Vordergrund stellen, hängt also davon ab, wie – d. h. in welcher Haltung und mithilfe welcher Maßnahmen – die Organisation ihre Beurteilungs- und Überwachungsprozesse angekündigt und begründet (kritisch, gutachterlich, defizitorientiert vs. wertschätzend, partnerschaftlich, chancenorientiert). Anders ausgedrückt: ob diese den Vermeidungs- oder den Promotionsfokus aktivieren.

Rechenschaftsverpflichtung und Wohlbefinden

Menschen, die Rechenschaftsverpflichtung als bedrohlich erleben, zeigen erhöhte Werte in emotionaler Erschöpfung und Depersonalisation (erlebte Entfremdung). Erste Befunde zeigen, dass der Zusammenhang zwischen Rechenschaftsverpflichtung und Irritation (Gereiztheit und Nicht-Abschalten-Können) bzw. Burnout über das Erleben von Selbstkontrollanforderungen vermittelt wird. Damit ist die erlebte Verpflichtung gemeint, innere Widerstände zu überwinden, Impulse zu kontrollieren und Ablenkungen von außen zu widerstehen. Wer sich beurteilt und zur Verantwortung gezogen fühlt, der glaubt, nicht nachlassen zu dürfen. Denn immerzu gilt es, den Erwartungen eines anspruchsvollen und sanktionsmächtigen Publikums gerecht zu werden. Irritation und Burnout können langfristige Folgen dieser Überzeugung sein.

Rechenschaftsverpflichtung und kontraproduktives Verhalten

Uns hat ferner interessiert, ob Rechenschaftsverpflichtung das Potenzial besitzt, kontraproduktive Aktivitäten einzudämmen. Als kontraproduktiv werden alle Verhaltensweisen bezeichnet, die darauf ausgerichtet sind, den legitimen Interessen einer Organisation oder einzelner Organisationsteilnehmer absichtlich zu schaden (Dienst nach Vorschrift, Blaumachen, Aggression gegen Kollegen, Betrug, Diebstahl etc.). Zu diesem Zweck haben wir das Zusammenspiel von erlebter Rechenschaftsverpflichtung und solchen Bedingungen untersucht, die sich in der Vergangenheit als wichtige Vorbedingungen für kontraproduktives Verhaltens erwiesen haben.

Diesen Bedingungen ist beispielsweise die Verletzung psychologischer Kontrakte zuzurechnen. Der psychologische Kontrakt ist kein Vertrag im rechtlichen Sinne, sondern die individuelle Sicht eines Mitarbeiters auf die wechselseitigen Verpflichtungen seiner selbst und des Unternehmens im Rahmen der gemeinsamen Arbeitgeber-Arbeitnehmer-Beziehung. Der psychologische Kontrakt gilt als gebrochen, wenn Unternehmen eine oder mehrere dieser vertragsgemäßen Pflichten (z.B. Arbeitsplatzsicherheit garantieren, die Persönlichkeitsentwicklung fördern, Entscheidungsspielräume und Aufstiegschancen gewähren) brechen. Wir wissen, dass wahrgenommene Vertragsbrüche kontraproduktives Verhalten zur Folge haben. Dabei hat letzteres zwei Funktionen. Es dient dazu, sich Luft zu machen, d. h. Ärger und Enttäuschung zu ventilieren. Es kann zweitens eine bewusst gewählte Vergeltungsmaßnahme sein, die für einen Ausgleich der Interessen sorgen und Gerechtigkeit wiederherstellen soll.

In dem beschriebenen Zusammenhang, so zeigen unsere Ergebnisse, wirkt Rechenschaftsverpflichtung tatsächlich im Sinne eines Vorbeugemechanismus. Menschen, die den psychologischen Kontrakt als verletzt erleben, zeigen wenig kontraproduktives Verhalten, wenn sie in einem hohen Maße Rechenschaftsverpflichtung erleben. Sie zeigen andererseits viel kontraproduktives Verhalten, sobald sie keine oder nur wenig Rechenschaftsverpflichtung erleben. Rechenschaftsverpflichtung erweist sich also als ein Mechanismus, der kontraproduktive Reaktionen unterdrückt und Compliance gewährleistet. Ähnliches findet sich, wenn man andere Vorbedingungen kontraproduktiven Verhaltens betrachtet.

Fazit

Grundsätzlich gilt: Wer Rechenschaftsverpflichtung erlebt, erbringt bessere Leistungen. Zugleich ist die Forcierung von Rechenschaftsverpflichtung ein Mittel zur Reduzierung unerwünschten Verhaltens am Arbeitsplatz. Rechenschaftsverpflichtung jedoch, die als bedrohlich erlebt wird, ist belastend – sie kann das psychische Wohlbefinden stören und Burnout hervorrufen. Deshalb gilt es, Maßnahmen zur Forcierung von erlebter Rechenschaftsverpflichtung stets verantwortungsvoll einzusetzen.

Cartoon

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011

Funkzellenabfrage muss eingeschränkt werden!

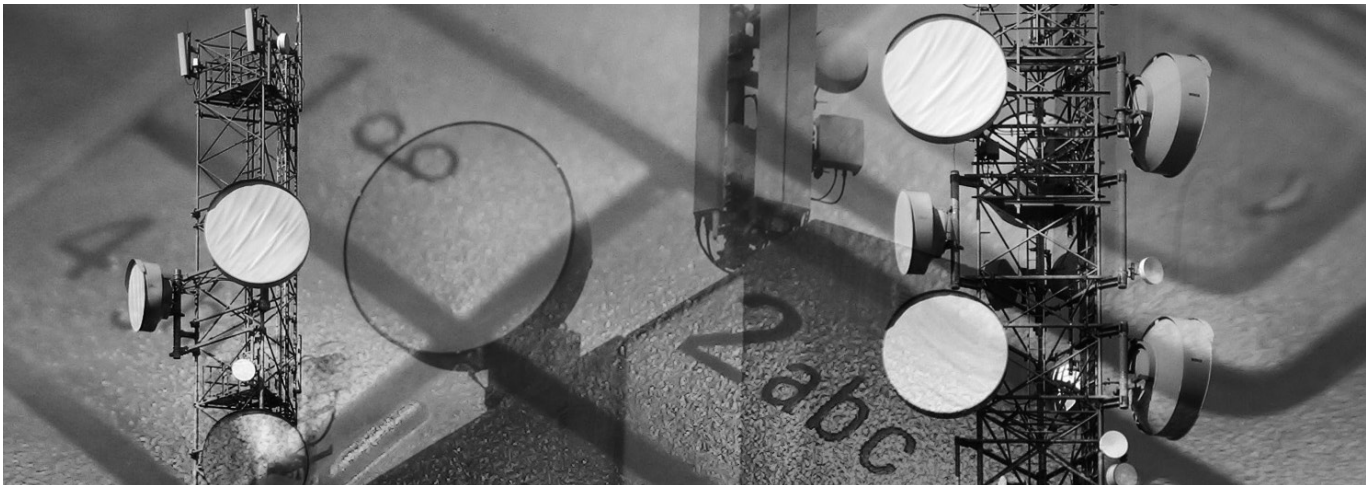
Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdner Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nicht-individualisierten Funkzellenabfrage ist bisher § 100g Abs. 2 S. 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Art. 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Möglichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nicht-individualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.



Pressemitteilung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) vom 02.08.2011

Gesichtserkennungsfunktion von Facebook verstößt gegen europäisches und deutsches Datenschutzrecht – Löschung biometrischer Daten bei Facebook gefordert

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat Facebook aufgefordert, die über die Gesichtserkennung gespeicherten biometrischen Daten der Nutzer zu löschen. Die Funktion der Gesichtserkennung ist an europäische und nationale Datenschutzstandards anzupassen oder abzuschalten.

Die Gesichtserkennung dient zur automatischen Erkennung von Freunden, die auf Fotos der Nutzer abgebildet sind. Hierfür wertet Facebook die von Nutzern auf ihren Fotos markierten Gesichter nach biometrischen Merkmalen aus und speichert sie. So entsteht die vermutlich weltweit größte Datenbank mit biometrischen Merkmalen einzelner Personen. Lädt ein Nutzer neue Fotos hoch, folgt ein Abgleich mit diesen Informationen. Sobald die Software auf diesen Fotos Übereinstimmungen mit Freunden erkennt, wird automatisch ein Vorschlag für die namentliche Markierung der erkannten Person generiert.

Dabei ist nicht der Einsatz der Gesichtserkennungssoftware zur Erleichterung des sogenannten Foto-Taggings von Freunden das Problem. Vielmehr ist bedenklich, dass Facebook für diese Funktion im Hintergrund eine Datenbank zur Gesichtserkennung mit Millionen von Nutzern aufbaut. Bei einer Gesamtzahl von über 75 Milliarden hochgeladener Fotos wurden bisher nach Angaben von Facebook mehr als 450 Millionen Personen getaggt. Schätzungen zu Folge werden pro Sekunde mehr als 1.000 Namens-Taggs eingetragen. Die Risiken einer derartigen Ansammlung biometrischer Daten sind immens.

Derzeit wird jeder auf einem Foto markierte Nutzer in der Datenbank erfasst, der der Speicherung seiner Fotoinformationen nicht ausdrücklich widerspricht. Das derzeitige Opt-Out durch Facebook ist dabei irreführend.

Unter den Privatsphäre-Einstellungen bietet Facebook den Nutzern an, das Unterbreiten von Markierungsvorschlägen zu unterbinden (unter „Freunden Fotos von mir vorschlagen“). Facebook hat dazu schriftlich mitgeteilt, dass nach Abschalten dieser Funktion auch eine Löschung der biometrischen Daten erfolge. Laut Facebooks Online-Hilfesystem werden damit aber lediglich die Markierungsvorschläge unterdrückt. Es ist davon auszugehen, dass die biometrischen Daten gespeichert bleiben. Wenn Nutzer ihre bereits gespeicherten biometrischen Informationen löschen wollen, müssen sie zunächst das Online-Hilfesystem durcharbeiten. Darin wird zur Löschung der biometrischen Daten ein Weg über die Privatsphäre-Einstellungen gewiesen.

Die entsprechende Funktion („Daten aus Fotovergleich löschen“) existiert jedoch nicht. An einer anderen Stelle im Hilfesystem findet sich ein Link, über den der Nutzer das „Facebook Foto-Team“ kontaktieren kann. Dort soll er um die Entfernung aller bisher über ihn selbst in der biometrischen Datenbank gespeicherten Fotoinformationen bitten. Eine Opt-Out-Möglichkeit ist damit zwar vorhanden, für den normalen Nutzer aber kaum zu finden. Angesichts dessen scheint besonders bedenklich, dass sogar für minderjährige Nutzer die Gesichtserkennung voreingestellt ist.

Aber selbst wenn Facebook ein nutzerfreundliches Verfahren zum Opt-Out anböte, würde es weder nationalen noch europäischen Datenschutzanforderungen genügen. Für eine Speicherung von biometrischen Merkmalen ist eine vorab erteilte, unmissverständliche Einwilligung der Betroffenen erforderlich. Zu unterstellen, durch bloßes Nichteinlegen eines Widerspruchs läge eine Zustimmung vor, reicht hierfür nicht aus. Auch die Art.-29-Gruppe, der Zusammenschluss der Datenschutzbeauftragten Europas, hat deutlich gemacht, dass die Beibehaltung von Voreinstellungen in sozialen Netzwerken keinen eindeutigen Erklärungsgehalt hat.

Dazu Johannes Caspar, der HmbBfDI: „Wir haben Facebook wiederholt aufgefordert, die Funktion der Gesichtserkennung abzuschalten und die bereits gespeicherten Daten zu löschen. Sollte Facebook diese Funktion weiterhin aufrechterhalten, muss sichergestellt werden, dass nur Daten von Personen in die Datenbank eingehen, die zuvor wirksam ihre Einwilligung zur Speicherung ihrer biometrischen Gesichtsprofile erklärt haben. Die automatische Gesichtserkennung ist ein schwerer Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen. Das muss auch ein global agierendes Unternehmen berücksichtigen. Daher darf Facebook nicht lediglich auf ein intransparentes Widerspruchsverfahren verweisen. Eine selbstbestimmte Entscheidung macht die Einwilligung des informierten Nutzers erforderlich. Facebook sollte dies erkennen und unseren Forderungen schnell nachkommen.“

Pressemitteilung des Arbeitskreises Vorratsdatenspeicherung (AK Vorrat) vom 16.09.2011:

Internetnutzer gegen geplantes Verbot des „Internet-Bargelds“

Der Arbeitskreis Vorratsdatenspeicherung warnt den Deutschen Bundestag in einem Brief vor dem Gesetzentwurf der Bundesregierung zur „Optimierung der Geldwäscheprävention“. Dessen Annahme würde das anonyme Bezahlen im Internet unmöglich machen und damit das „Bargeld des Internet“ abschaffen - mit schwerwiegenden Konsequenzen.

In dem Brief der im Arbeitskreis zusammengeschlossenen Datenschützer und Internetnutzer an die Mitglieder des Wirtschafts- und Innenausschusses des Bundestages heißt es, E-Geld zum Bezahlen im Internet (z.B. von Paysafecard oder UKash) wäre bei Verabschiedung des Gesetzentwurfs nur noch gegen Vorlage eines Ausweises erhältlich. Ein solches Verbot des „Bargelds des Internet“ würde Datenklau, Identitätsdiebstahl und Betrug mit Kreditkarten- und Bankdaten Vorschub leisten und den 50 Mio. deutschen Internetnutzern „das beste Mittel zum Selbstschutz vor Online-Kriminalität“ aus der Hand schlagen. Es hätte zudem unabsehbare wirtschaftliche Auswirkungen auf die Unterhaltungs- und Telekommunikationsbranche. Der AK Vorrat fordert die Volksvertreter deshalb auf, das Vorhaben zu stoppen.

Der Brief im Wortlaut:

11. September 2011

Vorratsspeicherung von Zahlungsdaten im Gesetzentwurf zur „Optimierung der Geldwäscheprävention“ (BT-Drs. 17/6804)

Sehr geehrte...,

mit großem Erstaunen und einigem Entsetzen haben wir zur Kenntnis genommen, dass die Bundesregierung den anonymen Zahlungsverkehr im Internet verbieten will, indem ohne jeden Anlass für die gesamte Bevölkerung auf Vorrat gespeichert werden soll, wer welche Guthabenkarte erworben hat („Gesetzentwurf zur Optimierung der Geldwäscheprävention“). Selbst E-Geld-Kleinbeträge bis 150 Euro sollen Unternehmen wie Paysafecard oder Ukash künftig nicht mehr ohne Identifizierung anbieten dürfen. Demgegenüber sollen anonyme Bankeinzahlungen bis 1.000 Euro und anonyme Bargeldtransaktionen unbegrenzt möglich bleiben. Das Vorhaben wird mit dem Argument begründet, durch Einsatz mehrerer Zahlkarten könnten „große Beträge von erheblicher geldwäscherechtlicher Relevanz bei der Ausgabe und dem Rücktausch von E-Geld anonym bewegt werden“.

Das Argument der Geldwäsche rechtfertigt aus unserer Sicht kein Totalverbot des anonymen Bezahlens im Internet. 2010 wurden in Deutschland 6.764 Fälle von Geldwäsche registriert, was 0,1% der registrierten Gesamtkriminalität entspricht. Auch ohne Identifizierungspflicht wurden 92,2% der Verdachtsfälle erfolgreich aufgeklärt. Es fehlt jeder Nachweis, dass E-Geld-Kleinbeträge in nennenswertem Umfang zur Geldwäsche oder gar Terrorismusfinanzierung eingesetzt werden und dass ein auf Deutschland beschränkter Identifizierungszwang nicht ohne weiteres umgangen werden könnte. E-Geld könnte im Ausland weiterhin anonym gekauft werden, und auch in Deutschland gekauftes E-Geld könnte nach der erstmaligen Identifizierung unkontrolliert weitergegeben werden. Der praktisch zu erwartende Nutzen einer Identifizierungspflicht zur Verfolgung von Geldwäsche wäre gering bis nicht gegeben.

Demgegenüber wären die Folgen eines Totalverbots des anonymen Bezahlens im Internet unzumutbar. Der Gesetzentwurf der Bundesregierung steht in klarem Widerspruch zu § 13 Absatz 6 des Telemediengesetzes, der aus guten Gründen Diensteanbieter im Internet zur Akzeptanz anonymer Zahlungsmittel verpflichtet. Dass im Internet noch verbreitet mit Kreditkarte, durch Angabe einer Bankverbindung oder gar Angabe einer Online-Banking-PIN („Sofortüberweisung“) bezahlt wird, ist eine ständige Ursache für Datenklau, Identitätsdiebstahl (z.B. „Phishing“) und Betrug. Datenskandale wie der Handel mit Millionen von Bankverbindungen auf CDs haben in den letzten Jahren immer häufiger in Erinnerung gerufen, dass nur nicht angegebene Kreditkarten- und Kontodaten sichere Daten sind. Jeder vierte deutsche Internetnutzer hat einer BITKOM-Umfrage bereits finanziellen Schaden im Internet erlitten. Anonyme Zahlungskarten sind das beste Mittel zum Selbstschutz vor Online-Kriminalität. Der Gesetzentwurf der Bundesregierung würde den 50 Mio. Internetnutzern in Deutschland dieses Mittel zur Kriminalprävention aus der Hand schlagen.

Eine Zwangsregistrierung aller E-Geld-Nutzer würde es außerdem ermöglichen, das alltägliche Zahlungsverhalten unbescholtener Menschen minutiös nachzuvollziehen, obwohl diese zu nahezu 100% keinerlei Anlass zu einer Protokollierung ihres Zahlungsverhaltens gegeben haben. Vergleichbares ist außerhalb des Internet, wo Barzahlung die Regel ist, undenkbar. Anonymes E-Geld als das „Bargeld des Internets“ zu verbieten, würde dem berechtigten Bedürfnis vieler Menschen nach Vertraulichkeit und Anonymität nicht gerecht: Wer beispielsweise einer gemeinnützigen Organisation Geld spenden möchte, kann ein berechtigtes Interesse daran haben, dass aus der Spende keine Rückschlüsse auf seine sexuelle Orientierung, seinen Glauben, seine religiösen oder poli-

tischen Anschauungen gezogen werden können. Auch wer beispielsweise Erotikinhalte konsumiert, hat ein berechtigtes Interesse daran, anonym zu bleiben. Zur Inanspruchnahme strafrechtlicher, psychologischer oder medizinischer Beratung über das Internet sind Menschen ebenfalls vielfach nur im Schutz der Anonymität bereit.

Neben den gesellschaftlichen sind auch die wirtschaftlichen Auswirkungen eines Verbots anonymer Zahlungen im Internet unabsehbar. E-Geld kommt unter anderem in der Unterhaltungs- und Telekommunikationsbranche verbreitet zum Einsatz. Wegen des Aufwands einer Identifizierung beim Erwerb von Kleinbeträgen würden ganze Vertriebskanäle für solche E-Geldkarten wegfallen. Studien zufolge verzichten viele Verbraucher auf Dienstleistungen im Internet, die eine Angabe persönlicher Daten wie Kredit- oder Kontodaten erfordern, insgesamt. Ein Identifizierungszwang droht dadurch die wirtschaftliche Existenz und die Arbeitsplätze von Dienstanbietern in einer Zukunftsbranche Deutschlands zu gefährden, die Entwicklung innovativer Geschäftsmodelle zu behindern und das wirtschaftliche Wachstum im Bereich der Informationstechnologie auszubremsen.

Insgesamt steht der erhoffte Nutzen eines unterschiedlosen Identifizierungszwangs für E-Geld-Nutzer in keinem Verhältnis zu den damit verbundenen Nachteilen. Einer zu erwartenden Verfassungsbeschwerde wegen Verletzung des informationellen Selbstbestimmungsrechts würde ein unterschiedsloser Identifizierungszwang für Kleinbeträge nicht stand halten.

Wir appellieren deshalb an Sie, jeder verdachtsunabhängigen Erfassung der Nutzer von E-Geld entschieden entgegen zu treten. Dienstleistungen im Internet müssen ebenso anonym und geschützt bezahlt werden können wie vergleichbare Leistungen außerhalb des Internets. Bitte setzen Sie sich für eine Änderung des „Gesetzentwurfs zur Optimierung der Geldwäscheprävention“ ein, um den von der EU eingeräumten Spielraum für anonymen Zahlungsverkehr im Internet zu nutzen.

Mit freundlichen Grüßen,
...
Arbeitskreis Vorratsdatenspeicherung

Der Gesetzentwurf der Bundesregierung: http://dipbt.bundestag.de/extrakt/ba/WP17/361/36164.html
Stellungnahme des Unabhängigen Landesdatenschutzzentrums (ULD) vom 01.07.2011: https://www.datenschutzzentrum.de/presse/20110701-geldwaeschepraevention.htm

Pressemitteilung 30/2011 Bonn/Berlin, 31.08.2011

Zwei Jahre Informationspflichten bei Datenpannen

Zum zweijährigen Bestehen der Informationspflicht bei Datenschutzpannen zeigt sich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar zufrieden mit der neuen Regelung, fordert aber deren Erstreckung auf staatliche Stellen:

„Die Schaffung einer Informationspflicht bei Datenschutzpannen war ein richtiger Schritt. Die Publizitätspflicht motiviert die verantwortlichen Stellen, mehr für die Datensicherheit und den Datenschutz zu tun, und versetzt die Betroffenen in die Lage, negative Konsequenzen rechtzeitig abzuwenden und Sicherheitsmaßnahmen zu ergreifen. Leider ist der Gesetzgeber auf halber Strecke stehen geblieben, indem er staatliche Stellen von der allgemeinen Informationspflicht bei Datenschutzpannen ausgenommen hat. Es ist nicht nachvollziehbar, warum das Gesetz bei Datenschutzverstößen öffentlicher und privater Stellen unterschiedliche Maßstäbe anlegt. Hier besteht weiterer Nachbesserungsbedarf.“

Nach einer bundesweiten Erhebung wurden den Datenschutzaufsichtsbehörden des Bundes und der Länder in den ersten 18 Monaten nach Inkrafttreten der Informationspflichten fast 90 Fälle gemeldet. In der überwiegenden Zahl handelte es sich um den Diebstahl oder Verlust von mobilen Datenträgern, wie Notebooks und USB-Sticks, oder um Fehlversendungen von E-Mails und Briefen. Daneben gab es Fälle des Ausspähens von Bankdaten (Skimming) und Datenverluste durch Hacking. Betroffen waren in aller Regel Bankverbindungs- und Kreditkartendaten, zum Teil aber auch besonders sensible Daten, wie Gesundheitsdaten.

Dazu Schaar: „Die Anzahl der bundesweit gemeldeten Fälle belegt, dass die Informationspflicht bei Datenschutzpannen von den verantwortlichen Stellen ernst genommen wird. Dennoch gehe ich von einer hohen Dunkelziffer nicht gemeldeter Vorfälle aus. Häufig ist auch die Kommunikation der verantwortlichen Stellen gegenüber der Öffentlichkeit und den Datenschutzbehörden noch stark verbesserungsbedürftig.“

Seit dem 1. September 2009 müssen nicht-öffentliche Stellen und ihnen gleich gestellte öffentlich-rechtliche Wettbewerbsunternehmen gravierende Datenschutzpannen der zuständigen Aufsichtsbehörde anzeigen sowie die Betroffenen informieren und ihnen Handlungsempfehlungen unterbreiten. § 42a des Bundesdatenschutzgesetzes sieht eine solche Informationspflicht vor, wenn sensible personenbezogene Daten unrechtmäßig in die Hände Dritter gelangt sind und schwerwiegende Beeinträchtigungen für die Betroffenen drohen. Bei einem Verstoß gegen § 42a des Bundesdatenschutzgesetzes droht ein Bußgeld von bis zu dreihunderttausend Euro oder sogar mehr.

Verantwortlich: Peter Schaar. Redaktion: Juliane Heinrich

Pressestelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit telefonisch 030 18 77 99 916 oder 0172 2503700 oder per E-Mail pressestelle@bfdi.bund.de

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

ELENA wird abgewickelt

Die Bundesregierung will den umstrittenen „Elektronischen Entgeltnachweis“ (ELENA) wieder abschaffen. Die Bundesministerien für Wirtschaft und Technologie sowie Arbeit und Soziales haben sich laut einer gemeinsamen Mitteilung vom 18.07.2011 darauf verständigt, „das Verfahren schnellstmöglich einzustellen“. Als Grund geben die Ministerien die noch ungenügende Verbreitung der qualifizierten elektronischen Signatur an. Diese sei für das ELENA-Verfahren aber „datenschutzrechtlich zwingend geboten“.

Mit dem Großprojekt ELENA sollte der Papier-Belegwesen bei den Sozialbehörden verringert werden. Der „elektronischen Entgeltnachweis“ sollte z. B. bei Anträgen auf Arbeitslosengeld, Wohngeld oder Elterngeld die Arbeitgeberbescheinigungen auf Papier ersetzen und Abläufe erleichtern. Schon Anfang der 2000er war das damals noch unter dem Namen „JobCard“ firmierende Projekt von den Landesbeauftragten für den Datenschutz konzeptionell als verfassungswidrig kritisiert worden. Diese Kritik wurde aber von der Politik nicht ernsthaft zur Kenntnis genommen. Januar 2010 war das Projekt in die erste Realisierungsphase gegangen. Seither müssen Arbeitgeber mit ihren monatlichen Gehaltsabrechnungen für jeden ihrer Beschäftigten zahlreiche Eckdaten wie Name und Anschrift, Versicherungsnummer, Gesamt-, Steuer- und Sozialversicherungs-Bruttoeinkünfte, Abzüge für die Sozialversicherung sowie steuerfreie Bezüge verschlüsselt an die zentrale Speicherstelle (ZSS) der Deutschen Rentenversicherung übermitteln.

Diese Datensammlung, die die Einkommensdaten der gesamten bundesdeutschen Bevölkerung erfasst, rief nicht nur die DatenschützerInnen auf den Plan. Das Bundesverfassungsgericht (BVerfG) wurde mehrfach angerufen, lehnte einen Eilantrag gegen ELENA im September 2010 aber ab. Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP) hatte ELENA im Januar 2011 grundsätzlich infrage gestellt. Ihr Parteikollege, der ehemalige Innenminister Gerhart Baum, hält das Verfahren für verfassungswidrig. Entsprechende Stellungnahmen gaben die Landesdatenschutzbeauftragten vor dem BVerfG ab. Die Bundesregierung will nun dafür sorgen, dass die bisher gespeicherten Daten unverzüglich gelöscht werden. In der Datenbank waren inzwischen bereits über 700 Mio. Datensätze gespeichert. Mitte 2011 lieferten etwa 3,2 Mio. Firmen Daten ihrer Beschäftigten an.

Im Wirtschaftsministerium gab es darüber hinaus Zweifel an der Praxistauglichkeit sowie Befürchtungen, vor allem mittelständische Unternehmen könnten unverhältnismäßig belastet werden. Offiziell sollte ELENA ab Anfang 2012 genutzt werden. Der Beginn war dann aber zunächst um zwei Jahre verschoben worden. Die Kommunen hatten vor Mehrkosten von bis zu 250 Millionen Euro gewarnt. Auch im Bundesarbeitsministerium und in der CDU/CSU regte sich Widerstand. Ein Antrag der Grünen auf ein Moratorium war vom Bundestag allerdings abgelehnt worden. Fürsprecher fand ELENA schließlich nur noch in der IT-Branche. Die Arbeitgeber müssen nun von den bestehenden elektronischen Meldepflichten entlastet werden. Das Wirtschaftsministerium werde in Kürze einen entsprechenden Gesetzentwurf vorlegen, teilten die Ministerien mit. Die Investitionen sollen aber nicht umsonst gewesen sein: Das Arbeitsministerium werde ein Konzept erarbeiten, wie die bereits bestehende ELENA-Infrastruktur für „ein einfacheres und unbürokratisches Meldeverfahren in der Sozialversicherung“ genutzt werden könne.

Der Deutsche Steuerberaterverband begrüßte das Aus für diese „Datenkrake“. Das Vorhaben wäre wohl vor dem BVerfG gescheitert. Der schleswig-holsteinische Datenschutzbeauftragte Thilo Weichert meinte: „Ein spätes Ende ist besser als gar kein Ende.“ Bürgerrechts- und Datenschutzorganisationen hatten beim ELENA-Verfahren den Missbrauch der hochsensiblen Daten befürchtet, die z. B. Aussagen über die Teilnahme an Streiks oder Fehlzeiten am Arbeitsplatz erlauben. Die kommunalen Verbände hatten sich beklagt, dass der bürokratische Aufwand eher zu- als abgenommen habe. Die Arbeitsgeberverbände sprachen nun von einem „Armutszeugnis für den Bürokratieabbau“. Zusammen mit den Investitionskosten seien die Unternehmen durch das Projekt mit mehreren 100 Mio. Euro belastet worden. Der Steuerzahlerbund wies darauf hin, dass ELENA den Staat 33 Mio. Euro gekostet habe (www.datenschutzzentrum.de/elena/; www.heise.de 18.07.2011; PM BfDI 19.07.2011; Öchsner SZ 20.07.2011, 1).

Bund

Papstbesuch: Datensammlung und Sicherheitsüberprüfung

JedeR, der eine Messe mit Papst Benedikt XVI. besuchen wollte, der vom 22. bis 25.09.2011 in Freiburg, Erfurt und Berlin in Großveranstaltungen erscheint, musste sich nach dem Willen der zuständigen Bistümer bzw. der deutschen Bischofskonferenz persönlich anmelden, entweder analog in den Kirchengemeinden oder digital über www.papst-in-deutschland.de. Dabei wurden nicht nur Namen und Adresse zwingend abgefordert, sondern auch Geburtsdatum, Geburtsort und E-Mail-Adresse. Weiterhin wurde gefragt nach Telefon, Fax, Bistum, Dekanat,

Pfarrgemeinde, Rollstuhlfahrer, Hörschädigung und Begleitperson. Die kirchliche Datenerhebung erfolgte auf Anregung der baden-württembergischen Polizei mit dem Ziel, diese im Bedarfsfall mit den dort verfügbaren Datenbeständen abzugleichen. Erfasst wurden damit mindestens 200.000 Menschen; schon 10 Wochen vor den Veranstaltungen hatten sich nach Angaben der Deutschen Bischofskonferenz in Bonn rund 175.000 Menschen registriert. Nach Ansicht des schleswig-holsteinischen Datenschutzbeauftragten Thilo Weichert wäre ein Abgleich der Anmeldedaten bei der Polizei „ganz klar ein Verstoß gegen das Recht auf informationelle Selbstbestimmung".

Matthias Kopp, Sprecher der Deutschen Bischofskonferenz, bestätigte die geplanten Sicherheitsüberprüfungen. Diese würden allerdings nicht routinemäßig bei allen PilgerInnen gemacht. Kopp: „Das wäre ja Datenmissbrauch". Der Datenabgleich werde aber alle PilgerInnen betreffen, die bei den Papstmessen einen Stehplatz oder Sitzplatz zugeteilt bekämen, „wo der Papst dicht vorbei fährt oder die Kommunion austeilt". Für Weichert ist der Fall einzigartig und ohne Vorbild. Daten in diesem Umfang zu sammeln sei unnötig, unverhältnismäßig und ohne Rechtsgrundlage – eine „unzulässige Rasterfahndung". Selbst wenn die Kirche die Daten nur im Einzelfall der Polizei übermittele, rechtfertige das noch lange nicht, alle BesucherInnen der Messen zu erfassen. Kopp verteidigte das Vorgehen. „Wir brauchen Planungssicherheit, um den Pilger auf ein Pilgerfeld zuzuteilen ... und für den Pilger Sicherheit, dass er auch wirklich auf dieses Feld kommt." Außerdem sei es besser, die Daten für eine Sicherheitsüberprüfung komplett vorab von allen BesucherInnen zu verlangen, denn dann „können wir sie nachher schneller löschen, als wenn wir sie kurz vor der Veranstaltung irgendwie erheben müssen".

Nachdem das Überprüfungverfahren öffentlich in Frage gestellt wurde, war auf der Webseite www.papst-in-deutschland.de zu lesen: „Warum werden die Daten Geburtsdatum, Geburtsort und Geburtsland nicht mehr erhoben? ... Aufgrund von Vorgesprächen, u. a. mit Institutionen, die für die Sicherheit zuständig sind, hatte sich zunächst ergeben, dass neben dem Namen und der Adresse auch die personenbezogenen Daten Geburtsdatum, Geburtsort und Geburtsland erhoben werden müssen. Im Rahmen der weiteren Vorbereitungen hat sich ergeben, dass die Daten Geburtsdatum ... nicht benötigt werden. Deshalb haben wir diese Daten umgehend gelöscht. Dieses Vorgehen entspricht der KDO (Kirchliche Datenschutzordnung)."

Seit der Fußball-WM 2006, für die Tickets personalisiert ausgegeben wurden, haben deutsche DatenschützerInnen mehrfach ähnlich intensive Sicherheitsüberprüfungen und „Zuverlässigkeitsabfragen" kritisiert, so zum Beispiel bei der Presseakkreditierung zum G8-Gipfel in Heiligendamm an der Ostsee im Jahr 2007. Für die Aktionen der Kirche sind die staatlichen DatenschützerInnen nicht zuständig. Es gilt nicht das staatliche Recht, sondern die von den Bischöfen erlassene KDO. Doch auch nach diesem Recht dürfte die Datensammlung illegal sein. Wie das staatliche Recht verlangt die KDO, dass so wenig Daten wie möglich erhoben werden sowie, dass Betroffene konkret in die Nutzung einwilligen müssen. Ob beide Voraussetzungen in diesem Fall erfüllt sind, ist umstritten.

Im Falle des Papstbesuches wurden - entgegen dem Kirchengesetz – die kirchlichen Datenschutzbeauftragten nicht einbezogen und nicht informiert, sagte der für die baden-württembergischen Diözesen und damit für den Freiburger Teil des Papstbesuches zuständige kirchliche Datenschutzbeauftragte Siegfried Fachet. Sein Kollege Lutz Grammann, zuständig für den Berliner Teil der Reise, schrieb einen Protestbrief an die Planer des Papstbesuches. Datenschützer Fachet hat sich nach eigener Aussage erst Mitte Juli die Anmeldewebsite zum Papstbesuch angeschaut und über die Hintergründe zu den dort verlangten Daten unterrichten lassen. Er verteidigte die Notwendigkeit der Datenerhebung, auch wenn man „über die Fragen nach Geburtsdatum und -ort geteilter Meinung" sein könne.

Aus dem Geltungsbereich der Landesdatenschutzgesetze und des Bundesdatenschutzgesetzes sind die Kirchen ausgenommen. Hintergrund ist der über das Grundgesetz fortgeltende Artikel 137 der Weimarer Reichsverfassung von 1919. Er räumt den Kirchen das Recht ein, „ihre Angelegenheiten selbständig innerhalb der Schranken des für alle geltenden Gesetzes" zu ordnen und zu regeln. Kopp meinte, die Briten seien beim Papstbesuch 2010 ähnlich verfahren wie die deutschen Bischöfe. Papstanhänger aus dem Osten Europas quittieren die deutschen Prozeduren dagegen eher mit Kopfschütteln. Für viele Polen sei es „ziemlich merkwürdig", sich überhaupt für eine Messe anmelden zu müssen, sagt der Deutschlandkorrespondent des polnischen Programms von Radio Vatikan, Thomas Kycia, und stellte in Frage, ob sich GottesdienstbesucherInnen so überhaupt willkommen fühlen. „Wenn ein Gast kommt, möchten ihn alle sehen und herzlich empfangen." Er sei gespannt, „wie viele Polen nach Berlin kommen werden und dann erst merken, dass sie gar nicht zur Messe zugelassen werden."

In Berlin werden laut Prälat Ronald Rother am 22.09.2011 unangemeldete BesucherInnen statt ins Olympiastadion zu einer Live-Übertragung der Eucharistiefeier auf die davor liegenden Wiesen gebeten. Auf den Erfurter Domplatz werden am 24.09. nur die bisher angemeldeten 32.0000 BesucherInnen zugelassen, während das Bistum Erfurt am Tag davor zur „Marianischen Vesper" im Eichsfeld eine Art von Abendkasse für den kostenlosen Eintritt einrichten wollte (Schauen www.wdr.de 13.07.2011).

Bund

Keine Fusion bei den Bundespolizeibehörden

Der neue Bundesinnenminister Hans-Peter Friedrich (CSU) erklärte, dass Bundespolizei und Bundeskriminalamt (BKA) als eigenständige Behörden erhalten bleiben sollen. Bestimmte Bereiche will er aber zusammenführen, so die Aus- und Fortbildung und die Informations- und Kommunikationstechnik. Zudem soll es eine engere Zusammenarbeit

mit dem Zoll geben. Im Dezember 2010 hatte die vom früheren Chef des Bundesamtes für Verfassungsschutz und Ex-Staatssekretärs Eckart Werthebach geleitete Kommission aus Kosten- und Effizienzgründen eine Fusion vorgeschlagen. Friedrichs Vorgänger Thomas de Maiziere hatte sich diese Vorschläge zu eigen gemacht und eine rasche Umsetzung angekündigt. Dies stieß auf heftigen Widerstand in der Bundespolizei und beim BKA, von der Belegschaft über die Gewerkschaften bis hin zu den Präsidenten Matthias Seeger und Jörg Ziercke (SZ 29.06.2011, 6; Prantl SZ 28.02.2011, 7).

Bund/Länder

Hacker dringen bei Sicherheitsbehörden ein

Anfang Juli luden Hacker heimlich Daten über Observationen deutscher Zoll- und Polizeibehörden im Zeitraum von Ende 2009 bis Ende 2010 von einem amtlichen Server herunter und stellten einige Daten auszugsweise ins Netz. Die Verantwortung dafür übernahm ein angeblicher Leiter einer Hacker-Gruppe namens „No-Name-Crew“. Betroffen von der Ausspähung waren das Zollkriminalamt (ZKA) und einige Landeskriminalämter (LKÄ). Die Staatsanwaltschaften in Karlsruhe und Köln ermitteln den Fall parallel wegen schwerer Computersabotage und anderer Delikte. Es gab zwei Festnahmen und einige Geständnisse. Die Daten waren auf einem russischen Server abgelegt worden und konnten gesichert werden, soweit das im Netz überhaupt möglich ist. Auf einer Internetseite führte die Gruppe als Motivation an, sich gegen einen Überwachungsstaat wehren zu wollen. So gäben „Signale seitens des politischen Establishments zu verstehen, dass die Unantastbarkeit gewisser Grundrechte nur eine Farce ist“.

Angegriffen wurden Daten aus dem Peil- und Ortungssystem „Patras“. Dabei bringen Spezialisten der Polizei oder des Zolls heimlich an Fahrzeugen oder auch an Containern Sender an, die mit Satelliten in Verbindung stehen. Die Ermittelnden können dann am Laptop oder am Computer verfolgen, wann der Verdächtige bzw. der markierte Gegenstand wo unterwegs ist. Früher war hierzu die Kreuzpeilung mit Hilfe von zwei Fahrzeugen nötig. Patras hielt fest, wann eine Fahrt wo begann, wie lange sie dauerte und wo sie endete. In den Dateien waren keine Namen von Verdächtigen festgehalten. Betroffen waren offensichtlich vor allem Leute aus dem Bereich der organisierten Kriminalität. Für die Maßnahme bedarf es eines richterlichen Beschlusses. Auch Testfahrten von BeamtInnen und Dienstfahrten wurden bei Patras gespeichert. Das Drittverwertungsinteressen an den Daten war eher gering. Doch ist der Imageschaden für die deutschen Sicherheitsbehörden gewaltig.

Der Fall „Patras“ zeigt jenseits des Medienzirkusses um die Hackerattacke ein reales Problem in den Sicherheitsbehörden. Das System war mehr oder weniger nebenher von Bundespolizisten gebastelt worden. Sie verwendeten dafür eine XAMPP-Installation ohne echte Absicherung. Das ZKA und auch LKÄ griffen gerne zu, da das System kostenfrei genutzt werden konnte. Eine vergleichsweise sichere Version hätte etwa 30.000 bis 50.000 Euro gekostet. Das Bundeskriminalamt (BKA) hatte das Angebot geprüft und es, offensichtlich aus Sicherheitsgründen, nicht verwendet. Hiervon erfuhren aber die anderen Sicherheitsbehörden nichts. In dem System wurde am 08.09.2010 ein Trojaner abgelegt, der aber keine Aktivität entfaltete. Ein junger Hacker berichtete in einem Internetforum, wie leicht es sei, bei Sicherheitsbehörden einzudringen. Im Mai 2011 wurden dann mindestens 42 Trojaner gepflanzt. Der Download fand zwischen dem 03. und dem 06.07.2011 statt, wobei der gesamte Server heruntergeladen wurde. Die Hacker glaubten, ihnen sei Großes gelungen, weil in den Dateien immer von „Bundespolizei“ die Rede war, die das System entwickelt hatte. Der Dilettantismus war offensichtlich auf beiden Seiten groß: Der wegen räuberischer Erpressung vorbestrafte arbeitslose Haupthacker der „No-Name-Crew“ verwendete als Pseudonym einen Namen, unter dem ihn seit Jahren die ganze Szene kennt (www.heise.de 18.07.2011; SZ 18.07.2011, 5; Leyendecker SZ 23./24.07.2011, 1, 5; Der Spiegel 30/2011, 16).

Bund

Heranwachsender verkauft gestohlene T-Online-Daten

Der 21jährige Heranwachsende Thore S. soll auf dem Schwarzmarkt Daten von T-Online-KundInnen angekauft und an Komplizen weitergegeben haben. Seit einigen Monaten ermitteln die Staatsanwaltschaften aus Hamburg und Bonn wegen gewerbsmäßigem Computerbetrug. Die Täter sollen mit Hilfe der Kundendaten sog. Software-Keys zum Freischalten von Downloads erworben und anschließend an Ebay-Händler verkauft haben. Den betroffenen KundInnen wurde das in Rechnung gestellt. Die Telekom geht davon aus, „dass die Daten über Phising bei den Kunden selbst gestohlen worden sind.“ Die Staatsanwaltschaft spricht von mindestens 4200 Geschädigten. Zudem gebe es „deutlich mehr als 4000 Beschuldigte“, die die Software-Keys bei Ebay gekauft haben sollen (Der Spiegel 25/2011, 67).

Bund

E-Mail-Betrüger fingieren Bundesfinanzministerium

Betrüger versuchten per E-Mail an Konto- und Kreditkartendaten von SteuerzahlerInnen zu gelangen, indem sie sich per Mail als „Bundesministerium der Finanzen“ ausgaben. Sie behaupteten, die betroffenen Menschen hätten zu viel Einkommenssteuer bezahlt. Um diese zurückzuerhalten, müsse ein an die E-Mail angehängtes Antragsformular ausgefüllt werden, bei dem die Kontoverbindung, die Kreditkartennummer und das Passwort angegeben werden sollen. Das Formular könne nur online ausgefüllt werden. Nachfragen per Telefon würden nicht beantwortet. Das Bundesfinanzministerium warnte davor, auf solche E-Mails zu reagieren. Es verschicke keine Änderungsbescheide per Mail. Zuständig für Änderungen von Steuerbescheiden und für Steuererklärungen sei das jeweilige Finanzamt (SZ 04./05.06.2011, 31).

Bund

„Esra“ im Internet

Im Jahr 2003 war der Roman „Esra“ von Maxim Biller gerichtlich verboten worden, weil sich zwei Frauen darin falsch dargestellt fühlten; ihre wahre Identität sei trotz Fiktionalisierung leicht zu erschließen. Im Jahr 2007 bestätigte das Bundesverfassungsgericht letztlich das gerichtliche Verbot und stellte damit den Schutz des Persönlichkeitsrechts der beiden betroffenen Frauen über die Freiheit der Kunst nach Art. 5 Grundgesetz (DANA 4/2007, 207 f.). Inzwischen wurde das vollständige unzensierte Buch von Unbekannten ins Netz gestellt und ist dort als Download auf verschiedenen Seiten leicht verfügbar. Helge Malchow, Chef von Kiepenheuer & Witsch, der „Esra“ verlegt hatte, beteuerte: „Der Verlag hat damit nichts zu tun. Zwar waren wir gegen das Verbot, aber es ist illegal, ein Buch im Internet zu veröffentlichen, dessen Rechte einem nicht gehören.“ Sein Verlag behalte sich rechtliche Schritte vor, um zu verhindern, dass „Esra“ weiterhin im Internet verfügbar ist (Der Spiegel 28/2011, 102).

Bund

Ströbele verlangt Auskunft über E-Mail-Überwachung

Das Parlamentarische Kontrollgremium für die Geheimdienste (PKGr) des Deutschen Bundestags unterstützt deren grünen Abgeordneten Christian Ströbele in seinem Bestreben, von der Bundesregierung Aufklärung zu bekommen, wie ein E-Mail-Austausch zwischen ihm und dem mutmaßlichen Islamisten Emrah E. an die Zeitschrift Focus gelangt ist. Ströbele bestätigte, dass er mit Emrah E. E-Mails ausgetauscht hat. Diese müssten Geheimdienste bei der Überwachung E.s entdeckt haben. Ströbele ist der Ansicht, dass diese E-Mail nicht aufgehoben und schon gar nicht an JournalistInnen weitergegeben werden durften (SZ 01.07.2011, 6).

Bund

„Bild“ wehrt sich gegen Presserat

Die Bild-Zeitung veröffentlichte am 02.08.2011 einen Text in eigener Sache, der dem Deutschen Presserat viele Anrufe und Zuschriften einbrachte: Unter dem Titel „Diesen Kindesentführer soll Bild nicht mehr zeigen dürfen“ erklärte das Blatt, weshalb man trotz einer Rüge der Medienwächter wegen des Persönlichkeitsschutzes des Täters weiter Fotos eines Mannes zeigt, der ein Kind entführte und Lösegeld erpresste. Bild rief dazu auf, dem Gremium die persönliche Meinung mitzuteilen, was laut Presserat „sekündlich“ geschah. Nur ein kleiner Teil der Bild-LerserInnen teilt demnach die Ansicht der freiwilligen Selbstkontrolle der Presse (SZ 03.08.2011, 15).

Bundesländer

Polizeiliche Identifizierung per Web2.0

Soziale Netzwerke wie Facebook oder Twitter helfen der Polizei in mehreren Bundesländern bei der Ermittlung von VerkehrssünderInnen. Dabei werden Fotos von Radarfallen mit Facebook-Fotos der FahrzeughalterIn und ihres Bekanntenkreises verglichen, um die Person zu finden, die beim Verkehrsverstoß hinter dem Steuer saß. Strafzettel wegen überhöhter Geschwindigkeit werden in der Regel an den Fahrzeughalter des geblitzten Autos geschickt. Saß dieser allerdings nicht am Steuer und weist er die Ordnungshüter darauf hin, kann er nicht bestraft werden. Außer beim Falschparken gibt es in Deutschland nicht die sogenannte Halterhaftung. Die Polizei muss vielmehr die tatsächliche FahrerIn ermitteln. Hierfür machen sich die Ordnungsbehörden neuerdings die sozialen Netzwerke im Internet zunutze. Mit dem Namen der HalterIn wissen die OrdnungsbeamtInnen, in welchem Umfeld sie suchen müssen, da das eigene Auto meist nur an Verwandte oder gute FreundInnen verliehen wird, bei Firmenwagen ist in der Regel einE MitarbeiterIn oder ein AngehörigeR mit dem Fahrzeug unterwegs. Dies grenzt die Suche erheblich ein. Früher bedeutete dies, dass man an den Haustüren geklingelt und nachgefragt hat, ob jemand die FahrerIn kennt. Gerade im Freundes- und Verwandtenkreis wollte jedoch niemand den Bekannten belasten.

Über die sozialen Netzwerke kann nun nach der FahrzeughalterIn gesucht werden, ohne den Büroarbeitsplatz zu verlassen. Bei Erfolg kann man bei Facebook und Co. die jeweiligen Verwandten und FreundInnen sehen, wenn die NutzerIn es in puncto Datenschutz nicht so eng sah und über sich und FreundInnen freizügig Auskunft gab. Die hinterlegten Fotos können dann mit dem „Knöllchenfoto“ abgeglichen werden. Bei Übereinstimmung hat man regelmäßig die VerkehrssünderIn. Ein konkretes Anwendungsbeispiel: Ein Fahrer aus Hamburg war im September 2010 auf der Autobahn zwischen Münster und Osnabrück beim Drängeln geblitzt worden. Bei seiner Firma hieß es, man habe das Auto einem Mitarbeiter zur Verfügung gestellt, ob dieser gefahren sei, wisse man aber nicht. Ein Polizeibeamter aus Münster recherchierte im Netz und stellte fest, dass das Facebook-Profilfoto der geblitzten Person so ähnlich sah, dass auch vor Gericht kein Zweifel bestand, wer da zu dicht aufgefahren war.

Der Sprecher des rheinland-pfälzischen Innenministeriums David Freichel kommentierte: „Ich kann dabei keinen Vorwurf erkennen.“ Schließlich seien die Daten öffentlich zugänglich. „Wenn Profile dafür gehackt werden, ist das natürlich illegal.“ Dennoch sieht dies Barbara Körffer vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) kritisch: „Ein sehr fragwürdiger Vorgang, da eine Vielzahl unverdächtiger Personen betroffen ist.“ Sie rät, so restriktiv wie möglich mit persönlichen Daten und Bildern umzugehen und die Einstellungen in sozialen Netzwerken so zu setzen, dass nicht jedeR alle Informationen sehen kann. In Rheinland-Pfalz wird erwogen, der Netzrecherche einen rechtlichen Rahmen zu geben. Dies ist nach Ansicht der stellv. Leiterin des ULD Marit Hansen auch nötig. Zwar könne man der Polizei nicht verbieten, öffentlich zugängliche Bilder zu verwenden.

Die BeamtInnen müssten sich jedoch im Klaren sein, dass der Betreiber des Web2.0-Dienstes, möglicherweise mit Sitz in den USA, herausfinden kann, für wen sich die deutsche Polizei interessiert. So kann z. B. Facebook Listen der Personen anlegen und Einblicke in interne Ermittlungen bekommen: „Wenn Facebook weiß, dass die Polizei mein Profil angesehen hat, kann es passieren, dass ich Probleme bekomme, z. B. bei der Einreise in die USA. Schließlich weiß niemand, ob ich wegen zu schnellen Fahrens oder Terrorismus überprüft wurde“ (Mormann, Havlat SH-Z 12.05.2011, 2, TM1; Thiele SZ 13.05.2011, 21).

Bayern

Viele Polizeitrojaner im Einsatz

Mehr als bisher bekannt nutzt die Polizei den sog. Bayerntrojaner. Auf Anfrage der Grünen im Landtag räumte das Justizministerium in München ein, dass die umstrittene Spionagesoftware zwischen 2009 und 2010 insgesamt fünfmal in Augsburg, Nürnberg, München und Landshut zur Anwendung kam. Dabei sollten banden- und gewerbsmäßiger Betrug, oder der Handel mit Betäubungs- und Arzneimitteln aufgeklärt werden. Die Software ermöglicht es den Ermittelnden, Internettelefonate und Chatverkehr abzufangen sowie Bilder und andere Dateien zu kopieren. Bei einem Überwachungsfall aus dem Jahr 2009 waren fast 30.000 Screenshots gemacht worden, in den anderen Fällen lagen die Zugriffe bei weit über 10.000. Die Rechtslage ist strittig. Ein 2008 von Bayern im Bundesrat vorgelegter Gesetzentwurf scheiterte. Das Landgericht Landshut hatte im Januar 2011 einen derartigen Lauschangriff als rechtswidrig eingestuft (DANA 1/2011, 37 f.). Die Fahndenden fanden trickreiche Wege zum Aufspielen der Trojaner: Einmal half der Zoll am Münchner Flughafen. Einmal wurde der Spion per Remote-Installation aufgespielt. Dreimal nutzten die Ermittelnden eine Hausdurchsuchung. Die innenpolitische Sprecherin der Grünen im Bayerischen Landtag Susanna Tausendfreund kommentierte: „Die bayerischen Behörden scheinen keinerlei Unrechtsbewusstsein an den Tag zu legen und offenbaren eine erschreckende Kaltschnäuzigkeit im Umgang mit rechtsstaatlichen Grundsätzen. Wer wahllos tausende von Seiten kopiert, kann doch kaum sicherstellen, dass nur Informationen gespeichert werden, die mit einem Kommunikationsvorgang in Verbindung stehen“ (Der Spiegel 26/2011, 18; gruen-digital.de/2011/06).

Bayern

Bing Streetside mit Vorab-Widerspruchsrecht

Nach einem längeren Streit mit deutschen Datenschutzbehörden hat der US-Konzern Microsoft eingelenkt und seine Strategie beim Umgang mit den Fotos für seinen geplanten Panorama-Kartendienst Bing Streetside geändert. Der Leiter des bayerischen Landesamts für die Datenschutzaufsicht in Ansbach, Thomas Kranig, teilte mit, dass die Betroffenen der Bilderfassung ihrer Häuser durch Kameraautos die Möglichkeit eingeräumt bekommen, eine Veröffentlichung bereits im Vorfeld abzulehnen. Vom 01.08. bis 31.09.2011 können die HausbesitzerInnen Microsoft mitteilen, „dass ihre Haus- oder Wohnungsansicht nicht online veröffentlicht werden darf“. Als Adressat des Widerspruchs wird angegeben: Microsoft Deutschland GmbH, Widerspruch Bing Maps Streetside, Postfach 101033, 80084 München. Das Widerspruchsformular wurde im Internet bereit gestellt. Nach der Frist haben Widersprüche erst eine Wirkung, nachdem die Straßenansichten bereits in Netz gestellt worden sind. Seit Ende Mai 2011 lässt Microsoft von der Firma Navteq die 50 größten Städte der Bundesrepublik abfahren und die Fronten der Wohnhäuser, Büros und Geschäfte fotografieren. Begonnen wurde in Nürnberg, Fürth und Erlangen. Insgesamt sollen gut 150.000 Streckenkilometer aufgenommen werden. Die ersten Aufnahmen sollen Herbst im Internet zugänglich gemacht werden.

Mit Streetside tritt Microsoft in Konkurrenz zu Googles Street View. Im Gegensatz zu Microsofts anfänglicher Absicht hatte Google vorab – auch auf Forderung der Datenschutzbehörden – einen Widerspruch vor dem Online-Start von Street View ermöglicht. Microsoft hatte wiederum geplant, das Material zunächst auf seine Internetseite zu stellen, ohne die Betroffenen zu involvieren. Diese sollten erst nachdem die Aufnahmen online stehen, eine Löschung des Materials beantragen können. Dies Vorgehensweise war vom Düsseldorfer Kreis, dem Zusammenschluss der Datenschutzaufsichtsbehörden, als nicht ausreichend kritisiert worden. Bundesverbraucherschutzministerin Ilse Aigner (CSU) begrüßte, dass das Unternehmen einlenkt: „Wichtig für die Bürger ist, dass eine zuverlässige und unbürokratische Widerspruchsmöglichkeit geschaffen wird“ (www.tagesschau.de 09.06.2011; www.taz.de 09.06.2011; SZ 10.06.2011, 30; PE LDI NRW 28.07.2011).

Bayern

Verdeckte Ermittler auf Pay-TV-Abo-Kundenfang

Der Münchner Abo-Fernsehsender Sky setzt verdeckte Ermittler ein, um an mehr KundInnen zu kommen. Diese werden vorwiegend Samstag nachmittags in Café-Bars und kleinere Gaststätten geschickt, um zu kontrollieren, ob den Gästen mit geborgten Sky-Codes-Karten eine Fernsehübertragung von Fußball-Bundesligaspielen geboten wird. Eine Anwaltskanzlei aus Berlin fordert die Wirte anschließend zur Zahlung von 3.000 Euro und zur Unterzeichnung einer strafbewehrten Unterlassungserklärung auf. Der Betrag wird auf 300 Euro reduziert, wenn der Gastwirt ein Sky-Abovertrag abschließt. Ein empörter Wirt im Raum Augsburg, der am 30.04.2011 das Spiel Bayern-Schalke gezeigt haben soll, erstattete nun seinerseits Anzeige wegen falscher Anschuldigung. Einige der Betroffenen versicherten, sie hätten nicht einmal einen Fernseher im Gastraum und bekamen recht. In den Augsburger Fällen hatte der Kontrolleur die verbotene Fußballübertragung frei erfunden. Dessen ungeachtet rechtfertigte Sky-Sprecher Wolfram Winter die Kontrollbesuche: „Wir machen das viel häufiger als früher. Unsere Beweise sind so, dass daraus durchaus valide juristi-

sche Vorgänge entstehen." Zur Reduktion der Strafe im Fall eines Abo-Vertrages: „Wir sind ja nicht an einer gerichtlichen Auseinandersetzung interessiert, wir wollen, dass die Leute unsere Kunden werden. Und die Umwandlungsquote ist inzwischen richtig hoch" (Der Spiegel 23/2011, 81).

Bayern

LDA wird unabhängiger

Mit Wirkung zum 01.08.2011 trat eine Änderung des bayerischen Datenschutzgesetzes in Kraft, wodurch das Landesamt für Datenschutzaufsicht (LDA) in Ansbach als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich gemäß dem Urteil des Europäischen Gerichtshof (EuGH) vom 09.03.2011 unabhängig werden soll. Gemäß dem Gesetz ist der Amtssitz des LDA Ansbach; es wird von einem Präsidenten mit der Besoldungsgruppe B3 geleitet, der die Befähigung zum Richteramt besitzen und über Verwaltungserfahrung verfügen muss und der für jeweils 5 Jahre gewählt wird. Regelungen zur Fach- und Rechtsaufsicht gibt es nicht; die Dienstaufsicht ist entsprechend der für den Präsidenten des Obersten Rechnungshofes geregelt.

Der bisherige Leiter des LDA, Thomas Kranig, wurde vom bayerischen Innenminister zum ersten Präsidenten des Amtes ernannt. „Im Zuge des letzten Schrittes der Unabhängigkeit", so das LDA, erhielt es eine eigene Homepage, die unter www.lda.bayern.de erreichbar ist. Das LDA ist für die aufsichtliche Kontrolle wie für den Erlass von Bußgeldbescheiden zuständig. Es bestand zur Zeit des rechtlichen Wechsels aus 12 MitarbeiterInnen und soll bis Ende 2011 auf 16 aufgestockt werden, wozu dann auch zwei IT-SpezialistInnen gehören sollen (PM LDA 04.08.2011; BayGVBl. Nr. 14/2011 v. 20.07.2011, 307 f.).

Berlin

Regierungssprecher Seibert bei Google+ nicht echt

Die Bundespressekonferenz teilte am 13.07.2011 in Berlin mit, dass ein mit Texten und Fotos des Sprechers der Bundesregierung Steffen Seibert getarnte Profil im neuen sozialen Netzwerk Google Plus (Google+) „nicht echt" sei. Deshalb werde Verbindung zum Internetkonzern Google hergestellt. Google wies darauf hin, dass alle Nutzenden bei dem Ende Juni gestarteten Dienst Profile melden können. Dabei könnten sie angeben, auf ein gefälschtes Profil gestoßen zu sein. Der falsche Seibert kopierte auf Google+ offensichtlich die Einträge des Regierungssprechers aus dessen offiziellem Profil bei Twitter. Dort ist der Sprecher von CDU-Bundeskanzlerin Angela Merkel seit Februar 2011 als @regsprecher präsent (SZ 14.07.2011).

Berlin

SchülerInnen bewerten Lehrkräfte

Die Berliner Lehrerschaft kann ihren Unterricht künftig durch SchülerInnen bewerten lassen. Das „Selbstevaluationsportal" des Instituts für Schulqualität gibt die Möglichkeit, Rückmeldungen zum Unterricht einzuholen. Die Senatsverwaltung für Bildung teilte mit, dass vom neuen Schuljahr 2011/2012 an alle LehrerInnen das Portal mindestens einmal in zwei Jahren nutzen sollen. Es wurde 2008 online gestellt und wird von einigen Schulen bereits genutzt. Enthalten sind sowohl Fragen zur Unterrichtsqualität als auch zu einzelnen Fächern. Die Befragungen sind anonymisiert. Rückschlüsse auf die bewertenden SchülerInnen sollen nicht möglich sein. Nach Abschluss der Befragung erhalten die Lehrkräfte eine elektronische Auswertung (SZ 01.08.2011, 18).

Hessen

Datenklau bei Neckermann mit über 1 Mio. Betroffenen

Hacker haben beim Versandhändler neckermann.de Namen und Mailadressen von 1,2 Millionen GewinnspielteilnehmerInnen gestohlen. Das Unternehmen berichtete, dass sich die Gewinnspieldaten auf einem „Neben-System" befunden haben, der Firmen-Hauptserver mit den Daten aller KundInnen des Onlineshops sei nicht betroffen. Dem Versandhändler ist der Angriff am 26.05.2011 aufgefallen. Am 31.05. informierte dann neckermann.de die Betroffenen in einer Rundmail über den Vorfall: „Nach Bekanntwerden der Straftat sowie nach umgehenden Ermittlungen des Tathergangs haben wir die Sicherheit des angegriffenen Servers wieder hergestellt und zusätzlich verstärkt."

Bis dahin soll es bereits zur Versendung von Spammails an die GewinnspielteilnehmerInnen gekommen sein. Neckermann.de riet seine KundInnen, keine Mails von unbekannten Absendern zu öffnen. Die Sicherheit im Sysem sei verstärkt worden. Keinen Schutz gibt dieser Ratschlag, wenn ein Angreifer Mails mit gefälschtem Neckermann-Absender verschickt. Für besorgte KundInnen hatte das Unternehmen eine kostenfreie Hotline mit einer 0800er Nummer eingerichtet. Neckermann.de hatte nach eigenen Angaben außerdem bei der Staatsanwaltschaft Frankfurt Anzeige gegen Unbekannt gestellt und die zuständige Datenschutzbehörde über den Vorfall informiert (www.heise.de 31.05.2011; SZ 01./02.06.2011, 20).

Niedersachsen

Unabhängigkeit des Datenschutzbeauftragten in Verfassung

In Umsetzung der Forderung des Europäischen Gerichtshofes (EuGH) vom März 2010, wonach die Datenschutzbehörden in Deutschland bei der Ausübung ihrer Kontrollfunktionen von staatlicher Aufsicht unabhängig sein müssen, wurde vom Niedersächsischen Landtag am 29.06.2011 einstimmig eine Verfassungsänderung beschlossen, wonach der dortige Landesbeauftragte für Datenschutz (LfD) seine völlige Unabhängigkeit garantiert bekommt. Der LfD Niedersachsen, Joachim Wahlbrink, begrüßte diese Stärkung der Grundrechte über die Rechtsposition der Aufsichtsbehörden: „Ihre Entscheidungen können nur so über jeden Verdacht der Parteilichkeit erhaben sein." In seiner Behörde sind 29 Personen beschäftigt, einige von ihnen in Teilzeit. Sie sind zuständig für ca. 300.000 Firmen, über 1000 Kommunen und die Landesbehörden bzw. -dienststellen. Im Jahr 2010 wurden rund 3000 Eingaben bearbeitet (PE LfD Nds. N.2 2/11 vom 29.06.2011).

Niedersachsen

Bankdaten von Westermann-KundInnen abgefischt

Zehntausende Internet-KundInnen des Schulbuchverlags Westermann sind Opfer eines Hackerangriffs geworden. Verlagssprecher Rainer Westermann teilte am 08.07.2011 in Braunschweig mit, dass von Russland aus Kundendaten mit Bankverbindungen kopiert worden sind. Alle betroffenen KundInnen sowie der Landesbeauftragte für Datenschutz (LfD) seien unverzüglich informiert worden. Die KundInnen wurden aufgerufen, ihre Kontobewegungen im Blick zu behalten und verdächtigen Abbuchungen zu widersprechen. In diesem Fall müsse die Bank das Geld zurückbuchen. „Wir gehen davon aus, dass unseren Kunden so kein Schaden entstehen wird." Die Sicherheitsmechanismen hätten den Hackerangriff am 27.06. erkannt und gemeldet. Der Verlag habe sein Online-Bestellsystem daraufhin überprüft und Schwachstellen geschlossen. Außerdem sei ein unabhängiger Experte mit der Kontrolle des gesamten Systems beauftragt worden. Für Rückfragen richtete der Verlag außerdem eine Hotline ein. Firmen müssen Hackerattacken seit April 2010 melden. Der LfD teilte mit, dass er prüfe, wie es um die Datensicherheit in dem Unternehmen bestellt sei, um eine Wiederholung zu vermeiden (www.heise.de 08.07.2011).

Nordrhein-Westfalen

Rewe-KundInnendaten im Internet

Nach einem Hackerangriff auf die Sammelbild-Tauschbörsen des Handelskonzerns Rewe haben unbekannte Hacker Zehntausende Datensätze von Rewe-KundInnen im Internet veröffentlicht, so ein Rewe-Sprecher am 20.07.2011: „Es wurde gestern eine signifikant hohe Anzahl unserer Daten ins Netz gestellt." Es handele sich um E-Mail-Adressen und dazu gehörende Passwörter von bis zu 45.000 KundInnen, die sich auf einer Rewe-Seite angemeldet hatten, um Tier- oder Fußballbilder zu tauschen. Andere Quellen sprachen 52.000 Datensätzen. Die Internet-Tauschbörse wurde von einem externen Dienstleister entwickelt und betrieben. Dieser hatte die Anmeldedaten unverschlüsselt gespeichert. In einigen Fällen hatten mit den erlangten Daten Unbekannte eingekauft.

Die Hacker hatten zwei Rewe-Kundendatenbanken geknackt. Die Sicherheitslücke hatte nach den Angaben des Sprechers etwa zwei Wochen lang bestanden, ehe sie bemerkt und behoben worden sei. Zunächst hatte es geheißen, es sei unklar, ob die Daten kopiert wurden. Ein Tippgeber aus der Szene hatte das Unternehmen auf das Leck hingewiesen. Sensible Daten wie Bankkonten- oder Kreditkartennummern waren laut Rewe nicht betroffen. Das Unternehmen hatte die Öffentlichkeit über die Panne informiert und Betroffenen geraten, ihre Passwörter zu ändern. Fremde E-Mail-Adressen werden von Datendieben nach Expertenangaben gerne für den Versand personalisierter Spam-Mails genutzt. Wird auch das Passwort geklaut, steigt die Gefahr des Missbrauchs. Da Internet-Nutzer oft dasselbe Passwort für verschiedene Dienste verwenden, können sich die Hacker Zugang zu diesen Diensten verschaffen oder unter fremdem Namen einkaufen.

Der Handelskonzern entschuldigte sich bei seinen KundInnen und versprach bessere Sicherheitsmaßnahmen. Künftig würden sämtliche Kundendaten, die auf Servern von Dienstleistern liegen, verschlüsselt. Vorstandsmitglied Lionel Souque: „Rewe entschuldigt sich bei allen Betroffenen für die Verunsicherung und die Unannehmlichkeiten, die ihnen durch diesen Hackerangriff entstanden sind." Der Landesbeauftragte für Datenschutz für Nordrhein-Westfalen, Ulrich Lepper, wies darauf hin, dass noch viele offene Fragen bestünden. Es sei zum Beispiel nicht ersichtlich, warum jemand, der an der Sammelbörse teilnimmt, seine Postadresse angeben soll. Auch die vertraglichen Regelungen zwischen Rewe und dem Dienstleister, der die Datenbank erstellt hat, seien der Datenschutzbehörde noch unklar. Nach Bekanntwerden des Datenlecks waren die Seiten von Rewe, der Discounttochter Penny und der Baumarktkette Toom für mehrere Tage offline und „wegen Wartungsarbeiten" nicht erreichbar. Schon wenig später ermittelte die Kölner Polizei den mutmaßlichen Täter. Ein 23jähriger Mann aus Issum am Niederrhein sei flüchtig. Bei einer Durchsuchung seiner Wohnung sei umfangreiches Datenmaterial sichergestellt worden (www.spiegel.de 19.07.2011 u. 22.07.2011; www.zeit.de 20.07.2011; SZ 21.07.2011, 19; SZ 06./07.08.2011, 12).

Nordrhein-Westfalen

Ergo-Versicherung diskriminierte AusländerInnen

Die Ergo-Versicherungsgruppe mit Sitz in Düsseldorf hat gemäß Presseberichten bei der Vergabe von Auto-Policen AusländerInnen besonders geprüft und diskriminiert. Gemäß Angaben von ehe-

maligen Vertretern der Ergo-Tochter DAS galten potenzielle KundInnen etwa aus Italien, Polen oder Russland mindestens bis Anfang 2010 als „unerwünschtes Risiko“. KundInnen mit ausländischen Namen seien auch bei Vorliegen der deutschen Staatsangehörigkeit nur in Ausnahmefällen angenommen worden. Die Vorwürfe basieren auch auf einem Entwurf für eine Prüfziffer des Versicherers, die sich „Kasko für Italiener“ nannte. Ein Ergo-Sprecher meinte, die sei „sicherlich eine sehr unglückliche Bezeichnung“ gewesen. Die Prüfziffer sei nur eine von vielen gewesen, die bei der Aufnahme von potenziellen KundInnen berücksichtigt worden sei: „In unseren Kfz-Tarifen gibt es seit 1995 keine Zuschläge oder Ähnliches, was an die Nationalität des Kunden geknüpft ist. Eine Auswertung unseres Bestandes `Deutsche versus andere Nationalität´ zeigt keine Ungleichbehandlung.“ Die Beschuldigungen bedeuten für die Versicherungsgruppe einen weiteren Imageschaden, nachdem Enthüllungen über eine Sex-Party in Budapest für seine Top-Vertreter bekannt wurden, und, dass die Tochter der Münchener Rück Riester-Verträge mit falschen Kostenberechnungen verkauft hatte und KundInnen ungeeignete Versicherungspolicen angedreht worden seien (SZ 25.07.201, 17).

Nordrhein-Westfalen

Anonymer Zwangs-Online-Eignungstest für Studierende

Die RWTH Aachen führt als erste deutsche Hochschule einen Online-Eignungstest für StudienanfängerInnen ein. Damit will die Universität die Zahl der Studienabbrüche senken. An der dreistufigen Eignungsbewertung sollen die Teilnehmenden sehen, ob das anvisierte Fach für sie ratsam ist. Vom Wintersemester 2011/2012 an wird der anonyme, bis zu zwei Stunden dauernde Test zur Pflicht. Dabei werden Grundkenntnisse zu dem jeweiligen Fach abgefragt, im Fach Maschinenbau etwa Fragen zum technischen Grundverständnis gestellt. An der Hochschule mit 33.000 Studierenden brechen in den Geisteswissenschaften 70% der Immatrikulierten ihr Studium vor dem Abschluss ab, in Naturwissenschaften ca. 60% (SZ 06./07.08.2011, 6).

Sachsen

Funkzellenabfrage bei Antinazi-Demonstration

Die Abfrage

Bei Protesten gegen Neonazi-Aufmärsche am 19.06.2011 in Dresden hat die sächsische Polizei zwischen 13 und 17.30 Uhr die Handy-Verkehrsdaten von tausenden DemonstrantInnen und Anwohnenden erfasst und anschließend ausgewertet. Mit Beschluss des Amtsgerichts wurde eine sogenannte Funkzellenauswertung durchgeführt. Von allen HandybesitzerInnen, die sich zu dieser Zeit in dem Gebiet aufhielten, waren ein- und ausgehende Anrufe, SMS und die jeweilige Position erfasst worden, einschließlich die von RechtsanwältInnen, Journalistinnen und einigen Bundestags- und Landtagsabgeordneten.

Dabei lässt sich die Polizei von den Mobilfunkbetreibern mitteilen, welche Handys wann an bestimmten Funkmasten eingebucht waren. Jedes angeschaltete Mobiltelefon sucht ständig nach Funkmasten in seiner Nähe und meldet in kurzen Abständen den Standort. Dabei übermittelt es u. a. seine Rufnummer und seine Gerätenummer, die sog. IMEI. Beim Funkmast werden die Daten genutzt, um Verbindungen zum Telefonieren oder Surfen herzustellen. Die Betreiber und einige Telefonhersteller speichern die Daten für eine begrenzte Zeit. Zwar besagen diese Daten nichts über den Inhalt der Kommunikation. Doch lassen sich Bewegungs- und Kommunikationsprofile der Betroffenen erstellen. Die Größe des Gebiets einer Funkzelle hängt von der Dichte der Besiedelung und der Auslastung ab. Daher sind in Städten die Funkzellen kleiner als auf dem Land und umfassen oft nur einen Stadtteil. Die Maßnahme, bei der zwangsläufig viele Unverdächtige und Unbeteiligte erfasst werden, ist in § 100g der Strafprozessordnung (StPO) geregelt.

Als Begründung wurde vom Sprecher der Staatsanwaltschaft Haase zunächst ein Verfahren wegen schweren Landfriedensbruchs gegen Unbekannt während gewalttätigen Ausschreitungen südlich des Hauptbahnhofs angegeben. In der richterlichen Anordnung wurde die Maßnahme damit begründet, es sollten gewaltsame Übergriffe von Gegendemonstranten auf Polizeibeamte besser verfolgt werden können. Die Daten wurden auch im Rahmen von Ermittlungen gegen Menschen genutzt, denen die friedliche Störung der angemeldeten Nazi-Demonstration vorgeworfen wurde. Die Maßnahme wurde über die Akteneinsicht von RechtsanwältInnen bekannt. Ein Sprecher der Staatsanwaltschaft erklärte, nachdem erste Kritik an der Datenerhebung aufkam, seine Behörde werde künftig die aktuellen Daten im Zusammenhang mit Verfahren wegen Verstoßes gegen das Versammlungsgesetz nicht mehr verwerten.

Trotz der aufkeimenden massiven Infragestellung führte die sächsische Polizei die massenhafte Auswertung der Handydaten fort. Bis Ende Juni 2011 hatten die Ermittlungsbehörden in über 40.000 Fällen die Namen, Adressen und Geburtsdaten, also sogenannte Bestandsdaten von Handynutzern ermittelt. Zuvor hatte das sächsische Innenministerium lediglich von 460 Fällen gesprochen. Geliefert worden waren bei den Funkzellenauswertungen über 1.034.000 „Verkehrsdaten“ von rund 330.000 Geräten.

Die Staatsanwaltschaft Dresden versicherte, dass auch die von den Betreibern zunächst mitgeschickten personenbezogenen Bestandsdaten nicht ausgewertet oder verwendet worden seien. Das Landeskriminalamt Sachsen habe später im Zuge weiterer Ermittlungen entsprechende Namen und Anschriften von rund 250 Personen selbst abgefragt. Diese sollen offenbar als potenzielle Täter in Betracht gekommen sein. Die restlichen Bestandsdaten würden, so die Staatsanwaltschaft, gelöscht, „sobald dies technisch möglich ist“. Mutmaßliche TäterInnen haben die Strafverfolgungsbehörden trotz der aufwändigen und datenintensiven Verfahren sowie der Befragungen von rund 4.000 ZeugInnen nicht dingfest

machen können. Die Betroffenen haben weder eine Benachrichtigung, eine Information über die Datenlöschung noch eine Entschuldigung erhalten. Die Innenexpertin der SPD-Fraktion in Sachsen, Sabine Friedel, wies darauf hin, dass zudem gleich von mehreren weiteren Tagen Handy-Daten abgefischt worden seien. Der Sinn und Zweck dieses Vorgehens erschließe sich ihr nicht.

...und mehr

Das polizeiliche Vorgehen gegen Gegendemonstranten des Neonazi-Aufmarschs hatte bereits zuvor für Furore gesorgt, weil Beamte des Landeskriminalamtes (LKA) am Rande der Demonstration eine Großrazzia gegen linke Gruppen durchgeführt hatten, die den Naziaufmarsch stören wollten. Dabei hatte die Polizei unter anderem ein Haus gestürmt, in dem sich ein Parteibüro der Linken, eine Anwaltspraxis sowie das Verbindungsbüro des linken Aktionsbündnisses befunden hatten. Als Legitimationsmuster diente der § 129 Strafgesetzbuch (StGB), also der Verdacht einer „kriminellen Vereinigung", der aufzuklären sei. Dieses Muster wurde dann auch bei der Funkzellenabfrage verwendet. Die Aktion wurde von Bundestags-Vizepräsident Wolfgang Thierse (SPD) massiv kritisiert.

Am 30.06. wurde außerdem zusätzlich bekannt, dass die Polizei im Umfeld der Anti-Nazi-Demonstration nicht nur Handydaten ausgewertet, sondern auch Gespräche abgehört und SMS-Nachrichten mitgelesen hat. In einer von Innenminister Markus Ulbig (CDU) im Sächsischen Landtag verlesenen Erklärung bestätigte die Staatsanwaltschaft Dresden Medienberichte, dass im Rahmen anderer Ermittlungen Gespräche von zwei Mobilfunkanschlüssen abgehört wurden. Darüber hinaus hatte es geheißen, die Behörden hätten auch einen sogenannten IMSI-Catcher eingesetzt. Damit lässt sich die auf der SIM-Karte eines Handys gespeicherte eindeutige Netzteilnehmerkennung (International Mobile Subscriber Identity, IMSI) in einer Funkzelle orten. Zudem können mit Hilfe des Catchers Gespräche mitgeschnitten werden. Das Innenministerium hatte den Einsatz eines IMSI-Catchers im Rahmen der Demonstrationsaufklärung zunächst dementiert, aber nicht ausschließen können, dass er „in einem anderen Ermittlungsverfahren" eingesetzt worden sei. Tatsächlich wurden im Rahmen von Ermittlungen gegen mutmaßliche LinksextremistInnen auf richterlichen Beschluss die Gespräche und SMS von zwei Mobilfunkanschlüssen überwacht. Zur Ortung sei ein IMSI-Catcher eingesetzt worden, mit dem aber keine Inhalte aufgezeichnet worden seien. Um das Verfahren nicht zu gefährden, seien die Informationen erst jetzt veröffentlicht worden.

Etwa einen Monat später wurde bekannt, dass Strafverfolgungsbehörden in Dresden schon knapp zwei Jahre zuvor umfangreiche Funkzellenabfragen vornahmen. Sie hatten sich im September 2009 mit einem richterlichen Beschluss an Mobilfunkbetreiber gewandt, um einen bereits fünf Monate zurückliegenden Brandanschlag auf einen Fuhrpark der Bundeswehr in der Elbstadt aufzuklären. Daraufhin erhielten sie über 1,1 Millionen Verbindungs- und Standortdaten. Zudem übermittelten die Telekommunikationsunternehmen unaufgefordert personenbezogene Informationen wie Name und Anschrift von 82.665 Personen.

In einem anderen Fall hatten sich die Ermittlungsbehörden 162.000 Kassenzettel einer Baumarktkette aus Filialen in ganz Deutschland schicken lassen, nachdem am Tatort ein ungezündeter Brandsatz in einer Kiste entdeckt wurde, die nur unter einer Handelsmarke erhältlich ist. Später fragten sie die Funkzellen ab, bei der die Mobilfunkanbieter die zuständigen Behörden dank der damals noch geltenden Vorratsdatenspeicherung auch im Nachhinein mit reichlich Informationen versorgen konnten. Das Auskunftsersuchen habe sich „auf den Umkreis des Tatortes des Brandanschlags" beschränkt, betonte die sächsische Landesregierung in ihrer Antwort auf eine Anfrage der SPD-Landtagsfraktion. Die dabei über mehrere Tage erhobenen Datensätze seien aber nicht mit den Zahlungsvorgängen der Baumarktkette abgeglichen worden.

Reaktionen

Ein Sprecher des Sächsischen Datenschutzbeauftragten Andreas Schurig erklärte, es werde geprüft, ob der Eingriff gerechtfertigt war und ob nicht viel zu viel Unschuldige betroffen waren. Schurig will auch die weiteren in diesem Zusammenhang bekannt gewordenen Fälle genau so untersuchen wie die Abfrage hunderttausender Verbindungs- und Standortinformationen im Rahmen der Protestaktionen gegen einen geplanten Neonazi-Aufmarsch im Februar. Immerhin sei das Ganze in einem Wohngebiet geschehen. Linke Gruppen und Anhänger der Antifa sahen im Vorgehen der sächsischen Polizei einen gezielten Versuch, vor künftigen Anti-Nazi-Demonstrationen abzuschrecken. Die Fraktionsvize der FDP-Bundestagsfraktion Gisela Piltz: „Das Grundrecht auf Versammlungsfreiheit darf nicht dadurch untergraben werden, dass jeder, der an einer Demonstration teilnimmt, einem Generalverdacht unterstellt wird." Das Vorgehen der sächsischen Ermittler sei „offensichtlich unverhältnismäßig". Ähnlich der rechtspolitische Sprecher der Bundestagsfraktion der Linkspartei, Wolfgang Neskovic: „Die Funkzellenabfrage trifft friedliche Demonstranten und Anwohner. Nach der einschlägigen Rechtsprechung dürfte sie rechtswidrig gewesen sein", weil sie nicht geeignet, erforderlich und auch nicht verhältnismäßig gewesen sei.

Bundestagsvizepräsident Wolfgang Thierse (SPD), der an der Demonstration teilgenommen hatte, sprach von einem „skandalösen Vorgang": „Die Geisteshaltung, die hinter einer solchen Respektlosigkeit gegenüber den Bürgerrechten steht, kann zu einer Bedrohung für die Demonstrationsfreiheit, für Rechtsstaat und die Demokratie werden." Der Deutsche Journalistenverband protestierte ebenfalls gegen die Maßnahme. Der grüne Bundesvorstand Malte Spitz äußerte, seine Partei sähe sich in ihrer Ablehnung der Vorratsdatenspeicherung bestärkt. Durch diese anlasslose Speicherung von Verbindungsdaten können noch Monate nach einer Demo ermittelt werden, wer an ihr teilgenommen habe.

Der sächsische CDU-Innenminister Markus Ulbig verteidigte bei der

Vorstellung eines Berichts am 24.06. die massenhafte Sammlung der Handydaten. Es gehe um die Aufklärung eines versuchten Totschlags gegen einen Polizeibeamten. Es sei Aufgabe der Polizei, solch schwere Straftaten aufzuklären. „Alles andere wäre absurd“. Allein 106 Polizisten seien am Februar bei Angriffen von DemonstrantInnen verletzt worden. Neben der Ermittlung wegen des versuchten Totschlages gäbe es weitere 60 Fälle von Landfriedensbruch und 37 Körperverletzungen. Justizminister Jürgen Martens (FDP) kündigte dagegen Konsequenzen für den Fall an, dass bei den Ermittlungen Fehler gemacht wurden. Der sächsische FDP-Fraktionschef Holger Zastrow wertete das polizeiliche Vorgehen als „unverhältnismäßig“.

Folgen

Auf Veranlassung der Grünen befasste sich der Innen- und Rechtsausschussrecht des Dresdner Landtags in einer Sondersitzung mit dem Vorfall. Die SPD-Fraktion stellte eine parlamentarische Anfrage. Auf Antrag der Linksfraktion fand eine Aktuelle Debatte im Landtag statt. Katharina König, Thüringer Landtagsabgeordnete der Linkspartei kündigte an: „Alle rund 15 Abgeordnete meiner Fraktion, die in Dresden dabei waren, werden ein Auskunftsersuchen an Polizei und Staatsanwaltschaft stellen.“ Sollte sich ergeben, dass auch Handydaten von Parlamentariern ermittelt und gespeichert wurden, werden sie dagegen klagen.“ Das Bündnis „Dresden Nazifrei“ startete am 22.06. eine Kampagne, in der alle potenziell betroffenen DemonstrantInnen und Anwohnende dazu aufgerufen wurden, von ihrem Auskunftsrecht Gebrauch zu machen. Hierfür wurde ein entsprechendes Musterschreiben online verfügbar gemacht. Nach dem Sächsischen Datenschutzgesetz können BürgerInnen kostenfrei Auskunft bei Behörden über ihre gespeicherten personenbezogene Daten, Zweck und Rechtsgrundlage der Verarbeitung sowie Herkunft beantragen. Drei Abgeordnete der sächsischen Grünen erhoben beim Amtsgericht Beschwerde gegen die von ihnen vermutete Erfassung und Auswertung ihrer Mobilfunkdaten. Sie gehen von einem schweren Eingriff in ihre Abgeordnetenrechte aus.

In dem Bericht des Innenministers wurde festgestellt, dass die Erfassung zwar grundsätzlich rechtmäßig gewesen sei; in 45 Fällen seien jedoch Daten unrechtmäßig an die Staatsanwaltschaft weitergeleitet worden. Am 27.06.2011 zog die Sächsische Landesregierung eine erste personelle Konsequenz. Innenminister Ulbig berief den Dresdner Polizeipräsidenten Dieter Hanitsch von seinem Posten ab und versetzte ihn. Als Grund nannte er „interne Informationsdefizite“. Nachfolger wurde Dieter Kroll, der bisher die Polizeidirektion Südwestsachsen leitete. Ministerpräsident Stanislaw Tillich forderte seine Minister Ulbig und Martens auf, „Berichtspflichten innerhalb der Ressorts zu optimieren.“ Die gesammelten Daten hätten nach § 21 Versammlungsgesetz nicht verwandt werden dürfen; es sei zu spät entschieden worden, die Daten nicht zu verwerten.

Hintergrund und Konsequenzen

Die Funkzellenabfrage ist eine in der jüngeren Zeit von der Polizei häufig eingesetzte Ermittlungsmethode. Erstmals bekannt wurde ein Fall in Schleswig-Holstein im Jahr 2005. Bei der Anfrage der Polizei an die Mobilfunkprovider nach dem Mobilfunkverkehr in einer bestimmten Funkzelle geht es zumeist nur um eine Phase von wenigen Minuten oder Stunden. Das Freiburger Max-Planck-Institut für Strafrecht hat im Rahmen einer 2008 veröffentlichten größeren Studie zur polizeilichen Nutzung von Telekommunikations-Verkehrsdaten auch untersucht, wie oft und in welchen Fällen die Polizei Funkzellenabfragen durchführte. Schon im Jahr 2005 wurde allein bei T-Mobile (damals 31 Millionen KundInnen) knapp 6.000 Mal der Verkehr einer oder mehrerer Funkzellen ausgewertet. Aktuellere Untersuchungen liegen nicht vor. Am häufigsten nutzte die Polizei diese Methode damals bei Entführungen und Raubüberfällen. Eine Polizei-Annahme lautete, dass bei arbeitsteiligen Delikten die Täter im Tatzeitraum öfter miteinander telefoniert haben müssen. Im Schnitt waren pro Funkzellenabfrage 111 Personen betroffen, das heißt, so viele Personen nutzten ihr Handy im fraglichen Zeitraum zu Telefonaten oder Kurznachrichten.

Funkzellenabfragen stehen meist am Anfang von Ermittlungen. Die Daten der so ausgesiebten Mobilfunk-TeilnehmerInnen werden dann mit anderen Datensätzen abgeglichen. TelefoninhaberInnen gelten in der Regel erst dann als verdächtig, wenn weitere Indizien auf sie hindeuten. Die Funkzellenabfrage ist mit anderen Verkehrsdatenabfragen in § 100g StPO geregelt. Sie ist zulässig zur Aufklärung von „Straftaten erheblicher Bedeutung“. Gemeint sind damit Straftaten, die mindestens der mittleren Kriminalität zuzurechnen sind, den Rechtsfrieden empfindlich stören und das Sicherheitsgefühl der Bevölkerung erheblich beeinträchtigen können. Eine Demo-Blockade kann hierunter wohl nicht gezählt werden. Eine Funkzellenabfrage darf grundsätzlich nur nach richterlicher Genehmigung angeordnet werden. Die Funkzellenabfrage soll laut Gesetz nur zulässig sein, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Der Bundesbeauftragte für Datenschutz, Peter Schaar, kritisierte die „immense Streubreite“ der Maßnahme und forderte den Gesetzgeber auf, die Funkzellenauswertung stärker als bisher einzugrenzen. Der Freistaat Sachsen kündigte an, über eine Bundesratsinitiative den Rechtsbegriff der „erheblichen Straftat“ nach § 100g StPO präzisieren zu lassen. Sachsens Justizminister Martens legte ein Eckpunktepapier für eine Bundesratsinitaitive vor. Danach soll die massenhafte Abfrage nur noch bei schweren Straftaten erlaubt sein. Zudem sollen Vorgaben zur Verhältnismäßigkeit und zur Dokumentationspflicht ins Gesetz; die zuständigen Landesdatenschutzbeauftragten sollen über solche Maßnahmen informiert werden. Künftig solle zudem ein Richter zustimmen müssen, wenn die Daten aus einer Funkzellenabfrage an andere Behörden weitergegeben werden.

Für den Vorstoß des sächsischen FDP-Ministers konnten sich spontan die SPD-Landesjustizminister erwärmen, die sich am 06.07. bei einem Treffen in Berlin mit dem Thema be-

schäftigten. Jeder Vorschlag, der dazu führt, die Bürgerrechte in dem Bereich zu stärken, sei willkommen, hieß es. Burkhard Lischka, rechtspolitischer Sprecher der SPD-Bundestagsfraktion, kommentierte die Bundesratsinitiative: „Die sächsische Regierung treibt das schlechte Gewissen." Dennoch seien es „Trippelschritte in die richtige Richtung." Man werde sich während der Sommerpause mit dem Thema befassen und überlegen, wie die StPO geändert werden muss, „um solche offensichtlich rechtswidrigen Eingriffe ins Grundrecht künftig zu verhindern".

Bündnis90/Grüne kündigten für den Herbst einen eigenen Gesetzentwurf dazu an, so ihr rechtspolitischer Sprecher Jerzy Montag: „Wir wollen dabei über die sächsischen Forderungen hinausgehen." Er fordert eine umfassendere Statistikpflicht sowie eine ausführliche Begründungspflicht der Richter, die die Maßnahme erlauben. Bundesjustizministerin Leutheusser-Schnarrenberger bezeichnete den sächsischen Vorstoß als richtig: „Funkzellenabfragen dürfen nicht beliebig vorgenommen werden." Die Hürden müssten erhöht werden. Ob sie selbst einen Gesetzesentwurf formulieren will und die Bundesratsinitiative damit überflüssig macht, ließ sie offen.

Sie hätte es jedenfalls schwer, sich gegen die Union durchzusetzen. Der CDU-Abgeordnete Siegfried Kauder, Vorsitzender der Bundestags-Rechtsausschusses, meinte: „Das Recht braucht nach jetzigem Kenntnisstand nicht geändert werden". In Dresden spreche einiges dafür, dass das geltende Recht nicht ordnungsgemäß angewandt wurde. Keinen Bedarf für gesetzliche Änderungen sahen auch etwa die Unionsländer Bayern und Niedersachsen. Die Datenschutzbeauftragten von Bund und Ländern haben mit Entschließung vom 27.07.2011 Einschränkungen der gesetzlichen Befugnis zur Funkzellenabfrage gefordert, da damit zu viele Informationen von Unbeteiligten erhoben würden. Als Reaktion hierauf sah die Bundesregierung keinen Nachbesserungsbedarf.

Ein Verbot der flächendeckenden Funkzellenabfrage fordert die Linkspartei. Diese Maßnahmen habe sich als „kriminalpolizeilicher Unfug erwiesen", sagte Wolfgang Neskovic: „Einen sinnvollen Anwendungsbereich besitzt die Maßnahme allenfalls in juristischen Lehrbuchfällen." Denn nur hier komme ein bei Nacht allein im Wald am Tatort telefonierender Mörder vor (ULD-Tätigkeitsbericht 2006, Kap. 4.3.2; www.heise.de 19.06.2011; Biermann www.zeit.de 20.06.2011; Wrusch www.taz.de 20.06.2011; Rath www.taz.de 21.06.2011; Hebestreit www.fr-online.de 21.06.2011; Kaul www.taz.de 24.06.2011; Schmeider SZ 24.06.2011, 2, 7; SZ 25./26.06.2011, 6; www.heise.de 27.06.2011; Schneider SZ 28.06.2011, 1, 4, 6; Wrusch www.taz.de 30.06.2011; www.heise.de 01.07.2011; Wrusch www.taz.de 07.07.2011; Janisch SZ 07.07.2011, 5; Krempl www.heise.de 28.07.2011; Prantl SZ 29.07.2011, 5; Popp/Winter Der Spiegel 32/2011, 25 ff.).

Sachsen

Auch antinazistische Busreisende ausspioniert

Die Dresdner Polizei überwachte am 19.02.2011 nicht nur Telefongespräche, sondern sammelte Informationen über zahlreiche Reisende, die von Busunternehmen zu den Anti-Nazi-Demonstrationen in die sächsische Hauptstadt transportiert wurden. Im Zuge der Ermittlungen forderte die Polizei die Unternehmen auf, Auskunft über Reisende, Strecken und geschlossene Verträge zu leisten. Es wurde erfragt, wo Fahrgäste ein- und ausstiegen, worüber die sprachen, welche Transparente sie bei sich trugen. Gefragt wurde nach Mietverträgen und Ausweiskopien der KundInnen. Die Ermittler der Soko 19/2 versprachen sich dadurch offenbar Hinweise auf TäterInnen, die am 19.02. in Dresden PolizistInnen angegriffen und verletzt hatten (Der Spiegel 27/2011, 17).

Sachsen

Justiz-Webseite veröffentlicht private Daten von JournalistInnen

Die persönlichen Daten von 117 nationalen und internationalen JournalistInnen, die im Herbst 2009 für der Prozess um den Mord an der Ägypterin Marwa El-Sherbini beim Landgericht Dresden akkreditiert waren, standen vom 09. bis 11.06.2011 auf der Homepage der sächsischen Justiz. Die Ägypterin war mit 16 Messerstichen in eben diesem Landgericht getötet worden, so dass der Prozess eine große mediale Aufmerksamkeit fand. Der Sprecher am Landgericht Dresden Ralf Högner bestätigte, dass durch eine Panne die in einem digitalen Ordner abgelegte Akkreditierungsliste im Netz sichtbar war und so Namen, Telefonnummern und Adressen der JournalistInnen per Suchmaschine auffindbar waren. Auf den Hinweis eines Radiojournalisten hin wurde die Datei entfernt. Wie viele Zugriffe auf die Seite es gab, habe man, so ein Sprecher, nicht feststellen können. Zunächst war völlig unklar, wie das Programm der Webseite die unerwünschte Verknüpfung zu der betreffenden Daten herstellen konnte (SZ 16.06.2011, 15).

Schleswig-Holstein

ULD startet Kampagne zu Facebook

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) forderte am 19.08.2011 alle Stellen im Land auf, ihre Fanpages bei Facebook und Social-Plugins wie den „Gefällt mir"-Button auf ihren Webseiten zu entfernen. Nach eingehender technischer und rechtlicher Analyse ist das ULD zu dem Ergebnis gekommen, dass derartige Angebote gegen das Telemediengesetz (TMG) und gegen das Bundesdatenschutzgesetz (BDSG) bzw. das Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH) verstoßen. Bei Nutzung der Facebook-Dienste erfolge eine Datenweitergabe von Verkehrs- und Inhaltsdaten in die USA und eine qualifizierte Rückmeldung an den Betreiber hinsichtlich der Nutzung des Angebots, die sog. Reichweitenanalyse. Wer einmal bei Facebook war oder ein Plugin genutzt habe, der müsse davon ausgehen, dass er von dem Unternehmen zwei Jahre lang getrackt wird. Bei Facebook werde eine umfassende persönliche, bei Mitgliedern sogar eine personifizierte Profilbildung vorgenommen.

Diese Abläufe verstoßen nach Ansicht des ULD gegen deutsches und europäisches Datenschutzrecht. Es erfolge keine hinreichende Information der betroffenen Nutzerinnen und Nutzer; diesen werde kein Wahlrecht zugestanden; die Formulierungen in den Nutzungsbedingungen und Datenschutzrichtlinien von Facebook genügten nicht annähernd den rechtlichen Anforderungen an gesetzeskonforme Hinweise, an wirksame Datenschutzeinwilligungen und an allgemeine Geschäftsbedingungen.

Das ULD forderte von allen Webseitenbetreibern in Schleswig-Holstein, dass sie bis spätestens Ende September 2011 die Datenweitergaben über ihre Nutzenden an Facebook in den USA einstellen, indem sie die entsprechenden Dienste deaktivieren. Anderenfalls werde das ULD weitergehende Maßnahmen ergreifen, d. h. nach Durchlaufen des rechtlich vorgesehenen Anhörungs- und Verwaltungsverfahrens könnten dies bei öffentlichen Stellen Beanstandungen nach § 42 LDSG SH, bei privaten Stellen Untersagungsverfügungen nach § 38 Abs. 5 BDSG sowie Bußgeldverfahren sein. Die maximale Bußgeldhöhe liegt bei Verstößen gegen das TMG bei 50.000 Euro.

Thilo Weichert, Leiter des ULD, erläuterte: „Das ULD weist schon seit längerem informell darauf hin, dass viele Facebook-Angebote rechtswidrig sind. Dies hat leider bisher wenige Betreiber daran gehindert, die Angebote in Anspruch zu nehmen, zumal diese einfach zu installieren und unentgeltlich zu nutzen sind. Hierzu gehört insbesondere die für Werbezwecke aussagekräftige Reichweitenanalyse. Gezahlt wird mit den Daten der Nutzenden. Mit Hilfe dieser Daten hat Facebook inzwischen weltweit einen geschätzten Marktwert von über 50 Mrd. Dollar erreicht. Allen Stellen muss klar sein, dass sie ihre datenschutzrechtliche Verantwortlichkeit nicht auf das Unternehmen Facebook, das in Deutschland keinen Sitz hat, und auch nicht auf die Nutzerinnen und Nutzer abschieben können. Unser aktueller Appell ist nur der Anfang einer weitergehenden datenschutzrechtlichen Analyse von Facebook-Anwendungen. Das ULD wird diese in Kooperation mit den anderen deutschen Datenschutzaufsichtsbehörden vornehmen. Eine umfassende Analyse ist einer kleinen Datenschutzbehörde wie dem ULD mit einem Wurf nicht möglich; zudem ändert Facebook kontinuierlich seine technischen Abläufe und Nutzungsbedingungen. Niemand sollte behaupten, es stünden keine Alternativen zur Verfügung; es gibt europäische und andere Social Media, die den Schutz der Persönlichkeitsrechte der Internet-Nutzenden ernster nehmen. Dass es auch dort problematische Anwendungen gibt, darf kein Grund für Untätigkeit hinsichtlich Facebook sein, sondern muss uns Datenschutzaufsichtsbehörden dazu veranlassen, auch diesen Verstößen nachzugehen. Die Nutzenden können ihren Beitrag dazu leisten, indem sie versuchen datenschutzwidrige Angebote zu vermeiden.“ Den NutzerInnen im Internet gibt das ULD den Ratschlag, ihre Finger vom Anklicken von Social-Plugins wie dem „Gefällt mir“-Button zu lassen und keinen Facebook-Account anzulegen, wenn sie eine umfassende Profilbildung durch das Unternehmen vermeiden wollen. Die Profile seien personenbezogen; Facebook fordert von seinen Mitgliedern, dass diese sich mit ihrem Klarnamen anmelden.

In einer ersten Stellungnahme zeigte sich ein Facebook-Sprecher „verwundert“ über die Aktion des ULD: „Facebook hält sich vollständig an die europäischen Datenschutzbestimmungen. Wenn ein Facebook-Nutzer eine Partner-Seite besucht, die ein soziales Plug-in wie den ‚Gefällt mir‘-Button verwendet, kann Facebook die technischen Informationen wie die IP-Adresse sehen. Wir löschen diese technischen Daten innerhalb von 90 Tagen. Damit entsprechen wir den üblichen Branchenstandards. Die Informationen erhalten wir ungeachtet, ob ein Nutzer bei Facebook eingeloggt ist oder nicht. Dies liegt im Wesen des Internets.“ Er bestritt, dass Facebook auch persönliche Daten von Nutzern erfasst, die eine fremde Seite mit eingebundenem „Gefällt mir“-Button besucht, den Button aber nicht anklicken: „Wir wissen nicht, wer der Nutzer ist, es sei denn, er ist gerade aktiv bei Facebook eingeloggt. Es werden bei Facebook keine Nutzerinformationen über Soziale Plugins mit Dritten geteilt. Unsere höchste Priorität ist die Sicherheit unserer Nutzer. Die Nutzer haben die volle Kontrolle über ihre Daten. In unserem Hilfe-Bereich erklären wir ausführlich, wie soziale Plug-ins funktionieren.“

Die Stellungnahme von Facebook geht jedoch an den ULD-Vorwürfen vorbei. Diese laufen darauf hinaus, dass Verkehrs- und Inhaltsdaten in die USA tranferiert werden und die Nutzenden nicht hinreichend informiert werden. Viele JuristInnen vertreten schon seit langem die Ansicht, dass Teile des Facebook-Angebots deutschem Datenschutzrecht widersprechen. Thomas Hoeren, Jura-Professor für Informations-, Telekommunikations- und Medienrecht in Münster, urteilt: „Das ULD hat recht, viele Funktionen von Facebook sind nicht mit dem Telemedien- und dem Bundesdatenschutzgesetz zu vereinbaren.“ Dass das ULD nur Website-Betreiber, nicht aber direkt Facebook attackiert, dürfte daran liegen, dass unklar ist, wie die Firma überhaupt in Deutschland datenschutzrechtlich zur Verantwortung gezogen werden kann: „Bis heute ist die Frage unbeantwortet, ob das Bundesdatenschutzgesetz überhaupt Anwendung bei Facebook findet - eine Firma mit Sitz in Irland und Kalifornien.“ Diese rechtliche Problematik umgehe das ULD nun geschickt, indem es direkt die in Deutschland sitzenden, verantwortlichen Betreiber zur Rechenschaft ziehe.

Die Kieler Staatskanzlei, die bei Facebook vertreten ist, setzt laut Staatssekretär Arne Wulff weiter auf das soziale Netzwerk, um „Bürgerbeteiligung an demokratischen Entscheidungsprozessen auszubauen. Landestagsabgeordnete von CDU, SPD und FDP befanden die Einwände des ULD als wichtig, äußerten sich jedoch kritisch in Bezug auf die angedrohten Bußgelder. Auch der Rechtsexperte der Grünen-Landtagsfraktion, Thorsten Fürter begrüßt das Vorgehen Weicherts gegen öffentliche Webseitenbetreiber, gegen private sei es aber falsch. Öffentliche Betreiber dürften die Daten nicht zu Werbezwecken in die Hände von Facebook treiben: „Das gilt auch für die Seiten, die von der Landesregierung betrieben werden.“ Bei privaten Anbietern sei dagegen die Politik gefragt, sich für den Schutz der Persönlichkeitsrechte der Nutzer einzusetzen.

Facebook hat rund 750 Millionen Mitglieder, darunter 20 Millionen in Deutschland. Das ULD hat seine datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook im Internet veröffentlich unter https://www.datenschutzzentrum.de/facebook/. Diese Analyse soll künftig fortgeschrieben, d. h. erweitert und präzisiert werden. Anregungen hierzu nimmt das ULD per E-Mail über facebook@datenschutzzentrum.de entgegen (ULD PE 19.08.2011; Lischka www.spiegel.de 19.08.2011; www.heise.de 19.08.2011; Tiede KN 20.08.2011, 1).

Datenschutznachrichten aus dem Ausland

Welt

Globale Wettdatenbank der FIFA geplant

Der Präsident des Weltfußballverbands (Fifa) Joseph Blatter, der im Frühjahr 2011 nach Korruptionsverdacht zum vierten Mal wiedergewählt wurde, gab kurz vor dem Wahlgang eine zunächst auf zehn Jahr angelegte Kooperation mit Interpol bekannt. Die Fifa hat mit Interpol den Aufbau einer globalen Datenbank vereinbart, die alle verdächtigen Spielmanipulationen erfasst, und zahlt bis 2021 an Interpol hierfür 20 Mio. Euro. Der Australier Chris Eaton, Chef einer neu eingerichteten Sicherheitsabteilung der Fifa, sieht in der Bekämpfung von Wettmanipulationen die zentrale Herausforderung für die Fifa in näherer Zukunft: „Es ist ähnlich wie mit den Hooligans; da kennen wir die Haupttäter auch allesamt und können gegen sie vorgehen.“ Der 60jährige Eaton hatte zuvor selbst zwölf Jahre in der Interpol-Zentrale im französischen Lyon gearbeitet. Interpol will zudem eng mit Quotenüberwachungssystemen zusammenarbeiten und Verdachtsmomente an die Polizeibehörden betroffener Länder weiterleiten, so Eaton: „Die Wettmanipulateure sind global tätig. Jetzt haben wir mit Interpol endlich auch eine Möglichkeit, uns international auszutauschen.“ Man stünde „erst am Anfang der Bekämpfung des illegalen Wettmarktes“. Bislang waren sämtliche Bemühungen der Fifa gescheitert, detaillierte Informationen von milliardenschweren asiatischen Wettanbietern zu erhalten (Der Spiegel 22/2011, 95).

Welt

Hacker schnüffeln bei Sport-Organisationen

Gemäß einem Bericht des Software-Unternehmens McAfee gehören das Internationale Olympische Komitee (IOC), die World-Anti-Doping-Agency (WADA) sowie nationale Olympische Komitees (NOKs) zu den Objekten systematischer Ausforschungsaktionen durch eine Gruppe von professionellen Hackern, die offensichtlich im Auftrag eines Staates aktiv war. Aus dem Bericht des Sicherheitsexperten Dmitri Alperovich vom kalifornischen Software-Unternehmen geht hervor, dass die Sport-Institutionen zu 72 Einrichtungen gehören, deren Daten in den vergangenen 5 Jahren in großem Umfang gestohlen und auf einen fremden Server übertragen wurden. Die Tatsache, dass auch Sportorganisationen unter den Zielen sind, lasse eigentlich den Schluss zu, dass andere als ökonomische Motive hinter den Angriffen stünden: „Das Interesse an den Informationen asiatischer und westlicher NOKs, genau wie des IOC und der WADA in der Zeit vor und direkt nach den Olympischen Spielen 2008 (in Peking) war besonders faszinierend und deutete darauf hin, dass hinter dem Eindringen ein staatlicher Auftrag steht.“ Wo sich der Zentralrechner befindet, über den die Software-Firma auf die Spur der umfangreichen Hacker-Organisation gekommen ist, wird nicht genannt. Mehrere Experten äußerten in US-amerikanischen Medien die Überzeugung, dass es sich um China handele. Ein Sprecher der Firma „Dell Secure Works“, die dem gleichen Datenklau auf der Spur war, meinte, es gebe Hinweise auf Server in Schanghai und Peking.

Das IOC zeigte sich keiner Eindringlinge bewusst, so Sprecher Mark Adams: „Wenn sich der Verdacht betätigen würde, wäre das natürlich verstörend. Allerdings ist das IOC transparent in seinen Handlungen und hat keine Geheimnisse, die seine Handlungen oder seinen Ruf kompromittieren könnten.“ Tatsächlich wurde das IOC laut McAfee nur einen Monat lang angezapft. Anders die WADA, die 14 Monate lang das Ziel der Hacker gewesen sei soll, beginnend allerdings erst ein Jahr nach den Spielen in Peking. Die in Kanada sitzende WADA wurde von Mc-Afee informiert und ist dabei, den Fall zu prüfen. Es wäre nicht der erste Bruch der Sicherheitsschranken bei der Organisation in Montreal, so Generaldirektor David Howman: „Im Februar 2008 wurde in das Mail-System der WADA eingedrungen. Deswegen haben wir bei der staatlichen Polizei in Quebec Anzeige erstattet und bei einer FBI-Untersuchung mitgewirkt.“ Man habe keinen Schaden festgestellt und die Sicherheitsvorkehrungen erhöht. Das ADAMS-System, in dem unter anderem die Aufenthaltsorte der Athleten gespeichert werden, die Teil des Doping-Kontrollsystems sind, werde auf einem anderen Rechner abgewickelt als der Mail-Verkehr der WADA.

Auch das Britische Olympische Komitee (BOA) geht davon aus, von Cyber-Angriffen betroffen zu sein. Simon Clegg, früherer Generalsekretär, berichtet, dass 2008 eine britische Behörde die Polizei habe hinzuziehen müssen, weil sie ausspioniert worden sei. In den Monaten vor den Peking-Spielen sei das BOA deswegen so besorgt gewesen, dass es eine Konferenz mit einer Computerfirma abgehalten habe, um bessere Sicherheitsvorkehrungen zu entwickeln. Wichtigstes Ziel der Staats-Hacker war laut Bericht ein nicht nä-

her benanntes asiatisches NOK, dessen Geheimnisse 28 Monate lang ausgespäht wurden. Die Erfolgsgeheimnisse der deutschen Olympiamannschaft blieben hingegen unangetastet. Hacker-Jäger Alperovich bestätigte dem Deutschen Olympischen Sportbund (DOSB), dass er nicht zu den Zielen der Cyber-Spione gehört habe (Simeoni www.faz.net 04.08.2011).

Großbritannien

Britische Polizei erprobt umfassende Geodatenüberwachung

Die Polizeibehörde von Greater London kann mit Hilfe einer neuen Software „Geotime" detaillierte Bewegungsprofile erstellen. Mit Hilfe dieser Software können die Bewegungsdaten einzelner Personen aus unterschiedlichen Datenquellen verknüpft werden. Informationen aus sozialen Netzwerken, Navigationsgeräten, Mobilfunknetzen, Finanztransaktionen und Internet-Aktivitäten werden als komplexes Muster aus Bewegungs- und Kommunikationsdaten aufbereitet. Die Programmfunktionen des Geotime-Herstellers erlauben nicht nur historische Bewegungen darzustellen, sondern daraus auch Verhaltensmuster und zuvor unbekannte Beziehungen herauszuarbeiten. Dies soll der Verfolgung von StraftäterInnen und der Analyse von organisierter Kriminalität dienen

Die Metropolitan Police Service (Met) bestätigte, dass mit Geotime nicht nur VerbrecherInnen gejagt werden sollen. Es sei nicht ausgeschlossen, dass der Met die Software auch zur Untersuchung von Störungen der öffentlichen Ordnung einsetzen werde - etwa bei Demonstrationen. Für britische BürgerrechtlerInnen ist das ein Alptraum; sie fürchten die Überwachung Unschuldiger. Noch sei, so ein Met-Sprecher, nicht klar, wie und ob die Software überhaupt eingesetzt werden soll. Bis jetzt habe man Geotime nur mit Pseudo-Daten gespeist, „um zu sehen, wie man damit die Bewegung von Polizeifahrzeugen, Kriminalitätsmuster und Telefon-Untersuchungen analysieren" könne. Neben der größten Polizeibehörde des Vereinigten Königreichs überlegt auch das britische Verteidigungsministerium den Kauf von Geotime. Vorbild dürfte die US-Militärbehörde Darpa sein, die derzeit Geotime-Knowhow in ihrem „Gefechtsstand der Zukunft" erprobt (Knoke www.spiegel.de/netzwelt/ 12.05.2011).

USA

Drei Mio. Dollar Strafzahlung für Disney wegen Verletzung des Kinderdatenschutzes

Die US-Verbraucherschutzbehörde Federal Trade Commission (FTC) einigte sich mit der Walt Disney Co. auf eine Strafzahlung in Höhe von 3 Mio. Dollar wegen der unzulässigen Speicherung und Übermittlung von tausenden von Kinderdaten durch Playdom, der Spieleabteilung von Disney, wegen eines Verstoßes gegen den Cildren´s Online Privacy Protection Act (COPPA). COPPA dient dem Datenschutz von Kindern unter 13 Jahren im Internet. Die Speicherung erfolgte auf verschiedenen Seiten, u. a. bei Pony Stars, wo zwischen 2006 und 2010 821.000 Kinder registriert waren. Weitere 403.000 Kinder waren durch andere der 19 Angebote von Playdom betroffen, z. B. 2 Moons, 9 Dragons und My Diva Doll. Die Strafzahlung erfolgt fast zeitgleich zu dem Versprechen der Abgeordneten Joe L. Barton (Republikaner, Texas) und Edward J. Markey (Demokrat, Massachusetts), den Kinderdatenschutz im Internet zu verbessern. Ihr Vorschlag eines Do Not Track Kids Act würde u. a. Unternehmen untersagen, Nutzerinformationen von Kindern gezielt für Werbung und Marketingaktionen zu nutzen.

In der FTC-Klage vor dem Landesbezirksgericht in Los Angeles wurde beanstandet, dass die Seiten von Playdom während der Registrierung E-Mail-Adressen und Altersangaben sammelten und den Kindern die Möglichkeit eröffneten, ihre persönlichen Daten einschließlich realen Namen und Adressen öffentlich preiszugeben, ohne dass zuvor die Einwilligung der Eltern eingeholt wurde. Ausgelöst wurden die Ermittlungen der FTC durch die Praktiken der durch die von Howard Marks gegründeten Acclaim Games Inc. Dieses Unternehmen war von Playdom am 18.05.2010 erworben worden. Playdom wurde dann am 27.08.2010 von Disney für 563 Mio. Dollar gekauft. Marks verließ Playdom im Februar 2011, um in Los Angeles eine andere Spielefirma mit dem Namen Gamzee zu gründen. Die Sprecherin der Disney Interactive Media Group Carrie Davis erläuterte: „Disney ist froh, dass Playdom und die FTC die Angelegenheit nun einvernehmlich geklärt haben." Zuvor hatte Playdom die meisten Onlinespiele vom Acclaim vom Markt genommen und einige auf Anbieter außerhalb der USA übertragen. Dies hinderte die FTC aber nicht daran, ihre Klage aufrecht zu halten. Die französische Firma Freerik Ltd. hatte Pony Stars und My Diva Doll übernommen, so dass die zuvor registrierten Kinder weiterspielen und ihre Accounts weiternutzen konnten. Freerik erklärte sich im November 2010 bereit, die beiden Onlinespiele vom Netz zu nehmen und gab die Daten an Playdom zurück (Chmielewski, Pham, Los Angeles Times, www.glendalenewspress.com 14.05.2011).

USA

Datenklau bei der Citibank

Computerhacker beschafften sich am 10.05.2011 Zugang zu über 300.000 KundInnendaten der Citibank. Die Daten waren beim Internet-Banking-Service Citi Account Online gespeichert. Dabei mussten die Kriminellen nicht tief in die Trickkiste greifen. Nach Mitteilung eines Sicherheitsexperten gelang der unberechtigte Zugriff, den die US-Bank bei einer Routinekontrolle Anfang Mai 2011 entdeckt hat, durch das simple Manipulieren eines URL-Parameters. Hierbei mussten sich die Kriminellen zunächst mit einem gültigen Account in den Kundenbereich für KreditkartenkundInnen einloggen. Anschließend konnten sie einfach eine Nummer in der Webseitenadresse hochzählen, um an die Daten der anderen

KundInnen zu gelangen – dies taten sie mit Hilfe eines Skripts mehrere zehntausend Mal. Bei dem Einbruch wurden Namen, Kontonummern, Mailadressen und Kaufhistorien entwendet, Ablaufdaten oder Sicherheitscodes wurden nicht erbeutet. Wer hinter dem Angriff steckt, hat die Citibank noch nicht bekannt gegeben. Der mit dem Fall vertraute Sicherheitsexperte, der anonym bleiben wollte, äußerte die Vermutung, dass die Angreifer aus dem osteuropäischen Raum stammen. Bekannt gegeben hat die Citigroup den Vorfall erst am 08.06.20111. Nach ihrer Darstellung waren von dem Vorfall 360.083 nordamerikanische KreditkartenkundInnen betroffen. Insgesamt mussten 217.657 Kreditkarten neu ausgestellt werden. Nachdem die unbekannte Hacker sich die Kundendaten beschafft hatten, begannen sie damit, die Konten der Betroffenen zu plündern. Nach Presseberichten waren innerhalb von 5 Wochen schon 3.400 Konten um insgesamt 2,7 Millionen US-Dollar erleichtert worden. Obwohl die Hacker angeblich weder auf die rückseitigen Sicherheitscodes der Kreditkarten, Sozialversicherungsnummern noch Geburtsdaten Zugriff gehabt hätten, konnten sie von den betroffenen Konten durchschnittlich fast 800 US-Dollar abheben.

Der Analyst Avivah Litan meinte, der erfolgreiche Angriff auf die Bank sei ungewöhnlich. Üblicherweise würden Konten- und Bankkartendaten eher auf indirektem Weg ausgespäht, z. B. über Geldautomaten oder Kreditkartenterminals in Geschäften: „Dass der Einbruch direkt bei der Bank gelang, ist schwerwiegend." Aber nicht die Ausnahme: Die Sicherheitslage ist in Deutschland nicht unbedingt besser, dies demonstrierte Anfang 2011 ein Schüler. Er entdeckte auf den Webseiten von insgesamt 17 Banken Sicherheitslücken; diese wurden darüber unterrichtet, woraufhin sie die Lücken beseitigten. Doch als der Schüler drei Monate später die Webauftritte der gleichen Banken analysierte, fand er bei jeder einzelnen erneut mindestens ein ernstzunehmendes Sicherheitsproblem (SZ 10.06.2011, 34; www.ftd.de 09.06.2011; www.heise.de 15.06.2011 u. 26.06.2011).

USA

Lance Armstrong rügt Schweigepflichtverletzung bei Doping-Untersuchung

Der siebenmalige Tour-de-France-Sieger und frühere US-amerikanische Radprofi Lance Armstrong beschuldigt Behörden und Medien, zwischen Mai 2010 und Juni 2011 illegal Informationen über Doping-Untersuchungen ausgetauscht zu haben. Seine Anwälte reichten am 13.07.2011 eine 20seitige Auflistung möglicher Rechtsverstöße bei einem Bundesgericht in Los Angeles/Kalifornien ein und forderten die Überprüfung von E-Mail-Kontakten und Telefonaten zwischen JournalistInnen und Regierungsangestellten: „Man versucht öffentliche Unterstützung für die Untersuchung gegen einen Nationalhelden zu erhalten, der bekannt ist für seine Rolle im Kampf gegen den Krebs. Diese taktischen Züge können nicht ignoriert werden, da sie einen starken Anschein der Parteinahme beinhalten." Empfänger illegaler Informationen seien die New York Times, das Wall Street Journal, die Nachrichtenagentur Associated Press, das Magazin Sports Illustrated und die CBS-Fernsehsendung „60 Minutes". Armstrong und seine Anwälte hoffen, die JournalistInnen zur Offenlegung ihrer Quellen zwingen zu können.

Gemäß US-Recht dürfen während einer laufenden Untersuchung und vor einer Anklage keine Details bekannt gegeben werden; Verstöße gegen diese Schweigepflicht können mit Gefängnisstrafen geahndet werden. Seit 2001 wird Armstrong von Dopingverdächtigungen begleitet. Damals gab er zu, mit dem umstrittenen Sportarzt Michele Ferrari zusammengearbeitet zu haben, besteitet aber die Dopingvorwürfe: „Ich habe niemals leistungssteigernde Mittel genommen." Die französische Sporttageszeitung L´Équipe hatte im August 2005 berichtet, dass in sechs 1999 entnommenen Urinproben Epo gefunden wurde. Diese wurden zweifelsfrei Armstrong zugeordnet, der 1999 zum ersten Mal die Tour de France gewann (SZ 20.07.2011, 29).

Ägypten

Mit „Jungfräulichkeitstests" gegen Demonstrantinnen

Die 20jährige Salwa Husseini Gouda, eine der vielen Demonstrantinnen, die auf dem Tahrir-Platz am 09.03.2011 in Kairo für mehr Demokratie und Freiheit in Ägypten demonstrierte, berichtete, wie sie und viele andere Frauen von staatlichem Sicherheitspersonal geschlagen wurden, um Ihnen dann den Befehl zu geben sich auszuziehen, sich vor glotzenden Soldaten auf den Rücken zu legen und die Beine anzuwinkeln, damit ein Mann in weißem Kittel ertasten konnte, ob sie Jungfrauen seien oder nicht. Sie sei mit etwa 20 anderen Frauen auf dem Tahrir-Platz von nichtuniformierten „Schlägertypen" verhaftet worden: „Sie beschimpften mich als Hure und schlugen mir ins Gesicht." Von diesen seien sie dem Militär übergeben und in ein Militärgefängnis gebracht worden." Salwa berichtete, dass sie mit zwei anderen Frauen in einen kleinen Raum geführt wurde, wo sie sich ausziehen und ihre Kleider durchsuchen lassen mussten. Ein Soldat vor dem offenen Fenster fotografierte die nackten Frauen: „Ich hatte Angst, dass sie die Fotos benutzen würden, um uns als Prostituierte darzustellen." In der Nacht wurden die Frauen in eine Zelle gesperrt; sie bekamen Wasser und Brot, das nach Kerosin stank. Am nächsten Tag stand im Flur vor ihrer Zelle eine Liege; dort, so verkündete ein Offizier, werde nun ein Arzt die Jungfräulichkeit der unverheirateten Frauen überprüfen. Salwa: „Wir fragten, ob es nicht wenigstens eine Ärztin sein könne, aber er sagte nein. Ein Mädchen, das sich wehrte, wurde mit Elektroschocks traktiert. Es war schrecklich demütigend." Nach der Prozedur hätten alle Frauen ein Formular unterzeichnen müssen, auf dem stand, ob sie Jungfrauen waren. Als der Mann im weißen Kittel bestätigt habe, dass ihr Jungfernhäutchen intakt sei, hätten die Soldaten sie mit neuen Anschuldigungen konfrontiert. Zwei Tage später sei sie von einem Militärgericht wegen angeblichen Waffenbesitzes, Sachbeschädigung und

Missachtung der Sperrstunde zu einem Jahr Haft auf Bewährung verurteilt worden.

Ein Monat zuvor war das Militär, das nach dem Rücktritt von Husni Mubarak die Macht im Land übernahm, noch von den Massen auf dem Tahrir bejubelt worden: „Das Volk und die Armee sind eins". Menschenrechtsorganisationen, u. a. Amnesty International, forderten die Behörden auf, „die schockierende und erniedrigende Behandlung von Demonstrantinnen zu stoppen" und die Ereignisse im Militärgefängnis zwischen dem 09. und 13.03.2011 aufzuklären. Das Europäische Parlament verurteilte „die erzwungenen Jungfräulichkeitstests" als Folter. Die Psychiaterin Mona Hamed vom Nadeem Center für die Rechte von Gewaltopfern hat die Aussagen mehrerer der betroffenen Frauen dokumentiert: „Das Neue daran ist, dass diesmal nicht die Polizei oder die Staatssicherheit hinter der Aktion steckt, sondern das Militär. Die „Tests" seien eine Botschaft an die Bevölkerung, die Armee wolle die Bewegungsfreiheit der Menschen kontrollieren. Werde eine Demonstrantin verprügelt oder verhaftet, könne ihre Familie das vielleicht noch akzeptieren, nicht aber, wenn sie der Prostitution beschuldigt werde: „Das ist eine unvorstellbare Erniedrigung für die Frau und ihre Familie." MenschenrechtlerInnen beklagen, dass in der Zeit nach dem Sturz von Mubarak Tausende ÄgypterInnen verhaftet, gefoltert und vor Militärgerichte gestellt worden seien.

Im „Global Gender Gap Report 2010" des Weltwirtschaftsforums, der die Gleichberechtigung der Geschlechter in 134 Staaten bewertet, kam Ägypten auf Platz 125. 42% der Ägypterinnen können weder lesen noch schreiben; die Mehrheit hat keinen Beruf. Die Genitalverstümmelung von Mädchen ist seit 1967 verboten, aber immer noch weit verbreitet. Frauen, die ohne männliche Begleitung in Kairo unterwegs sind, müssen damit rechnen, sexuell belästigt zu werden. Ende Mai, also fast drei Monate nach der Verhaftung der 20 Frauen, gab ein General dem US-Nachrichtensende folgende Erläuterung: „Die Mädchen, die festgenommen wurden, waren nicht wie Ihre Tochter oder meine. Es waren Mädchen, die mit männlichen Demonstranten auf dem Tahrir gezeltet hatten, in den Zelten fanden wir Molotow-Cocktails und Drogen." Die Jungfräulichkeitstests seien durchgeführt worden, damit die Frauen hinterher nicht behaupten konnten, im Gefängnis belästigt oder vergewaltigt worden zu sein: „Wir wollten beweisen, dass sie sowieso keine Jungfrauen mehr waren." Amnesty International nannte dies eine „zutiefst perverse Rechtfertigung einer herabsetzenden Form von Missbrauch" und forderte die Behörden auf, die Verantwortlichen zur Rechenschaft zu ziehen. Die prompte Antwort der Armee war, dass die Anschuldigungen der Frauen haltlos seien (Shafy, Der Spiegel 23/2011, 102 f.).

China

WLAN-Betreiber werden zur Nutzerüberwachung gezwungen

Die chinesischen Behörden zwingen WLAN-Hotspot-Betreibende mit einer neuen Verordnung dazu, die Identität ihrer KundInnen zu ermitteln und den Surfverlauf mitzuloggen. Bars, Restaurants, Hotels, Buchhandlungen und andere Unternehmen müssen hierfür eine umgerechnet 2.100 Euro teure Software anschaffen. Das Programm hat eine Softwarefirma aus Shanghai entwickelt und mit dem Auftrag nach Behördenangaben umgerechnet etwa 210.000 Euro verdient. Die neue Hürde wurde ohne viel Aufsehen errichtet. Das von einem chinesischen Softwarekonzern entwickelte Programm kann bis zu 100 Nutzende gleichzeitig verwalten. Unternehmen, die die Weisung nicht umsetzen, müssen mit Strafzahlungen von umgerechnet 1.500 Euro rechnen. Zudem droht der Verlust der Konzession zum Betrieb eines Gewerbes in der Volksrepublik. Einige Gastronomen, die der behördlichen Forderung nicht nachgekommen sind und seitdem offline sind, klagen bereits über erhebliche Umsatzeinbußen, weil viele KundInnen wegbleiben. Nach Angaben des Ministeriums für innere Sicherheit dient die Verordnung zur Verfolgung von „Erpressung, unerlaubtem Handel, Glücksspiel, der Propagierung schädlicher Informationen und der Verbreitung von Computerviren". Die Software ermöglicht es Behörden, unliebsame Elemente herauszufiltern. Hierzu zählen ChinesInnen, die Demokratie einfordern oder auf ihre von der Verfassung garantierte Meinungsfreiheit pochen. Die Jasmin-Revolution in Nordafrika versetzte die Sicherheitsbehörden in höchste Alarmbereitschaft, da trotz Beobachtung und Kontrolle das Internet diese verunsichert. Immer wieder entwickelt sich zu heiklen Themen in kürzester Zeit eine kaum zu lenkende öffentliche Meinung in Chats und Foren. Die Regierung fürchtet, dass sich hieraus Massenproteste entwickeln könnten, die das Machtmonopol der Kommunistischen Partei gefährden.

China ist eines der Länder, die das Internet am stärksten repressiv regulieren. Ähnlich wie in anderen Staaten wird auch in China das Internet zur Organisation regimekritischer Aktionen genutzt. Suchmaschinen müssen ihre Resultate nach den Vorstellungen der Regierung filtern und unliebsame Treffer blockieren. Viele Kommentarfunktionen können die Nutzenden nur nutzen, wenn sie persönliche Angaben hinterlassen. Aufsehen erregte auch der Plan, Computerherstellern den Verkauf im Land nur zu gestatten, wenn die Rechner von sich aus Inhalte zensieren. Das Vorhaben wurde nach massiven Industrieprotesten aufgegeben. Allein im Jahr 2010 ließ die regierende kommunistische Partei 60.000 Websites schließen, angeblich aufgrund pornografischer und vulgärer Inhalte. Zudem wurden 7.000 Internetcafés außer Betrieb gesetzt, die ohne ordnungsgemäße Lizenz operierten. In China gab es Ende 2010 457 Millionen Internetnutzende, mehr als in jedem anderen Land der Welt (www.heise.de 26.07.2011; Grzanna SZ 27.07.2011, 8).

Malaysia

Mann zur Twitterentschuldigungen gerichtlich verpflichtet

Ein Mann in Malaysia musste sich 100 Mal über den Internet-Kurznachrichtendienst Twitter dafür entschuldigen, dass er den Arbeitgeber einer Freundin beleidigt hatte. Ein Gericht legte

diese Strafe in einem Einigungsverfahren zwischen dem Beschuldigten und der Firma fest. Der Verpflichtete hatte im Januar 2011 auf Twitter beschrieben, dass seine schwangere Freundin von ihrem Arbeitgeber schlecht behandelt worden sei. Mit der gerichtlichen Einigung konnte der Mann eine Klage der Firma und einen Prozess gegen sich abwenden: „Sie haben verlangt, dass ich mich innerhalb von drei Tagen hundert Mal über Twitter entschuldigen muss“. Dann werde der Fall keine weiteren rechtlichen Konsequenzen haben (SZ 03.06.2011, 9).

Südkorea

Datensätze von ´zig Millionen KoreanerInnen geklaut

Nach südkoreanischen Behördenangaben haben sich Kriminelle Zugriff auf persönliche Daten von bis zu 35 Millionen Internetnutzenden verschafft, was wohl der größte bekannt gewordene Fall von Datenklau in dem ostasiatischen Land wäre, das insgesamt rund 50 Millionen EinwohnerInnen hat. Ziel des Hackerangriffs waren gemäß den Angaben der Koreanischen Kommunikationskommission (KCC) das Suchportal Nate mit 25 Millionen NutzerInnen und das soziale Netzwerk Cyworld mit 33 Millionen NutzerInnen. Beide Seiten werden vom Internetunternehmen SK Communications betrieben. Die Kriminellen hätten dabei eine IP-Adresse in China benutzt. SK Communications bestätigte, dass ein Teil der Daten von 35 Millionen KundInnen aufgrund eines Angriffs am 26.07.2011 nach außen gedrungen sind. Betroffen seien Namen, Passwörter, Handynummern und E-Mail-Adressen. Die ganze Reichweite des Hackerangriffs werde noch untersucht. SK Communications ist eine Tochter der SK-Gruppe. Zum Mischkonzern gehört auch der größte Mobilfunkanbieter SK Telecom.

Der Fall bei SK folgte einer Reihe von Hackerangriffen auf Finanzunternehmen in Südkorea in den vorangegangenen Monaten. Im April hatte in Südkorea ein Hackerangriff auf die Datenbank von Hyundai Capital, ein Unternehmen zur Fahrzeugfinanzierung, Schlagzeilen gemacht. Dabei wurde ein großer Teil der Daten von 1,8 Millionen KundInnen kopiert. Im Jahr 2009 war ein wichtiges Bankensystem gehackt und für mehrere Tage lahmgelegt worden. Kurz nach Veröffentlichung des jüngsten Angriffs gab die südkoreanische Polizei bekannt, dass sie fünf mutmaßliche Mitglieder eines internationalen Hackerrings mit Verbindung nach Nordkorea festgenommen hat. Einer der Verdächtigen sei ein Mann aus China. Den Festgenommenen wird vorgeworfen, sie hätten über Angriffe auf die Internetseiten von Online-Spielen umgerechnet etwa 4,2 Mio. Euro gestohlen. Die südkoreanischen Behörden werfen vor allem Nordkorea vor, in den vergangenen Jahren Cyber-Attacken gegen das Bruderland verübt zu haben (www.heise.de 28.07.2011).

Südkorea

Sammelklage gegen Apple wegen Ortsdatenspeicherung

26.691 Menschen haben in Südkorea wegen der Speicherung von Ortsdaten auf iOS-Geräten eine Sammelklage gegen Apple und dessen südkoreanische Niederlassung beim Bezirksgericht in der südöstlichen Stadt Changwon eingereicht. Die KlägerInnen werfen dem iPhone-Hersteller einen Verstoß gegen das Datenschutzgesetz vor. Sie forderten Schadenersatz für den „erlittenen emotionalen Schaden“. Die Gruppe fordert pro KlägerIn eine Million Won (etwa 648 Euro) von Apple. Das ist die gleiche Summe, die die südkoreanische Apple-Vertretung wegen der Datenspeicherung Ende Juni 2011 per gerichtlicher Anordnung an einen Anwalt der Kanzlei auszahlte. Der Anwalt bereitete daraufhin die Sammelklage vor. Eine Entscheidung zu Gunsten der KlägerInnen könnte dies Apple umgerechnet fast 18 Millionen Euro kosten. Die südkoreanische Telekommunikationsaufsicht hatte gegen Apple im August eine Schadenszahlung in Höhe von rund 2000 Euro verhängt. In Südkorea benutzen etwa 3 Millionen Menschen das weltweit populäre Gerät.

Im April hatten Forschende darauf hingewiesen, dass iOS-Geräte Informationen zu Mobilfunkmasten und WLAN-Basisstationen in der Umgebung des Nutzers speichern (DANA 2/2011, 82). Apple hatte die Sammlung der Ortsdaten damit begründet, die Positionsbestimmung für Kartenanwendungen und andere ortsbezogene Dienste beschleunigen und verbessern zu wollen. Die langfristige lokale Speicherung der Daten bezeichnete das Unternehmen als Programmierfehler, der schließlich mit iOS 4.3.3 beseitigt wurde (www.heise.de 17.08.2011).

Technik-Nachrichten

Lügendetektor am Bankautomat

In Russland testet die Sberbank, die dortige Sparkasse, derzeit einen Automaten, der Bankmitarbeitende bei der Vergabe von Kredite ersetzen soll und dabei prüft, ob die KundIn die Wahrheit über ihre Kreditwürdigkeit und Bonität sagt. Überprüfen soll das ein im Bankomat eingebauter Lügendetektor. Bisher gibt es einen Prototyp: Die Sberbank kann sich aber einen Einsatz der Geräte in Bankfilialen und Einkaufszentren vorstellen. Die Bonität einer KreditnehmerIn wird über Fragen ermittelt wie: Haben Sie einen regelmäßigen Job? Oder: Haben Sie derzeit Kreditschulden? Anhand der gesprochenen Antworten soll die Maschine erkennen, ob die AntragstellerIn die Wahrheit sagt - oder ob sie lügt. Möglich wird das durch die Auswertung von Geschwindigkeit und Intensität der Sprache, die mit Sprachbeispielen aus Polizeiverhören abgeglichen wird. Wirkt die Betroffene nervös, dürfte es schwierig werden mit

dem Geld. Ist sie gelassen, kann sie sogar dann eine Kreditkarte bekommen, wenn sie zuvor nicht KundIn der Sberbank war. Die Maschine scannt zudem den Reisepass, speichert Fingerabdrücke und erstellt ein dreidimensionales Bild des Kopfes zur Gesichtserkennung. Das Prozedere soll nach Angaben der Bank den russischen Anforderungen an den Datenschutz entsprechen. Die Firma, die das Sprachsystem entwickelt hat, arbeitet auch mit dem russischen Geheimdienst FSB zusammen (Bilger SZ 15.06.2011, 25).

Altersbestimmung über DNA

Wie das Fachmagazin PLoS one (online) berichtete, haben GenetikerInnen der University of California in Los Angeles einen Test patentieren lassen, mit dem sich sog. Methylisierungsmuster aus dem Gencode, der DNA von Menschen, erkennen lassen. Dabei handelt es sich um Veränderungen im Erbgut, die sich u. a. mit dem Alter der Person ergeben. Für die Entwicklung des neuen Biomarkers untersuchten die Forschenden u. a. die Speichelproben von 34 eineiigen männlichen Zwillingen und identifizierten so 88 DNA-Orte, wo Alter und Methylierung besonders stark korrelierten. Gemäß Studienautor Sven Bocklandt ist diese Beziehung so stark, „dass wir das Alter bestimmen können, indem wir nur zwei der drei Milliarden Bausteine untersuchen, die unser Genom ausmachen." Derart sei es ihnen gelungen, das Alter der ProbandInnen auf immerhin fünf Jahre genau zu bestimmen. Die Forschenden hoffen, dass ihr Test sich bei kriminaltechnischen Untersuchungen bewähren wird. Theoretisch wäre es dann möglich, aus Speichelspuren an einer Bisswunde oder an einer Kaffeetasse das Alter eines noch unbekannten Täters abzulesen (SZ 24.06.2011, 20).

Distanz-Lügendetektor bei Kontrollstellen

In den USA wird im „Kampf gegen den Terrorismus" eine neue Überwachungstechnik getestet, die wie eine Art Lügendetektor auf Entfernung funktionieren soll. Über spezielle Sensoren erfasst das Gerät Atemgeschwindigkeit, Herzschlag und Mimik von Menschen, die eine Kontrollstelle passieren. Eine Psycho-Software versucht auszurechnen, ob der gescannte Mensch böse Absichten verfolgt oder nicht. Das US-Heimatschutzministerium bestätigte, dass an einem geheimen Ort im Nordosten ein Feldversuch läuft. Als Teil der Tests erhalten Personen die Anweisung, eine „Störhandlung" vorzutäuschen. Im Labor liegt die Trefferquote des Systems angeblich bei ca. 70%. Der Böse-Absicht-Detektor könnte auch auf Flughäfen bei der Sicherheitskontrolle zum Einsatz kommen (Der Spiegel 23/2011, 124).

Gendatenbanken durch fremde Quellen verunreinigt

Die Londoner Wissenschaftler Bill Langdon und Matthew Arno stießen nun schon zum zweiten Mal bei ihrer Erforschung von Krankheitsgenen in einer öffentlichen Humangenom-Datenbank auf Erbgutabschnitte von Mykoplasmen, also auf Erbgut, das offensichtlich nicht von der Spezies stammt, die untersucht werden soll. Scheinbar wurden bei der Analyse des menschlichen Genoms Abschnitte der Bakterien aus den Labors mit abgelesen und sind in den Datenbestand gelangt: „Es ist anzunehmen, dass auch viele Genome anderer Spezies kontaminiert sind." Es sei höchste Zeit, die wachsende Zahl von Gendatenbanken neuen Qualitätssicherungsmaßnahmen zu unterwerfen. Unerwünschte Erbgutschnipsel finden sich auch anderswo: US-Molekularbiologen warnen im Fachblatt „PLoS One", dass sich in rund 18% der Genomdatenbanken von Bakterien, Pflanzen oder Fischen auch Sequenzen von Menschen fänden, vermutlich von LabormitarbeiterInnen, die die Sequenzierung durchgeführt hatten (Der Spiegel 27/2011, 120).

Finger sollen Penislänge verraten

Koreanische Wissenschaftler um Kim Tae Beom vom Gachon University Gill-Hospital kamen in einem Bericht im „Asian Journal of Andrology" zu dem Ergebnis, dass aus der Untersuchung der Hand von Männern auf deren Penislänge Rückschlüsse möglich sind. Je kleiner der Quotient aus den Längen von Zeige- und Ringfinger der rechten Hand, also wenn der Ringfinger deutlich länger ist als der Zeigefinger, desto stattlicher sei der Penis. Das Verhältnis der beiden Finger werde bereits in der Embryionalentwicklung festgelegt. Der Quotient gilt als Biomarker für die pränatale Konzentration des Sexualhormons Testosteron und die Sensitivität der Androgenrezeptoren. Anhand solcher Marker erhoffen sich die Forschenden auch Erkenntnisse auf klinisch relevanterem Terrain, etwa über die individuelle Anfälligkeit für Prostatakrebs (Der Spiegel 27/2011, 120).

Rechtsprechung

EGMR

Mehr Schutz für Whistleblower

Der Europäische Gerichtshof für Menschenrechte (EGMR) in Straßburg gab am 21.07.2011 der Altenpflegerin Brigitte Heinisch Recht, die nach Aufdecken von Missständen durch ihren Arbeitgeber entlassen worden war. Der deutsche Staat wurde gerügt - weil deutsche Richter die Kündigung der Frau nicht beanstandeten und wurde wegen Verletzung der Menschenrechtskonvention verurteilt. Die Berlinerin Heinisch hatte 2004 ihren Arbeitgeber angezeigt, weil im Altenpflegeheim schwere Mängel bei der Versorgung Hilfsbedürftiger bestanden. Die daraufhin ausgespro-

chene fristlose Kündigung wurde bis hin zum Bundesarbeitsgericht bestätigt. Eine Verfassungsbeschwerde der Frau wurde vom Karlsruher Bundesverfassungsgericht nicht angenommen. Der EGMR entschied einstimmig, dass die deutschen Gerichte nicht zwischen dem Interesse des Arbeitgebers und dem Recht auf freie Meinungsäußerung abgewogen hatten und sprachen der Betroffenen 10.000 Euro Schmerzensgeld plus Prozesskosten zu, die Deutschland bezahlen muss.

Das Urteil hat über den Einzelfall hinaus Bedeutung für den Schutz sogenannter „Whistleblower". Darunter versteht man ArbeitnehmerInnen, die Korruption oder Missstände im eigenen Unternehmen öffentlich machen. Whistleblower (von engl.: Alarm schlagen) machen auf Missstände oder Gefahren in ihrer Firma oder Behörde aufmerksam. In Deutschland haben sie bisher meist mit negativen Konsequenzen, etwa dem Verlust des Arbeitsplatzes, zu rechnen. Arbeitslos wurde zum Beispiel eine Altenpflegerin, die Misshandlungen von Senioren in einem Pflegeheim gemeldet hatte. Gekündigt wurden auch Lagerarbeiter, die Medien über das betrügerische Umetikettieren von abgelaufenem Fleisch informierten. 2002 verlor ein Zöllner seinen Job, weil er auf dem Frankfurter Flughafen Hightech-Geräte für den Iran beschlagnahmen ließ, die man zu Atomwaffenzündern umfunktionieren könnte. Die Begründung: Er habe „dienstliche Kompetenzen durch eigenmächtige Korrespondenz mit dem Bundeskriminalamt, Zollkriminalamt überschritten". Wirksam gekündigt wurden auch die Prokuristin, die Verstöße der damaligen DG-Bank gegen Insiderregeln publik gemacht hatte, und der Revisor, der auf gefälschte Statistiken der Arbeitsämter aufmerksam machte.

Die heute 49 Jahre alte Klägerin war bei der Vivantes Netzwerk GmbH beschäftigt, die mehrheitlich dem Land Berlin gehört. Zusammen mit KollegInnen hatte sie 2003 die Geschäftsleitung mehrfach auf die Überlastung des Personals in einem Altenpflegeheim hingewiesen. Pflegeleistungen würden deshalb nicht korrekt erbracht und nicht richtig dokumentiert. Der Medizinische Dienst der Krankenkassen stellte bei einem Kontrollbesuch genau dieselben Mängel fest. Dennoch änderte sich nichts. Im Dezember 2004 erstattete die Altenpflegerin schließlich Strafanzeige wegen Betrugs. Die Pflegebedürftigen erhielten aufgrund des Personalmangels nicht die Leistungen, für die sie bezahlten. Die Ermittlungen gegen Vivantes wurden allerdings von der Staatsanwaltschaft eingestellt. Als das Unternehmen von der Strafanzeige erfuhr, wurde Brigitte Heinisch fristlos gekündigt. Die Vorwürfe wurden bestritten. Heinisch ging mit Unterstützung der Gewerkschaft Ver.di vor Gericht, scheiterte jedoch. Die Altenpflegerin erhielt von der Vereinigung Deutscher Wissenschaftler 2007 deren Whistleblower-Preis.

Die sieben Straßburger Richter begründeten ihr Urteil damit, dass die öffentlichen Informationen über mutmaßliche Mängel „zweifellos von öffentlichem Interesse" waren, zumal die betroffenen PatientInnen möglicherweise nicht selbst auf die Missstände aufmerksam machen konnten. Es gebe keine Hinweise, dass sie falsche Angaben machte, ihre Kritik sei vielmehr vom Medizinischen Dienst bestätigt worden. Der EGMR räumte ein, dass die öffentlichen Vorwürfe Ruf und Geschäftsinteressen der GmbH schädigten, meinte aber, „dass in einer demokratischen Gesellschaft das öffentliche Interesse an Informationen über Mängel in der … Altenpflege in einem staatlichen Unternehmen so wichtig ist, dass es gegenüber dem Interesse dieses Unternehmens am Schutz seines Rufes … überwiegt".

Der EGMR gab Kriterien vor, die für den Schutz der Whistleblower Voraussetzungen sind, da ArbeitnehmerInen zur Loyalität gegenüber dem Arbeitgeber verpflichtet sind: Der Whistleblower muss in guter Absicht handeln, die Information korrekt und von öffentlichem Interesse sein. Zudem darf er seinen Arbeitgeber im Normalfall nicht gleich bei der Presse anschwärzen; der erste Weg sollte zum Chef führen, der zweite zur zuständigen Behörde.

Der EGMR entscheidet immer nur über Einzelfälle. Die nationalen Gerichte müssen aber dessen Urteile bei ihrer Rechtsprechung beachten. Folglich muss künftig bei Fällen von Whistleblowing die Freiheit der Meinungsäußerung gegenüber den Geschäftsinteressen des Unternehmens abgewogen werden. Dieter Deiseroth, Richter am Bundesverwaltungsgericht und Mitglied der Jury, die Brigitte Heinisch 2007 den Whistleblower-Preis zusprach, wies anlässlich der Urteilsverkündung auf den mangelnden gesetzlichen Schutz in Deutschland hin. Der G20-Gipfel habe 2010 auch Deutschland aufgefordert. „bis Ende 2012 Regeln zum Whistleblower-Schutz zu erlassen". Deiseroth begrüßte, dass mehrere Fraktionen des Bundestages entsprechende Gesetzesinitiativen angekündigt haben. Das sei ein „überfälliger Fortschritt". In anderen Ländern, z. B. in Großbritannien und in den USA, gibt es schon einen solchen Schutz (Knapp www.fr-online.de 22.07.2011; Janisch u. Prantl, SZ 22.07,2011, 1, 4, 5).

BGH

Ungepixelte Fotos von verurteilten Straftätern zulässig

Der Bundesgerichtshof hat mit Urteil vom 07.06.2011 entschieden, dass das unverpixelte Veröffentlichen von Fotos von rechtskräftig verurteilten Straftätern grundsätzlich zulässig ist (Az. VI ZR 108/10). Der Kläger, ein inzwischen rechtskräftig wegen Mitgliedschaft in einer ausländischen terroristischen Vereinigung in Tateinheit mit versuchter Beteiligung an einem Mord zu einer Freiheitsstrafe von sieben Jahren und sechs Monaten verurteilter Straftäter, klagte gegen die „Bild"-Zeitung auf Unterlassung, weil diese in ihrer Ausgabe vom 16.07.2008 im Rahmen einer Berichterstattung über die Urteilsverkündung unter der Überschrift „Irak-Terroristen müssen für Attentatsplan ins Gefängnis!" ein Foto des Klägers veröffentlicht hatte, auf dem sein Gesicht zu erkennen ist. Das Strafverfahren hatte einen geplanten Anschlag der Terrorgruppe „Ansar al-Islam" auf den damaligen irakischen Ministerpräsidenten Allawi zum Gegenstand. Während der Hauptverhandlung vor dem Oberlandesgericht Stuttgart waren Fernseh- und Bildaufnahmen nach

der sitzungspolizeilichen Anordnung der Vorsitzenden nach § 176 Gerichtsverfassungsgesetz (GVG) am Tag der Urteilsverkündung nur mit der Maßgabe zulässig, dass bei Abbildungen der Angeklagten deren Gesichter durch geeignete Maßnahmen (Pixeln) unkenntlich gemacht werden.

Das Landgericht hatte die Bild-Zeitung verurteilt, es zu unterlassen, das Foto ungepixelt oder sein Antlitz in anderer Weise unkenntlich gemacht zu verbreiten. Deren Berufung hatte keinen Erfolg. Auf die Revision der Beklagten entschied der BGH dem gegenüber, dass dem Kläger kein Anspruch auf Unterlassung der ihn identifizierenden Bildberichterstattung zusteht. Die Zulässigkeit einer Bildveröffentlichung sei grundsätzlich nach dem abgestuften Schutzkonzept der §§ 22, 23 Kunsturhebergesetz (KUG) zu beurteilen. Danach dürfen Bildnisse einer Person grundsätzlich nur mit deren - hier nicht vorliegenden - Einwilligung verbreitet werden (§ 22 Satz 1 KUG). Hiervon besteht allerdings gemäß § 23 Abs. 1 KUG eine Ausnahme, wenn es sich um Bildnisse aus dem Bereich der Zeitgeschichte handelt. Diese Ausnahme gilt aber nicht für eine Verbreitung, durch die berechtigte Interessen des Abgebildeten verletzt werden (§ 23 Abs. 2 KUG). Der BGH bewertete im Streitfall die Berichterstattung über die Urteilsverkündung als ein zeitgeschichtliches Ereignis im Sinne des § 23 Abs. 1 KUG, an dem ein erhebliches Informationsinteresse der Öffentlichkeit bestand. Demgegenüber musste der Persönlichkeitsschutz des Klägers zurücktreten. Dem Umstand, dass der Kläger nur im Vertrauen auf die sitzungspolizeiliche Anordnung die Fotoaufnahmen ermöglicht haben will, maß der BGH nicht das vom Berufungsgericht angenommene Gewicht zu. Es sei nämlich zu berücksichtigen, dass nach dem Schutzkonzept der §§ 22, 23 KUG ungepixelte Bildaufnahmen auch ohne Einwilligung des Klägers zulässig gewesen wären und er letztlich durch sein Verhalten allenfalls Bildaufnahmen hätte vereiteln können, die wegen des erheblichen Informationsinteresses der Öffentlichkeit grundsätzlich zulässig waren. Das Persönlichkeitsrecht sei auch im Rahmen der Sitzungspolizei nicht in weiterem Umfang zu schützen als dies nach §§ 22, 23 KUG der Fall ist.

Vor dem BGH-Urteil hatten sich Strafkammern gegen allzu aufdringliche Medien immer häufiger mit dem Kompromiss zwischen Persönlichkeitsschutz von Angeklagten und Öffentlichkeitsinteresse beholfen, vor und nach der Verhandlung Medienkameras in der Gerichtssaal zu lassen und zugleich anzuordnen, dass die Gesichter der Angeklagten gepixelt werden, also durch Verschleierung nicht erkennbar gemacht werden. Das Bundesverfassungsgericht hatte diesen Weg im Jahr 2008 ausdrücklich gut geheißen. Damals ging es um den Prozess gegen Bundeswehrausbilder wegen der Misshandlung von Rekruten. Die Suggestivkraft der TV-Bilder könne für den Angeklagten wie ein Pranger wirken. Hierauf hatten sich die Vorinstanzen berufen und der Kläger - vergeblich - verlassen. Das Berliner Kammergericht (KG) hatte zwar den Pixelzwang in dem Strafverfahren vor dem Oberlandesgericht Stuttgart bei der Verhandlung im Juli 2008 eigentlich für rechtswidrig erklärt, weil es hier um einen spektakulären Terrorplan gegen einen ausländischen Regierungschef gegangen war. Die Öffentlichkeit habe „ein legitimes Interesse daran zu erfahren, um was es geht“. Trotzdem hatte das KG dem Kläger Recht gegeben, weil sein Vertrauen in die rechtswidrige Pixelverfügung schützenswert gewesen sei; vielleicht hätte er sich sonst ja eine Mappe vor das Gesicht gehalten. Der BGH sah das nun anders (Vorinstanzen: LG Berlin, U. v. 26.02.2009, Az. 27 O 982/08; KG, U. v. 06.04.2010, Az. 9 U 45/09; BGH PM Nr. 99/2011 v. 07.06.2011; Janisch SZ 08.06.2011, 1).

AG Bonn

Telekom zu Auskunft über Vater verpflichtet

Nach einem am 10.05.2011 bekannt gegebenen Urteil des Amtsgerichts (AG) Bonn muss die Deutsche Telekom einem Fünfjährigen Auskunft darüber geben, wer sein mutmaßlicher Vater ist (Az. 104 C 593/10). Die heute 29jährige Mutter des Jungen verbrachte eine Nacht mit dem Mann, von dem sie nur Vornamen und Handynummer kannte. Als sie ihn am Telefon über ihre Schwangerschaft informierte, brach er den Kontakt ab und gab seine Handynummer auf. Eine erste Klage der Frau auf Auskunft zur Identität des Mannes war abgewiesen worden. In einem zweiten Anlauf trat nun der Junge als Kläger auf und bekam Recht. Nach Ansicht des Amtsgerichts (AG) Bonn überwiegen die Interessen des Kindes an seiner Herkunft und Unterhaltszahlungen eindeutig die des Vaters auf Schutz seiner Daten (SZ 11.05.2011, 9; beck-online.de 11.05.2011).

VG Hannover

Öffentliche Polizeivideoüberwachung unzulässig

Das Verwaltungsgericht Hannover entschied mit Urteil vom 14.07.2011, dass die Videoüberwachung des öffentlichen Raums in Hannover durch die Polizeidirektion unzulässig ist (Az. 10 A 5452/10). Geklagt hatte ein Mitglied der Bürgerinitiative „Aktionskreis Vorratsdatenspeicherung“. Vor Klageerhebung hatte er vergeblich versucht, die Polizei zu einer besseren Kennzeichnung der Videokameras zu veranlassen. Im Folgenden werden aus den Entscheidungsgründen wesentliche Passagen zitiert:

„Der Kläger kann sich nicht nur auf eine mögliche Verletzung seines Rechts auf informationelle Selbstbestimmung durch die Aufzeichnung der übermittelten Bilder berufen, sondern bereits durch die bloße Bildübermittlung. ... Auch entfällt der grundrechtliche Schutz nicht schon deshalb, weil der Einzelne sich in die Öffentlichkeit begibt (vgl. BVerfG, Beschl. v. 23.02.2007 - 1 BvR 2368/06 -, NVwZ 2007, 688, 690 f.). ...Unter den Bedingungen der von dem Beklagten eingesetzten Kameratechnik ist das Recht auf informationelle Selbstbestimmung nach der Überzeugung der Kammer darüber hinaus bereits durch die bloße Bildbeobachtung mittels Bildübertragung in die Leitzentrale der Polizeidirektion beeinträchtigt. ... Die Überwachungskameras gestatten nicht nur durch ihre mehrere Meter erhöhte

Installierung einen Übersichtsblick, sie sind überdies schwenkbar und mit einer Zoomfunktion ausgestattet. Dies ermöglicht eine gegenüber dem menschlichen Auge großflächigere und intensivere Beobachtung. Die Beobachtung kann darüber hinaus zu jeder Tages- und Nachtzeit stattfinden. ...Bei dieser Wertung hat die Kammer auch in Rechnung gestellt, dass die anlasslose, großflächige Bildbeobachtung der Bevölkerung nicht nur ein Gefühl der Sicherheit geben soll (s. LT-Drs. 14/2788, S. 8) und vermutlich auch gibt, sondern dass sie als Kehrseite des Sicherheitsgefühls auch Einschüchterungseffekte haben kann, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können (vgl. BVerfGE 65, 1, 42; 113, 29, 45). Denn die Unbefangenheit des Verhaltens wird gefährdet, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen (vgl. BVerfGE 107, 299, 328; 115, 320, 354 f.). ...

Nach § 32 Abs. 3 Satz 1 Nds.SOG dürfen die Verwaltungsbehörden und die Polizei öffentlich zugängliche Orte mittels Bildübertragung offen beobachten, wenn dies zur Erfüllung von Aufgaben nach § 1 Abs. 1 Nds.SOG, mithin zur Gefahrenabwehr und Gefahrenvorsorge erforderlich ist. ... (Die Kammer) hegt Bedenken hinischtlich der Verfassungsmäßigkeit insbesondere von § 32 Abs. 3 Satz 1 Nds.SOG. Selbst unter Berücksichtigung der geringen Eingriffstiefe einer offenen Beobachtung im öffnetlichen Straßenraum genügt die Vorschrift jedenfalls nach ihrem Wortlaut nicht den Anforderungen, die das Bundesverfassungsgericht an die Bestimmtheit und Normenklarheit einer Rechtsgrundlage stellt, die Behörden zu Eingriffen in Grundrechte der Bürger ermächtigt. ... Da die Vorschrift auch der Gefahrenverhütung dienen soll und damit eine Anknüpfung an eine konkrete Gefahrenlage, wie sie die Maßnahmen der Gefahrenabwehr nach dem Nds. SOG kennzeichnen, entfällt, müssen die Bestimmtheitsanforderungen an dieser Vorfeldsituation ausgerichtet werden. Dies bedeutete, die Norm muss handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist (vgl. BVerfGE 113, 348, 377). ... Da der Begriff der Gefahr denkbar weit ist und jede Sachlage erfasst, bei der im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass ein Schaden für die öffentliche Sicherheit und Ordnung - Begriffe, die ihrerseits weit sind (vgl. BVerfGE 69, 325, 352) - einzutreten droht (vgl. § 2 Nr. 1a Nds.SOG), ist eine tatbestandliche Begrenzung über die Zielrichtung der Bildbeobachtung kaum möglich. ... Letztlich erlaubt die Vorschrift jedenfalls nach ihrem Wortlaut (in den Grenzen von Art. 13 GG) die flächendeckende Beobachtung öffentlich zugänglicher Orte in Niedersachsen. ...

Die Videoüberwachung, der der Kläger ausgesetzt ist, ist rechtswidrig. Die Bildbeobachtung (und folglich auch die Aufzeichnung der übermittelten Bilder) in der von dem Beklagten praktizierten Art ist schon deshalb rechtswidrig, weil sie nicht offen erfolgt. Der Begriff der offenen Datenerhebung bedeutet nicht, dass die Datenerhebung nicht verdeckt erfolgt. Das Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung kennt neben dem Begriff der offenen Datenerhebung auch den Begriff der verdeckten Datenerhebung, etwa in § 30 Abs. 2 Satz 2 Nds.SOG. Hiermit gemeint ist nicht die Datenerhebung, die nicht als solche erkennbar ist (so Saipa, a.a.O., § 30 Rz. 6), sondern die nicht erkennnbar sein soll (§ 30 Abs. 2 Satz 2 Nds.SOG). Zur mangelnden Erkennbarkeit hinzukommen muss also als subjektives Element ein zielgerichtetes Verdecken (vgl. auch Ziff. 30.2 der Ausführungsbestimmungen). Im Hinblick auf die datenschutzrechtliche Zielsetzung ist vielmehr zu fordern, dass die Videoüberwachung für den Betroffenen als Datenerhebung erkennbar ist. ...

Gefordert ist im Hinblick auf den Schutzzweck des § 32 Abs. 3 Satz 1 Nds.SOG nach Überzeugung der Kammer darüber hinaus, die Reichweite der Beobachtung kenntlich zu machen. ... Nach Auffassung der Kammer ist der Umstand der Datenerhebung durch Bildbeobachtung und -aufzeichnung in Hannover durch die von dem Beklagten eingesetzten Kameras nicht erkennbar, sei es, dass die Kameras mit bloßem Auge nicht erkennbar sind, weil sie zu hoch angebracht sind, weil sie bei der Vielzahl technischer Einrichtungen im öffentlichen Raum bei unbefangener Betrachtung allen möglichen Zwecken dienen können. Die von der Polizeidirektion Hannover eingerichtete Internetseite stellt die Offenheit der Datenerhebung nicht her, weil sich auf der Seite nur diejenigen informieren können, die dies recherhieren, nicht aber unbefangene Bürger, die nicht mit einer Dateerhebung rechnen. Im Übrigen ergibt sich aus der Darstellung im Internet auch nicht die Reichweite der Kameras, so dass es den Betroffenen selbst dann, wenn sie eine Kamera als solche erkannt haben oder sich im Internet auf der Seite der Polizeidirektion Hannover über die Standorte informiert haben, verwehrt ist, ihr Recht auf informationelle Selbstbstimmung wirksam auszuüben und sich ggf. dere Datenerhebung zu entziehen.“ ...

ArbG Düsseldorf

Heimliche Videoüberwachung nur bei Anhaltspunkten für Fehlverhalten

Vor dem Arbeitsgericht (ArbG) Düsseldorf wurden zwei Verfahren um die Kündigung von Mitarbeitern im Ausschank eines Düsseldorfer Brauhauses geführt. In dem Verfahren 11 Ca 7326/10 ging es um die Wirksamkeit einer bereits seitens des Arbeitgebers ausgesprochenen Kündigung. Im Verfahren 9 BV 183/10 begehrte der Arbeitgeber die Ersetzung der Zustimmung des Betriebsrates zur Kündigung eines seiner Mitglieder. In beiden Verfahren warf der Arbeitgeber den Arbeitnehmern vor, die ausgeschenkten Biere nicht korrekt abgerechnet zu haben. Zum Beweis seiner Behauptung berief er sich auf Videoaufzeichnungen, die er heimlich in dem Ausschankraum gemacht hatte.

Das Gericht erklärte in beiden Fällen mit Urteilen vom 03.05.2011 die angebotenen Videobeweise für nicht verwertbar und gab der Kündigungsschutzklage statt bzw. wies den Antrag des

Arbeitgebers auf Zustimmungsersetzung zurück. Nicht jeder pauschale Verdacht auf Unterschlagung von Getränken durch in einem Brauhaus beschäftigte ArbeitnehmerInnen rechtfertige eine heimliche Videoüberwachung durch den Arbeitgeber, entschieden die befassten Kammern des ArbG. Erst wenn der Arbeitgeber aufgrund tatsächlicher, nachprüfbarer Anhaltspunkte seinen Verdacht auf bestimmte Personen sowie eine bestimmte Tat konkretisieren kann, komme nach umfassender Interessenabwägung eine heimliche Überwachung des Arbeitsplatzes in Betracht. Diese Voraussetzungen haben die Kammern des ArbG in beiden Fällen nicht festgestellt. Die gewonnenen Daten unterlagen damit einem Beweisverwertungsverbot und konnten als Beweismittel nicht herangezogen werden (PM ArbG Düsseldorf v. 09.05.2011, KN 20.08.2011, AuB VI).

Buchbesprechung

Lars Mortsiefer,
Datenschutz im Anti-Doping-Kampf - Grundlagen und Spannungsfelder
Gardez! Verlag Remscheid, 2010,
280 S.

tw Die Doktorarbeit des Justiziars und neuerdings Vorstandsmitgliedes der Nationalen Anti Doping Agentur (NADA) in Bonn behandelt systematisch die Frage der Rechtmäßigkeit der Datenerhebung, -auswertung und -nutzung bei der Dopingbekämpfung in Deutschland. Die beginnt mit der Unterwerfung der SportlerInnen unter ein rigides Meldeverfahren: Sie müssen sich jeweils ein Vierteljahr im Voraus in einem in Kanada gehosteten internetbasierten System ADAMS mit ihrer täglichen Erreichbarkeit anmelden, so dass daraus Bewegungs-, Sozial- und Kontaktprofile entstehen. Sie werden im Fall einer Urin- und Blutkontrolle einer kurzfristigen Totalüberwachung bis in den Intimbereich hinein unterworfen. Im Fall von Verstößen gegen das Melde- und Kontrollregiment sowie bei unzulässigen Urin- und Blutwerten wird dies der Öffentlichkeit preisgegeben.

Die Arbeit von Mortsiefer zeigt, dass er und damit die NADA die Datenschutzprobleme erkannt haben. Die Arbeit dient aber nicht einer Weiterentwicklung des Datenschutzes angesichts einer unbefriedigenden Situation, sondern deren Legitimation: Diese erfolgt zunächst über die Annahme einer wirksamen Einwilligung durch die betroffene SportlerIn in das Verfahren generell wie in die konkrete Erhebung beim Meldeverfahren (den sog. „Whereabouts“) und bei den Tests. Da die Einwilligungen mangels Freiwilligkeit auf dünnen Beinen stehen, versucht der Autor hilfsweise den Rückgriff auf die gesetzliche Verarbeitungsbefugnis des § 28 BDSG. Dabei tut er insbesondere bei der Interessenabwägung den SportlerInnen und ihren Persönlichkeitsrechten keinen Gefallen: Wegen der Wichtigkeit der Dopingbekämpfung, die unhinterfragt als alternativlos behandelt wird, werden selbst die massiven Eingriffe im Bereich des Meldeverfahrens als - noch - verhältnismäßig anerkannt. Der Hintergrund ist, dass das nationale Kontrollverfahren in das weltweite der World Anti Doping Agency (WADA) eingebunden ist und dort dem Datenschutz nicht die rechtliche und politische Anerkennung zukommt wie in Deutschland oder in Europa.

Bei der Verarbeitung der Gesundheitsdaten und bei der Datenübermittlung ins Drittausland ohne Datenschutzniveau werden vom Autor die Grenzen der möglichen Rechtsauslegung überschritten, wobei jeweils äußerst geschickt argumentiert wird: Sollte eine bestimmte Datenverarbeitung im Einzelfall dann doch unverhältnismäßig scheinen, was aber mit einem Verweis auf die Zweckbindung der Daten und der großen Relevanz der Dopingbekämpfung eher nicht der Fall sei, so könne Rückgriff auf die vermeintlich wirksame Einwilligung der SportlerInnen genommen werden. Es handelt sich hier um eine erkennbar interessengeleitete Arbeit. Damit soll deren Bedeutung nicht kleingeschrieben werden: Zum Einen enthält sie eine konsistente Darstellung des Anti-Doping-Systems und der zu Grunde liegenden Strukturen, zum Anderen werden Argumente vorgetragen, mit denen man sich auseinandersetzen kann (und muss). Bei dieser Auseinandersetzung kann dann ja herauskommen, dass die real praktizierte Dopingbekämpfung vielleicht doch nicht so alternativlos ist, wie sie hier dargestellt wird.

Robert Kazemi, Anders Leopold
Datenschutzrecht in der anwaltlichen Beratung
DeutscherAnwaltVerlag Bonn 2011,
ISBN 978-3-8240-1107-0, 486 S.

tw Es ist nicht zu leugnen, dass das Datenschutzrecht in der anwaltlichen Beratungspraxis angekommen ist. Bisher lässt aber die Qualität dieser Beratung zu Wünschen übrig. Insofern ist es begrüßenswert, dass für die

AnwältIn eine konsistente Datenschutz-Orientierungshilfe zur Verfügung gestellt wird. Das ist ganz offensichtlich die Funktion des Buches von Kazemi und Leopold. Es geht nicht darum, umfassend und in aller Tiefe das Datenschutzrecht zu behandeln. Hierfür gibt es die dicken Kommentare, Promotionen und Fachaufsätze. Vielmehr wollen die Autoren den in Datenschutzfragen noch unerfahrenen KollegInnen ein Einführungs- und Nachschlagewerk zur Seite stellen, das zunächst einen historischen und systematischen allgemeinen Teil mit der Darstellung der zentralen Instrumente und Begriffe liefert und dann ausgewählte „Anwendungsfälle" darstellt, die Schwerpunkte in der Beratungspraxis einer AnwältIn sind. Diese Anwendungsfälle sind unter der etwas missdeutbaren Überschrift „Datenschutz in Vertrieb" das allgemeine Datenschutzrecht für Unternehmen generell (Einwilligung, gesetzliche Grundlagen, Werbung, AGB, Adresshandel) sowie Spezialthemen wie Internet, Auftragsdatenverarbeitung, Auskunfteien, Scoring, Beschäftigtendatenschutz, unternehmensinterne Datenschutzorganisation mit betrieblichem Datenschutzbeauftragten, Datenex- und -import. Ein Unterkapitel befasst sich mit dem „Datenschutz in der Anwaltskanzlei", ein in der anwaltlichen Praxis bisher wohl noch ebenso defizitärer Bereich wie manche anwaltliche Beratung.

Das Buch ist in vieler Hinsicht erfreulich: Gut und verständlich geschrieben, trotz der Orientierung auf Unternehmensberatung datenschutzfreundlich, gut recherchiert und mit Nachweisen versehen sowie aktuell hinsichtlich der Praxisbeispiele und der Lösungen hierfür. Es ist offensichtlich den Autoren ein Anliegen, nicht nur anwaltliche Tricks im Umgang mit dem Datenschutzthema zu vermitteln, sondern auch, die Lage des Datenschutzes in Beratung und Praxis zu verbessern. Dabei stellen sie kontroverse Diskurse dar und entscheiden sich regelmäßig für fortschrittliche und zugleich für die Praxis pragmatische Positionen. Das Buch greift auf die klassische aktuelle Kommentarliteratur zurück, gibt dann aber auch unter Nutzung von Spezialbeiträgen in Schrift oder im Internet Einsichten in Einzelfragen, die in der Kommentarliteratur nicht unbedingt zu finden sind. Äußerst erfreulich ist die offensichtlich vorhandene technische Kompetenz, die Voraussetzung ist, um die teilweise nicht ganz einfachen Verarbeitungssachverhalte in eine für JuristInnen verstehbare Sprache zu übersetzen. Nicht ganz erschließt sich der LeserIn manchmal der Aufbau des Buches, der nicht dem klassischen Muster entspricht, der dann aber z. B. auch dazu führt, dass die Auskunfts-, Benachrichtigungs- und Informationsrechte, vom BDSG über das TMG bis hin zu arbeits- und zivilrechtlichen Regeln, instruktiv in einem Kapitel abgehandelt werden.

Das Ganze wird abgerundet durch detailliere Verzeichnisse (Inhalt, Literatur, Glossar, Stichworte, Adressen) und einen Anhang mit Vertragsmustern und Vorlagen (zu Einwilligung, Vertragsgestaltung, Auftragsdatenverarbeitung, Checklisten). Das Buch liefert also keine neuen wissenschaftlichen Erkenntnisse, wohl aber für die juristisch anspruchsvollen Interessierten eine gute solide Ausbildung wie für einige wichtige Beratungsthemen handbuchartige Informationen.

Tim Wybitul,
Handbuch Datenschutz im Unternehmen,
Verlag Recht und Wirtschaft,
Frankfurt am Main, 2011,
ISBN 978-3-8005-1524-0, 543 S.

tw Noch ein Datenschutzhandbuch - als gäbe es nicht schon genug davon! Tatsächlich besteht kein Mangel an allgemeiner Datenschutzliteratur. Es erfolgt eine Ausdifferenzierung nach Adressatenkreisen - Wybitul zielt auf Wirtschaftsunternehmen und damit auf eine möglicherweise bestehende Marktlücke, wenn sein Handbuch nicht nur Datenschutzbeauftragte, sondern auch „Compliance-Officer, Mitarbeiter in Rechtsabteilungen und andere für die Einhaltung gesetzlicher Vorschriften im Unternehmen verantwortliche Personen" anspricht. Das Werk ist eine verständlich geschriebene umfassende Bearbeitung, die nach einer Einführung die BDSG-Grundregeln und -Grundbegriffe behandelt, um dann systematisch die Zulässigkeit der Datenverarbeitung gemäß den einzelnen Rechtsgrundlagen, die Regeln für den betrieblichen Datenschutzbeauftragten, die Betroffenenrechte und - für Unternehmen wichtig - die Sanktionsmöglichkeiten abzuarbeiten. Auch eine Kurzkommentierung der relevanten BDSG-Regelungen wird mitgeliefert. Ausführlich dargestellt ist die Verarbeitung von Beschäftigtendaten; abgedruckt und kommentiert wird der dazu vorgelegte Regierungsentwurf vom 25.10.2010. Zu kurz kommt die praktisch äußerst relevante, in der Unternehmenspraxis viel zu wenig problematisierte Verarbeitung von Gesundheitsdaten. Praktisch nicht behandelt werden alle technisch-organisatorischen Fragen der Datensicherheit. Antworten werden nur zu den klassischen Rechtsfragen gegeben.

Dies erfolgt in einer nachvollziehbaren Weise unter Hinzuziehung der aktuellen (Kommentar-) Literatur, wobei in der Regel eine verarbeitungs- und damit unternehmensfreundliche, aber zugleich den Datenschutz voll akzeptierende Sichtweise gewählt wird. Die Gliederung ist übersichtlich; das Stichwortverzeichnis verweist nicht immer auf die für ein Thema relevanten Passagen. Das Werk zielt nicht auf den Experten, sondern auf die professionellen Laien und soll diesen das Nötige aus einer Hand bereitstellen, weshalb Gesetzestexte, Praxistipps und – was äußerst praktisch ist – Formularformulierungen mitgeliefert werden. Angesprochen werden das Problemspektrum des rechtlichen Datenschutzes im Unternehmen. Bei der Suche nach detaillierten Problemlösungen stellt man dann aber oft fest, dass die Erläuterungen vage bleiben. So bleibt dann doch nur als Ausweg die Inanspruchnahme von Spezialliteratur, auf die in den Fußnoten

hingewiesen wird. Für den Nutzer mit einem Datenschutzansatz interessant ist das Literaturverzeichnis, das auch die Unternehmensrechtsliteratur mit erfasst, eine Englischübersetzung des BDSG und ein Glossar Deutsch-Englisch, das zur Vermittlung des Datenschutzes an englischsprachige Vertreter eines Mutterkonzerns von Nutzen sein kann.

Kühling, Jürgen/Seidel, Christian/ Sivridis, Anastasios
Datenschutzrecht
C. F. Müller, Heidelberg u. a., 2. Aufl. 2011, ISBN 978-3-8114-9692-7, 264 S.

tw Nach der Erstauflage 2008 (DANA 1/2009, 39) haben die Autoren 2011 schon eine zweite Auflage ihres Lehr- und Lernbuches zum Datenschutzrecht vorgelegt. Der umfassend aktualisierte Text ist eine gute Studiengrundlage für Jurastudierende und für PraktikerInnen zur Vermittlung der Grundbegriffe, des Aufbaus und der Funktionsprinzipien des Datenschutzrechts. An Hand von 15 Fällen , die zumeist aus der Rechtsprechung entnommen sind, wird in die Themen eingeführt, die systematisch und umfassend dargestellt werden. Zumeist am Ende der Kapitel werden schulmäßige Lösungsskizzen präsentiert und teilweise kommentiert. Erfreulich ist, dass die Autoren unterschiedliche Lösungen als vertretbar darstellen, wobei sie sich zumeist an den getroffenen Entscheidungen orientieren. Dies führt, trotz der durchgängig äußerst datenschutzfreundlichen Grundeinstellung des gesamten Werkes, im Einzelfall dazu, dass Positionen dargestellt werden, die vom Rezensent anders gesehen werden (z. B. Lindquist-Fall, Finanzdienstleistungsauskunft). Im Vordergrund steht die Vermittlung von Datenschutzrechtswissen, was in einer gut verständlichen Sprache, praxisnah und nachvollziehbar gelingt. Schematische bzw. bildliche Darstellungen erhöhen die Anschauung.

Ein Defizit des Lehrbuchs ist, dass die Schnittstellen zur Technik zu kurz kommen, also der Systemdatenschutz bzw. die technisch-organisatorischen Maßnahmen nach § 9 BDSG, was in der Praxis eine wichtige Rolle spielt. Auch der Medizindatenschutz spielt weiterhin keine Rolle. Erfreulich ist ein kurzes informatives Kapitel zum Thema Datenschutzaudit. Ausführlich dargestellt wird der Datenschutz im Bereich der neuen Medien und der Telekommunikation. Als Einzelanwendung behandelt wird die Videoüberwachung; der Beschäftigtendatenschutz wird nur beispielhaft abgehandelt. Diese Beschränkung ist dem Lehr- und Lernbuchcharakter geschuldet. Auf die grundlegende Kommentar- und Handbuchliteratur wird verwiesen. Für Erschließungszwecke gut geeignet sind insofern auch die Verzeichnisse (detailliert Inhalt, Abk., Literatur, Literatur, ausgewählte Stichworte). Wer sich mit einem überschaubaren Aufwand mit dem Datenschutzrecht vertraut machen und dort einarbeiten möchte, dem ist dieses Buch zu empfehlen.

19.10.2011 Brüssel

Am 19.10.2011 führt die DVD im Europäischen Parlament in Brüssel eine Veranstaltung zur Integration des Arbeitnehmerdatenschutzes in zukünftige europäische Regelungen durch.
Es geht darum, Europaabgeordneten darzulegen, warum Beschäftigtendatenschutz unbedingt Teil jeder zukünftigen europäischen Regelung sein sollte – sei es nun eine Richtlinie oder eine Vollregelung.

Da die Deutsche Vereinigung fuer Datenschutz e.V. – DVD selbst keine Veranstaltungen im Parlament durchführen kann, sind wir sehr dankbar, dass Cornelia Ernst (MEP, Linksfraktion) formal die Gastgeberrolle übernimmt.

Als Berichterstatter für Ihre Fraktionen haben neben Cornelia Ernst als Gastgeberin bereits Alexander Alvaro, Jan Phillipp Albrecht und Armin Duttine als Vertreter des Berichterstatters Peter Morgan für das EESC seine Teilnahme zugesagt.

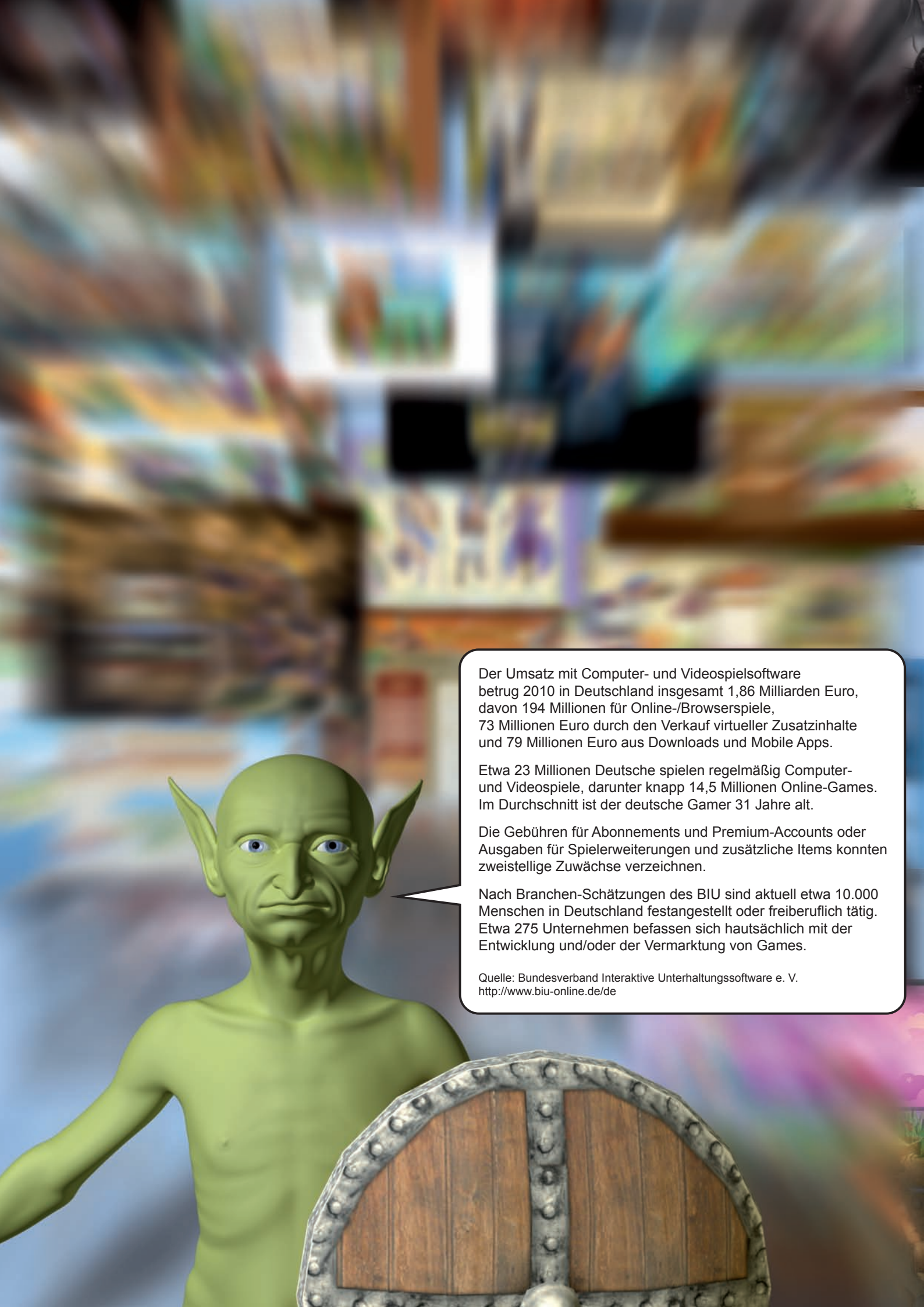
Wir werden mit einer einstündigen Runde beginnen, die den Berichterstattern die Gelegenheit geben soll, den Teilnehmern ihre Position darzulegen.

Anschließend werden wir das Podium erweitern und „ins Detail gehen“ – und zwar mit

- Peter Gola, Vorsitzender der GDD
- Thomas Spaeing, Vorsitzender des BVD
- Karin Schuler, Vorsitzende der DVD

Die grundlegende Position der DVD findet sich in der Stellungnahme zum Vorhaben der Kommission, die Richtlinie 95/46/EC zu novellieren:

www.datenschutzverein.de/Themen/Stellungnahme EURiLi DVD.pdf



Der Umsatz mit Computer- und Videospielsoftware betrug 2010 in Deutschland insgesamt 1,86 Milliarden Euro, davon 194 Millionen für Online-/Browserspiele, 73 Millionen Euro durch den Verkauf virtueller Zusatzinhalte und 79 Millionen Euro aus Downloads und Mobile Apps.

Etwa 23 Millionen Deutsche spielen regelmäßig Computer- und Videospiele, darunter knapp 14,5 Millionen Online-Games. Im Durchschnitt ist der deutsche Gamer 31 Jahre alt.

Die Gebühren für Abonnements und Premium-Accounts oder Ausgaben für Spielerweiterungen und zusätzliche Items konnten zweistellige Zuwächse verzeichnen.

Nach Branchen-Schätzungen des BIU sind aktuell etwa 10.000 Menschen in Deutschland festangestellt oder freiberuflich tätig. Etwa 275 Unternehmen befassen sich hautsächlich mit der Entwicklung und/oder der Vermarktung von Games.

Quelle: Bundesverband Interaktive Unterhaltungssoftware e. V.
http://www.biu-online.de/de