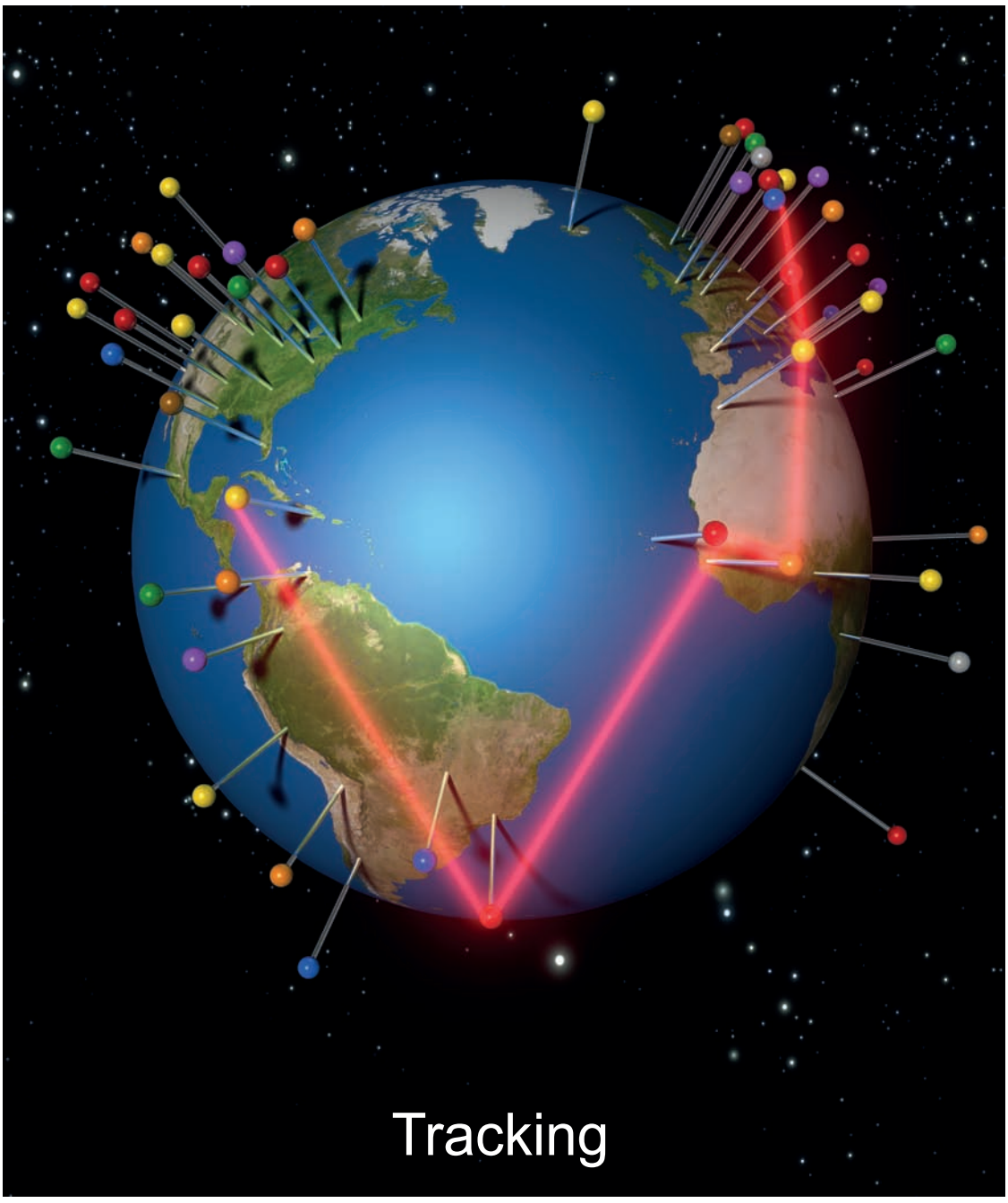
3/2010

Datenschutz Nachrichten

33. Jahrgang
ISSN 0137-7767
9,00 Euro



■ Geolokalisierung und Geotracking ■ Tracking im Internet zu Werbezwecken ■ Deutsche Daten auf Geheimservern in den USA ■ Ambulante Hospizvereine und Datenschutz ■ Großdemonstration „Freiheit statt Angst“ in Berlin ■ Datenschutznachrichten ■ Rechtsprechung ■

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

Inhalt

Termine

Donnerstag, 7. Oktober 2010, 14:00 h
18. Wiesbadener Forum Datenschutz
40 Jahre Datenschutz in Hessen
Plenarsaal des Hessischen Landtags
Weitere Informationen unter: www.datenschutz.hessen.de/aktuell.htm

Samstag/Sonntag, 16./17.10.2010
Datenspuren 2010: Mind the Gap!
Chaos Computer Club Dresden
Kulturzentrum Scheune,
Alaunstraße 36-40, 01099 Dresden
Weitere Informationen unter: http://events.ccc.de

1. November 2010
Redaktionsschluss für die DANA 4/2010
Thema: „Arbeitnehmerdatenschutzgesetz“
Fragen und Anregungen bitte an:
dvd@datenschutzverein.de

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

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

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

Donnerstag, 11. November 2010, 17:00 h
Datenschutz an Hochschulen – Beispiele und Praxistipps
Fachhochschule Gießen-Friedberg, Campus Gießen
Weitere Informationen unter: www.fh-giessen-friedberg.de/datenschutz

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

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

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

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

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

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

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

Abbildungen
Frans Jozef Valenta

In 80 Tagen um die Welt

Als Jules Verne 1873 den Roman über eine Wette zu einer Weltumrundung schrieb, gab es zur Personenidentifikation bei Reisen keine Ausweise und zur Kommunikation benutzte man den Telegrafen.

Im Laufe der letzten 137 Jahre hat sich sehr viel verändert: Inzwischen gibt es biometrische Pässe mit RFID-Chips – Mobiltelefone, Funkgeräte und Internet machen Gespräche von fast jedem Punkt der Erde aus möglich. Weltumrundungs-Beobachter können durch GPS- und Funkzellen-Ortung ständig den Aufenthaltsort des Reisenden abfragen, wenn Kommunikationsgeräte mitgeführt werden. Digitalkameras machen „Beweisfotos“ der besuchten Orte mit GPS-Koordinatenangaben, das Abheben von Bargeld am Automaten wird registriert, das Bezahlen mit Kreditkarte ebenso wie die Buchung eines Fluges oder die Übernachtung im Hotel. Als Fußgänger wird man in Städten kaum 100 Meter ohne Videoüberwachung gehen können, mit Gesichtserkennungs-Software lassen sich dabei unter Verwendung von HD-Kameras und Verknüpfung der Daten Bewegungsprofile aller Passanten erstellen.

Die Summe dieser Errungenschaften mag für die Dokumentation einer Weltreisen-Wette eine Erleichterung bedeuten, aber eine, die schwerer und schwerer wiegen wird. Die ich rufe, die Geister...

Technisch gesehen ließe sich eine Reise um die Welt bequem in 8 Tagen bewerkstelligen, aber im Gegensatz zu Jules Vernes Zeit dürfte es heutzutage fast unmöglich sein, ohne (Daten-)Spuren von Kontinent zu Kontinent zu gelangen. Wollen wir wetten?

Frans Jozef Valenta

Autorinnen und Autoren dieser Ausgabe:

Prof. Dr. Rainer Erd
von 1993 bis 2010 Professor für Informationsrecht sowie Datenschutzbeauftragter an der Hochschule Darmstadt, Mitherausgeber der Zeitschrift Kritische Justiz, seit März 2010 Rechtsanwalt in der Sozietät Schmalz (Frankfurt am Main). r.erd@schmalzlegal.com

Marit Hansen
Stellvertretende Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel
marit.hansen@privacyresearch.eu

Michael Marc Maisch
Dipl. jur. (univ.), wissenschaftlicher Mitarbeiter an der Universität Passau und der Zeppelin University Friedrichshafen. Marc.Maisch@uni-passau.de.
www.michaelmarcmaisch.de

Manfred von Reumont
Diplom-Verwaltunswirt und EPHK i.BGS i.R.,
bis 2001 behördlicher DSB im Bereich des BMI, danach freiberuflich tätig in Beratung und Realisierung im nicht-öffentlichen Datenschutz.
mvr13@t-online.de, www.mvr-datenschutz.de

Marit Hansen

Geolokalisierung und Geotracking – Herausforderungen für Location Privacy

1 Einführung

Geoinformationen zur Positionsbestimmung sind nicht nur für Weltreisende interessant. Viele Autofahrer nutzen mittlerweile Navigationssysteme bei der Routenplanung und lassen sich von ihnen während der Fahrt leiten – sogar unter Einbeziehung aktueller Verkehrsinformationen. Ein Großteil der Bevölkerung ist mit Handys ausgestattet, deren Position im angeschalteten Zustand im Mobilfunknetz jederzeit bekannt ist. Es lassen sich vielfältige „Location-Based Services“ (ortsbasierte Dienste) hinzuschalten, z.B. Informationsdienste, die Auskunft über Restaurants, Kinos, Sehenswürdigkeiten oder Apotheken in der näheren Umgebung geben oder in deren Auftrag Werbebotschaften kommunizieren. Auch Bekannte lassen sich über ortsbasierte Dienste aufspüren, wenn sie bei „Buddy-Finder“-Diensten mitmachen. Tracking-Dienste ermöglichen es, die Position eines Objektes über die Zeit zu verfolgen. Dies können Fahrzeuge in einem Unternehmen sein, Produkte auf ihrem Weg vom Hersteller zum Verkäufer oder auch weiter zum Käufer, oder es kann sich um Endgeräte handeln, die einem Nutzer oder einer Nutzerin zugeordnet sind. Außerdem gibt es Notfalldienste, mit deren Hilfe sich Rettungskräfte alarmieren und an den richtigen Ort schicken lassen.

Automatische Erstellung von Karten durch Kamera-GPS-Daten in iPhoto von Apple.

Im Folgenden werden die wichtigsten Begriffe in diesem Text erklärt:

Unter Geolokalisierung versteht man den Prozess der Positionsbestimmung (auch: Ortung). Das Ergebnis einer Geolokalisierung ist in vielen Fällen nicht exakt, sondern weist Unschärfen auf, deren Grad zumeist vom gewählten Verfahren abhängt.

Einige Formen der Geolokalisierung erfolgen nutzergesteuert – dann stoßen Nutzer selbst die Anfrage nach ihren jeweiligen Geokoordinaten an –, andere geschehen ohne ihr Zutun, oft auch ohne dass es ihnen bewusst ist. In einigen Fällen erfährt nur der/die jeweilige Nutzer(in) die Koordinaten der Position, in anderen erhalten weitere an dem Verfahren Beteiligte diese Information.

Geotracking bezeichnet das Sammeln und Verketten von Positionsdaten über einen gewissen Zeitraum: Bewegungen im Raum über die Zeit lassen sich damit aufzeichnen; ein Nachverfolgen der betroffenen Personen wird ermöglicht. Solche Bewegungsprofile können sehr aussagekräftig sein (siehe auch Abschnitt 3) und erlauben vielfach recht zuverlässige Einschätzungen über künftiges Verhalten der Betroffenen.

Location Privacy ist eine Kategorie des Datenschutzes, die den Schutz der aktuellen oder vergangenen Ortsinformationen einer Person in den Fokus rückt. Eine häufig zitierte Definition lautet: „The ability to prevent other parties from learning one’s current or past location“ („die Fähigkeit, andere Parteien daran zu hindern, seine gegenwärtige oder frühere Position zu kennen“; vgl. Beresford/Stajano 2003). Im deutschen Kontext wäre hier eher das Recht auf informationelle Selbstbestimmung – eben mit Fokus auf Ortsinformationen – anzulegen. Darüber hinaus reicht es nicht, allein die Ortsinformationen zu betrachten, sondern es müssen ebenfalls etwa damit in Zusammenhang stehende Informationen einbezogen werden (so auch White 2003), wenn sie geeignet sind, die Privatsphäre der Betroffenen zu beeinträchtigen oder sie zu diskriminieren. Beispiele dafür wäre eine Einstufung von Wohngegenden aufgrund von statistischen Aussagen zu Krankheitshäufungen oder zu der zu erwartenden Zahlungsfähigkeit der Bewohner.

Dieser Text ist wie folgt aufgebaut: Abschnitt 2 gibt einen Überblick über die technischen Möglichkeiten der Geolokalisierung. Anschließend werden in Abschnitt 3 zwei Versuche zum Geotracking und ihre Ergebnisse zur Interpretation der erhobenen Daten kurz dargestellt. Abschnitt 4 widmet sich datenschutzrechtlichen Aspekten der Geolokalisierung. Die Herausforderungen für Location Privacy werden in Abschnitt 5 angesprochen. Schließlich fasst das Fazit wesentliche Resultate zusammen und zeigt aktuelle Trends auf.

2 Technische Möglichkeiten der Geolokalisierung

Geolokalisierung bedeutet das Feststellen der räumlichen Position. Aus Datenschutzsicht ist insbesondere die Geolokalisierung von Personen oder von Objekten, die mit Personen in einem Zusammenhang stehen, interessant. Selbst bei Eigenauskünften einer Person über ihren Aufenthaltsort kann man von einer (mit einer gewissen Unsicherheit behafteten) Geolokalisierung sprechen – solche Informationen teilen viele Nutzer beispielsweise über Twitter oder Facebook ihren Freunden oder der Öffentlichkeit mit. Im Folgenden werden diejenigen Formen von Geolokalisierung in den Mittelpunkt gestellt, die innerhalb einer technischen Infrastruktur automatisch und oft unbemerkt von den Betroffenen geschehen.

Bei mobilen Endgeräten kommen verschiedene Verfahren zur Positionsbestimmung zum Einsatz (s.a. Steiniger et al. 2006; Royer et al. 2009). Einige basieren auf der Technik des Mobilfunknetzes, andere verwenden Satelliten zur Ortsbestimmung, und schließlich ist auch eine Lokalisierung mit Hilfe von Sendern an bekannten Standorten möglich:

Mobiltelefone funktionieren nur, wenn sie sich im Funknetz eingebucht haben. Das Funknetz kennt die aktuelle Position des Handys zumindest in einer gewissen Auflösung, nämlich die Funkzelle. Das Verfahren zur Ortsbestimmung nennt sich daher „Cell of origin"-Ortung (COO) oder Cell-ID. Funkzellen können in städtischen Gegenden 100 Meter oder weniger in ihrer Ausdehnung umfassen; in ländlichen Bereichen decken sie bis zu 35 km im Durchmesser ab. Die jeweilige Funkzellengröße bestimmt die Genauigkeit der Positionsbestimmung.

Ein weiteres netzseitiges Verfahren ist die „Time Difference of Arrival"-Ortung (TDOA). Diese Methode basiert auf mindestens drei Basisstationen im Mobilfunknetz, die die (ungefähre) Position aus den unterschiedlichen Laufzeiten der Signale des Endgeräts durch Triangulation errechnen.

Eine verbesserte Variante von TDOA stellt die „Enhanced Observed Time Difference"-Ortung (E-OTD) dar. Während bei COO- und TDOA-Ortung keine Zusatzausrüstung auf dem Mobiltelefon erforderlich ist, muss das Handy für die Nutzung von E-OTD dieses Verfahren unterstützen, da es selbst die Laufzeitmessungen durchführt. Die Genauigkeit der Positionsbestimmung kann 25 m betragen.

Auf wenige Meter genau ist eine Ortung per „Global Navigation Satellite System (GNSS)" möglich. Bei diesem Verfahren bestimmt das Endgerät seine Position über ein satellitengestütztes System (z.B. GPS oder Galileo). Diese Möglichkeit der Ortsbestimmung muss hardwareseitig vom Endgerät unterstützt werden. Die GNSS-Satelliten übertragen per Funk ihre genaue Position und die Zeit. Das Endgerät errechnet aus den Signallaufzeiten von mindestens vier Satelliten die Position (einschließlich der Höhe); außerdem kann per GNSS die Geschwindigkeit festgestellt werden. GPS (Global Positioning System) ist zurzeit das am weitesten verbreitete Verfahren zur Positionsbestimmung und Navigation. Die Position kann auf etwa 15 m genau ermittelt werden; verbesserte Verfahren wie Differential-GPS (DGPS) lassen eine Genauigkeit von wenigen Zentimetern bis 5 m zu. Da GPS zunächst militärischen Zwecken der USA diente, wurde bis zum Jahr 2000 eine künstliche Ungenauigkeit hinzugeschaltet, so dass damals die Position von nicht-militärischen Nutzern nur bis auf 100 m genau bestimmt werden konnte.

Nachteile der Nutzung von GPS-Empfängern im Handy bestehen zum einen im hohen Stromverbrauch und zum anderen darin, dass die Funktionsweise von der freien Sicht zum Himmel abhängig ist, also ein Einsatz innerhalb von Gebäuden gar nicht oder nicht gut funktioniert. Zumindest teilweise Abhilfe leisten Erweiterungen wie „Enhanced GPS (E-GPS)", das die GPS-Methode um die Verfahren im Funknetz (u.a. Cell-ID) ergänzt, oder „Assisted GPS (A-GPS)", bei dem das Mobilfunknetz Hilfsdaten an das Handy überträgt, um die Ortsbestimmung schneller und energieärmer ausführen zu können, oder sogar Daten vom Handy entgegennimmt, um die Berechnung selbst durchzuführen.

Hinzu kommen Verfahren für die Positionsbestimmung von Endgeräten, die auf Datenbanken von Lokalisierungsdiensten wie Skyhook oder Google zurückgreifen (vgl. Köhntopp 2010). Solche Anbieter haben in den vergangenen Jahren in vielen Gegenden der Welt Informationen über Sender wie Basisstationen in Mobilfunknetzen und WLAN-Access-Points gesammelt. Nimmt man an, dass die Standorte und Sendeleistungen dieser Sender relativ stabil sind, kann für ein Endgerät eine recht genaue Position ermittelt werden, wenn es an den Lokalisierungsdienst die Informationen über alle Sender im Empfangsbereich und deren gemessene Sendeleistung überträgt. Diese Methode funktioniert besonders gut in Städten, da dort viele Sender zu empfangen sind, und ist sehr viel schneller als eine GPS-Abfrage.

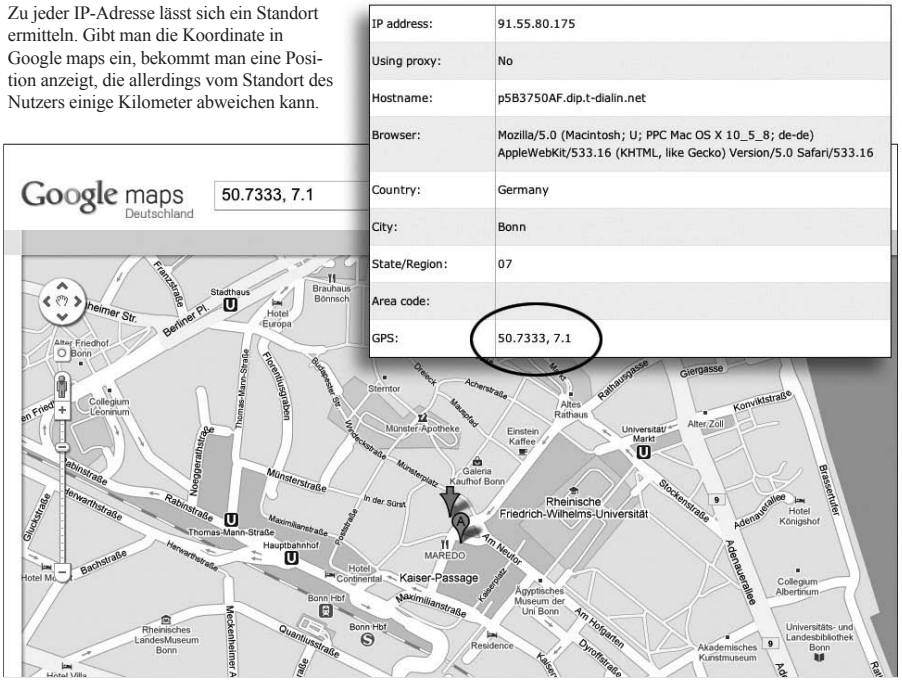
Für die Erhebung der Daten, die zusammen mit Geokoordinaten in den Datenbanken der Lokalisierungsdienste gespeichert werden, werden Empfangsgeräte eingesetzt, die die per Funk

von den Sendern übertragenen Daten aufzeichnen, sobald sie sich im Ausstrahlungsbereich der Sender befinden. Dies würde bereits mit normalen Handys und WLAN-fähigen Computern funktionieren – beispielsweise mit der Software „Net Stumbler“, die WLAN-Access-Points mit ihrer SSID (Service Set ID), Kanalnummer o.ä. darstellt. Im professionellen Einsatz werden die Kanäle mehrfach pro Sekunde gewechselt, um alle Frequenzen durchzuprobieren, auf denen Sender zu finden sein können. Zu jedem WLAN-Access-Point erfassen Skyhook und Google laut eigenen Aussagen u.a. die MAC-Adresse (d.h. einen eindeutigen Identifikator aus der Hardwareadresse der Netzwerkkarte), die SSID (d.h. einen konfigurierbaren Identifikator zur Bezeichnung des WLANs) sowie den WLAN-Namen (frei vom Netzbetreiber festgelegt).

Der Aufwand, um diese Datenbank zu erstellen, erscheint zwar recht hoch, wird aber offensichtlich von den Betreibern als lohnenswerte Investition eingeschätzt. Skyhook hatte zu diesem Zweck Straßen in Ballungszentren abfahren lassen, und die Firma Google, die zunächst auf entsprechenden Informationen bei Skyhook zurückgriff, hat mittlerweile im Rahmen der Erfassungsarbeiten für Google Street View gleich eine eigene Datenbank mit WLAN-Access-Points erstellt. Die Pflege der Datenbank wird vermutlich nur selten erneute Befahrungen erforderlich machen, denn es ist zu erwarten, dass die Aktualisierung während des Betriebes durch Smart Phones erfolgt, die bei jeder Positionsbestimmung über einen solchen Lokalisierungsdienst Daten über die Sender in ihrer Umgebung offenbaren. Auf diese Art baut auch Apple seine eigene Datenbank mit Lokalisierungsinformationen auf.

Eine andere Art der Geolokalisierung funktioniert im Internet anhand der IP-Adresse: Da bekannt ist, welche IP-Adressblöcke an welche Zugangs-Provider vergeben sind und wo diese ihren Sitz haben, können die zu den IP-Adressen gehörenden Ortsinformationen abgefragt werden (z.B. mit dem Dienst IP2Location). Sehr häufig wählen Nutzer einen Zugangs-Provider in ihrer räumlichen Nähe aus, beispielsweise um die Telefonkosten

Zu jeder IP-Adresse lässt sich ein Standort ermitteln. Gibt man die Koordinate in Google maps ein, bekommt man eine Position anzeigt, die allerdings vom Standort des Nutzers einige Kilometer abweichen kann.



gering zu halten. Mit einer gewissen Unschärfe gelten die Ortsinformationen des Zugangs-Providers auch für die Nutzer. Viele Inhaltsanbieter nutzen Geolokalisierungsdienste, um festzustellen, woher ihre Nutzer kommen.

Schließlich wird mit der Entwicklung von Smart Homes und einer zunehmenden Sensorik des ubiquitären Computings die technische Infrastruktur für das Lesen und Auswerten von RFID-Chips aufgebaut werden. Bei einer naiven Implementierung besteht dann das Risiko, dass über das Auslesen von RFID-Informationen aus Kleidungsstücken, Verpackungen der eingekauften Produkte, Bibliotheksausweisen, ÖPNV-Tickets, Geldkarten usw. die Bewegung von Personen nachverfolgbar wird. Selbst wenn keine Zuordnung zwischen RFID-Nummern und Namen abrufbar ist, kann durch entstehende Bewegungsprofile oder Verkettung mit weiteren RFID- oder anderen Datenspuren recht einfach auf die Identität der betroffenen Personen geschlossen werden (vgl. Hansen/Meissner 2008)

.

3 Ergebnisse von Geotracking-Versuchen

In dem europäischen Projekt „FIDIS – Future of Identity in the Information Society“ (2004-2009) wurde ein Versuch mit vier Personen durchgeführt, deren Positionsdaten per GPS über den Zeitraum von einem Monat mehrfach pro Minute erfasst und regelmäßig in eine Datenbank übertragen wurden (Gasson 2009). Ziel dieser nichtrepräsentativen Untersuchung war ein „Normality Mining“, d.h. mit Hilfe der Positionsdaten Informationen über den Alltag der Versuchsteilnehmer zu gewinnen und daraus Schlüsse zu ziehen. Die Teilnehmer waren genau aufgeklärt worden und hatten ihre Einwilligung gegeben. Die GPS-Positionsbestimmung funktionierte nur außerhalb von Gebäuden; die Teilnehmer konnten jederzeit den Versuch unterbrechen; sie hatten stets unbeschränkten Zugriff auf die erhobenen Daten und konnten sie insbesondere vor der Auswertung löschen.

Das Team, das die Auswertung der Daten vornahm, kannte die Versuchsteilnehmer nicht. Um die Daten leichter interpretieren zu können, wurden sie automatisch in Spuren umgewandelt, die auf Karten die zurückgelegten Wege darstellten. Sobald ein Teilnehmer sich mindestens drei Minuten lang an derselben Stelle aufgehalten hatte, wurde hier ein „Point of Interest“ eingezeichnet, der sich dann anhand seiner Adresse näher bestimmen ließ.

Aus den Daten ließen sich bei den meisten der Teilnehmer regelmäßige Tagesabläufe ablesen, in denen beispielsweise die Wege zur Arbeit und

nach Hause oder der Gang in der Mittagspause eindeutig identifizierbar waren. Aus diesen Informationen konnte das Auswertungsteam mit ziemlicher Sicherheit die Wohngegend und den sozialen Status ermitteln sowie auf Arbeitsort und Beruf schließen. Der Familienstatus wurde ebenfalls korrekt bestimmt, auch wenn das Auswertungsteam zunächst davon irritiert war, dass sich bei einigen Teilnehmern die Geschwindigkeit auf einigen Fußwegen des Öfteren änderte und manchmal Zickzackkurse statt des direkten Weges eingeschlagen wurden – dies lag an den begleitenden Kleinkindern, die das Tempo bremsten und die Welt auf ihre Weise erkundeten. Auf Basis der Versuchsdaten waren Geschlecht und Einkaufsgewohnheiten der Teilnehmer nicht eindeutig zu identifizieren, doch dies wäre vermutlich bei einer Erhebung über einen längeren Zeitraum möglich. Die Analyse ergab weiterhin, dass die Teilnehmer keine Fitnessstudios aufsuchten oder sich wahrscheinlich auch nicht außerhalb von Gebäuden besonders sportlich betätigten, z.B. durch Joggen oder längeres Fahrradfahren. Die gewählten Verkehrsmittel waren in der Regel ermittelbar. In einigen Fällen wurden Geschwindigkeitsüberschreitungen mit dem Auto festgestellt.

Insgesamt wäre es nicht schwierig, mit wenigen Zusatzinformationen von den Daten auf die Person zu schließen. In dem Versuch war eine längerfristige Weitergabe des Tracking-Geräts an andere Personen durch regelmäßige Abgleiche von Fingerabdruck-Scans gegenüber dem Endgerät ausgeschlossen worden. Eine solche Weitergabe ist aber ohnehin eher ungewöhnlich, sofern Endgeräte mit Tracking-Funktionalität für die sie einsetzenden Menschen einen persönlichen Nutzen haben: Die meisten Handys und Smart Phones werden die meiste Zeit von nur einer Person genutzt.

Zusätzlich zu den Analysen des Alltags der einzelnen Teilnehmer konnte in einigen Fällen festgestellt werden, dass dieselben Orte besucht wurden. Hieraus ließ sich korrekt eine Bekanntschaft ableiten. Dies wird auch von einer größeren Studie des MIT Media Lab bestätigt, in denen erfolgreich das individuelle soziale Netzwerk aus Ortsinformationen und Daten zur Nutzung verschiedener Handy-Applikationen analysiert wurde (Eagle et al. 2009).

4 Datenschutzrechtliche Aspekte der Geolokalisierung

In den beiden Versuchen, die im vorherigen Abschnitt angesprochen wurden, verwendeten die Forscher gesonderte Tracking-Software, damit die Daten an die wissenschaftlichen Teams zur Auswertung übertragen wurden. Bei Benutzung von GPS-Empfängern ließe sich der Aufenthaltsort von Nutzern nicht verfolgen, da die Geräte nur passiv arbeiten. Daher wurde jeweils eine aktive Komponente eingebaut, um die Positionsdaten zu übertragen.

Im Mobilfunknetz ist dies anders: Hier sind die Positionsdaten in der Regel nicht so exakt, doch wenn man annimmt, dass sich mobile Nutzer für bestimmte Verkehrswege entscheiden, wäre ein grobes Tracking für die Betreiber technisch durchaus möglich. Ähnliches gilt in den Fällen, in denen sich Personen für die Nutzung von ortsbasierten Diensten anmelden: Auch dann machen sie deren Anbietern in der Regel seine Positionsdaten bekannt.

Mit der Zunahme von Smart Phones wie dem iPhone von Apple oder Googles Android Handys wird eine Weitergabe der Ortsinformationen zur Regel: Die Datenschutzerklärung von Apple stellt unter der Überschrift „Standortbezogene Dienste“ beispielsweise fest: „Um standortbezogene Dienste auf Apple-Produkten anzubieten, können Apple und unsere Partner und Lizenznehmer präzise Standortdaten erheben, nutzen und weitergeben, einschließlich des geographischen Standorts Ihres Apple-Computers oder Geräts in Echtzeit. Diese Standortdaten werden in anonymisierter Weise erhoben, durch die Sie nicht persönlich identifiziert werden.“ Wie allerdings diese Anonymisierung funktioniert, erklärt Apple bislang nicht. Dass in derselben Datenschutzerklärung das „[E]rheben […] individuelle[r] Geräteidentifizierungsmerkmale sowie Ort und Zeitzone“ unter „nicht-personenbezogen“ eingestuft wird, wirkt nicht gerade beruhigend – mehr Transparenz über die tatsächliche Datenverarbeitung wäre dringend erforderlich. Immerhin sollen Apple-Nutzer die Verwendung ortsbasierter Dienste ausschalten können.

Im deutschen Recht lassen sich ortsbasierte Dienste in aller Regel als Telemediendienste einordnen, so dass das Telemediengesetz (TMG) von Anbietern solcher Dienste zu berücksichtigen ist. Sofern netzbasierte Verfahren zur Geolokalisierung eingesetzt werden, werden diese Standortdaten auch durch den Telekommunikationsanbieter verarbeitet; dafür ist das Telekommunikationsgesetz (TKG) einschlägig (Jandt 2007). Nach § 98 TKG darf der Telekommunikationsanbieter die Standortdaten nur anonym oder mit der Einwilligung des Betroffenen zur Bereitstellung von Diensten mit Zusatznutzen – einschließlich ortsbasierter Dienste – verwenden. Der Telekommunikationsanbieter darf also personenbezogene Standortdaten nur dann an den Anbieter eines ortsbasierten Dienstes übermitteln, wenn der jeweilige Nutzer zuvor eingewilligt hat. Der Anbieter des ortsbezogenen Dienstes hingegen darf die Standortdaten nach § 15 Abs. 1 TMG verarbeiten, soweit sie für die Inanspruchnahme des ortsbezogenen Dienstes erforderlich sind. Hier ist eine rechtmäßige Verwendung der Standortdaten also auch ohne eine Einwilligung des Nutzers möglich, weil

sich sonst der jeweilige Vertragszweck nicht erreichen ließe.

§ 98 TKG regelt auch die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder an Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind. Dies könnte beispielsweise ein „Partner-Tracking-Dienst" sein. Hier ist es erforderlich, dass der Teilnehmer seine Einwilligung ausdrücklich, gesondert und schriftlich erteilt. Außerdem muss der Diensteanbieter den Teilnehmer nach höchstens fünfmaliger Feststellung des Standortes des Mobilfunkendgerätes über die Anzahl der erfolgten Standortfeststellungen mit einer Textmitteilung informieren. Zusätzlich erwächst eine Pflicht für den Teilnehmer in Bezug auf Mitbenutzer, die dann ebenfalls dem Tracking unterworfen wären: Er hat die Mitbenutzer über eine erteilte Einwilligung zu unterrichten. Schließlich kann die Einwilligung jederzeit widerrufen werden.

Diese detaillierten Regelungen zeigen, dass der Gesetzgeber Standortdaten und insbesondere Bewegungsprofile, die durch Geotracking entstehen können, als sensibel eingestuft hat. Wie bereits in Abschnitt 3 argumentiert, sind solche Bewegungsprofile in aller Regel als personenbezogen einzustufen. Durch eine umfassende Verkettung von Standortdaten zu Bewegungsprofilen lässt sich eine räumliche und zeitliche Überwachung realisieren (ULD/TUD 2007). Weiterhin erlauben diese Bewegungsprofile Rückschlüsse auf Beziehungen und Gewohnheiten der betroffenen Personen.

Weitere rechtliche Aspekte betreffen die von Lokalisierungsdiensten erfassten Informationen zu privaten WLAN-Access-Points – ob per Abfahren einer Straße mit entsprechend ausgerüsteten Empfangsgeräten oder durch Smart Phones. Die juristische Diskussion soll an dieser Stelle nicht wiedergegeben werden. In jedem Fall ist anzumerken, dass dieses Lokalisierungsverfahren für professionelle Hotspots durchaus sinnvoll sein kann, jedoch Privatnutzer durchaus ein berechtigtes Interesse daran haben können, nicht in einer Datenbank in den USA mit den eindeutigen, nicht änderbaren MAC-Adressen ihres WLAN-Access-Points aufzutauchen – selbst wenn nur die Geokoordinaten und nicht ihr Name dazu abgespeichert sind. Dies gilt in besonderem Maße für mobile WLAN-Access-Points, wie sie zunehmend eingesetzt werden, wodurch sonst wiederum Bewegungsprofile der Nutzer entstehen können.

5 Herausforderungen für Location Privacy

Seit etwa fünfzehn Jahren wird an technischen Lösungen für Location Privacy geforscht. Ideen für ein vollständiges Neudesign von Mobilfunknetzen sind auf absehbare Zeit nicht umsetzbar. Typisch für Anwendungen im Bereich der Geolokalisierung und des Geotrackings ist die Vielzahl von Beteiligten, die jeweils unterschiedliches Wissen über die orts- oder personenbezogenen Informationen erhalten. Für einen datenschutzgerechten oder gar datenschutzfördernden Systementwurf sind insbesondere die Anforderungen darüber zu spezifizieren, wer welche Informationen bekommen oder gerade nicht bekommen darf und von welchen Bedingungen (z.B. Konfiguration der Betroffenen) dies abhängen soll (vgl. Langheinrich 2009): Soll die Location Privacy der Betroffenen vor anderen Teilnehmern geschützt werden? Vor dem Anbieter des ortsbasierten Dienstes? Vor dem Lokalisierungsanbieter oder dem Betreiber der technischen Infrastruktur?

Verschiedene Vorschläge für Location Privacy im Systemdesign werden heutzutage von Wissenschaftlern diskutiert (vgl. Fritsch 2007, Schnabel 2009 sowie Scipioni/Langheinrich 2010 – hier finden sich Verweise auf verschiedene Forscherteams, die zu dem Thema arbeiten). Zu den Ansätzen für eine verbesserte Transparenz und geeignete Möglichkeiten für die Betroffenen, ihre Selbstbestimmung wahrzunehmen, gehören maschinenlesbare Privacy Policies, wie sie in der Initiative GEOPRIV (http://tools.ietf.org/wg/geopriv/) vorgeschlagen werden, oder Arbeiten an verständlichen Nutzungsoberflächen, mit Hilfe derer die Betroffenen gewünschte Zugriffsbeschränkungen oder Freigaben erteilen können. Andere Ansätze bestehen in verschiedenen Arten der Anonymisierung der Daten, in der Verteilung des Wissens auf mehrere Parteien oder im Hinzufügen von „Rauschen" oder anderen Verschleierungsinformationen, damit die exakten Positionsdaten nicht offensichtlich sind. Spätestens beim Geotracking, also dem Nachverfolgen einer Person über einen gewissen Zeitraum, klappt es zumeist nicht, die anfallenden Daten so zu verschleiern, dass ein Anbieter von ortsbasierten Diensten kein genaues Bild über die Bewegung erhält (mit beschränktem Erfolg: Krumm 2009).

Der Dienst Google Latitude bietet Nutzern immerhin gewisse Datenschutzkonfigurationsmöglichkeiten dazu an, wie genau oder ungenau sie ihre Position für wen freigeben möchten. Nutzer können auch manuell einen Standort für die Darstellung bei ihren Freunden

eintragen, der nicht unbedingt der echte ist – die Information wird entsprechend als Selbstaussage gekennzeichnet. Natürlich besteht weiter das Risiko, dass der Anbieter die vollständigen Positionsdaten auswertet oder jemand Unberechtigtes Zugriff auf die beim Anbieter zwischengespeicherten Daten nimmt. Auf Nutzerseite ist jedoch noch ein ganz anderes Problem zu erwarten: Hat sich jemand für Google Latitude angemeldet und seine Freunde, den Ehepartner, die Eltern o.ä. über einen gewissen Zeitraum mit automatisch generierten Informationen zu seiner Position versorgt, wird er sich rechtfertigen müssen, sobald er seinen Standort nur noch unscharf oder gar nicht mehr offenbaren möchte.

6 Fazit und Ausblick

Mit der Zunahme von ortsbasierten Diensten über Smart Phones und soziale Netzwerke sind viele Nutzer bereit, ihre Positionsdaten gegenüber Freunden oder gar der gesamten Öffentlichkeit zu offenbaren. Die damit verbundenen Risiken sind ihnen zumeist nicht bewusst. Die Diskussion in den Medien über die Erweiterung von Apples Datenschutzerklärung um die automatische Übertragung von Standortdaten hat aber auch deutlich gemacht, dass Nutzer und Politiker besorgt sind, wenn exakte Positionsdaten in zentralen Datenbanken gesammelt werden, die dem Einflussbereich von Nutzern und europäischen Datenschutzaufsichtsbehörden faktisch entzogen sind.

Dass es sich bei Ortsinformationen um potenziell sensible Daten handelt, ist zwar in der akademischen Diskussion akzeptiert, hat jedoch bislang wenig Einfluss auf die Gestaltung von Technik gehabt. Schon 2003 warnten die Wissenschaftler Dobson und Fisher vor „Geoslavery“ („Geo-Sklaverei“: ein Master bestimmt die erlaubten Aufenthaltsorte und Bewegungen seiner Sklaven; Dobson/Fisher 2003). Ansätze dazu sind bei einigen Firmen gegenüber ihren Arbeitnehmern zu sehen. Zumindest für den Privatbereich ist das Schreckgespenst der „Geoslavery“ zwar (noch) nicht real, aber denkbar ist es schon, dass Navigationssysteme in Handys oder Fahrzeugen in Kürze die Route vorschlagen, an der die meisten Werbepartner sitzen, für die der Betroffene empfänglich sein könnte. Perfide wären Systeme, die Spielsüchtige stets am Casino vorbeileiten. Oder man würde alle ortsbasierten Dienste verpflichten, genau dies nicht zu tun, und ihnen dafür gar Datenbanken über alle Spielsüchtigen an die Hand geben, was wiederum einige Datenschutzimplikationen hätte.

Der Umgang mit Geolokalisierung und Geotracking verlangt nach einem gesellschaftlichen Diskurs, der national und international geführt werden muss. Insbesondere müssen juristische und technische Ansätze für Location Privacy im Sinne einer wirklichen Selbstbestimmung der Betroffenen und im Sinne eines Schutzes vor Diskriminierung mit soziologischen, ökonomischen und politischen Vorschlägen zusammengebracht werden. Gerade in Bezug auf die Ausbreitung von RFID und der Kopplung von Mobilfunk- und Internet-Diensten, die immer mehr eine Geolokalisierung der Betroffenen ermöglichen, sollten schnell Lösungen gefunden werden.

Literatur

(Beresford/Stajano 2003) Alastair R. Beresford, Frank Stajano: Location Privacy in Pervasive Computing, IEEE Pervasive Computing, 2(1):46-55, 2003.

(Dobson/Fisher 2003) Jerome E. Dobson, Peter F. Fisher: Geoslavery, IEEE Technology and Society Magazine, 22(1):47-52, 2003.

(Eagle et al. 2009) Nathan Eagle, Alex (Sandy) Pentland, David Lazer: Inferring friendship network structure by using mobile phone data, Proceedings of the National Academy of Sciences of the United States of America (PNAS), 106(36):15274-15278, 2009.

(Fritsch 2007) Lothar Fritsch: Privacy-Respecting Location-Based Service Infrastructures: A Socio-Technical Approach to Requirements Engineering, Journal of Theoretical and Applied Electronic Commerce Research 2(3):1-17, Dezember 2007.

(Gasson 2009) Mark Gasson (Hrsg.), FIDIS Deliverable D12.10: Normality Mining: Results from a Tracking Study, Frankfurt a.M., 2009. http://www.fidis.net/.

(Hansen/Meissner 2008) Markus Hansen, Sebastian Meissner: Identification and Tracking of Individuals and Social Networks using the Electronic Product Code on RFID Tags, in: Simone Fischer-Hübner et al. (Hrsg.): The Future of Identity in the Information Society, IFIP International Federation for Information Processing, Vol. 262, 2008, S. 143-150.

(Jandt 2007) Silke Jandt: Datenschutz bei Location Based Services – Voraussetzungen und Grenzen der rechtmäßigen Verwendung von Standortdaten, Multimedia und Recht (MMR) 2007, S. 74-78.

(Köhntopp 2010) Kristian Köhntopp: WLANs mappen, Blog-Eintrag vom 17. Mai 2010. http://blog.koehntopp.de/archives/2861-WLANs-mappen.html#extended.

(Krumm 2009) John Krumm: Realistic Driving Tracks for Location Privacy, in: Pervasive Computing, LNCS Vol. 5538, 2009, S. 25-41.

(Langheinrich 2009) Marc Langheinrich: Privacy in Ubiquitous Computing, in: John Krumm (Hrsg.): Ubiquitous Computing, CRC Press, 2009, S. 95-160.

(Royer et al. 2009) Denis Royer, André Deuker, Kai Rannenberg: Mobility and Identity. Chapter 5 in: Kai Rannenberg, Denis Royer, André Deuker (Hrsg.): The Future of Identity in the Ifnormation Society – Challenges and Opportunities, Springer, 2009, S. 195-242.

(Schnabel 2009) Christoph Schnabel: Datenschutz bei profilbasierten Location Based Services. Die datenschutzadäquate Gestaltung von Service-Plattformen für Mobilkommunikation, Dissertation an der Universität Kassel, Kassel University Press, 2009.

(Scipioni/Langheinrich 2010) Marcello Paolo Scipioni, Marc Langheinrich: I'm Here! Privacy Challenges in Mobile Location Sharing, in: Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Mai 2010, Helsinki, Finland.

(Steiniger et al. 2006) Stefan Steiniger, Moritz Neun and Alistair Edwardes: Foundations of Location Based Services, Lesson 1 CartouCHe 1 – Lecture Notes on LBS, V 1.0, 2006, Department of Geography, University of Zürich. http://www.geo.unizh.ch/~sstein/.

(ULD/TUD 2007) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Technische Universität Dresden: Verkettung digitaler Identitäten, Untersuchung für das Bundesministerium für Bildung und Forschung, 2007. https://www.datenschutzzentrum.de/projekte/verkettung/.

(White 2003) James White: People Not Places: A Policy Framework for Analyzing Location Privacy Issues, 2003. http://epic.org/privacy/location/jwhitelocationprivacy.pdf.

Michael Marc Maisch

Tracking im Internet zu Werbezwecken

A. Einleitung

In der US-amerikanischen Zeitung „The New Yorker“ erschien am 5. Juli 1993 ein Cartoon, der zwei Hunde zeigt. Der eine Hund, auf einem Bürostuhl vor einem PC sitzend, spricht zu dem anderen, auf dem Boden sitzenden und aufschauenden Hund. Unter der Zeichnung wurde ein heute legendärer Satz angeführt, der wie kein zweiter Debatten über Anonymität und informationelle Selbstbestimmung inspiriert hat: „On the Internet, nobody knows you’re a dog.“[1] Siebzehn Jahre später stellt sich die Lage anders dar: Das Nutzerverhalten wird gezielt aufgezeichnet und ausgewertet. Mit verschiedenen Methoden und technischen Hilfsmitteln wird eine hinreichende Identifizierung von Nutzern durch Telemediendiensteanbieter, Werbende, Arbeitgeber, Behörden und der Justiz angestrebt (sog. Tracking).

Die Zunahme von Tracking im Internet ist im Werbesektor bei zielgruppenspezifischer Werbung zu verzeichnen. Besonders der Einsatz neuer Methoden zur Identifikation einzelner Browser-Programme verdient eine datenschutzrechtliche Bewertung.

B. Darstellung der technischen Grundlagen

1. Werbung im Internet

Viele Informations- und Kommunikationsangebote im Internet stehen ihren Nutzern kostenlos zur Verfügung. Diese Dienste werden durch Werbung finanziert. Im Unterschied zu Printmedien und Rundfunk eröffnet sich dem Werbenden im Internet ein erheblich größerer Adressatenkreis. Die Möglichkeit interaktive, kontextbezogene oder individualisierte Werbung zu schalten, kommt noch hinzu.

Im Internet erfordert zielgruppenspezifische Werbung eine hinreichende Identifizierung des Nutzers. Bisher konzentrierte sich die technische Auswertung von Nutzerspuren im Internet auf IP-Adressen.[2] Beim Internetprotokoll (IP) handelt es sich derzeit um eine vierstellige Gerätekennung bspw. nach dem Muster 132.231.51.59, mit der ein am Internet angebundenes Gerät, sei es ein Server, PC, Laptop oder Smartphone, für den Austausch von Datenpaketen erreichbar ist. Statische IP-Adressen (bspw. bei DSL-Flatrates) können dauerhaft einen Anschluss adressierbar machen und werden daher überwiegend als personenbezogene Daten bewertet. Aus Kostengründen weisen die Internet-Service-Provider ihren Anschlussteilnehmern zumeist dynamische IP-Adressen zu, die sich bei jeder Einwahl ändern.[3]

Zur Optimierung von Websites und zur Auswertung des Nutzerverhaltens zu Werbezwecken bedienen sich Telemediendiensteanbieter bspw. der umstrittenen Software Google Analytics.

Dieser Beitrag zeigt auf, dass es auch andere Wege der Aufzeichnung und Auswertung von Nutzerverhalten im Internet gibt. Denn neben der Zuordnung von Nutzungsprofilen durch IP-Adressen, Cookies oder Spyware, besteht nach neuen Erkenntnissen auch die Möglichkeit aus der Konfiguration des Internetbrowsers eine eindeutige Kennzeichnung abzuleiten, die gleich dem menschlichen Fingerabdruck eine Zuordnung zu einer Identität erlaubt. Diese Kennung wird als Browser Fingerprint bezeichnet. Mit Hilfe dieser Daten kann daher nicht nur ein Browser, bzw. ein Rechner im Internet, unabhängig von anderen Daten und Hilfsmitteln zuverlässig wiedererkannt werden. Browser Fingerprinting ermöglicht eine erheblich genauere Identifikation einzelner Rechner, da hinter einer IP-Adresse, bspw. bei einem Universitätsnetzwerk, variable Nutzerzahlen verborgen sein können.

Die Erhebung, Verarbeitung und Nutzung der Browser Fingerprints und die Erstellung von telemedienrechtlichen Nutzungsprofilen werfen daher datenschutzrechtliche Fragen auf.

2. Behavioral Targeting

Zielgruppenspezifische Werbung im Internet ist kein Novum. In Deutschland ist der Umsatz mit Werbebannern, Pop-Ups und Streaming Ads im Internet im vergangenen Jahr im Vergleich zu 2008 um 17,8 Prozent auf 1,5 Milliarden Euro angestiegen.[4] Um das Interesse der Nutzer zu steigern, wird die Werbung zielgruppenspezifisch zugeschnitten. Dazu wird das Nutzerverhalten im Internet oder auf einem Webportal analysiert und zur Erstellung von Nutzer- und Nutzungsprofilen verarbeitet, sog. Behavioral Targeting.[5] Wer zum Beispiel häufig Informationen über Segelboote sucht, dem wird entsprechende Werbung zu Booten, Zubehör oder Modeartikeln präsentiert. Die Zuordnung dieser Profile setzt die Identifikation eines Nutzers voraus, um über ihn vorhandene Nutzer- und Nutzungsprofile abzurufen und anzuwenden. Der Nutzer kann über personenbezogene Daten oder technische Spuren im Internet identifiziert werden. Neben Namens- und Adressdaten können auch E-Mailadressen[6], IP-Adressen[7] und daraus abgeleitete Einwahlorte[8] oder Cookies[9] personenbezogene Daten sein. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Telemediendienste sind nur gem. §§ 11 ff. TMG zulässig.

3. Browser Fingerprint

Bei Browser Fingerprinting handelt es sich um eine Methode einen Browser eindeutig zu identifizieren. Dabei wird auf Daten zurückgegriffen, die von jedem Browser automatisch preisgegeben werden. Der Browser verrät permanent neben dem Host und der IP-Adresse die Browserversion, sog. User Agent String[10], Header

und Detailinformationen zu Plugins (Java, Quicktime etc.), Zeitzone, Monitorkonfiguration, Systemschriftarten, Konfiguration bzgl. Cookies und Supercookies[11]. Um aus der Kombination dieser browserspezifischen Daten einen eindeutigen Fingerabdruck des Browsers zu generieren, bedient man sich mathematischen Grundlagen der Informationstheorie. Eine Information wird darin als messbare, rein mathematische Größe betrachtet, ohne auf deren Bedeutung einzugehen.[12] Der Informationsgehalt einer Nachricht ist in der Informationstheorie eine Größe (sog. Entropie), die von der Wahrscheinlichkeit, mit der diese Nachricht auftritt, abhängt. Die Entropie wird in Bit gemessen. Dabei ist 1 Bit der Informationsgehalt, der in einer Auswahl aus zwei gleich wahrscheinlichen Möglichkeiten enthalten ist (n Bits = 2n verschiedene Zustände). Die Electronic Frontier Foundation[13] leitet aus dieser Informationstheorie ab, dass bei 7 Milliarden Menschen Weltbevölkerung ca. 33 Bits Entropie erforderlich sind, um eine unbekannte Person als bestimmte Person zu identifizieren ($\Delta S = - \log 2\ Pr(X=x)$).[14] Aus der Berechnung der Entropie jeder Browserinformation kann für den Einzelfall berechnet werden, wie einzigartig die Browserinformationen eines Nutzers sind. Somit kann ein einzelner Browser bzw. am Internet angeschlossener Rechner unabhängig von der IP-Adresse bestimmt oder bestimmbar identifiziert werden.[15]

Beispielsweise kann aus dem User-Agent-String (bspw.: „Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6“), der dem Server das Betriebssystem, Sprache, Sicherheitsprofil und Browserversion mitteilt, bereits eine Entropie von 10,5 Bits abgeleitet werden.[16] Die Browser Fingerprints können daher anstatt von oder zusätzlich zu Cookies oder IP-Adressen zur Zuordnung eines Internetnutzerkreises, der berechtigterweise über einen bestimmten oder bestimmbaren Browser surft, zu Nutzungsprofilen verwendet werden. Telemedienrechtlich ist daher bedeutsam, ob diese Fingerprints als personenbezogene Daten einzuordnen sind.

C. Telemediendatenschutzrechtliche Bewertung

Unter den Voraussetzungen des § 3 Abs. 1 BDSG handelt es sich um personenbezogene Daten, wenn Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person gegeben sind. Einzelangaben über persönliche und sachliche Verhältnisse sind Informationen, die einen, wie auch immer geartete Information über eine Person enthalten (bspw. innere oder äußerliche Merkmale, Vermögen, Motive etc.). Der Browser Fingerprint enthält die Information, dass ein bestimmter Browser von einer Person genutzt wird. Da Browser Fingerprints somit einen Aussagewert über eine Person enthält, handelt es sich um Einzelangaben. Ausschlaggebend ist ferner, ob die Einzelangaben einer bestimmten oder bestimmbaren Person zugeordnet werden können. Ersteres dürfte nur mit entsprechenden Hilfsmitteln[17] gelingen. Für die Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle[18] oder des legal verfügbaren Zusatzwissens[19] an. Der Personenbezug muss mit den der Stelle normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand durchgeführt werden können.

Im Unterschied zur Personalausweisnummer oder zur IP-Adresse besteht jedoch keine Möglichkeit seitens der verantwortlichen Stelle oder eines dazu berechtigten Dritten, den Fingerprint bspw. anhand einer Referenzdatei[20] einer bestimmten Person zuzuordnen. Eine Zuordnung ist ausschließlich in Verbindung mit Zusatzwissen über den Nutzer möglich.

Hier lässt sich eine Parallele zur Cookie-Problematik ziehen. Beim Personenbezug von Cookies ist entscheidend, welche Daten die Cookies im Einzelfall aufzeichnen und welche Daten dem Diensteanbieter bereits über den Nutzer zur Verfügung stehen. Stellt der Nutzer, auf dessen Festplatte ein Cookie abgelegt wird, für den Diensteanbieter bereits eine bestimmte oder bestimmbare Person dar, sind die Daten, die durch den Cookie gesammelt werden, ebenfalls personenbezogene Daten.[21] Personenbezogene Daten liegen insbesondere dann vor, wenn die durch den Cookie selbst übermittelten Informationen für sich genommen bereits einen Personenbezug enthalten. Keine personenbezogenen Daten liegen dagegen vor, wenn durch den Cookie nur Daten ohne Personenbeziehbarkeit übermittelt werden.[22]

Browser Fingerprints sind daher personenbezogene Daten, wenn der Nutzer für den Diensteanbieter bereits eine bestimmte oder bestimmbare Person darstellt, da über diesen Namens- und Adressdaten oder personenbezogenes Zusatzwissen aus Nutzer- oder Nutzungsprofilen wie die Browser History, Eingaben bei Suchmaschinen, Cookies oder die (statische) IP-Adresse verfügbar sind. Browser Fingerprints als browserspezifische Daten enthalten keine Namens- oder (IP-) Adressdaten, sodass sie für sich genommen keinen Personenbezug aufweisen.

Sind Browser Fingerprints demnach als personenbezogene Daten einzuordnen, ist eine Erstellung von Nutzungsprofilen für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien unter Zuhilfenahme dieser Daten nur zulässig, soweit es sich bei Browser Fingerprints um Nutzungsdaten gem. § 15 Abs. 1 TMG handelt. Nutzungsdaten sind personenbezogene Daten deren Erhebung und Verwendung erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen oder abzurechnen. Ist der Nutzer dem Diensteanbieter bekannt und handelt es sich bei den Fingerprints entsprechend um personenbezogene Daten, dann sind die Fingerprints dann Nutzungsdaten, soweit Informationen über die Hardwarekonfiguration und Browsereinstellungen für die Inanspruchnahme des Telemediums erforderlich sind. Diese darf der Diensteanbieter erheben und für Nutzungsprofile zur Verwendung von Pseudonymen zum Zweck der Werbung erstellten, sofern der Nutzer nicht widerspricht.

Abhängig vom vorhandenen Zusatzwissen können Browser Fingerprints personenbezogene Daten sein. In diesem Fall hat der Diensteanbieter den Nutzer auf sein Widerspruchsrecht im

Rahmen der Unterrichtung nach § 13 Abs. 1 TMG hinzuweisen. Ist allein der Browser Fingerprint bekannt, aus dem mit normalen Hilfsmitteln oder ohne unverhältnismäßigem Aufwand kein Personenbezug abgeleitet werden kann, handelt es sich nicht um personenbezogene Daten. In diesem Fall ist ein schrankenloser Einsatz für die Erstellung von Nutzungsprofilen denkbar.

D. Fazit

Jede IP-Adresse, jeder Cookie und jeder Browser und vielfach auch jedes Klickverhalten eines Nutzers im Internet wird heute aufgezeichnet und ausgewertet. E-Mails werden nach Stichworten zur kontextsensitiven Werbung durchsucht, Cookies auf individuelle Werbung hin ausgewertet. Was der Nutzer auch macht, wird heutzutage beobachtet und bewertet. Browser Fingerprinting ergänzt das Repertoire um eine sehr subtile und passive Tracking-Methode. Unter diesen Umständen würde Peter Steiner im Jahr 2010 nichts anders übrig bleiben, als zu konstatieren: „On the Internet, almost everybody knows you're a dog".

1 Dt. „Im Internet weiss niemand, dass Du ein Hund bist", Peter Steiner, The New Yorker, 05.07.1993.

2 Heckmann, in: jurisPK-Internetrecht, 2. Aufl. 2009, Kap. 1.15, § 15 TMG, Rn. 9.

3 Die eigene IP-Adresse mit Angaben zum Einwahlort kann durch Aufrufen der Website http://whatismyipaddress.com/ in Erfahrung gebracht werden.

4 Bitkom, Pressemitteilung v. 02.02.2010, http://www.bitkom.org/de/presse/8477_62318.aspx.

5 Heckmann in: jurisPK-Internetrecht, 2. Aufl. 2009, Kap. 1.11, § 11 TMG, Rn 8.

6 Schaffland/Wiltfang, BDSG, § 3, Rn. 5.

7 Statische IP-Adressen sind nach herrschender Literatur personenbezogene Daten. Die Einordnung dynamischer IP-Adressen wird auch von der Rechtsprechung unterschiedlich beurteilt, vertiefend Heckmann in: jurisPK-Internetrecht, 2. Aufl. 2009, Kap. 1.12, § 12 TMG, Rn. 28; Schöttler, AnwZert ITR 16/2008, Anm. 3.

8 Schaffland/Wiltfang, BDSG, § 3, Rn. 5; Zur Geolokalisation anhand von IP-Adressen einführend Backu, ITRB 2009, 88.

9 Entscheidend ist der Dateninhalt eines Cookies im Einzelfall, vgl. Heckmann in: jurisPK-Internetrecht, 2. Aufl. 2009, Kap. 1.12, § 12 TMG, Rn. 34.

10 Aufbau des User-Agent-Strings, vgl. http://www.firefox-browser.de/wiki/User_Agent.

11 Supercookies können Klickwege eines Nutzers auf eine Website dokumentieren, vlg. Söldner, PC-Welt, Beitrag v. 07.05.2006.

12 Klimant/Piotraschke/Schönfeld, Informations- und Kodierungstheorie, 2. Aufl. 2003, S. 10.

13 Electronic Frontier Foundation (EFF), http://www.eff.org/.

14 Eckersley, A Primer on Information Theory and Privacy, Beitrag v. 27.01.2010, https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy.

15 Der Browser Fingerprint kann getestet werden unter: https://panopticlick.eff.org/.

16 Ausführlich zur Informationstheorie und Browser Fingerprinting, s. Electronic Frontier Foundation, Projekt Panopticlick, https://panopticlick.eff.org/.

17 vgl. Projekt Panopticlick, Testversion unter https://panopticlick.eff.org/.

18 Gola in: Gola/Klug, BDSG, 9. Aufl. 2007, § 3, Rn. 10.

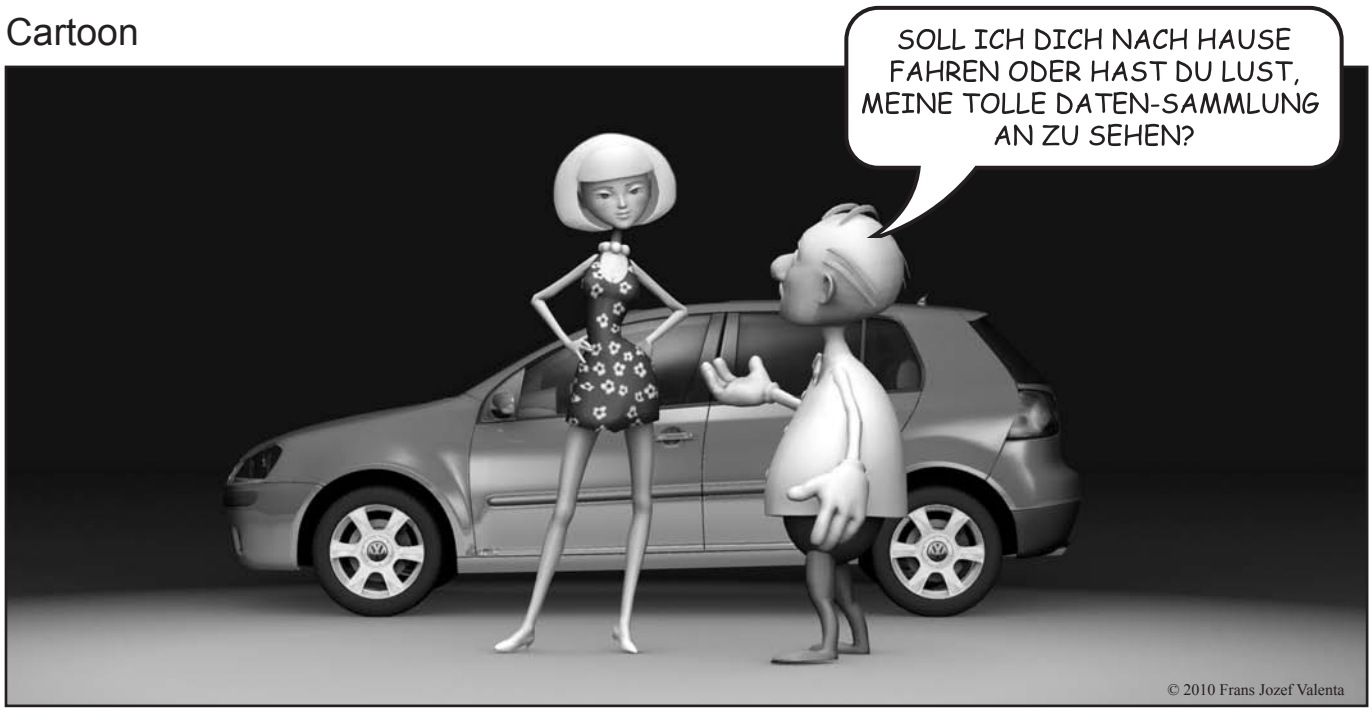
19 Dammann in: Simitis, BDSG, 6. Aufl., 2006, § 3 Rn. 37.

20 Heckmann in: jurisPK-Internetrecht, 2. Aufl. 2009, Kap. 1.15, § 15 TMG, Rn. 29.

21 Heckmann in: jurisPK-Internetrecht, 2. Aufl. 2009, Kap. 1.12, § 12 TMG, Rn. 34.

22 Heckmann in: jurisPK-Internetrecht, 2. Aufl. 2009, Kap. 1.12, § 12 TMG, Rn. 35.

Cartoon



Prof. Dr. Rainer Erd

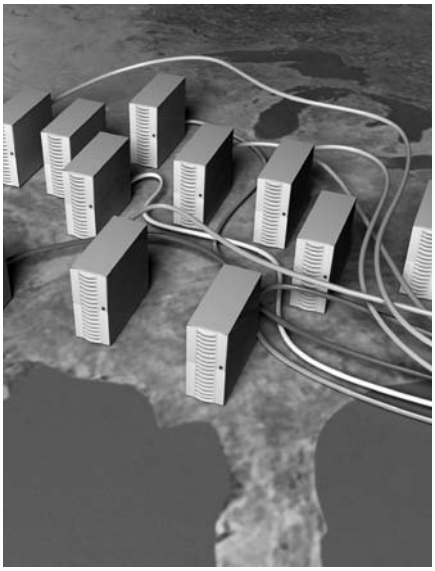
Deutsche Daten auf Geheimservern in den USA

Google und viele andere Internetunternehmen missachten internationale Abkommen*

Google ist der Lieblingsfeind der Datenschützer geworden. Zu Recht. Denn Google missachtet nahezu jede Regel, die das deutsche Datenschutzrecht vorsieht. Darüber ist viel geschrieben worden. Was bislang jedoch kaum öffentliche Beachtung gefunden hat, ist die Tatsache, dass der amerikanische Internetriese sämtliche in Deutschland erhobenen Daten in die USA übermittelt und dort auf Servern an geheim gehaltenen Orten speichert. Das wäre dann kein Problem, wenn in den USA dieselben Datenschutzregeln gelten würden wie in Deutschland. Das ist aber nicht so. Denn das amerikanische Datenschutzrecht gilt nur für bestimmte gesellschaftliche Gruppen (wie zum Beispiel für Kinder oder für Mitglieder einer Versicherung) und nicht – wie in Deutschland – für alle Bürger.

Um die Differenz zwischen dem kaum existenten amerikanischen und dem deutschen Datenschutzrecht zu überbrücken, hat der Gesetzgeber in Paragraph 4b Bundesdatenschutzgesetz eine Formulierung eingeführt. Dort heißt es, dass personenbezogene Daten nur in Länder übermittelt werden dürfen, die ein „angemessenes Datenschutzniveau" garantieren. Das tun die USA nicht. Um das datenschutzrechtliche Gefälle zwischen den USA und Europa auszugleichen, vereinbarten die EU-Kommission und das amerikanische Handelsministerium im Jahr 2000 das „Safe Harbor Abkommen". Es soll garantieren, dass alle ihm beigetretenen Unternehmen sich an die Regeln des europäischen, also auch des deutschen Datenschutzrechts halten. Google ist dem Abkommen beigetreten.

In seinen Datenschutzbestimmungen vom 11. März 2009 schreibt das amerikanische Unternehmen deshalb stolz: "Google erkennt an, dass Datenschutz wichtig ist (…) Google beachtet die Datenschutzbestimmungen der US Safe Harbor-Grundsätze zu Benachrichtigungen, Wahlrecht, Weiterleitung, Sicherheit, Datenintegrität, Zugriffsrechten und Durchsetzung und ist beim Safe Harbor-Programm des US-Handelsministeriums registriert". Der Nutzer von Google wähnt sich deshalb in einem „sicheren Hafen". Und nicht nur er, sondern alle Nutzer von Internetdiensten, die in den jeweiligen Datenschutzbestimmungen erfahren, dass ihr Dienst dem Abkommen beigetreten ist.



Doch der verbal so sichere Hafen ist in Wirklichkeit ein Sumpf voller Unsicherheiten. Anlässlich des zehnjährigen Bestehens des Abkommens hat im April dieses Jahres der Düsseldorfer Kreis, ein Zusammenschluss der Aufsichtsbehörden für den Datenschutz im privaten Bereich, eine Erklärung verfasst, die keinen Grund zum Feiern gibt. Die Erklärung, die von Misstrauen in das datenschutzadäquate Funktionieren des Safe Harbor Abkommens geprägt ist, weist darauf hin, dass deutsche Unternehmen, die Daten in die USA exportieren, sich nicht darauf verlassen sollen, dass die Behauptung des Datenimporteurs zutreffend ist, er habe sich einer Safe Harbor-Zertifizierung unterzogen. Deutsche Unternehmen, so verlangt der Düsseldorfer Kreis, sollen sich die Safe Harbor-Selbstzertifizierungen amerikanischer Unternehmen vorlegen und sich überzeugen lassen, dass die Grundsätze des Abkommens auch eingehalten werden.

In der Tat sind größte Zweifel angebracht, dass Unternehmen, die dem Safe Harbor Abkommen beigetreten sind, auch tatsächlich deutsches Datenschutzrecht beachten. Das hat eine in Deutschland kaum bekannte Untersuchung einer australischen Unternehmensberatung schon im Jahr 2008 festgestellt. Die „Galexia"-Studie zum „Safe Harbor Treatment" begründet mit umfangreichem Zahlenmaterial und überzeugenden Ausführungen die These, dass nur 3,4 Prozent der amerikanischen Unternehmen, die vorgeben, die Regeln des Safe Harbor Abkommens zu beachten, dies in Wirklichkeit auch tun. Das sind 53 von 1.570 Unternehmen.

Wenn das so ist, dann landet die Mehrheit der personenbezogenen Daten, die von Europa in die USA übermittelt werden, in keinem „sicheren Hafen", sondern bei Institutionen, die – wie in den USA üblich - regen internationalen Gebrauch von den Daten machen, ohne dass die betroffenen Personen in

** Der Erstabdruck des Beitrages findet sich in der Süddeutschen Zeitung vom 23.08.2010. Wir danken dem Autor und der Redaktion der Süddeutschen Zeitung für die Zustimmung zum Abdruck in der DANA.*

Europa dies wissen. Woher der indische Herrenschneider die E-Mail-Adresse hat, mit der er einen deutschen, gerade zugelassenen Rechtsanwalt bewirbt, kann man deshalb erahnen.

Warum die Zahl der Unternehmen, die europäische Regeln des Datenschutzes befolgen, so klein ist, liegt daran, dass viele der Unternehmen entgegen ihrer Angabe dem Safe Harbor Abkommen nicht beigetreten sind. Andere behaupten eine Zertifizierung nach den Anforderungen des Safe Harbor Abkommens durchgeführt zu haben, die aber nicht stattgefunden hat. Wiederum andere verwenden ohne Berechtigung selbstgefertigte Zertifikate. Manche veröffentlichen überhaupt keine Datenschutzerklärung („privacy policy"), die eine Überprüfung möglich macht. Google publiziert zwar umfangreiche Datenschutzbestimmungen, die aber – wie eine Veröffentlichung von „Öko-Test" im April dieses Jahres gezeigt hat - nicht im entferntesten deutschen Datenschutzregeln entsprechen.

Wesentlich für die Garantie eines effektiven Datenschutzes sind auch Verfahren der Konfliktlösung. Die „Galexia"-Studie hat gezeigt, dass in den wenigsten Fällen angeblich zertifizierte amerikanische Unternehmen solche anbieten, in denen die Verbraucher angemessen vertreten sind. Unter diese Kategorie fällt auch Google. Wer überprüft wissen will, was mit seinen von Google gespeicherten und in die USA übermittelten Daten geschieht, sieht sich an eine amerikanische Adresse verwiesen, von der er – wenn überhaupt - keine adäquate Antwort erhält.

Zu allen bisher gegen Google und andere soziale Netzwerke (wie z. B. Facebook) zu Recht vorgetragenen kritischen Argumenten ist eines hinzuzufügen. Der Verweis darauf, dass ein Unternehmen dem „Safe Harbor Abkommen" beigetreten ist, will Vertrauen suggerieren, sollte aber das Gegenteil tun. So verdienstvoll die Verabschiedung des Abkommens zwischen der EU-Kommission und dem amerikanischen Handelsministerium war, so wenig effektiv ist seine Umsetzung. Wer „safe harbor" liest, sollte eher an ein unsicheres Gewässer denken, in dem personenbezogene Daten in einem intransparenten Sumpf verschwinden.

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (Düsseldorfer Kreis) am 28./29. April 2010 in Hannover

Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens" (Safe Harbor).[1] Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Die FTC veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Habor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifzierungungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, wann die Safe Habor-Zertifizierung des Importeurs erfolgte. Eine mehr als sieben Jahre zurückliegende Safe Habor-Zertifizierung ist nicht mehr gültig. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor[2] gegenüber den von der Datenverarbeitung Betroffenen nachkommt. Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.

Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren.

Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.

1 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, S. 7.

2 Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Manfred von Reumont

Ambulante Hospizvereine und Datenschutz

In Zeiten einer zunehmend älter werdenden Bevölkerung gewinnt das Hospizwesen auch in Deutschland immer mehr an Bedeutung.

Ein „Hospiz“ (lat. hospitium = Herberge) war ursprünglich eine Herberge für Pilger, Fremde, Bedürftige oder Kranke und ist der heutigen Bedeutung nach eine Einrichtung der Pflege, Beratung, Betreuung, Unterstützung und Begleitung für Schwerstkranke und Sterbende, sowie für Angehörige. Nach deren Bedürfnissen richten sich vielfältige Angebote, die von ambulanten, teilstationären und stationären Hospiz- und Palliativeinrichtungen in unterschiedlichsten Organisationsformen und von verschiedensten Trägern erbracht werden.

Hier verrichten ehrenamtliche Helfer einen Dienst am Mitmenschen, der Achtung und höchsten Respekt verdient.

Obwohl Umsetzungsaspekte des Datenschutzes in allen bestehenden Organisationsformen bedacht werden müssen, soll in diesem Artikel speziell auf die ambulanten Hospizvereine und deren Umgang mit dem Datenschutz eingegangen werden. Die Zahl solcher Dienste steigt kontinuierlich an. Waren 1996 noch lediglich 451 Dienste verzeichnet, zählte man 2002 schon derer 1156 und im Jahre 2008 schließlich 1500 (Quelle: Wegweiser Hospiz und Palliativmedizin und DHPV).

Als Träger ambulanter Hospize fungieren in Deutschland Kirchen (Diakonie, Caritas), gemeinnützige Organisationen und Stiftungen, aber auch gemeinnützige Vereine.

Letztere gründen sich nach dem deutschen Vereinsrecht, i.d.R. als eingetragene Vereine, verfügen über Vorstand und Mitgliederversammlung als Organe, eine Satzung und sind als gemeinnützig anerkannt.

Organisation und Arbeit eines ambulanten Vereins sind definiert in § 39 a SGB V in Verbindung mit der daraus entstandene Rahmenvereinbarung zwischen dem „Spitzenverband Bund der Krankenkassen gem. § 217 a SGB V“ und den Trägern der Hospizarbeit, u.a. der Arbeiterwohlfahrt, der Caritas, dem Deutschen Hospiz- und Palliativ-Verband, dem Deutschen Paritätischen Wohlfahrtsverband, dem DRK und dem Diakonischen Werk.

In der Rahmenvereinbarung sind die Voraussetzungen für die Förderung der Hospizvereine durch die Krankenkasse sowie Inhalt, Qualität und Umfang der ambulanten Hospizarbeit festgelegt.

Ein ambulanter Hospizdienst muss demnach mindestens eine fest angestellte, fachlich verantwortliche Kraft („Koordinator/in“) beschäftigen, die bestimmte Voraussetzungen vor Aufnahme ihrer Tätigkeit erfüllen muss. Dazu gehören unter anderem eine abgeschlossene Palliative-Care-Weiterbildungsmaßnahme, ein 40stündiges Koordinatoren-Seminar und ein 80stündiges Seminar zur Führungskompetenz. Weiterhin ist in den Vorschriften geregelt, dass

- die Krankenkasse ambulante Hospizdienste durch einen angemessenen Zuschuss zu den notwendigen Personalkosten fördern muss,
- der ambulante Hospizdienst die Gewinnung, Schulung, Koordination und Unterstützung der ehrenamtlich tätigen Personen („Helfer/innen“), die für die Sterbebegleitung zur Verfügung stehen, sicherstellen muss und
- der ambulante Hospizdienst mit palliativmedizinisch erfahrenen Pflegediensten und Ärzten zusammenarbeitet.

Diese und weitere Bestimmungen wirken sich unmittelbar auf Vorstandsentscheidungen aus. So hat der Vorstand die Auswahl der Fachkraft sorgfältig zu treffen, die Ausbildung der ehrenamtlichen Helfer/innen durch die Fachkraft

zu organisieren und durchzuführen und im Rahmen der Weiterbildung die Teilnahme an Supervisionen sicherzustellen.

Der kundige Leser erkennt schon jetzt, dass bei dem beschriebenen Konstrukt eine Reihe personenbezogener Daten anfallen. Betroffene sind sowohl die Mitglieder des Vereins, die die satzungsgemäßen Vereinsziele durch ihren Mitgliedsbeitrag fördern, als auch die Helfer/innen und deren Koordinator/in und natürlich die Patienten und deren Angehörige. Vor allem die Daten letzterer sind als Gesundheitsdaten i.S. des § 3 Abs. 9 BDSG besonders sorgfältig vor unberechtigtem Zugriff zu schützen.

Zum Umgang mit diesen Daten bestehen einerseits spezialgesetzliche Vorgaben, die beispielsweise zur Durchführung der Abrechnung bestimmte Datenübermittlungen an Leistungsträger (Krankenkassen) erfordern. Andererseits richtet sich der datenschutzkonforme Umgang mit diesen Daten, soweit es keine konkreten gesetzlichen Vorgaben gibt, nach den allgemeinen, im BDSG gefassten Auffangregeln.

Leider kann man beobachten, dass – wie übrigens vielfach im nicht-öffentlichen Bereich – die Datenschutz-Vorschriften kaum bekannt sind und daher nicht beachtet werden. Insbesondere trifft dies für die Verarbeitung besonderer Arten personenbezogener Daten durch Koordinator/in, Helfer/innen und das für die Zuschussbeantragung zuständige Vorstandsmitglied zu.

Da auf eine Vorabkontrolle nach § 4 d Abs. 5 BDSG durch eine förmliche Einwilligung und/oder die Begründung eines rechtsgeschäftsähnlichen Schuldverhältnisses verzichtet werden kann, könnte eine Einwilligung in die am Anfang der Betreuung stehende Pflegevereinbarung integriert werden. Schon die Gestaltung beider Rechtsakte dürfte einem Datenschutzunkundigen schwer fallen.

Eine dem besonderen Schutzbedarf angemessene Gestaltung der IT-Infrastruktur, der Berechtigungsgestaltung und ganz allgemein der Auswahl angemessener Schutzmaßnahmen im Sinne von § 9 BDSG unterbleibt häufig aufgrund mangelnden technischen Verständnisses. Es kann aber nicht hingenommen werden, dass Patientendaten auf unprofessionelle und nachlässige Weise auf halbherzig eingerichteten IT-Systemen verarbeitet werden, die auch noch ans Internet angeschlossen und dadurch zusätzlichen Gefahren ausgesetzt sind. In dieser Frage muss, bei aller Sympathie für ehrenamtliches Engagement, ein absolut professioneller Umgang mit der IT-Infrastruktur gefordert werden, der dem Schutzbedürfnis der betroffenen Patienten gerecht wird.

Selbst wenn ein Verein zunächst mit einem Laptop oder einem einzelnen privaten Rechner beginnt, muss einer möglichen, späteren Ausweitung der automatisierten Datenverarbeitung Rechnung getragen werden.

Leider bleiben selbst grundlegende, wörtlich aus dem Gesetz abzulesende Datenschutzpflichten häufig unerfüllt. So finden sich unter den ambulanten Hospizvereinen nur wenige, die einen Datenschutzbeauftragten (DSB) bestellt haben, deren Helfer/innen und Vorstandsmitglieder auf das Datengeheimnis verpflichtet sind und die eine Übersicht nach § 4 g Abs. 2 BDSG erstellt haben und für eine Veröffentlichung („öffentliches Verfahrensverzeichnis“) auf Antrag verfügbar halten. Auch eine Datenschutzerklärung auf der Website, die über die üblichen, nichtssagenden Disclaimer hinausgeht und tatsächlich eine hinreichende Erklärung des realisierten Datenschutzmanagements darstellt (auch wenn dieses nur rudimentär die notwendigen Schutzmaßnahmen beinhaltet), ist kaum zu finden.

Selbst wenn das Quorum von mindestens zehn mit der Datenverarbeitung beschäftigten Personen nicht erreicht wird, ein DSB also nicht bestellt werden muss, bedeutet dies keinen Freibrief für jegliche Verarbeitung personenbezogener Daten. Vielmehr muss in diesem Fall der Leiter der verantwortlichen Stelle selbst für eine angemessene Datenschutzorganisation und die Einhaltung aller einschlägigen Vorschriften sorgen. Dass gem. § 4 g Abs. 2 a BDSG der Vorsitzende eines Vereins in diesem Fall die Erfüllung der Aufgaben des DSB sicherzustellen hat, wird i.d.R. nicht beachtet oder ist schlicht unbekannt.

Verbände und Organisationen des Hospizwesens auf Bundes-, Landes- oder Kommunalebene, die ja gerade damit werben, dass sie örtliche ambulante Hospizvereine bei deren Gründung beraten und unterstützen, könnten hier eine Lücke schließen. Leider schließt die angebotene Beratung bisher offensichtlich keinerlei Unterstützung bei der datenschutzgerechten Gestaltung der Vereinsarbeit ein. Offenbar besteht auch hier noch nicht die ausreichende Sensibilität. Gelegentliche Hinweise des Autors in diese Richtung fanden bisher kaum Widerhall. Vielmehr wird auf eine allgemeine Schweigepflicht verwiesen.

Es ist jedoch aus unterschiedlichen Gründen notwendig, dass der Umgang mit Datenschutzfragen auch bei ehrenamtlicher Tätigkeit professionalisiert wird. Zur Wahrung der Menschenwürde der Patienten, dem Grundgedanken des Hospizwesens, gehört eben auch ein die Persönlichkeitsrechte wahrender Umgang mit Patientendaten. Und darüber hinaus wäre es das falsche Signal, wenn ausgerechnet Hospize wegen Datenschutzverstößen ins Gerede kämen. Wir haben schon genug Datenschutzskandale!

Die ehrenamtlich tätigen Hospizhelfer/innen haben es nicht verdient, dass ihr aufopferungsvoller Einsatz durch mangelnde Datenschutzorganisation in der Öffentlichkeit diskreditiert wird.

Eine offensive, transparente und bewusste Umsetzung von Datenschutzvorgaben, gerade im hochsensiblen Bereich des Hospizwesens, würde zusätzlich Vertrauen bei denjenigen schaffen, die für einen Partner oder einen Angehörigen eine vertrauenswürdige Organisation für die Betreuung suchen und dabei das Recht auf informationelle Selbstbestimmung für beide Seiten gewahrt wissen wollen.

Übrigens: Den genannten Organisationen wurde vor Veröffentlichung dieser Artikel mit der Bitte um Stellungnahme zugeleitet, da möglicherweise – für den Außenstehenden nicht erkennbar – Maßnahmen zur Initiierung eines „Datenschutzminimum“ schon eingeleitet oder zumindest vorbereitet sind: Keine Antwort, kein Kommentar, keine Äußerung, deren Inhalt an dieser Stelle dargestellt werden sollte...

§ 39a SGB V
Stationäre und ambulante Hospizleistungen

(1) Versicherte, die keiner Krankenhausbehandlung bedürfen, haben im Rahmen der Verträge nach Satz 4 Anspruch auf einen Zuschuß zu stationärer oder teilstationärer Versorgung in Hospizen, in denen palliativ-medizinische Behandlung erbracht wird, wenn eine ambulante Versorgung im Haushalt oder der Familie des Versicherten nicht erbracht werden kann. Die Höhe des Zuschusses ist in der Satzung der Krankenkasse festzulegen. Er darf kalendertäglich 6 vom Hundert der monatlichen Bezugsgröße nach § 18 Abs. 1 des Vierten Buches nicht unterschreiten und unter Anrechnung der Leistungen anderer Sozialleistungsträger die tatsächlichen kalendertäglichen Kosten nach Satz 1 nicht überschreiten. Die Spitzenverbände der Krankenkassen gemeinsam und einheitlich vereinbaren mit den für die Wahrnehmung der Interessen der stationären Hospize maßgeblichen Spitzenorganisationen das Nähere über Art und Umfang der Versorgung nach Satz 1; der Kassenärztlichen Bundesvereinigung ist Gelegenheit zur Stellungnahme zu geben.

(2) Die Krankenkasse hat ambulante Hospizdienste zu fördern, die für Versicherte, die keiner Krankenhausbehandlung und keiner stationären oder teilstationären Versorgung in einem Hospiz bedürfen, qualifizierte ehrenamtliche Sterbebegleitung in deren Haushalt oder Familie erbringen. Voraussetzung der Förderung ist außerdem, dass der ambulante Hospizdienst

1. mit palliativmedizinisch erfahrenen Pflegediensten und Ärzten zusammenarbeitet sowie

2. unter der fachlichen Verantwortung einer Krankenschwester, eines Krankenpflegers oder einer anderen fachlich qualifizierten Person steht, die über mehrjährige Erfahrung in der palliativmedizinischen Pflege oder über eine entsprechende Weiterbildung verfügt und eine Weiterbildung als verantwortliche Pflegefachkraft oder in Leitungsfunktionen nachweisen kann.

Der ambulante Hospizdienst erbringt palliativpflegerische Beratung durch entsprechend ausgebildete Fachkräfte und stellt die Gewinnung, Schulung, Koordination und Unterstützung der ehrenamtlich tätigen Personen, die für die Sterbebegleitung zur Verfügung stehen, sicher. Die Förderung nach Satz 1 erfolgt durch einen angemessenen Zuschuss zu den notwendigen Personalkosten, der sich insbesondere nach dem Verhältnis der Zahl der qualifizierten Ehrenamtlichen zu der Zahl der Sterbebegleitungen bestimmt. Die Ausgaben der Krankenkassen für die Förderung nach Satz 1 sollen insgesamt im Jahr 2002 für jeden ihrer Versicherten 0,15 Euro umfassen und jährlich um 0,05 Euro bis auf 0,40 Euro im Jahr 2007 ansteigen; dieser Betrag ist in den Folgejahren entsprechend der prozentualen Veränderung der monatlichen Bezugsgröße nach § 18 Abs. 1 des Vierten Buches anzupassen. Die Spitzenverbände der Krankenkassen gemeinsam und einheitlich vereinbaren mit den für die Wahrnehmung der Interessen der ambulanten Hospizdienste maßgeblichen Spitzenorganisationen das Nähere zu den Voraussetzungen der Förderung sowie zu Inhalt, Qualität und Umfang der ambulanten Hospizarbeit.

Abschließend ein herzliches Dankeschön an Frau K. Schuler, die mit einem Review und wertvollen Ergänzungen an diesem Artikel mitgewirkt hat.

Manfred von Reumont berät u.a. einen ambulanten Hospizverein in datenschutzrechtlichen Fragen durch Wahrnehmung der Aufgaben eines externen DSB.

transparenz . arbeit . kontrolle

FIfF DVD Deutsche Vereinigung für Datenschutz e. V.

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

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

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

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

http://www.fiff.de/2010

Großdemonstration „Freiheit statt Angst“ 2010 in Berlin

Etwa 7500 Demonstranten bekundeten am 11. September 2010 in Berlin ihren Unmut über staatliche Eingriffe in Bürgerrechte und Datenschutz.

Padeluun, FoeBuD e.V. und Arbeitskreis Vorratsdatenspeicherung:

„Ja, jetzt ist der 11. September. Hier stehen tausende auf dem Potsdammer Platz. Tausende Menschen, die trotz der vielen Erfolge, die unsere Bewegung bereits erreicht haben, wissen: Man muss hartnäckig sein – man muss immer wieder kommen.“

Anne Roth, Journalistin und Netzaktivistin:

„Der Hau-Drauf-Schäuble ist weg und stattdessen haben wir einen Schäuble im Schafspelz. De Maizière sagt die richtigen Sachen, hält netzpolitische Dialoge ab, es gibt eine Internet-Enquetekommission im Bundestag. Die Qualitätsmedien laufen ihm nach wie die Dackel und plötzlich sind alle gegen Google-Streetview.
Aber auch er will die Vorratsdatenspeicherung, europäische Datensammlungen, Bankdatenaustausch, mehr Bundeswehr im Inneren. Auch er will Gesetze verschärfen, weil angeblich die Gewalt gegen die Polizei zunimmt – dabei ist das überhaupt nicht belegbar. Zuletzt hat er angekündigt, die vom Grundgesetz gebotene Trennung zwischen Polizei und Geheimdiensten aufzuweichen.“

Frank Bsirske, Vorsitzender der Vereinigten Diestleistungsgewerkschaft ver.di:

„Seit zwei Wochen liegt jetzt ein Gesetzentwurf zum Beschäftigtendatenschutz vor. Das ist zunächst einmal zu begrüßen, ebenso wie das im Entwurf vorgesehene Verbot heimlicher Videoaufnahmen. Dem stehen jedoch auf der Negativseite weitreichende neue Erhebungs-, Kontroll- und Überwachungsbefugnisse gegenüber, die den Arbeitgebern eingeräumt werden, bis hin zu der Befugnis, Daten von ausschließlich dienstlich genutzten Kommunikationsdiensten mit samt den Inhaltsdaten von E-Mails für stichprobenartige Leistungs- und Verhaltenskontrollen zu verwenden. Damit nicht genug: Die Bundesregierung eröffnet auch neue Möglichkeiten zur Datenerhebung ohne Kenntnis der Beschäftigten. „Zur Verhinderung von Straftaten und anderen schwerwiegenden Pflichtverletzungen“ wie es heißt – auf bloßen Verdacht hin. Arbeitgebern werden hierdurch Möglichkeiten eingeräumt, die bisher staatlichen Strafverfolgungsbehörden vorbehalten waren.“

Martin Grauduszus, Präsident der Freien Ärzteschaft:

„Die eCard ist, so schrieb es in der vergangenen Woche eine große westdeutsche Zeitung „schlimmer als die Google-Krake“!
Der gläserne Patient, der Datenkörper Mensch verkommt – staatlich gewollt – zur Verfügungsmasse! Und Behörden, Versicherungen und nicht zuletzt die Gesundheitsindustrie mit ihrer Maxime der industrialisierten Gesundheitsversorgung erfreuen und bereichern sich an dieser gigantischen Vernetzung!
Welch ein Szenario: der Arbeitgeber sortiert per Mausklick seinen Mitarbeiter aus, der sich in nervenärztlicher Behandlung befindet, Versicherungen selektieren via Bildschirm ihre Kunden und der Aids-Patient ist im Netz dem allgemeinen Begaffen ausgeliefert.“

Dr. Patrick Breyer, Arbeitskreis Vorratsdatenspeicherung:

„Wir denken heute an die Opfer des Anschlags von vor neun Jahren. Massenmord und Gewalt haben nichts mit „Freiheit statt Angst“ zu tun, sondern mit Angst durch Freiheit, nämlich der Erzeugung von Angst durch den Missbrauch unserer Freiheit. Deswegen muss natürlich mit rechtsstaatlichen Mitteln gegen die Täter und Planer solcher Terroranschläge vorgegangen werden. Es ist überhaupt keine Frage, ob man auf solche Verbrechen reagiert, sondern ob man richtig und intelligent darauf reagiert. Und da ist ganz klar: Der Einsatz verbrecherischer Mittel wird nicht dadurch richtig, dass er von einer gewählten Regierung ausgeht..“

Prof. Dr. Rosemarie Will, Vorsitzende der Humanistischen Union:

„Für uns als Bürgerrechtsorganisation ist das Recht ein wichtiges Instrument, um unsere Ansprüche auf ein freiheitliches und selbstbestimmtes Leben durchzusetzen. Dabei dürfen wir uns jedoch nicht auf die Gerichte allein verlassen, wenn es um den Schutz unserer Privatsphäre geht. Die Hoffnung, dass Richterinnen und Richter uns vor übermäßiger Überwachung beschützen könnten, wurde schon häufig getrübt. Leider auch bei der Entscheidung zur Vorratsdatenspeicherung: Im berühmten Volkszählungsurteil von 1983 hatte es noch geheißen, dass eine pauschale Datensammlung, eine Datensammlung ohne konkreten Verdacht auf Vorrat verfassungswidrig ist. Der Staat sollte keine Informationen über uns erfassen, wenn wir nicht wissen, ob und wofür diese Daten später einmal benutzt werden. Genau das ist mit der Entscheidung doch passiert. Zwar gab das Verfassungsgericht der Massenbeschwerde des AK Vorrat statt – darüber haben wir uns gefreut. Doch dieser Sieg hat einen bitteren Beigeschmack. Das Gericht hat nicht gesagt, dass die Vorratsdatenspeicherung an und für sich verfassungswidrig ist. Es ließ eine Hintertür offen, wonach eine verfassungskonforme Vorratsdatenspeicherung möglich sein kann.“

Monty Cantsin, Hedonistische Internationale:

„Während der Innenminister seine Thesen säuselt und Frau Aigner ihrem Pseudo-Aktionismus frönt, werden die Projekte der Sicherheitsfreaks – und die sitzen nicht nur im BKA, dem Bund deutscher Kriminalbeamter und den Polizeigewerkschaften – nein sie sitzen auch in der Regierung und den Ministerien und die treiben diese Projekte wie eh und je voran. Die gute alte Salamitaktik gibt es immer noch. Sie sieht nur ein bisschen mehr nach Feinkost statt nach Aldi-Billigware aus.
Die Bundesregierung ist also gut von PR-Agenturen beraten worden. Sie haben aus Stasi 2.0 und Zensursula gelernt. Sie haben gesehen, dass wir hier mit unseren Demos, Aktionen, Petitionen und Blogs ganz schön Alarm machen können. Sie haben gesehen, dass wir Menschen mit Argumenten überzeugen und Ministerinnen einen neuen Namen verpassen können. Sie haben gesehen, dass wir Politik machen. Und, das gefällt ihnen nicht.
Und deswegen wird jetzt ein milderer Ton angeschlagen. Da wird der Nacktscanner zum Körperscanner und der Innenminister zum Freund des demokratischen Dialogs. Das ist gefährlich, weil so für viele Bürgerinnen und Bürger nicht mehr deutlich wird, in welche Richtung sich dieser Staat eigentlich entwickelt.“

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund

Anonyme Bewerbungen in Erprobung

Die Antidiskriminierungsstelle des Bundes im Familienministerium hat fünf große Unternehmen in Deutschland für ein im Herbst 2010 beginnendes Projekt gewinnen können, Bewerbungen ohne Alter, Namen und Foto entgegenzunehmen. Dies sind der Kosmetikkonzern L´Oréal, der Haushaltswarenriese Procter&Gamble, der Geschenkedienstleister Mydays, die Deutsche Telekom und die Deutsche Post. Bei den drei deutschen Firmen handelt es sich um Dax-Unternehmen; die beiden anderen sind internationale Konzerne. Durch diesen Pilotversuch mit anonymisierten Bewerbungen sollen sich z.B. für türkischstämmige BewerberInnen bessere Chancen eröffnen. Neben der Bekämpfung ethnischer Benachteiligungen zielt das Projekt auch auf eine Besserbehandlung älterer Menschen. Die Leiterin der Antidiskriminierungsstelle Christine Lüders hat das Vorhaben initiiert: „Ich bin mir sicher, dass dies gegen Benachteiligung bei der Stellensuche hilft, beispielsweise bei Migranten oder Frauen mit Kindern.“ In anderen Ländern wie den USA habe man bereits gute Erfahrungen mit weitgehend anonymen Bewerbungen gesammelt.

Geplant ist, dass JobinteressentInnen in ihren Bewerbungsunterlagen Angaben weglassen sollen oder diese Daten vor der Entscheidung aus den Unterlagen entfernt werden. Getilgt werden sollen folgende Angaben: Namen, Geschlecht, Alter, Familienstand, Religion, Nationalität und mögliche Behinderung. Es geht Lüders darum, dass bestimmte Gruppen nicht bereits in der ersten Bewerbungsrunde, also noch vor der Einladung zu einem Bewerbungsgespräch, „durchs Raster fallen“. Die Anonymität wird beim Bewerbungsgespräch, das nach wie vor stattfinden soll, aufgehoben. Auch der nordrhein-westfälische Arbeits- und Integrationsminister Guntram Schneider (SPD) kündigte an, in der Verwaltung anonymisierte Bewerbungen einführen zu wollen. Dieses Projekt soll in den Pilotversuch eingebunden werden. Das auf ein Jahr angelegte Pilotprojekt wird wissenschaftlich begleitet vom Bonner Institut zur Zukunft der Arbeit (IZA). Dort trägt man auch Erfahrungen mit anonymen Bewerbungen aus anderen Ländern zusammen. Die längste Erfahrungen liegen aus den USA vor, wo diese Vorgehensweise schon in den 60er Jahren aufkam, als verschiedene Gesetze gegen Diskriminierung in Kraft traten. In den USA gibt es keine verpflichtenden Gesetze zu anonymen Bewerbungen. Doch sprechen US-Gerichte Diskriminierten mitunter hohe Millionensummen als Entschädigung zu.

Der Personal-Geschäftsführer der Deutschen Telekom Kundenservice GmbH Martin Seiler nennt sein Ziel, „die personellen Monokulturen aufzubrechen. Gerade angesichts des Fachkräftemangels können wir es uns nicht leisten, den Bewerbungspool durch Vorurteile von vornherein einzugrenzen.“ Der Deutsche Gewerkschaftsbund (DGB) begrüßte die Pläne, so die Leiterin der DGB-Rechtsabteilung Helga Nielebrock. Damit könne man Diskriminierung von vornherein verhindern. Der Schwerpunkt werde mehr auf Qualifikation und Eignung gelegt, nicht auf unerwünschte Kriterien.

Patrick Adenauer, Präsident des Verbandes Die Familienunternehmer warnte dagegen: „Unternehmen benötigen die Angaben von Alter und Geschlecht, weil dies für die Vergabe der meisten Arbeitsplätze von entscheidender Bedeutung ist. Bewerbungsunterlagen, die Arbeitssuchende fast völlig unkenntlich machen, verteuern die Personalsuche und Einstellungen ganz erheblich. Auswahlverfahren ohne Informationen zu Alter und Geschlecht erforderten „unzählige zusätzliche Bewerbungsgespräche und Nachfragen“. Vorschriften dazu mündeten in „ein großes Arbeitsbeschaffungsprogramm für Headhunter und Zeitarbeitsagenturen“. Durch die Verlängerung des Verfahrens würde den Bewerbenden selbst geschadet. Der Arbeitgeberverband BDA kritisierte, durch die anonymisierten Bewerbungen würden die Bemühungen der Unternehmen um Vielfalt in den Belegschaften konterkariert. Denn dann könnten Arbeitgeber zu Vorstellungsgesprächen nicht mehr gezielt Frauen oder Bewerbende mit ausländischen Wurzeln einladen. Dass mit dem Instrument ein real existierendes Problem angegangen werden soll, zeigt eines Studie der Universität Konstanz vom Februar 2010: Die Forschenden hatten mehr als 1.000 Bewerbungen auf Praktikumsstellen für Wirtschaftsstudierende verschickt mit inhaltlich gleichwertigen Unterlagen, denen per Zufall eindeutig deutsch oder türkisch klingende Namen zugeordnet wurden. Bewerbende mit türkischen Namen erhielten insgesamt 14% weniger positive Antworten; kleinere Firmen luden sie sogar zu 24% seltener zum Vorstellungsgespräch ein (SZ 03./04.07.2010, V2/9; Preuß SZ 04.08.2010, 1, 4, 5; SZ 05.08.2010, 18; Kuhr SZ 25.08.2010 1, 6; zu Frankreich vgl. DANA 1/2005, 24).

Bund

Bericht über Videoüberwachung

Gemäß einem Bericht der Bundesregierung auf eine kleine Anfrage der Linksfraktion werden bundesweit an rund 300 Bahnhöfen etwa 3.000 Videokameras zur Überwachung eingesetzt. Es wurden mehr als 12 Millionen Euro an Fördergeldern für die

Erforschung der Videoerkennung ausgegeben. Die Antwort teilt mir, dass das Bundeskriminalamt seit 2001 insgesamt 42 Personen zur „Verhinderung oder Aufdeckung terroristischer Straftaten und terroristischer Aktivitäten“ mit Kameras überwacht hat. Dazu kommen 794 vom Bundesverfassungsschutz per Video überwachte Personen aus dem „Bereich des islamistisch motivierten Terrorismus“. In wie vielen Fällen so Straftaten verhindert wurden, konnte die Regierung nicht sagen. Eine „statistisch erfassbare, ‚wesentliche‘ Kausalität“ sei „kaum darstellbar“, was vom Linken-Bundestagsabgeordneten Jan Korte kritisiert wird: „Entweder ist die Videoüberwachung erfolgreich, dann sollte die Bundesregierung benennen können, wo was verhindert oder aufgeklärt werden konnte. Wenn sie das nicht kann, soll sie auch endlich damit aufhören, die Videoüberwachung als unverzichtbares Instrument zu propagieren.“ Die Regierung verweigerte eine Aufschlüsselung der 3.000 auf Bahnhöfen eingesetzten Kameras nach Bundesländern, da dies das „Staatswohl“ gefährden würde - eine Ansicht, die der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, nicht teilt. Er hielte sogar die Nennung der einzelnen Bahnhöfe und die Zahl der jeweils eingesetzten Kameras für unproblematisch. Dies würde „zu keiner Gefährdung der öffentlichen Sicherheit“ führen (Schmidt, www.taz.de 17.08.2010; BT-Drs. 17/2349 - 18 Seiten).

Bund

Skimming nimmt weiter zu

Nach Angaben des Bundeskriminalamtes (BKA) in Wiesbaden vom 16.07.2010 ist im ersten Halbjahr 2010 die Zahl der kriminellen Skimming-Attacken auf Geldautomaten auf 1927 gestiegen. Damit hat es in den ersten 6 Monaten so viele Vorfälle gegeben wie 2009 im gesamten Jahresverlauf. Häufig machten sich Kriminelle mehrfach an den gleichen Geldautomaten zu schaffen, um die Kontodaten von BankkundInnen auszuspähen. Die meisten Attacken gab es in Nordrhein-Westfalen, Baden-Württemberg und Berlin. Geheimzahlen werden dabei häufig mit Minikameras ausgespäht. Alternativ nutzten die Betrüger auch Tastatur-Attrappen, die über die Originaltastatur gelegt werden (SZ 17./18.07.2010, 25).

Bund

Stasi-Überprüfung bis 2019?

Die Koalition auf Bundesebene aus CDU/CSU und FDP plant, die Regelüberprüfung von Beschäftigten im öffentlichen Dienst auf eine mögliche Stasi-Vergangenheit um acht Jahre bis zum Jahr 2019 zu verlängern. Geplant ist zudem eine Ausweitung des Kreises der Betroffenen auf Beamte und Angestellte in leitenden Funktionen. Gemäß dem FDP-Berichterstatter im zuständigen Bundestagsausschuss für Kultur und Medien, Reiner Deutschmann, liegt der Entwurf einer entsprechenden Novelle des Stasi-Unterlagen-Gesetzes vor. Nach bisherigem Recht laufen die Stasi-Überprüfungen Ende 2011 aus. Überprüft werden bislang nur Beschäftigte in der obersten Leitungsebene. Gemäß Deutschmann könnten künftig etwa auch ehrenamtliche BürgermeisterInnen betroffen sein (SZ 07./08.08.2010, 5).

Bund/Länder

Ausländerrechtliche Kontrolle von SchülerInnen umstritten

In einem Brief des Staatssekretärs im Bundesinnenministerium (BMI) Ole Schröder vom Juli 2010 an den Menschenrechtsverein Aktion Courage teilt dieser mit, dass das BMI sich „weiter dafür einsetzen wird, die Zustimmung der Länder zu den erforderlichen Rechtsänderungen herbeizuführen“, um zu verhindern, dass über den Schulbesuch Ausländerbehörden vom illegalen Aufenthalt ausländischer Familien erfahren. Gemäß der Koalitionsvereinbarung auf Bundesebene von CDU, CSU und FDP sollen die Meldepflichten der Behörden so geändert werden, „dass der Schulbesuch von Kindern ermöglicht wird“. Eine Untersuchung des Sachverständigenrats für Integration ergab, dass an die 30.000 Kinder im schulpflichtigen Alter in Deutschland leben, deren Eltern illegale ZuwanderInnen sind. Ein Großteil geht nicht zur Schule aus Angst der Familien, entdeckt zu werden. Einzelne Länder beharren auf der Meldepflicht der Schulen gegenüber den Ausländerbehörden, v.a. Bayern und Niedersachsen. Das bayerische Innenministerium erklärte, dass die Grundschulkinder im Land ohnehin nach einer Liste des Einwohnermeldeamtes eingeschult werden, weil nach Schulsprengseln verteilt wird. Die Meldepflicht sei „hilfreich“, weil es „für alle Beteiligten Rechtsklarheit schafft“. Niedersachsens Innenminister Uwe Schünemann (CDU) meinte, die Verpflichtung des Staates, einen unrechtmäßigen Aufenthalt zu beenden, würde „ad absurdum“ geführt werden, wenn es den Behörden freigestellt würde, ob sie diese Zuwanderer weitermelden. Dies würde nur weitere illegale Zuwanderer anziehen. AusländerrechtlerInnen weisen dagegen darauf hin, dass die UN-Kinderrechtskonvention das Recht aller Kinder auf Schulbildung festgeschrieben hat. Im Mai 2010 hatte die Bundesregierung die Konvention voll anerkannt. Gerd Pflaumer vom Aktion-Courage-Vorstand meinte: „Nun wird der unionsinterne Streit auf dem Rücken der Schwächsten ausgetragen, obwohl alle ihre Ministerpräsidenten dem Koalitionsvertrag ja zugestimmt haben“ (Preuß SZ 13.08.2010, 6).

Baden-Württemberg

Datenpanne bei Schlecker

Bis zum 26.08.2010 waren 150.000 Datensätze von OnlinekundInnen des schwäbischen Drogerie-Discounters Schlecker frei über das Internet einsehbar. Neben Anschrift, Mailadresse und Geburtsdatum ließen die unzureichend geschützten Daten Rückschlüsse auf bestellte Waren zu. Der Entdecker der Lücke Tobias Huch hatte schon

mehrfach in Verbindung mit Datenlecks und mehr oder weniger skurrilen Gerichtsverfahren auf sich aufmerksam gemacht. Er will zudem Zugriff auf 7,1 Millionen Mailadressen der Newsletter-AbonnentInnen des Drogerie-Discounters gehabt haben. „Durch Zufall sind wir über diese Datenlücke gestolpert. Dann merkten wir: Das ist keine Lücke, das ist der Tag der offenen Tür." Schlecker erklärte, dass „die Sicherheitslücke ... umgehend von unserem Dienstleister geschlossen" wurde. Außerdem wolle der Discounter die betroffenen KundInnen „umfassend informieren". Es habe nur wenige unbefugte Zugriffe auf die Daten gegeben. Hochsensible Informationen wie Kontonummern oder Passwörter seien durch die Panne nicht öffentlich geworden. Die betroffenen Daten hätten ausschließlich der Werbekommunikation gedient. Der Angriff sei offenbar durch einen „internen Angriff" möglich geworden; deshalb habe das Unternehmen Anzeige gegen Unbekannt erstattet. Die Aufsichtsbehörde Baden-Württemberg hat Schlecker zu einer Stellungnahme aufgefordert. Der Online-Dienstleister, bei dem die Schlecker-Kundendaten gehostet waren, soll auch Bundesministerien, das Bundesverwaltungsgericht, die Allianz-Versicherung und den SPD-Parteivorstand beraten (Deckstein SZ 28./29.08.2010, 1, 23; www.heise.de 27.08.2010).

Bayern

Änderungen zum Versammlungsrecht in Kraft

Am 01.06.2010 traten wesentliche datenschutzrechtliche Änderungen des Bayerischen Versammlungsgesetzes in Kraft. Der bayerische Gesetzgeber reagiert damit auf eine Eilentscheidung, in der das Bundesverfassungsgericht am 17.02.2009 vor allem die sehr weit gehenden polizeilichen Befugnisse zu Anfertigung und Speicherung sog. Übersichtsaufnahmen und -aufzeichnungen beschränkt hat. Die Gesetzesänderung verbietet es der Polizei nunmehr, regelmäßig Übersichtsaufnahmen von Versammlungen anzufertigen. Versammlungsteilnehmer müssen mit Übersichtsaufnahmen in Zukunft nur noch rechnen, wenn sie wegen der Größe oder Unübersichtlichkeit der Versammlung im Einzelfall erforderlich sind. Darüber hinaus dürfen sog. Übersichtsaufzeichnungen nicht mehr anlasslos und zeitlich unbegrenzt gespeichert werden.

Die vom Gericht bestätigten und nun Gesetz gewordenen Einschränkungen hatte der Bayerische Landesbeauftragte für den Datenschutz Thomas Petri in Anbetracht der negativen Erfahrungen mit der Praxis polizeilicher Übersichtsaufzeichnungen bereits bei der Schaffung des Bayerischen Versammlungsgesetzes 2008 gegenüber dem Innenministerium gefordert. Petri erklärte nun zu den Änderungen: „Trotz wesentlicher datenschutzrechtlicher Verbesserungen ist es nach wie vor unbefriedigend, dass Versammlungsteilnehmer nicht erkennen können, ob sie einzeln oder im Rahmen von Übersichtsaufnahmen polizeilich gefilmt werden. Dies können die Betroffenen kaum in Erfahrung bringen. Allenfalls können sie von ihrem allgemeinen datenschutzrechtlichen Auskunftsanspruch Gebrauch machen. Damit können sie allerdings nur erfahren, ob die Polizei ihre Teilnahme an einer Versammlung in Akten und in polizeilichen Dateien gespeichert hat." Er veröffentlichte in einem Informationsblatt einen Überblick über die ab 01.06.2010 geltenden datenschutzrechtlich relevanten Änderungen im Bayerischen Versammlungsgesetz (PE BayLfD 01.06.2010; das Informationsblatt kann unter www.datenschutz-bayern.de heruntergeladen werden).

Berlin

Alexander Dix als Datenschutzbeauftragter bestätigt

Das Berliner Abgeordnetenhaus bestätigte den dortigen Beauftragten für Datenschutz und Informationsfreiheit, den 59jährigen Alexander Dix, am 03.06.2010 für weitere fünf Jahre einstimmig in seinem Amt. Parlamentspräsident Walter Momper (SPD) vereidigte Dix anschließend im Parlament. Der promovierte Jurist ist bereits seit Juni 2005 oberster Datenschützer in Berlin. Zuvor war Dix sieben Jahre lang in gleicher Funktion in Brandenburg tätig. Dix ist zudem Vorsitzender der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (www.heise.de 04.06.2010).

Hessen

Tausende KundInnendaten von Alte Leipziger im Netz

Am 19.08.2010 standen auf einem Server der Versicherung Alte Leipziger rund 3.600 Versicherungsanträge in einem Unterverzeichnis ungeschützt zum Download über das Internet bereit. Die Anträge wurden über den Tarifrechner der Sparte Rechtsschutz-Union aufgenommen und enthielten vertrauliche Daten wie etwa Bankverbindung, Beruf, Fahrzeuge, eventuelle Vorschäden sowie den bisherigen Versicherer des Antragsstellers. Auch Geburtsdatum, Nationalität, Familienstand und Angaben zu den Kindern fanden sich in den Anträgen sowie private Angaben. Ein Leser von heise Security war über das Datenleck gestolpert und hatte die Redaktion über seinen Fund informiert. Nachdem die Versicherung auf das Problem aufmerksam gemacht worden war, beseitigte sie die Lücke innerhalb weniger Stunden. Laut Unternehmenssprecher Manfred Kühlmeyer entstand der Fehler wohl schon Anfang des Jahres, als die Versicherung den Rechner an einen neuen Tarif angepasst hat. Als Konsequenz habe man die Umstellung auf ein anderes Vermittlerportal vorzeitig durchgeführt. Ein Sprecher meinte, die „regelmäßige Überprüfung der Zugriffsmöglichkeiten auf unsere Vermittlerportale wird aufgrund dieses Anlasses vorgezogen". Der Konzern will die betroffenen KundInnen zeitnah informieren (www.heise.de 20.08.2010).

Hamburg

Erster Körperscanner im Flughafen Fuhlsbüttel

Das Bundesinnenministerium (BMI) kündigte an, dass Flugpassagiere ab

September 2010 auf dem Hamburger Flughafen Fuhlsbüttel mit einem sog. Körperscanner durchleuchtet und kontrolliert werden können. Damit soll schneller und besser als bisher überprüft werden können, ob Fluggäste gefährliche Stoffe, insbesondere Sprengstoff am Körper tragen. Die Passagiere sollen zunächst wählen, ob sie gescannt werden oder die bislang üblichen Kontrollschranken durchschreiten wollen, um danach eventuell noch von Sicherheitskräften persönlich abgetastet zu werden. Nach der intensiven öffentlichen Debatten über die damals Nacktscanner genannten Geräte sollen nun Geräte zum Einsatz kommen, die die Passagiere nur schematisch darstellen. Bundesinnenminister Thomas de Maizière (CDU) versicherte, der Schutz der Intimsphäre bleibe gewährleistet. Es gäbe keine wirklichen Körperbilder; die Menschen würden wie Strichmännchen dargestellt. Die Aufnahmen sollen unmittelbar nach der Kontrolle gelöscht werden. Gefahren für die Gesundheit gingen von dem Apparat, der das Abtasten des Körpers in Sekundenschnelle vornimmt, nicht aus.

Noch Anfang 2010 hatten PolitikerInnen fast aller Bundestagsparteien gegen diese Scanner votiert. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar, der bisher gegen diese Kontrolle von Passagieren eintrat, kündigte nun an, das Gerät in Hamburg vor Beginn des Probelaufs zu prüfen: „Es muss sichergestellt sein, dass es keine gesundheitlichen Belastungen gibt, dass alle Persönlichkeitsrechte gewahrt werden und dass der Scanner tatsächlich effektiv ist.“ Körperliche Behinderungen und Krankheiten von Flugpassagieren, z.B. Inkontinenz-Leiden, müssten den Geräten verborgen bleiben. Auch dürften Passagiere, die sich in Hamburg gegen eine Scannerkontrolle entscheiden, nicht intensiver überprüft werden als bislang üblich. Das BMI will im Fall eines erfolgreichen Probelaufs die Geräte auch in anderen Flughäfen einsetzen. Noch gäbe es, so ein Sprecher, „kleinere Kinderkrankheiten“. Die Geräte schlügen bislang noch bei nichtigen Anlässen an, etwa bei Falten in Hosenbeinen. Am Flughafen Amsterdam Schiphol werden Scanner seit drei Jahren getestet. Italien und Großbritannien planen auch den Einsatz. In den USA und in Russand wird schon gescannt.

Derweil kritisierten Nichtregierungsorganisationen, dass das BMI Körperscanner von der Tochterfirma eines Streubombenherstellers bestellt habe. Die im Hamburg zum Einsatz kommenden Geräte stammten von der Firma L3 Communications Security and Detection Systems, eine Tochter des sechstgrößten US-Rüstungskonzerns L3 Communications. Ein Sprecher des BMI wies jedoch darauf hin, dass der Vertrag zur Beschaffung der zwei Körperscanner mit einem anderen Vertragspartner abgeschlossen worden sei. Die Bundesregierung werde jetzt weitere Prüfungen vornehmen und danach eine juristische und politische Bewertung abgeben (Höll SZ 09.08.2010, 4, 6; SZ 12.08.2010, 5).

Hamburg

Studie: Videoüberwachung bringt nichts

Eine Wirksamkeitsanalyse der hamburgischen Innenbehörde zur Kameraüberwachung auf der Reeperbahn, die am 05.07.2010 dem schwarz-grünen Senat vorgelegt wurde, kommt zu dem Ergebnis, dass seit der Einführung Gewalttaten um ein Drittel gestiegen sind: „Das Ziel der Reduzierung des Fall-Aufkommen insgesamt in dem Bereich Reeperbahn ist in den erstens drei Jahren der Überwachung nicht erreicht worden“. Erst zwei Wochen zuvor hatte das Hamburgische Oberverwaltungsgericht Teile der Videoüberwachung des Kiezes für rechtswidrig und als Eingriff in das „informationelle Selbstbestimmungsrecht“ erklärt, wenn von der Polizei live in die Hauseingänge von Reeperbahn-BewohnerInnen gefilmt wird. Es gebe keine gesetzliche Grundlage für das Filmen der AnwohnerInnen. „Das Fall-Aufkommen in den ausgewählten Deliktsbereichen im videoüberwachten Bereich der Reeperbahn stieg im dritten Jahr der Videoüberwachung gegenüber dem Jahr vor Inbetriebnahme der Videoüberwachung um 32 Prozent“, heißt es in der Wirksamkeitsanalyse. Die Zahl der Körperverletzungen sei von 2006 bis 2009 gar um 75 Prozent gestiegen - innerhalb des zur Abschreckung vor Straftaten eingerichteten Überwachungsbereichs. In der Umgebung der Reeperbahn sei die Zahl um 46 Prozent nach oben geschossen. Waren es 2006 also noch 182 gefährliche und 369 einfache Körperverletzungen, so waren es drei Jahre später 239 gefährliche und 646 leichte Körperverletzungen.

Der Datenschutzbeauftragte von Hamburg Johannes Caspar hatte immer wieder die präventive Videoüberwachung des Kiezes zur Gefahrenabwehr als rechtswidrig kritisiert. Er bemängelte nicht, dass die Videoaugen zwecks Strafverfolgung eingesetzt werden, sondern dass der Polizei der Hansestadt nach Polizeirecht präventiv einen solchen Eingriff in das „informationelle Selbstbestimmungsrecht“ nicht zustehe. Die Polizei hatte April 2006 12 Videokameras entlang der Amüsiermeile installiert. Die Aufnahmen der um 180 Grad schwenkbaren Zoom-Kameras werden zu Monitoren ins Polizeipräsidium übertragen. Danach erfolgt eine vierwöchige Speicherung der Aufnahmen der KiezbesucherInnen und Anwohnenden zum Zwecke der Strafverfolgungsvorsorge. Für die Innenpolitikerin der mitregierenden Grünen Antje Möller ist die Wirksamkeitsanalyse einerseits spannend, weil sie der „Dunkelfeldaufhellung“ von Straftaten diene. Sie sei aber nicht das, was im Koalitionsvertrag 2008 vereinbart worden sei. Damals habe man eine Evaluation von Videoüberwachung öffentlicher Plätze vereinbart. „Das hat nicht stattgefunden. Ich sehe keine präventive Effekte.“

Für die Linkspartei meinte die Innenpolitikerin Christiane Schneider: „Die Videoüberwachung an der Reeperbahn muss sofort beendet werden. Sie ist nicht nur ein unverhältnismäßiger Eingriff in die Grundrechte, sondern hat keinerlei präventive Wirkung, wie die gestiegene Zahl der Delikte und insbesondere der Gewaltdelikte in dem überwachten Gebiet belegt.“ Außerdem koste die Überwachung viel Geld. Hier habe der Senat die Gelegenheit, endlich mal am richtigen Ende zu sparen. Dass auch die Videoüberwachung von nichtstaatlicher Seite immer mehr zunehme, verwundere angesichts der ausufern-

den staatlichen Überwachung nicht: „Das Grundrecht auf informationelle Selbstbestimmung kommt in Hamburg immer stärker unter die Räder.“ Ein Gutachten des Verwaltungsjuristen Carsten Gericke im Auftrag der Linkspartei spricht dem Landesgesetzgeber die Gesetzgebungskompetenz für Videoüberwachung zum Zwecke der Prävention ab: „Videoüberwachung zur Strafverfolgung ist verfassungskonform“ und sei durch die Strafprozessordnung vom Bundesgesetzgeber zu regeln. „Zum Zwecke der Prävention nach Polizeirecht ist Videoüberwachung verfassungsrechtlich mehr als bedenklich“ (von Appen www.taz.de 05.07.2010).

Hamburg

Verfahrenseinstellung gegen Beierdorf wegen Bewerber-Bluttests

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) Johannes Caspar hat ein Bußgeldverfahren gegen die Beiersdorf AG wegen illegaler Einstellungsbluttests bei Stellenbewerbungen wegen einer zu unklaren Rechtslage eingestellt. Ende 2009 war bekannt geworden, dass im Zeitraum von Januar 2007 bis Dezember 2009 in ca. 400 Fällen medizinische Untersuchungen bei Bewerbungen für Verwaltungs- und Bürotätigkeiten durchgeführt wurden. Die Untersuchungen bestanden aus einem ärztlichen Gespräch, einer ärztlichen Standard-Untersuchung mit Blutentnahme und einer Urinprobe. Eine Testung auf HIV, Drogenmissbrauch oder Schwangerschaft wurde nicht durchgeführt. Für die Untersuchungen hatte Beiersdorf eine schriftliche Einwilligung der Bewerbenden eingeholt. Laut Aussagen der Firmenleitung seien die Bewerbenden vor der Untersuchung stets mündlich darauf hingewiesen worden, dass die Teilnahme freiwillig erfolge und auch das Untersuchungsergebnis für die Einstellungsentscheidung keine Rolle spiele. Es habe sich lediglich um einen Gesundheitscheck der Bewerbenden nach Abschluss des Auswahlverfahrens gehandelt, der einem präventiv-medizinischen Zweck diente.

Seitens des HmbBfDI blieben erhebliche Zweifel, ob die von Beiersdorf eingeholten Einwilligungen der Bewerbenden rechtswirksam erteilt wurden. Nach seiner Auffassung hätten die Bewerbenden hierzu auch schriftlich über die Folgenlosigkeit der Nichtteilnahme an der Untersuchung unterrichtet werden müssen. Nur dies hätte ihnen die Möglichkeit gegeben, sich rechtswirksam auf diese Zusage zu berufen und es ihnen ermöglicht, sich aus freien Stücken gegen eine Untersuchung zu entscheiden. Allerdings fehle im Bundesdatenschutzgesetz eine eindeutige Regelung, dass auch die Hinweise über die Folgen einer Einwilligung der Schriftform bedürfen. Unklar bleibe zudem, ob tatsächlich alle Bewerbenden über die Freiwilligkeit der Untersuchung informiert wurden.

Dies lässt sich nachträglich nicht mehr rekonstruieren, da sich Beiersdorf auf das ihr im Verfahren zustehende Auskunftsverweigerungsrecht berief und eine weitere Aufklärung wenig Erfolg versprach, so Caspar: „Aufgrund des nicht mehr aufzuklärenden Sachverhalts sowie der unklaren Rechtslage, aber auch aufgrund der Tatsache, dass die Beiersdorf AG die Untersuchungspraxis sofort nach unserem Intervenieren gestoppt hat, haben wir das Bußgeldverfahren eingestellt. Der Fall verdeutlicht einmal mehr, dass wir ein wirksames Arbeitnehmerdatenschutzgesetz benötigen. Vor dem Hintergrund der aktuellen Aktivitäten auf Bundesebene zur Schaffung eines Arbeitnehmerdatenschutzgesetzes muss sichergestellt werden, dass ärztliche Untersuchungen im Zuge der Aufnahme von Beschäftigungsverhältnissen künftig nur noch unter sehr engen Voraussetzungen erfolgen dürfen. Die Art der auszuübenden Tätigkeit muss dabei eine wesentliche und entscheidende Voraussetzung für die Untersuchung darstellen. Dies ist bei Büro- und Verwaltungstätigkeiten regelmäßig nicht der Fall. Aufgrund des strukturellen Ungleichgewichts zwischen Arbeitgeber und Bewerber müssen scheinbar auf Freiwilligkeit beruhende Untersuchungen zur individuellen Gesundheitsvorsorge im Einstellungsverfahren in Zukunft gänzlich ausgeschlossen werden“ (PE 02.07.2010 HmbBfDI).

Nordrhein-Westfalen

Cyberspanner beobachtete Schülerinnen über Webcams

Ein Computerkrimineller aus dem Rheinland ist in die PCs von mindestens 150 Mädchen eingedrungen und hat die Kinder über Webcams ausspioniert. Für den Zugriff auf die Webcam nutzte er einen Trojaner, den er über E-Mails mit gefälschtem Absender als Bildschirmschoner verteilte. An die Adressen ist er durch den Einbruch in ein ICQ-Konto eines Versmolder Gymnasiasten gelangt. Der Täter soll über einschlägige Internetforen noch eine Vorauswahl getroffen haben, welchen Mädchen er das Schadprogramm unter dem Namen eines Schülers über den Chat-Dienst ICQ zusendet. Zuvor hatte der Spanner das Nutzerkonto des Schülers geknackt. Den Trojaner hatte er in einer Bilddatei versteckt. Die Staatsanwaltschaft Aachen bestätigte die Ermittlungen.

Die Sache war aufgeflogen, weil sich zwei Mädchen an ein Mitglied des Berufsverbands der Datenschutzbeauftragten (BvD) wandten, das im Rahmen eines Projekts Vorträge an Schulen hielt. Die Mädchen berichteten, dass die Kontrollleuchte der Webcam an ihrem Laptop leuchtete, obwohl sie die Internetkamera gar nicht eingeschaltet hatten. Der Datenschutzbeauftragte und Eletrotechniker Thomas Floß untersuchte daraufhin die Rechner und fand den Schädling. Über die IP-Adresse wurde der Wohnsitz des Spanners festgestellt. Als die Polizei bei ihm klingelte, sollen auf seinem Computer gerade Videos aus etlichen Kinderzimmern gelaufen sein. Floß erklärte, dass viele der Mädchen zu leichtfertig die vermeintlich von einem Schüler geschickte Mail geöffnet und sich so das Schadprogramm auf ihrem Computer eingefangen haben (www.heise.de 16.07.2010; SZ 17./18.07.2010, 12).

Datenschutznachrichten aus dem Ausland

Belgien

Geheime Dutroux-Akten bei Wikileaks im Internet

Wikileaks veröffentlichte im Internet aus geheimen Dutroux-Akten ein Dossier von 1.235 Seiten mit Aussagen von Marc Dutroux, vertraulichen Aufzeichnungen von Zeugen-Anhörungen sowie Adressen und Telefonnummern. Die Dokumente stammen aus Verhandlungsakten, die der Geheimhaltung unterliegen. Die Internet-Veröffentlichung der Ermittlungsakten aus dem Fall des verurteilten Kinderschänders Marc Dutroux sorgt in Belgien für Ärger. Der Generalstaatsanwalt von Lüttich Cedric Visart de Bocarme meinte, er sei „unglücklich, weil die Dokumente aus Verhandlungsakten stammen, die immer noch der Geheimhaltung unterliegen". Für Zeugen, die sich nichts zuschulden kommen ließen, bestehe jetzt die Gefahr, in der Öffentlichkeit bloßgestellt zu werden. Der inzwischen 53 Jahre alte Dutroux hatte in den 90er Jahren mehrere Mädchen entführt, von denen vier während ihrer Gefangenschaft in seinem Haus qualvoll starben. Er wurde im Juni 2004, etwa acht Jahre nach seinen Verbrechen, wegen mehrfachen Mordes zu einer lebenslangen Freiheitsstrafe verurteilt (www.kleinezeitung.at 25.08.2010; SZ 26.08.2010, 10).

Schweiz

Fifa-Partner im Verdacht des Fandatenhandels

Auftragnehmer des Fußball-Weltverbands Fifa werden verdächtigt, mit dem Schwarzhandel Geschäfte gemacht zu haben. Nach Informationen einer norwegischen Zeitung hat mindestens ein Mitarbeiter der Schweizer Agentur Match, die für die Fifa den Weltmeisterschafts-(WM)-Ticketverkauf organisiert, Schwarzhändlern Daten von TicketkundInnen mit Passnummern sowie Sitzplatznummern der georderten WM-Karten angeboten. Der Kaufpreis der Daten habe zwischen einem und 2,50 Euro pro Kundennamen gelegen. Allein für die WM 2006 seien so Listen mit mehr als 60.000 Namen und Passnummern in Umlauf gekommen. Der Zeitung liegt eine E-Mail eines angeblichen Match-Mitarbeiters vor, in der dieser VIP-Pakete für neun Spiele der WM 2010 in Südafrika anbot, die nicht frei verkäuflich waren - für 422.400 Dollar. Der Fifa sind die Vorwürfe bekannt; Match hat - so ein Sprecher - interne Ermittlungen eingeleitet. Match-Chef Jaime Byrom meinte, man nehme das „sehr ernst" (Der Spiegel 34/2010).

Spanien

Verwertungsverbot von Telefonabhörprotokollen für Ermittlungen im Fußball-Korruptionsskandal

Am 11.08.2010 entschied der spanische Ermittlungsrichter José Luis de la Fuente in zweiter Instanz, dass Aufnahmen abgehörter Telefongespräche im Korruptionsskandal des nationalen Fußballverbandes RFEF um den Erstliga-Aufstieg von Hércules Alicante unter Verschluss bleiben und nicht für Ermittlungen genutzt werden dürfen. Der Richter ließ aber Rechtsmittel vor das Berufungsgericht in Alicante zu. Daraufhin hat der RFEF nach längerem Abwarten eigene Ermittlungen eingeleitet. Aus den Gesprächen soll nach Medienberichten hervorgehen, dass Alicantes Mehrheitsaktionär Enrique Ortiz in der vorangegangenen Saison versuchte, zur Sicherung des Aufstiegs vier Zweitliga-Rivalen zu bestechen. In einem Fall soll der Unternehmer damit Erfolg gehabt haben. Der Torwart von Córdoba soll im Umfeld der 0:4-Niederlage seiner Mannschaft gegen Hércules 100.000 Euro erhalten haben. Die Justiz stellte ihre Ermittlungen ein, da Schiebung im Sport nach spanischem Recht nicht strafbar ist. Der RFEF wurde auf Antrag des Zweitliga-Absteigers FC Cádiz aktiv, der hofft, seinen Abstieg wegen eines Zwangsabstiegs von Hércules Alicante in die dritte Liga verhindern zu können.

Die Justiz lehnte eine Herausgabe der Tonbänder mit der Begründung ab, dass damit die Privatsphäre des Bosses von Hércules verletzt würde. Der Schutz der Privatsphäre, so die Richter, sei ein Grundrecht. Dies dürfe nicht geopfert werden, nur um gegen Alicante sportliche Sanktionen verhängen zu können. Die Gespräche von Ortiz seien im Zug einer anderen Korruptionsaffäre und nur für die Verfolgung strafrechtlicher Delikte abgeschöpft worden, nicht für sportrechtliche Zwecke. Ortiz ist in einen Bestechungsskandal rund um die Müllabfuhr in Alicante verstrickt. Staatsanwälte suchen nun nach Präzendenzfällen, um die Justiz doch noch von der Herausgabe der Abhörprotokolle zu überzeugen. Derartige Fälle gibt es, die zum Verbot von Parteien aus dem Umfeld der Terrororganisation Eta führten. Das Justizministerium sieht in der offenkundigen Verfälschung der Toto-Ergebnisse einen weiteren Hebel. Diverse Tippgemeinschaften tragen sich scheinbar mit dem Gedanken zu klagen. Bislang keine Rolle spielte die Überlegung, zur Eindämmung der sportlichen „Motivationsprämien" die Steuerbehörden einzuschalten, um die Geldflüsse zu verfolgen (Cáceres SZ 07./08.08.2010, 33; SZ 12.08.2010, 27).

Großbritannien

Webcam und Facebook retten Katze

Auf Youtube wurde ein Katzenfilm besonderer Art hochgeladen: Eine etwa 50jährige Frau trifft ein Katze und streichelt diese. Dann schaut sich die Frau kurz verstohlen um, packt die Katze am Nacken und wirft sie in eine Mülltonne: Klappe zu, Katze weg. Die Überwachungskamera über ihrem Kopf hatte die Tierquälerin nicht bemerkt, weshalb es für die Polizei und die britische Tierschutzorganisation RSPCA, unterstützt durch eine Facebook-Gruppe

ein Leichtes war, sie zu identifizieren. 15 Stunden nach der Tat konnte das Haustier, Lola genannt, von seinen Besitzern befreit werden. Zwar ist unklar, ob die Täterin rechtlich belangt werden kann; jedenfalls war die Entrüstung im Internet groß und steigerte sich bis zu Bedrohungen, weshalb die Tierquälerin unter Polizeischutz gestellt werden musste (Beitzer SZ 25.08.2010, 9).

Israel

Politisch kritische Menschen unerwünscht

Israel registriert systematisch KritikerInnen des Staates, um Ihnen die Einreise zu verweigern oder sie gezielt zu drangsalieren. Immer wieder werden politisch missliebige Menschen bei ihrer Ankunft auf dem Ben-Gurion-Flughafen von Tel Aviv vom Inlandsgeheimdienst festgehalten, verhört und ausgewiesen. Ende April 2010 verweigerten die Sicherheitskräfte dem spanischen Clown Ivan Prado die Einreise und warfen ihm vor, Kontakte zu „Terroristen" zu pflegen. Prado wollte nur in der palästinensischen Stadt Ramallah ein Clown-Festival ins Leben rufen. Nachdem er die Zurückweisung in Madrid publik machte, beschwerte sich die israelische Botschaft im Außenministerium in Jerusalem über die durch den Vorfall produzierten Negativschlagzeilen. Auch der US-amerikanische Autor Norman Finkelstein und der UNO-Sondergesandte für die palästinensischen Gebiete Richard Falk durften nichts ins Land, obwohl sie Juden sind. Wären sie nicht als Besucher, sondern als Einwanderer eingereist, hätte man ihnen automatisch die israelische Staatsangehörigkeit geben müssen (Der Spiegel 20/2010, 108).

Russland

FSB-Geheimdienst erhält mehr Macht

Der russische Präsident Dmitrij Medwedjew unterschrieb ein umstrittenes Gesetz, das dem dortigen Inlandsgeheimdienst FSB zusätzliche Vollmachten verleiht. Das russische Parlament hatte zuvor der Machterweiterung des FSB zugestimmt. Mit 313 Stimmen der Kreml-Partei „Einiges Russland" gegen 91 Abgeordnete von Kommunisten, „Gerechtes Russland" und rechtspopulistischen Liberaldemokraten wurde beschlossen, dass der FSB, offiziell zum Schutz vor Terrorismus und sozialen Unruhen, künftig JournalistInnen und verdächtige BürgerInnen vorladen können soll, und wenn sie dem nicht Folge leisten, sogar einsperren darf. Nach der Begründung förderten „einzelne Medien negative geistige Kräfte"; sie betrieben einen „Kult des Individualismus und der Gewalt, des Unglaubens in die Fähigkeit des Staates, seine Bürger zu schützen". Der FSB kann künftig BürgerInnen bereits bei einem Verdacht auf Extremismus verwarnen und vorladen.

Die Leiterin der Moskauer Helsinki-Gruppe, Ljudmila Alexejewa, kritisierte das Gesetz als „Unsinn". Der FSB bekomme „uneingeschränkte Kompetenzen". Russland versinke im „Autoritarismus". Der Menschenrechtsbeauftragte des Präsidenten Wladimir Lukin meinte, das Gesetz diskreditiere die „angesehene Institution des FSB". Die Menschenrechtsbeauftragte des Kreml, Ella Pamfilowa trat am Tag nach Medwedjes Unterzeichnung von ihrem Amt zurück. Sie gehe freiwillig und sei zu diesem Schritt in keiner Weise gedrängt worden. Pamfilowa hatte von dem Gesetz abgeraten, weil es die Gefahr von Willkür gegen Andersdenkende erhöhe. Der Entwurf stammt von Ministerpräsident Wladimir Putin, ein früherer Geheimdienstler und Vorsitzender von „Einiges Russland". Unklar bleibt die Rolle des Präsidenten Dmitrij Medwedjew, der viel und leidenschaftlich von einer neuen Bürgergesellschaft redet, ohne insofern Konsequenzen zu zeigen (SZ 12./13.06.2010, 10; SZ 30.07.2010, 7; Nienhuysen SZ 31.07/01.08.2010, 8).

USA

Social Engineering-Angriff über soziale Netzwerke

Der IT-Experte Thomas Ryan offenbarte Ende Juli 2010 auf der Hackerkonferenz „Black Hat" in Las Vegas, wie er mit einem Social-Engineering-Angriff in sozialen Netzwerken an geheime Informationen gelangen konnte. Er schuf sich eine hübsche Frau mit dem Namen Robin Sage und einem leicht slawischen Aussehen, 25 Jahre alt, Absolventin der Technischen Hochschule Massachusetts, Analystin für Cybersicherheit der US-Marine, 10 Jahre Berufserfahrung, Fotos und einiges mehr, und erreichte, dass sich mit ihr etwa 300 Menschen über soziale Netzwerke wie Facebook, Twitter oder Linkin anfreundeten, darunter Mitglieder der US-Armee, von Geheimdiensten, Sicherheitsunternehmen und Auftragnehmer des Weißen Hauses. In ihrem nur einmonatigen Leben tauschte Robin mit ihren Internet-Bekanntschaften allerlei Daten aus, darunter vertrauliche Regierungsinformationen. Robin erhielt Zugang zu E-Mail- und Bankkonten. Sie erfuhr, wer mit wem im exklusiven Sicherheitsmilieu der USA verkehrt. Sie bekam mehrere Jobangebote, u.a. als Referentin für Google oder vom weltgrößten Rüstungskonzern Lockheed Martin.

Ryan zählt zum Kreis der „ethischen Hacker", sog. White Hats, die in IT-Systeme eindringen, um Sicherheitslücken aufzudecken. Bei seinem letzten Experiment von Dezember 2009 bis Januar 2010 gelang es ihm mit Hilfe der fingierten Robin Sage, unbemerkt in das Innenleben der US-amerikanischen Sicherheit einzudringen. Über einen in Afghanistan stationierten US-Feldjäger eröffnete sich dem Hacker aus New York eine ungeahnte Fülle vertraulichen Wissens. Klicks im Fotoalbum des Soldaten erlaubten festzustellen, wann die Bilder wo - mit genauen Koordinaten - erstellt worden waren und wo sich seine Einheit aufhielt. Treffer erzielte Ryan auch im Umgang mit dem Stabschef eines Parlamentariers, dem Informationsdirektor der Marine und mit Mitarbeitern der National Security Agency (NSA). Nicht alle, die Robin Sage umgarnte, ließen sich verführen. Auch berühmte Hacker bekamen Einladungen, doch ihnen kam das Profil der jungen Frau suspekt vor. Ryan hatte es absichtlich mit auffälligen Merkmalen gespickt. Die wenigsten schöpften Verdacht. In seinem Vortrag

„Robin Sage ins Bett kriegen“ berichtete Ryan, dass fast alle Opfer Männer waren. Um Robin ein Gesicht und einen Körper zu geben, hatte Ryan Fotos einer Porno-Webseite heruntergeladen (Jiménez SZ 02.08.2010, 1).

USA

Wie unbescholtene Menschen zu Terroristen erklärt wurden

Der in Portland/Oregon als staatlicher Pflichtverteidiger arbeitende Anwalt Steven T. Wax demonstriert in seinem Buch „Kafka in Amerika - Wie der Krieg gegen den Terror Bürgerrechte bedroht“ anhand von zwei dokumentierten Fällen, wie die sicherheitspolitischen Maßnahmen nach dem 11. September 2001 individuelle Freiheiten, Rechtsstaatlichkeit und Demokratie beeinträchtigen. Der Buchtitel spielt an auf Kafkas Romanfragment „Der Prozess“, der mit dem Satz beginnt: „Jemand musste Josef K. verleumdet haben, denn ohne dass er etwas Böses getan hätte, wurde er eines Morgens verhaftet.“ Ebendies passierte den beiden Protagonisten des Buches, dem Rechtsanwalt Brandon Mayfield im Mai 2004 und dem Sudanesen Adel Hamad.

Brandon Mayfield, ein Moslem, führte mit Frau und 2 Kindern ein völlig unauffälliges Leben. Bestimmte Merkmale machten ihn jedoch nach dem 11.09.2001 für das Federal Bureau of Investigations (FBI) interessant: Seine Frau stammte aus Ägypten und ist ebenfalls Muslimin. Als Andenken an seine militärische Dienstzeit in einer Einheit, die über Patriot-Raketen verfügte, verwahrte er in seiner Bibliothek ein Handbuch über diese Raketen, das im Buchhandel frei zugänglich war. Seine Frau mietete ein Schließfach in einer Bank, in dem sie 10.000 Dollar aufbewahren ließ, und las u.a. eine Biographie über Bin Laden. Im März 2004 wurden in Madrid fünf Anschläge auf Vorortzüge verübt. Die Täter stammten aus Algerien und Marokko und konnten relativ schnell identifiziert werden. Das FBI interessierte sich dabei für den Fingerabdruck Nr. 17. Entgegen den Nachweisen der spanischen Behörden, die diese Spur einem Algerier zuordneten, unterwarfen die US-Justiz- und Polizeibehörden Mayfield wochenlangen Verhören, um ihn als Täter oder Mittäter zu überführen. Die Behörden fütterten eine Zeitlang die Presse mit Details aus den Ermittlungen und anderen „Erkenntnissen“, die Mayfield als „islamistischen Terroristen“ abstempelten. Erst durch den Einsatz von Wax als Rechtsanwalt und einen aufrechten Richter konnte dem frivolen Zusammenspiel von Ermittlern, Staatsanwälten, Geheimdienstlern und Medien ein Ende bereitet und Mayfield wieder in Freiheit gebracht werden.

Adel Hamad, ein aus dem Sudan stammender Mitarbeiter, die in Pakistan arbeitet, erwischte es noch schlimmer. Nach der Folterung auf einem US-Luftwaffenstützpunkt in Afghanistan wurde er nach Guantánamo gebracht, wo er nach der Rechtsauffassung der Bush-Regierung als „feindlicher Kombattant“ zeitlich unbegrenzt und ohne Rechtsbeistand und Gerichtsverfahren festgehalten werden konnte. Dem „Center for Constitutional Rights“ und dem Rechtsanwalt Wax gelang es in einem schwierigen Verfahren, die Argumentation der US-Regierung anzufechten, wonach „feindliche Kombattanten“ außerhalb des Rechts stünden. Obwohl es hierfür keinen einzigen belastbaren Beleg gab, wurde Hamad fast fünf Jahre lang als Kämpfer in Guantánamo festgehalten. Trotz diesen bedrückenden Erfahrungen der beiden Männern mit der US-amerikanischen Justiz und Politik kommt Wax zu der bemerkenswert optimistischen Schlussfolgerung, dass „nach einem schrecklichen Auftakt die traditionelle Strafgerichtsbarkeit funktionierte“, trotz der „außerordentlichen Verhörtaktiken“. Damit gemeint sind Folter und andere andere Menschenrechtsverletzungen, die die Bush-Administration zu verantworten hat und mit denen sich die Obama-Regierung - oft ohne die nötige Sensibilität - weiterhin herumschlägt (Teven T. Wax: Kafka in Amerika - Wie der Krieg gegen den Terror Bürgerrechte bedroht, übersetzt von Werner Roller, Hamburger Edition, Hamburg 2009, 496 S., 29,90 Euro; Walther SZ 02.08.2010, 14).

USA

FBI erhält Zugriff auf Nutzerspuren im Netz

Mit einer Gesetzesänderung will die US-Regierung das Federal Bureau of Investigations (FBI) ohne Richtergenehmigung Zugriff auf „Transaktionsdaten elektronischer Kommunikation“ zur Terrorismusbekämpfung gewähren. Durch die Änderung des Electronic Communications Privacy Act (ECPA) erhielte das FBI vor allem leichteren Zugang zu Internet-Verbindungsdaten, also zu den Protokollen von Providern, z.B. wann ein Nutzer von welcher Adresse aus an wen eine E-Mail gesandt hat. Betroffen sein dürfte auch - so das federführende Justizministerium - der Verlauf von Webseiten-Besuchen, nicht aber der weitere Inhalt elektronischer Nachrichten oder anderer Formen der Internetkommunikation.

Eine Verpflichtung zur Vorratsspeicherung von Telekommunikationsdaten mit entsprechenden Zugangsregelungen für die Sicherheitsbehörden gibt es in den USA im Gegensatz zur EU nicht. Das FBI darf aber bereits mit offiziellen Autorisierungsschreiben in Form der sogenannten National Security Letters (NSL) auf Telefonverbindungsdaten zugreifen. Diese für die Terrorabwehr vorgesehene Ermittlungsmöglichkeit, die laut Regierungsuntersuchungen und Zeitungsberichten in den vergangenen Jahren massiv missbraucht wurde, soll nun auf den Internetbereich ausgedehnt werden. Bislang weigerten sich viele Anbieter von Internet-Services, dem FBI geforderte Daten auszuhändigen. Dies wird auf nicht eindeutige Gesetze zurückgeführt. Gemäß dem Sprecher des Justizministeriums handelt es sich also nur um eine Klarstellung der Absicht, die der US-Kongress mit der jüngsten größeren Novellierung des ECPA verbunden habe. Es würden keine Auflagen eingeführt, neue Datenkategorien zu sammeln. Stewart Baker, ein früherer Geheimdienstmitarbeiter und Ex-Vertreter des Department of Homeland Security (DHS), begrüßte das Vorhaben, da das FBI damit „schneller und einfacher an die Daten herankäme“. Er räumte

aber auch ein, dass die Zugangsanbieter damit deutlich mehr Informationen herausgeben müssten als bisher.

Rechtsexperten und Bürgerrechtsvereinigungen kritisierten den Entwurf. Eine große Menge an Verbindungsdaten und darüber hinausgehende Informationen würden aus der gerichtlichen Kontrolle herausgenommen, so der mehrere Internetfirmen vertretende Rechtsanwalt Michael Sussmann. Die American Civil Liberties Union (ACLU) kritisierte, die Obama-Regierung rücke mit dem „vermessenen Vorschlag" erneut von ihrem Wahlversprechen ab, Bürgerrechte und Belange der inneren Sicherheit in eine neue Balance zu bringen. Ein Anwalt der Electronic Frontier Foundation (EFF) wies darauf hin, dass der entscheidende Begriff elektronischer Transaktionsdaten nirgends definiert sei. Man fürchte daher, dass die Polizeibefugnisse letztlich etwa auch auf Internet-Suchanfragen oder Protokolle aller besuchten Webseiten ausgedehnt werden sollten. ExpertInnen vom Center for Democracy and Technology (CDT) forderten, dass ein Zugriff auf die „sensiblen Informationen" allenfalls per Gerichtsanordnung erfolgen darf (Krempl www.heise.de 29.07.2010; SZ 31.07./01.08.2010, 8)

USA/Deutschland

Sicherheitsbehörden verstärken Online-Ermittlungen

Von der Electronic Frontier Foundation (EFF) und Forschenden der University of California in Berkeley wurden auf Basis des „Freedom of Information Act" erlangte Dokumente veröffentlicht, die Aufschluss über Tätigkeiten von US-Sicherheitsbehörden im Internet geben. Die CIA nutzt seit 2005 ein „Open Source Center", um aus öffentlich verfügbaren Internetquellen wie Blogs, Chat-Foren oder sozialen Netzwerken gezielt personenbezogene Informationen zu sammeln und auszuwerten. Auf die dahinter stehende Datenbank und die darin eingespeiste Analysen, Videos, Übersetzungen oder Presseübersichten haben demnach rund 15.000 US-Regierungsangestellte von der kommunalen bis hin zur Bundes-Ebene Zugang. Die Quellen würden bis Mitte der 1990er Jahre zurückreichen. Ein anderes Dokument legt das Interesse des FBI am „Dark Web Project" der University of Arizona offen. Dabei geht es um einen Versuch von Computerwissenschaftlern, alle Terrorismus-bezogenen Inhalte aus dem Web systematisch zusammenzutragen und zu analysieren. Das Projekt wird wegen seiner Effizienz beim Durchsuchen und Erschließen von Kommunikationsforen bis hinein in die „verborgenen Ecken des Internets" gelobt. Es werde an Werkzeugen gearbeitet, um die AutorInnen eigentlich anonymer Online-Informationen zu ermitteln. Gemäß einem Schreiben von 2007 hält es die US-Polizeibehörde für besonders aufschlussreich, entsprechende Hilfsmittel mit den eigenen Ressourcen zur „Ausnutzung" von Internet-Daten zu verknüpfen. Für die EFF ist das ein weiterer Hinweis darauf, dass US-Ermittler inner- und außerhalb des Strafverfolgungskontextes Unmengen an Daten aus dem Netz durchforsten.

US-Bürgerrechtsorganisation hatten schon im Frühjahr 2010 auf US-Verwaltungspapiere verwiesen, wonach US-Strafverfolger und -Finanzbeamte aktiv Dienste wie Facebook, MySpace oder Twitter für ihre Arbeit auswerten. „Undercover-Agenten" mit gefälschten Profilen sollen danach Nutzende gezielt ausspähen. Demgemäß fordert der Vorsitzende des Bundes Deutscher Kriminalbeamter (BDK), Klaus Jansen, für die hiesige Polizei eine Befugnis für „offene und verdeckte Ermittlungen im Internet". Die entsprechende rechtliche Grundlage solle sich vor allem auf soziale Netzwerke beziehen. Polizisten hierzulande sollen so mit ihren KollegInnen in den USA gleichziehen können. Gemäß Jansen sind aufgrund mangelnder technischer Ausrüstung und fehlenden Kompetenzen nur 1% der 260.000 deutschen PolizistInnen fähig, im Internet zu ermitteln. Ein Artikel von Dozenten einer Landespolizeischule in der Fachzeitschrift „Kriminalistik" meint, Online-Plattformen seien aufgrund der Offenheit vieler ihrer Nutzenden „wahre Fundgruben". Daraus abziehbare Informationen seien von „hohem taktischen Nutzen" – vor allem in Kombination mit Polizei-Datenbanken und verdeckten Ermittlungen. Spezialstreifen des Bundeskriminalamtes (BKA) und einiger Landeskriminalämter sind heute schon „anlassunabhängig" im Netz unterwegs. Dabei spüren die Cybercops nach eigenen Angaben etwa Fällen von Kinderpornographie, Volksverhetzung, Betrug oder Gewaltaufrufen nach. Details zur Vorgehensweise bleiben aus „kriminaltaktischen" Überlegungen geheim. Mitarbeitende versichern, dass die Möglichkeiten zur Datengewinnung im Netz im Rahmen der tatsächlichen und rechtlichen eigenen Befugnisse genutzt werden.

Die Hamburger Polizei will zwecks Ermittlung im Internet derzeit stark aufrüsten und alle BeamtInnen mit einem Online-Zugang ausstatten, so ein Behördensprecher: „Die Recherche im World Wide Web wird immer wichtiger". Bislang sei diese nur für Spezialdienststellen an ausgewählten Rechnern möglich gewesen. Selbst der Staatsschutz im Landeskriminalamt hätte bisher nur zwei voll internetfähige PCs in Betrieb. Privates Surfen der Beamten am Arbeitsplatz solle aber die Ausnahme bleiben. Für die Kontrolle sämtlicher Erkundungen im Cyberspace sei ein Chipkarten-System in Planung (Krempl www.heise.de 17.08.2010).

Dubai

Spanner filmt unter Röcken

Einem 29jährigen ägyptischen Fremdarbeiter drohen in Dubai bis zu 15 Jahre Haft wegen sexueller Belästigung, weil er ein Handy in eine durchlöcherte Socke gesteckt und damit Frauen heimlich unter ihren Röcken gefilmt haben soll. Er legte seine mit der Kamera präparierte Socke im Supermarkt in einen Einkaufskorb. Als er vier Frauen unter die Miniröcke filmte, wurden Wachleute auf ihn aufmerksam. Der Prozess wurde am 15.06.2010 eröffnet. Die Videoaufnahmen wurden vor Gericht als Beweismittel präsentiert. Dennoch streitet der Anklagte alles ab. In dem Emirat leben dreimal so viel Männer wie Frauen; ein Großteil sind Bauarbeiter aus anderen Staaten, v.a. aus Südostasien (SZ 17.06.2010, 10).

China

Einreiseverweigerung für kritische Sportlerin

Der deutschen 34jährigen Fechterin Imke Duplitzer wurde in China die Einreise zur Teilnahme an einem Grand-Prix-Turnier in Nanking verweigert. Offiziell hatte es geheißen, das Konsulat habe nicht genügend Zeit gehabt, den Antrag zu prüfen. Die zeitgleich abgegebenen Visum-Anträge der anderen deutschen Fechterinnen waren positiv beschieden worden. Duplitzer hatte sich im Vorfeld der Olympischen Spiele 2008 in Peking als Kritikerin hervorgetan und hatte die Eröffnungsfeier boykottiert. Duplizters Erklärung: „Ich bin offensichtlich der Staatsfeind, weil ich für Menschenrechte eintrete. Kürzlich war ich bei einem Tibet-Hearing des Europaparlaments in Brüssel. So was kommt bei den Chinesen nicht gut an." Da jede Platzierung bei einem Grand-Prix-Turnier Einfluss auf die Weltrangliste hat, erwartet die Sportlerin, dass der Deutsche Fechterbund gegen die Wertung der Veranstaltung Einspruch einlegt (Der Spiegel 20/2010, 129).

Technik-Nachrichten

Vertraulichkeit bei Blackberry als Sicherheitsgefahr

Die Mobiltelefone der kanadischen Firma Research In Motion (RIM) mit dem Namen Blackberry sind bei Geschäftsleuten und privaten Nutzenden wegen ihrer Merkmale äußerst beliebt: RIM ist nach Nokia der zweitgrößte Hersteller von Smartphones weltweit. Diese sind äußerst praktisch beim schnellen Austausch von E-Mails und schließen durch eine starke Verschlüsselung Mitlesende praktisch vollständig aus. Den Empfängerkunden werden die Botschaften mit einem gegengleichen Schlüssel geöffnet. Selbst die billigere Variante der Blackberry-Mails für PrivatkundInnen geben einen gewissen Schutz und können bei Mobilfunkanbietern schon zu Monatspreisen ab 5 Euro gebucht werden. Auch darüber hinausgehend enthalten Blackberrys datenschutzfreundliche Technologien: So können für den Fall, dass ein Handy einem Unbefugten in die Hände geraten, die Daten aus einer Zentrale per Fernbefehl durch siebenmaliges Überschreiben unwiederbringbar überschrieben werden. Diese hinsichtlich Vertraulichkeit positiven Eigenschaften haben nun zu Aktivitäten vieler arabischen Golfstaaten, Saudi-Arabien, der Vereinigten Arabischen Emirate und Kuweit, aber auch von Indien, Algerien und vom Libanon geführt, die alle staatliche Mithörmöglichkeiten forderten.

Die indische Regierung behauptet, die Attentäter von Mumbai, die im Jahr 2008 166 Menschen töteten, hätten Backberrys verwendet. Arabische Staaten fürchten, dass ihre BürgerInnen mit Hilfe der Blackberrys unbemerkt Internet-Pornografie ansehen oder sich unverheiratete Männer und Frauen mit RIM-Geräten unkontrolliert austauschen können. Die Vereinten Arabischen Emirate, wo es allein 500.000 Blackberry-Nutzende gibt, drohten bis Oktober 2010 mit einem Verbot mobiler E-Mails und anderer Datenfunktionen der Blackberrys. In Saudi-Arabien wurde der Messengerdienst, den besonders die Jugend gern zum digitalen Geplauder nutzt, Anfang August 2010 vorübergehend stillgelegt, so dass 700.000 Nutzende betroffen waren. Dies trifft RIM, da es in den Schwellenländern Asiens und in der Golfregion ihr größtes Wachstum verzeichnen konnte; ein Grund für den Erfolg der Geräte war dabei bisher deren Abhörsicherheit - insbesondere bei den Unternehmenskunden. Aus Besorgnis um ihre Reputation schloss die Firma RIM zu Beginn des Konflikts aus, die Verschlüsselung ihrer Geräte für einzelne Regionen zu schwächen: „RIM hat in 175 Ländern ein- und dieselbe sichere Infrastruktur für Unternehmenskunden. Diese Lösung wird nicht an die verschiedenen Märkte, in denen wir operieren, angepasst."

Die staatlichen Abhörbedürfnisse richten sich tatsächlich weniger gegen mögliche Terroristen. Diese sind nicht auf Blackberrys angewiesen, um nicht abgehört werden zu können. Mit frei verfügbarer Software wie z.B. PGP können normale E-Mails unknackbar chiffriert werden; bei besseren E-Mail-Programmen sind derartige Funktionen bereits eingebaut. Vielmehr zielen die Abhörgelüste offensichtlich vor allem auf die kleinen AktivistInnen und Oppositionellen, die sich über perfekte Verschlüsselung weniger Gedanken machen und mit dem Privatkunden-Service auskommen. Das Privatangebot von RIM ist zwar nicht viel sicherer als sonstige E-Mail-Versandmöglichkeiten, doch ist es mühsamer zu knacken: Die Nachrichten werden, u.a. um Leitungskosten zu sparen, für den Versand komprimiert. Das Gleiche gilt für den direkten Austausch von Nachrichten zwischen Geräten, wie ihn der Messenger von Blackberry bietet. In beiden Fällen bedeutet es viel Arbeit für staatliche Sicherheitsbehörden, an die Mail-Inhalte zu kommen, wenn ihnen hierbei RIM nicht hilft. Davon nicht betroffen ist der Unternehmens-Datenverkehr, der über separate Kanäle stattfindet. Es war wohl kein Zufall, dass Saudi-Arabien als erste Maßnahme den Messenger-Dienst ausschaltete. Die Firma RIM beteuerte zunächst, sie schließe auch bei den Privatkunden-Mails Zugeständnisse aus.

Die Botschaft war aber klar: Wenn RIM keinen lesbaren Zugriff auf alle Mails, Textmeldungen und andere Dienste gewährt, ist der Blackberry aus dem arabischen Geschäft draußen. Nach der angekündigten Sperrung der Blackberry-Dienste in Saudi-Arabien lenkte aber RIM ein und erklärte sich be-

reit, im Lande eigene Server zu installieren. Auf die dort vermittelten Daten von Blackberrynutzenden kann zugegriffen werden, sofern dies zum Zweck der „Terrorabwehr und -bekämpfung“ notwendig ist. Zuvor hatten sich die US-amerikanische und die kanadische Regierung bei den Saudis eingeschaltet. Der kanadische Handelsminister Peter von Loan meinte: „Wir arbeiten eng mit den Vertretern von RIM und mit den Behörden vor Ort zusammen, um bei der Bewältigung dieser Herausforderung zu helfen.“ Und US-Außerministerin Hillary Clinten sagte: „Wir wissen, dass es berechtigte Sicherheitsbedenken gibt.“ Zugleich hätten die Nutzenden der Smartphones Interesse an „freier Nutzung und freiem Zugang“. In Indien passierte Entsprechendes: Ein Vertreter der Sicherheitsbehörden meinte: „Unsere Haltung ist klar: Blackberry-Dienste, die von unseren Behörden nicht voll überwacht werden können, müssen unterbrochen werden. Den Zugang zu den Daten offenzuhalten ist Teil der Lizenzvorschriften und muss geleistet werden.“ Verwiesen wurde auf die „doppelten Standards“ von RIM, da die USA und europäische Länder bereits über einen Zugang zu verschlüsselten Informationen verfügten. Die indischen Gesetze sähen vor, dass Telekommunikationsunternehmen Behörden Zugang zu sämtlichen Dienstleistungen gewähren müssen. Eine Million InderInnen verwenden Blackberrys. Nach der Androhung einer RIM-Blockierung, falls sich RIM weigere, den indischen Geheimdiensten Datenzugriff zu gewähren, gab RIM auch hier nach. Bis zum 01.09.2010 wollte RIM den Zugang zu seinem Kurznachrichtendienst teilweise, bis zum Ende des Jahres dann vollständig öffnen. Auch Nokia erklärte sich bereit, den Anforderungen aus Delhi zu entsprechen.

In Europa wird seit Jahren an einer eigenen Technik für einen sicheren Datenaustausch gearbeitet. Hier wurde lange die Meinung verbreitet, die Blackberrys seien weniger stark gesichert; v.a. britische oder US-Geheimdienste könnten die RIM-Server im Ausland anzapfen. In Frankreich sind Blackberrys seit 2007 für hohe Regierungsbeamte nicht mehr zugelassen. In Deutschland erklärte das Bundesamt für Sicherheit in der Informationstechnik (BSI) schon 2005, die Geräte seien für die öffentliche Verwaltung nicht geeignet. Im selben Jahr begann die Telekom-Tochter T-Systems mit der Entwicklung einer eigenen Technik namens SiMKo (Sichere Mobile Kommunikation). Nach Verzögerungen war die erste Version der Software erst 2007 einsatzbereit und das zugrundeliegende Betriebssystem veraltet. Der Durchbruch kam 2009, als das BSI das Eigengewächs SiMKo als bis heute einzige Lösung für die Geheimhaltungsstufe „Verschlusssache - nur für den Dienstgebrauch“ zuließ. Die Bundesregierung nahm als erster Kunde unter Rückgriff auf das Konjunkturprogramm 4.000 SiMKo-Geräte. Nach Ansicht des BSI-Präsidenten Michael Hange bringt diese nationale Lösung einen „deutlichen Gewinn an Sicherheit“. Nutzende von SiMKo beklagen aber eine gewisse Umständlichkeit bei der Bedienung, was auch nach Ansicht von Hange ein Vorteil für RIM mit seiner langjährigen Erfahrung ist: „Das lässt sich mit einer ersten Gerätegeneration kaum einholen“ (Dworschak/Müller/Rosenbach Der Spiegel 32/2010, 122 f.; Martin-Jung SZ 04.08.2010, 19; SZ 05.08.2010, 17; Avenarius SZ 07./08.08.2010, 21, 23; Avenarius SZ 09.08.2010, 15; SZ 11.08.2010, 7; SZ 18.08.2010, 20; www.heise.de 15.08.2010).

Datenlöschung im Internet

Der Saarbrücker Informatiker Michael Backes hat ein Verfahren entwickelt, mit dem man das Problem der Löschung von nicht mehr gewünschten Bildern im Internet wenigsten teilweise in den Griff bekommen soll. An seinem Lehrstuhl wurde eine Erweiterung für Internetbrowser entwickelt, die alle Arten von digitalen Dateien, egal ob Musik, Video, Fotos oder Text, mit einem wählbaren Verfallsdatum versieht. Ist dieses erreicht, erscheint z.B. anstelle eines Bildes nur noch der Hinweis, dass die Datei nicht mehr abrufbar ist. Die oder der Nutzende muss beim Einstellen einer Datei angeben, wann diese verfallen soll. Die Software verschlüsselt dann im Hintergrund die Datei und erzeugt dazu einen Schlüssel, der auf einem oder mehreren Rechnern abgelegt werden kann. Backes: „Der Browser des Betrachters erkennt, dass die Datei, die er anzeigen soll, verschlüsselt ist, und fordert den Schlüssel an.“ Dies geht alles so schnell, dass die Betrachtenden davon nichts mitbekommen. Ist das eingestellte Verfallsdatum erreicht, wird anstelle des Bildes nur ein Hinweis angezeigt. Um zu verhindern, dass große Anbieter wie z.B. Suchmaschinen sich einfach Bilder und Schlüssel anfordern und so die Dateien entschlüsselt speichern können, hat Backes eine Abrufsicherung mit sog. Captchas vorgesehen. Dies sind Bilder mit verzerrten Ziffern, die Computer nicht automatisch entziffern können. Um ein Bild zu sehen, müssen die Betrachtenden die Buchstaben oder Ziffern eintippen.

Einen ersten Prototyp der Software hat Backes für Mozilllas Browser Firefox entwickelt. Die Bundesregierung ist an entsprechenden Verfahren interessiert. Das Verbraucherschutzministerium fördert Firmen, Forschende und InformatikerInnen, die entsprechende datenschutzfreundliche Techniken entwickeln. So meinte Verbraucherschutzministerin Ilse Aigner (CSU): „Ich verspreche mir viel von der Möglichkeit, Eingaben im Internet mit einem Verfallsdatum versehen zu können“. Die Nutzenden müssten aber wissen, dass sich auch mit einem Verfallsdatum nicht verhindern lässt, dass jemand Daten kopiert und an anderer Stelle ohne Verfallsdatum wieder ins Netz stellt. Dabei handelt es sich, so Backes, nicht um den „digitalen Radiergummi“, wie ihn Innenminister Thomas de Maizière gefordert hat: „Wenn eine Datei einmal ihre Kreise gezogen hat, ist sie der Kontrolle entzogen.“ Eine ähnliche Technik hatten schon ein Jahr zuvor Forschende der University of Washington in Seattle vorgestellt. Dabei werden die Schlüssel in Fragmente zerlegt und auf vielen Computern gespeichert. Um eine Datei anzuzeigen, wird eine Mindestzahl dieser Fragmente benötigt. Irgendwann sind aber so viele Rechner nicht mehr online, dass der Schlüssel nicht mehr

zusammengepuzzelt werden kann und die Dateien dadurch nicht mehr abrufbar sind. Dabei bleibt jedoch unklar, wie lange es dauert, bis eine Datei verfällt. Bei der Saarbrücker Variante können die Nutzenden selbst das Verfallsdatum bestimmen: „Solange nicht ein Interesse daran besteht, einen Nutzenden zu unterwandern, wird die Methode funktionieren. Im schlimmsten Fall ist aber mit technischen Lösungen nichts zu machen, wenn jemand z.B. ein Bild kopiert und unverschlüsselt ins Internet stellt. Auch Captchas sind letztlich keine unüberwindbare Hürde, so Backes: „Im Extremfall hole ich mir 10.000 Billigarbeiter, die den ganzen Tag nur Captchas eingeben“ (Martin-Jung, SZ 15.07.2010, 16).

Spionage-Drohnen für 299 Euro

Parrot, ein Spezialist für kabellose Geräte rund um die Mobiltelefonie, bietet seit Kurzem einen per WLAN gesteuerten Quadcopter für 299 Euro an. Der mit zwei Kameras ausgestattete Mini-Helikopter „Parrot AR.Drone“ wird als Spielgerät angeboten. Extra in vier verschiedenen Farben ausgeliefert, können die Quadcopter gegeneinander ist den virtuellen Luftkrieg geschickt werden, so die Werbung: „Die intuitive Bedienung der Parrot AR.Drone ermöglicht spektakuläre Flüge und Videogames in der Augmented Reality. Bei der Steuerung des einzigartigen Quadcopters verschmelzen die wirkliche und die virtuelle Welt und schaffen so ein überwältigendes Spielerlebnis. Die vordere Kamera überträgt auf den iPod touch- oder iPhone-Bildschirm, was die AR.Drone sieht; die Bildverarbeitung erlaubt Echtzeit-Special Effects in die Augmented Reality einzublenden. ... Rund um das Cockpit sind vier Propeller angeordnet, die jeweils von einem bürstenlosen Motor angetrieben werden. Die Parrot AR.Drone erhält dadurch verblüffende Möglichkeiten bei der Steuerung, eine exzellente Manövrierfähigkeit und eine außergewöhnliche Flugstabilität. Die Parrot AR.Drone baut ihr eigenes WLAN-Netzwerk auf, eine Internet- oder Routerverbindung ist nicht notwendig. Es muss lediglich die Verbindung zum iPod touch oder iPhone hergestellt werden. Ist einmal die „AR.FreeFlight“ Applikation heruntergeladen, verwandelt sich der iPod touch das iPhone in eine echte Kommandozentrale.“ Wozu das Spielzeug auch geeignet ist, liegt auf der Hand: Mit dem Fluggerät können aus der Luft - ob in Räumen oder im Freien - für einen geringen Preis und kinderleicht ferngesteuert Bilder erstellt werden und kann so in die Privatsphäre von Dritten eingegriffen werden (www.markengold.de 01.07.2010).

Fahrende Kfz-Bordelektronik geknackt

WissenschaftlerInnen haben es geschafft, sich über das Funknetz des Reifendruckkontrollsystems von fahrenden Autos Zugang zur Kfz-Bordelektronik zu verschaffen. So könnten auch Kriminelle vom Straßenrand aus Sicherheitssysteme manipulieren. Die Forschenden der Universität von South Carolina, USA, haben gemäß der Zeitschrift Technology Review bei ihrem Angriff die nicht abgesicherte Funkverbindung zwischen den Luftdrucksensoren in den Reifen und dem Bordcomputer genutzt. Im Test wurde die Steuereinheit derart manipuliert, dass sie nicht mehr funktionierte (SZ 13.08.2010, 10).

„Radiergummi“ für digitale Personendarstellungen

Forschende der University of California in San Diego/USA haben einen virtuellen „Radiergummi“ entwickelt, der z.B. für den vor allem in Deutschland umstrittenen Straßenansichtsdienst Google Street View genutzt werden kann. Mit der Software lassen sich Fußgänger, die sich auf den digitalen Straßenansichten befinden, eliminieren. Die dabei entstehenden Lücken in den Aufnahmen werden durch Hintergrundinformationen gefüllt, die aus jeweils davor oder danach gemachten Fotosequenzen stammen. Während auf den Google-Bildern derzeit nur Gesichter und Autokennzeichen unkenntlich gemacht werden, bleiben bei der neuartigen Entwicklung von den PassantInnen nur Pixelwolken übrig. Doch hat das System noch Macken: Die Hintergrundrekonstruktion gelingt nur, wenn sich die PassantInnen vor relativ monotonen, flächigen Ansichten bewegen. Außerdem können bisher nur Einzelpersonen digital getilgt werden; für Gruppen funktioniert die Methode noch nicht (Der Spiegel 34/2010, 125).

DNA-Analyse soll weiter beschleunigt werden

Die Onlineausgabe von Technology Review berichtete, wie ein Team von Forschenden der MIT und der Harvard University in Cambridge, USA, unter Einsatz des ultradünnen Materials Graphen neuartige DNA-Analyseverfahren voranbringen will. Die sogenannte Nanoporen-Sequenzierung erlaube es, lange Erbgutstränge deutlich schneller zu erfassen als bisherige Verfahren. Bei dem Prozess wird ein langer DNA-Strang durch ein winziges Loch einer Membran gezogen, die in einer unter Spannung stehenden Salzlösung steckt. Ionen bewegen sich von einer Seite der Membran auf die andere und erzeugen so elektrischen Strom. Mit jeder der vier verschiedenen DNA-Basen, die sich durch die Nanoporen bewegen, verändert sich die Stromstärke um einen eindeutigen Wert, was sich dann sehr schnell auslesen lässt. Derzeit basieren die Nanoporen für die DNA-Sequenzierung i.d.R. auf Bakterien-Proteinen oder werden in Membranen aus Silizium-Nitriden geätzt. Die Membrane messen zwischen 20 und 30 Nanometer. Da der Abstand zwischen zwei DNA-Basen 0,5 Nanometer beträgt, bleiben dabei 40 bis 60 Basen zugleich in der Pore stecken. Ein dünnerer Membran wie Graphen erlaubt ein deutlich genaueres Auslesen. Das Material ist in einer einzelnen Schicht nur einen Nanometer dick – atomdick, so die Forschenden (Schwan www.heise.de 24.08.2010).

Rechtsprechung

EUGH

Datenschutz für Lobbyisten

Der Europäische Gerichtshof (EuGH) entschied mit Urteil vom 29.06.2010 im Fall „Bavarian Lager", dass bei Einsicht in Dokumente, bei welcher der Schutz der Privatsphäre oder der Integrität der betroffenen Personen beeinträchtigt würde, deren Zustimmung notwendig ist (Az. C-28/08 P). Geklagt hatte einen Importeur, der bayerisches Bier – in Flaschen – in Großbritannien vertreiben wollte. Dort aber begünstigte eine Regelung Fassbier. Vertreter der britischen Regierung und des Bierbrauerverbands trafen sich mit der EU-Kommission. Der Importeur wollte, aber durfte nicht dabei sein. Bei dem Treffen wurde das ursprüngliche Problem aus der Welt geschafft und die Regelung zugunsten von Flaschenbier geändert. Der misstrauisch gewordene Importeur verlangte ein vollständiges Protokoll des Treffens, bekam es aber nicht: Die Namen der Teilnehmer, soweit sie ihrer Preisgabe widersprochen hatten, verweigerte ihm die Kommission. Seit 2001 gelten zwei Verordnungen, um die es hier geht: Die eine betrifft den Schutz persönlicher Daten, die andere den Zugang der Bürger zu Dokumenten der Europäischen Union. Die Kommission stand vor dem Konflikt zwischen Transparenz und Datenschutz und entschied sich für den Datenschutz und gegen den Antrag auf Informationszugang.

Das Gericht erster Instanz hatte zuvor keinen legitimen Grund erkennen können, warum das Interesse der Brauerei-Lobbyisten, anonym auf die Entscheidungsträger in Brüssel und London einwirken zu können, schutzwürdiger sei und hatte den Bescheid der Kommission für nichtig erklärt. Die Kommission legte Rechtsmittel ein. Auch die Generalanwältin Eleanor Sharpston engagierte sich für mehr Transparenz. Ihre Schlussanträge eröffnete sie mit einem Zitat von Isaac Asimov:

„`Was geschähe, wenn eine unwiderstehliche Kraft auf einen unbewegbaren Gegenstand träfe?´ Setzt man für `unwiderstehliche Kraft´ das Recht auf Zugang zu Dokumenten und für `unbewegbarer Gegenstand´ personenbezogene Daten ein, ergibt sich ein recht anschauliches Bild von der Komplexität, die dem beim Gerichtshof anhängigen Rechtsmittel der Kommission innewohnt." Sie schlug eine andere Möglichkeit vor als das Gericht erster Instanz, Datenschutz und Informationsfreiheit zum Ausgleich zu bringen: Die Datenschutz-Verordnung betreffe die (elektronische) Verarbeitung von Daten und nicht den Zugang zu Dokumenten. Dokumente, in denen Namen beiläufig erwähnt sind, müssten somit zugänglich gemacht werden, ohne dass die Datenschutz-Verordnung im Wege stehe. Die Schlussanträge verfolgten das Ziel, dem freien Zugang der Bürger zu Dokumenten der EU zur Geltung zu verhelfen. Der Europäische Datenschutzbeauftragte Peter Hustinx hatte sich im Vorfeld der Entscheidung eingesetzt, dass die Entscheidung der ersten Instanz bestätigt wird.

Dem wollte sich der EuGH nicht anschließen. Er meinte kühl, dass die Namen der Lobbyisten persönliche Daten und damit von der Datenschutz-Verordnung geschützt seien. Damit hätten sie der Weitergabe zustimmen müssen. Da dies nicht der Fall war, seien die Namen zu Recht geschwärzt worden. Der EuGH erinnerte daran, dass die Verordnung über den Zugang zu Dokumenten als allgemeine Regel festlegt, dass Dokumente der Unionsorgane der Öffentlichkeit zugänglich sind, jedoch wegen bestimmter öffentlicher und privater Interessen Ausnahmen vorsieht. Namentlich die Bestimmung der Verordnung, die – für den Fall, dass durch die Verbreitung der Schutz der Privatsphäre oder der Integrität des Einzelnen beeinträchtigt würde – eine Ausnahme vom Zugang zu Dokumenten vorsieht, enthalte eine spezifische, verstärkte Schutzregelung für Personen, deren personenbezogene Daten veröffentlicht werden könnten.

Wenn ein nach der Verordnung über den Zugang zu Dokumenten gestellter Antrag auf die Gewährung des Zugangs zu Dokumenten gerichtet ist, die personenbezogene Daten enthalten, seien die Bestimmungen der Verordnung über den Schutz personenbezogener Daten in vollem Umfang anwendbar, einschließlich derjenigen, nach der der Empfänger der Übermittlung personenbezogener Daten verpflichtet ist, die Notwendigkeit der Preisgabe dieser Daten nachzuweisen, und derjenigen, nach der der Betroffene jederzeit aus zwingenden, schutzwürdigen, sich aus seiner besonderen Situation ergebenden Gründen gegen die Bearbeitung von ihn betreffenden Daten Widerspruch einlegen kann.

Die Liste der Teilnehmer des Treffens vom 11.10.1996 im Protokoll enthalte personenbezogene Daten. Die Personen, die an diesem Treffen teilgenommen hätten, könnten im Protokoll identifiziert werden könnten. Nach der Feststellung, dass Bavarian Lager Zugang zu allen Informationen über das Treffen vom 11.10.1996 einschließlich der von den Beteiligten in ihrer beruflichen Eigenschaft abgegebenen Meinungsäußerungen gewährt wurde, prüfte der EuGH, ob die Kommission Zugang zu dem Schriftstück mit den fünf Namen der Teilnehmer des Treffens gewähren durfte, und gelangt zum Schluss, dass die Kommission zu Recht geprüft hat, ob diese Personen der Preisgabe der sie betreffenden personenbezogenen Daten zugestimmt hatten. Da die Zustimmung der fünf Teilnehmer des Treffens von Oktober 1996 nicht vorlag, habe die Kommission mit der Weitergabe einer Fassung des streitigen Schriftstücks, in der ihre Namen geschwärzt waren, hinreichend die ihr obliegende Pflicht zur Transparenz beachtet. Da Bavarian Lager keine ausdrückliche rechtliche Begründung gegeben und kein überzeugendes Argument vorgetragen habe, um die Notwendigkeit der Übermittlung dieser personenbezogenen Daten darzutun, sei es der Kommission nicht möglich gewesen, die verschiedenen Interessen der Beteiligten gegeneinander abzu-

wägen. Sie habe auch nicht gemäß der Verordnung über den Schutz personenbezogener Daten prüfen können, ob ein Grund für die Annahme, dass durch diese Übermittlung möglicherweise die berechtigten Interessen der Betroffenen beeinträchtigt werden konnten, bestand oder nicht (Steinbeis verfassungsblog.de 29.07.2010; kostenlose-urteile.de 29.07.2010).

BVerfG

Blitzgeräte zur Geschwindigkeitskontrolle erlaubt

Gemäß einem Nichtannahmebeschluss des Bundesverfassungsgerichts (BVerfG) vom 05.07.2010 dürfen VerkehrssünderInnen durch die Bildaufnahmen eines sog. Blitzers überführt werden (Az. 2 BvR 759/10). Die Fotos griffen zwar in das Grundrecht auf informationelle Selbstbestimmung ein, der Zweck der Sicherheit im Straßenverkehr rechtfertige jedoch diesen Grundrechtseingriff. Die Richter wiesen damit die Verfassungsbeschwerde eines Rasers ab, der durch die Aufnahmen eines Blitzers überführt worden war und eine Geldbuße zahlen musste. Es handele sich nicht um eine verdeckte Datenerhebung, sondern um für jedermann sichtbare Vorgänge auf öffentlichen Straßen. Außerdem fotografiere das Messgerät nicht Unbeteiligte, sondern nur die VerkehrsteilnehmerInnen, die durch ihr unkorrektes Verhalten im Straßenverkehr selbst Anlass dazu gäben. Die Maßnahmen seien damit nicht unverhältnismäßig (SZ 21.07.2010, 6).

BVerwG

Speicherung in Datei „Gewalttäter Sport“ rechtmäßig

Mit Urteil vom 09.06.2010 entschied das Bundesverwaltungsgericht (BVerwG) in Leizig, dass die Speicherung der Daten eines Fußball-Fans in der Datei „Gewalttäter Sport“ zulässig sei (Az. 6 C 5.09). Damit wurde endgültig die Klage eines Mannes abgewiesen, der die Löschung seiner Daten in der beim Bundeskriminalamt eingerichteten Datei erreichen wollte. Die Datei stünde mit der am 09.06.2010 in Kraft getreten Verordnung zur Art der zu speichernden Daten auf einer neuen rechtlichen Grundlage. Zudem sei die Speicherung nur dann unzulässig, wenn sich aus den Gründen der staatsanwaltschaftlichen Einstellungsentscheidung ergebe, dass der Betroffene die Tat nicht oder nicht rechtswidrig begangen habe. Dies sei hier nicht der Fall.

Der Kläger ist Fan des Fußballvereins Hannover 96. Kurz nach Beginn eines Regionalliga-Spiels im Leine-Stadion in Letter im Mai 2006 betrat er mit einer Gruppe von etwa 40 weiteren Fans von Hannover 96 das Stadion, überkletterte die Absperrung und lief vor den gegnerischen Fan-Block. Aus der Gruppe wurden 2 oder 3 Feuerwerkskörper, ein Bengalfeuer und ein fester Gegenstand geworfen. Nach Zeugenberichten lief der Kläger an der Spitze der Gruppe. Das gegen ihn eingeleitete Verfahren wegen Landfriedensbruch wurde von der Staatsanwaltschaft gemäß § 170 StPO eingestellt, weil dem Kläger eine Beteiligung an Ausschreitungen nicht nachzuweisen war. Auf ein Auskunftsersuchen hin wurde ihm von der beklagten Polizeidirektion Hannover mitgeteilt, dass er im Zusammenhang mit den o.g. Ereignissen wegen des Verdachts des Landfriedensbruchs in der Verbunddatei „Gewalttäter Sport“ mit Name, Vorname, Geburtsdatum und -ort, Geschlecht, Staatsangehörigkeit, Personalausweisdaten und Vereinszuordnung erfasst sei und dass die Löschung des Datensatzes im Mai 2011 anstehe.

Mit seiner auf Löschung gerichteten Klage hatte er beim Verwaltungsgericht Hannover und beim Oberverwaltungsgericht (OVG) Lüneburg Erfolg: Die Datei „Gewalttäter Sport“ sei errichtet und betrieben worden, ohne dass der Bundesminister des Innern eine gem. § 7 Bundeskriminalamtsgesetz (BKAG) vorgesehene Verordnung über die Art der zu speichernden Daten erlassen habe. Gegen das Urteil des OVG hatte die Polizeidirektion Revision eingelegt. Nach Vorlage vom 28.05.2010 durch das Bundesministerium des Innern hatte der Bundesrat am 04.06.2010 die nötige Verordnung für die Datei erlassen, die fünf Tage später in Kraft trat. Auf dieser Grundlage wurde jetzt die Klage durch das BVerwG abgewiesen. Es folgte nicht dem Einwand des Klägers, dass nach Einstellung des strafrechtlichen Ermittlungsverfahrens die weitere Speicherung der Daten nicht mehr zulässig sei. Nach § 8 BKAG sei die Speicherung nur dann unzulässig, wenn sich aus den Gründen der staatsanwaltschaftlichen Einstellungsentscheidung ergibt, dass der Betroffene die Tat nicht oder nicht rechtswidrig begangen hat. Dies sei nach den bindenden Feststellungen des OVG aber nicht der Fall (www.beck-aktuell.beck.de 09.06.2010).

VG Berlin

Verdachtsunabhängige Demo-Videoüberwachung rechtswidrig

Das Verwaltungsgericht (VG) Berlin hat in einem Urteil vom 05.07.2010 die verdachtsunabhängige Videoüberwachung friedlicher Demonstrationen durch die Polizei wegen nicht gerechtfertigter Eingriffe in die Grundrechte der Betroffenen für rechtswidrig erklärt (Az.: VG 1K 905.09). Die langjährige polizeiliche Praxis in der Hauptstadt, Protestkundgebungen angeblich zu Zwecken der Einsatzlenkung und zur Gewährleistung der Verkehrssicherheit zu filmen, greife in den Schutzbereich der „vorrangigen Versammlungsfreiheit“ und in den der informationellen Selbstbestimmung ein; eine rechtfertigende gesetzliche Grundlage sei nicht vorhanden. Anlass der Entscheidung war die Überwachung einer Anti-Atom-Demonstration mit mindestens 25.000 Teilnehmenden zwischen Hauptbahnhof und Brandenburger Tor am 05.09.2009. Während des Aufzuges fuhren Einsatzkräfte der Polizei mit einem Kleintransporter wenige Meter vor der Spitze der Demonstration her und filmten das Geschehen mit mehreren auf dem Dach des Wagens montierten Kameras. Die Aufnahmen wurden ohne Zeitverzögerung an die Einsatzleitstelle übertragen. Dagegen

klagte ein Bürger, der in der ersten Reihe marschierte und sich so eindeutig innerhalb des von den elektronischen Augen der Gesetzeshüter erfassten Bereichs befand. Beschwerden gegen eine teils offene und teils verdeckte Videoüberwachung hatte es zuvor etwa bereits im Rahmen der sich gegen den Überwachungswahn in Staat und Gesellschaft richtenden Großdemo „Freiheit statt Angst“ im Oktober 2008 gegeben. Der Senat verteidigte die Aufnahmen später mit einem Hinweis auf einen eingegangenen „Aufruf zu Gewalttaten“.

Das VG Berlin stellte nun hinsichtlich der Anti-Atom-Demo fest, dass der einzelne Teilnehmer bei einer Beobachtung der Versammlung im „Kamera-Monitor-Verfahren“ damit rechnen müsse, aufgezeichnet und registriert zu werden. Dies könne ihn vom Begleiten einer entsprechenden Veranstaltung abschrecken oder zu ungewollten Verhaltensweisen zwingen, um den beobachtenden Polizeibeamten möglicherweise gerecht zu werden. Durch diese Einschüchterung könnte mittelbar auf den Prozess der Meinungsbildung und der demokratischen Auseinandersetzung eingewirkt werden. Erlaubt seien Bild- oder Tonaufnahmen durch die Berliner Polizei gemäß dem Versammlungsgesetz des Landes nur, wenn „tatsächliche Anhaltspunkte die Annahme rechtfertigen“, dass von Teilnehmenden öffentlicher Versammlungen „erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen“. Dafür müsse eine entsprechende Gefahrenprognose ersichtlich sein. Nach Angaben eines Sprechers des VG hat das Urteil Auswirkungen auf andere Demonstrationen in der Stadt: „Wenn man davon ausgehen kann, dass es eine friedliche Demonstration wird, darf die Polizei nicht filmen“. Fredrik Roggan, stellvertretender Vorsitzender der Bürgerrechtsorganisation Humanistische Union, begrüßte das Urteil wegen seiner „grundlegenden“, über den aktuell verhandelten Fall hinausgehenden Bedeutung: „Das Verwaltungsgericht hat mit seinem Beschluss die Demonstrationsfreiheit erheblich gestärkt.“ Es gebe ein Recht darauf, ohne Angst vor Videoüberwachung an friedlichen Versammlungen teilzunehmen. Den Berliner Gesetzgeber forderte er auf, bei einer eventuellen Novellierung des Versammlungsrechts den Grundgedanken dieser Entscheidung zu beachten.

Das Land hat die Einlegung eines Rechtsmittels angekündigt. Die Polizei betrachtet das Filmen von Demonstrationen für die spätere Verfolgung von Straftätern als unerlässlich, so Berlins Innensenator Ehrhart Körting: „Wir teilen die Rechtsauffassung des Verwaltungsgerichts nicht. Nach unserer Auffassung ist bei allen Großveranstaltungen eine Live-Beobachtung durch die Einsatzleitung der Polizei aus Gründen der Gefahrenabwehr notwendig.“ Sollte die Entscheidung obergerichtlich bestätigt werden, „dann ist der Gesetzgeber in Berlin gefordert“. Auch bei der Gewerkschaft der Polizei (GdP) reagierte man mit Unverständnis auf das Urteil. Angesichts der Gewaltbereitschaft in Berlin sei das Urteil nicht nachvollziehbar (Krempl www.heise.de 27.07.2010; Berg www.taz.de 27.07.2010; von Bullion SZ 28.07.2010).

BGH

Präimplantationsdiagnostik nach Befruchtung ist nicht strafbar

Der Bundesgerichtshof (BGH) stellte in einem Grundsatzurteil vom 06.07.2010 klar, dass ÄrztInnen künstlich gezeugte Embryonen im Rahmen der sog. Präimplantationsdiagnostik (PID) auf mögliche Genschäden untersuchen dürfen (Az. 5 StR 386/09). Er bestätigte ein Urteil des Landgerichts (LG) Berlin, das einen Frauenarzt mit dem Schwerpunkt Kinderwunschbehandlung vom Vorwurf einer dreifachen strafbaren Verletzung des Embryonenschutzgesetzes freigesprochen hatte. Der 47 Jahre alte Mediziner hatte sich nach vorheriger Beratung selbst angezeigt. In den Jahren 2005 und 2006 hatten sich drei Paare mit dem Ziel einer extrakorporalen Befruchtung an den Angeklagten gewandt. In allen Fällen wies einer der Partner genetische Belastungen auf. Aufgrund dessen bestand die Gefahr, dass auch die erzeugten Embryonen genetisch belastet sein würden, was einen Abort, eine Totgeburt, ein Versterben des Neugeborenen nach der Geburt oder die Geburt eines schwerkranken Kindes hochwahrscheinlich machte. In einem Fall bestand die Gefahr, der Fötus könnte im Mutterleib nicht lebensfähig sein. Im zweiten Fall hatte die Mutter bereits eine schwerstbehinderte Tochter zur Welt gebracht. Im dritten Fall hatten Schädigungen des Erbguts bereits zu zwei Fehlgeburten und einer Abtreibung geführt. Im Hinblick auf die Gefahrenlage und dem Wunsch seiner PatientInnen entsprechend führte der Angeklagte jeweils eine PID an pluripotenten, d.h. nicht zu einem lebensfähigen Organismus entwicklungsfähigen Zellen durch. Die Untersuchung diente dem Zweck, nur Embryonen ohne genetische Anomalien übertragen zu können. Dies geschah in allen Fällen. Embryonen mit festgestellten Chromosomenanomalien wurden hingegen nicht weiter kultiviert und starben in der Folge ab.

Der 5. („Leipziger“) Strafsenat des Bundesgerichtshofs verwarf die Revision der Staatsanwaltschaft gegen den Freispruch des LG Berlin. Der Angeklagte habe nicht § 1 Abs. 1 Nr. 2 ESchG (missbräuchliche Anwendung von Fortpflanzungstechniken) und § 2 Abs. 1 ESchG (missbräuchliche Verwendung menschlicher Embryonen) verletzt. Aus den genannten Strafbestimmungen könne nicht mit der im Strafrecht erforderlichen Bestimmtheit (Art. 103 Abs. 2 GG) ein Verbot der bei Erlass des Embryonenschutzgesetzes im Jahr 1990 erst im Ausland entwickelten PID abgeleitet werden, die den Embryo nach derzeitigem medizinisch-naturwissenschaftlichem Kenntnisstand überdies nicht schädigt. Das Vorgehen des Angeklagten verstoße weder gegen den Wortlaut noch gegen den Sinn des Gesetzes. Auch dem bei jeder Gesetzesauslegung zu würdigenden Willen des historischen Gesetzgebers lasse sich ein Verbot einer solchen PID, die der Gesetzgeber nicht ausdrücklich berücksichtigt hat, nicht entnehmen.

Dem mit dem Gesetz verfolgten Zweck des Schutzes von Embryonen vor Missbräuchen laufe die PID nicht zuwider. Das Embryonenschutzgesetz erlaubt die extrakorporale Befruchtung zur Herbeiführung einer Schwangerschaft ohne weitere Einschränkungen. Ein strafbewehrtes Gebot, Embryonen auch bei genetischen Belastungen der Eltern ohne Untersuchung zu übertragen, berge hohe Risiken in sich; vor allem sei zu besorgen, dass sich die Schwangere im weiteren Verlauf nach einer ärztlicherseits angezeigten und mit denselben Diagnosemethoden durchgeführten Pränataldiagnostik, hinsichtlich derer eine ärztliche Aufklärungspflicht besteht, für einen Schwangerschaftsabbruch entscheidet. Die PID sei geeignet, solch schwerwiegende Gefahren zu vermindern. Es könne nicht davon ausgegangen werden, dass der Gesetzgeber sie verboten hätte, wenn sie bei Erlass des Embryonenschutzgesetzes schon zur Verfügung gestanden hätte. Dagegen spräche auch eine Wertentscheidung, die der Gesetzgeber in § 3 Satz 2 des Embryonenschutzgesetzes getroffen hat. Dort ist eine Ausnahme vom Verbot der Geschlechtswahl durch Verwendung ausgewählter Samenzellen normiert worden. Mit dieser Regelung ist der aus dem Risiko einer geschlechtsgebundenen Erbkrankheit des Kindes resultierenden Konfliktlage der Eltern Rechnung getragen worden, die letztlich in einen Schwangerschaftsabbruch einmünden kann. Eine gleichgelagerte Konfliktlage habe in den zu beurteilenden Fällen bestanden. Der BGH betonte, dass Gegenstand seiner Entscheidung nur die Untersuchung von Zellen auf schwerwiegende genetische Schäden zur Verminderung der genannten Gefahren im Rahmen der PID sei. Einer unbegrenzten Selektion von Embryonen anhand genetischer Merkmale, etwa die Auswahl von Embryonen, um die Geburt einer „Wunschtochter“ oder eines „Wunschsohnes“ herbeizuführen, wäre damit nicht der Weg geöffnet, so der Senatsvorsitzende Clemens Basdorf: „Es geht nicht um die Billigung irgendwelcher Selektionen von Embryonen, um die Geburt eines Wunschkindes herbeiführen zu können“ (PE BGH 06.07.2010; Janisch SZ 07.07.2010, 1, 4).

BAG

Schadensersatz wegen Altersdiskriminierung bei Ausschreibung

Das Bundesarbeitsgericht (BAG) verurteilte am 19.08.2010 auf Klage eines 1958 geborenen Volljuristen eine juristische Fachzeitschrift zu Zahlung eines Schadensersatzes in Höhe von einem Monatsgehalt wegen Nichtberücksichtigung bei einer Ausschreibung und der damit erfolgten Altersdiskriminierung (Az. 8 AZR 530/09). Die Zeitschrift suchte im Jahr 2007 „eine(n) junge(n) engagierte(n) Volljuristin/Volljuristen“; den Zuschlag erhielt eine 33 Jahre alte Frau. Der nicht berücksichtigte Bewerber hatte auf eine Entschädigung von 25.000 Euro und Schadenersatz in Höhe eines Jahresgehaltes geklagt. Das Landesarbeitsgericht (LAG) München und das BAG hielten aber nur ein Monatsgehalt für angemessen; um das Jahresgehalt zu bekommen, hätte er nachweisen müssen, dass er bei einer diskriminierungsfreien Auswahl eingestellt worden wäre; dies war ihm nicht gelungen (Vorinstanz LAG München U.v. 03.06.2010, Az. 10 Sa 719/08; SZ 28./29.08.2010, V2/9; www.rechtslupe.de 20.08.2010).

LAG Mecklenburg-Vorpommern

Arbeitnehmer dürfen trotz Schweigeklausel über Gehalt reden

Das Landesarbeitsgericht (LAG) Mecklenburg-Vorpommern urteilte am 21.10.2009, dass ArbeitnehmerInnen nicht gezwungen werden können, über ihren Lohn zu schweigen (Az. 2 Sa 237/09). Ein Arbeitnehmer war abgemahnt worden, weil er die Höhe seines Lohnes mit einem Kollegen besprochen hatte. Dies hatte seine Firma im Arbeitsvertrag aber untersagt. Das Unternehmen hatte seine Arbeitnehmer zur Verschwiegenheit verpflichtet, weil es befürchtete, dass Gespräche über Lohnunterschiede den Betriebsfrieden stören könnten. Der Arbeitnehmer klagte und verlangte, dass die Abmahnung aus der Personalakte gelöscht wird. Die Richter gaben ihm Recht. Die Verschwiegenheitsklausel im Arbeitsvertrag sei unwirksam, weil sie verhindere, dass der Arbeitnehmer die Höhe seines Lohns mit anderen vergleichen und sich dann wehren könne, wenn er für gleiche Arbeit weniger verdiene. Die Verschwiegenheitsverpflichtung stelle eine unangemessene Benachteiligung des Arbeitnehmers entgegen den Geboten von Treu und Glauben im Sinne von § 307 BGB dar. Nach der ständigen Rechtsprechung des Bundesarbeitsgerichts sei der Arbeitgeber auch bei der Lohngestaltung dem Gleichbehandlungsgrundsatz verpflichtet (vgl. Bundesarbeitsgericht, Urteil v. 15.07.2009 - 5 AZR 486/08 -). Die einzige Möglichkeit für den Arbeitnehmer festzustellen, ob er Ansprüche aus dem Gleichbehandlungsgrundsatz hinsichtlich seiner Lohnhöhe hat, sei das Gespräch mit Arbeitskollegen. Ein solches Gespräch sei nur erfolgreich, wenn der Arbeitnehmer selbst auch bereit ist, über seine eigene Lohngestaltung Auskunft zu geben. Könnte man ihm derartige Gespräche wirksam verbieten, hätte der Arbeitnehmer kein erfolgversprechendes Mittel, Ansprüche wegen Verletzung des Gleichbehandlungsgrundsatzes im Rahmen der Lohngestaltung gerichtlich geltend zu machen. Die Rechtsanwaltskammer Düsseldorf hatte zuvor ausdrücklich auf dieses Rederecht hingewiesen, zumal in etwa einem Viertel aller Arbeitsverträge eine solche „Schweigeklausel“ bestehen soll (Finanztest 8/2010; Prummer SZ 16.08.2010, 22).

Buchbesprechung

Gregor Thüsing
Arbeitnehmerdatenschutz und Compliance
Effektive Compliance im Spannungsfeld von reformiertem BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung
C. H. Beck 2010
ISBN 978-3-406-60497-3
308 Seiten, kartoniert, 79,00 Euro

(sj) Gregor Thüsing, Arbeitsrechtler an der Universität Bonn, hat ein mutiges Buch geschrieben. Zusammen mit seinen Mitarbeitern Gerrit Forst, Thomas Granetzny und Wolfgang Schorn hat er sich an die Themen Compliance und Arbeitnehmerdatenschutz gewagt, obwohl – oder gerade weil – die Mitarbeiterüberwachung durch den Arbeitgeber demnächst gesetzlich neu geregelt werden soll. Dass Thüsing trotzdem Zeit und Energie in das Buchprojekt gesteckt hat, spricht für ihn – und für eine zweite, aktualisierte Auflage.

Mutig ist das Werk aber auch unter einem ganz anderen Gesichtspunkt: Bei zahlreichen Streitfragen stellt sich Thüsing konsequent gegen die so genannte herrschende Meinung. Dies kann beim Leser für Begeisterung, aber auch für Befremdung sorgen. Doch dazu später.

Thematisch kann „Arbeitnehmerdatenschutz und Compliance“ grob in vier Teile untergliedert werden: Knapp ein Zehntel des Buchs widmet Thüsing dem Thema Compliance; dieser erste Part ist vor allem für den Leser von Interesse, der sich als Datenschützer dem Thema nähert. Im zweiten Teil erläutert Thüsing auf gut 40 Seiten das System des Beschäftigtendatenschutzes. Im dritten Abschnitt des Buchs werden dann fünf „Konfliktfelder des Arbeitnehmerdatenschutzes“ dargestellt: der elektronische Datenabgleich, die Sichtung und Speicherung von E-Mails und Logfiles, die Sichtung von Telefonverbindungsdaten, die Videoüberwachung und das Fragerecht des Arbeitgebers bei der Einstellung. Der vierte und letzte Teil behandelt den Datentransfer im Konzern, die Datenweitergabe an Dritte, verschiedene Informationspflichten, die Rechtsfolgen einer unerlaubten Datenverarbeitung sowie betriebsverfassungsrechtliche Aspekte.

Schon dieser allgemeine Überblick belegt, dass das Werk inhaltlich mehr bietet, als der Titel suggeriert. Beispielsweise werden Fragerecht und Datennutzung bei Einstellung auf etwa 20 Seiten abgehandelt, ohne dass deutlich wird, in welchem Zusammenhang sie zur Compliance stehen. Ob diese und andere Ausführungen nun als „Sahnehäubchen“ verstanden werden oder als „Sättigungsbeilage“, muss jeder Leser für sich entscheiden. Aber wer wie Thüsing laut Klappentext „Vorstände und Geschäftsführer“ als Zielgruppe im Auge hat, sollte sich vielleicht eher knapper fassen. (Nebenbei: Datenschutzbeauftragte werden nicht als Zielgruppe genannt.)

Sinnbildlich beschreibt Thüsing Compliance als einen Weg zwischen Scylla und Charybdis, als eine Passage zwischen Mitarbeiterüberwachung und Beschäftigtendatenschutz. Anders als weiland Odysseus steuert Thüsing jedoch nicht elegant zwischen diesen beiden Gefahren hindurch, sondern wagt sich gemeinsam mit dem Leser bedenklich nah an die Überwachungs-Scylla heran. Oder um es mit deutlicheren Worten zu sagen: Thüsing vertritt eine Compliance-freundliche Position, die für Datenschützer stellenweise schwer erträglich ist.

Ausgehend von der Prämisse, dass „gebotene“ Compliance-Maßnahmen letztendlich nicht gegen Datenschutzvorschriften verstoßen können, konstruiert Thüsing eine Rechtswirklichkeit, die außerhalb seines Werks so nicht existiert. So vertritt Thüsing beispielsweise die Auffassung, dass das Telekommunikationsgesetz (TKG) im Arbeitsverhältnis auch dann nicht anwendbar sei, wenn der Arbeitgeber die private Nutzung von Telefonie- und Internet-/E-Mail-Diensten erlaubt. Leider kann er seine Rechtsmeinung nicht überzeugend begründen. Gewagt ist auch die Behauptung, Betriebsvereinbarungen seien „gesetzliche Vorschriften“ im Sinne des Telekommunikationsrechts (und damit Rechtsgrundlage für eine Datenverarbeitung). Dass diese Behauptung dem eindeutigen Wortlaut des TKG widerspricht, ficht Thüsing nicht an. Es handele sich um eine „bloße Ungenauigkeit bei der Formulierung“, also um eine Nachlässigkeit des Gesetzgebers.

Befremdlich wirkt auch die These, dass sich Arbeitnehmer und Arbeitgeber in keinem Über-/Unterordnungsverhältnis befinden, sondern sich als autonome Privatrechtssubjekte gegenüberstehen. Dies mag rechtlich der Fall sein, die Realität sieht angesichts des Weisungsrechts des Arbeitgebers und der wirtschaftlichen Abhängigkeit des Arbeitnehmers anders aus. Wie Thüsing aus der rein juristischen Gleichstellung des Arbeitnehmers auf eine „freiwillige Datenherausgabe“ zu schließen, geht an der betrieblichen Wirklichkeit vorbei.

Thüsing wäre insgesamt überzeugender, wenn er keine Rosinenpickerei betreiben würde. Mal zieht er die Gesetzesbegründung heran, um gegen den Wortlaut des Gesetzes zu argumentieren. An anderer Stelle lehnt er die Begründung als „Motivirrtum“ ab, weil sie seine Auslegung des Gesetzestextes nicht stützt. In der Gesamtheit gesehen

wirkt diese Art der Beweisführung wenig überzeugend.

Seinen argumentativen Tiefpunkt erreicht das Werk auf Seite 78. Dort geht es um die Angemessenheitsprüfung bei Datenabgleichen: Laut Thüsing indiziert die Üblichkeit eines Datenabgleichs seine Angemessenheit. Daran ändere auch der Missbrauch im Einzelfall nichts. Oder etwas schlichter formuliert: Wenn alle es so machen, dann ist es auch rechtlich in Ordnung.

Nun könnte man aus Sicht des Datenschutzes Thüsings Buch als einziges Ärgernis abtun und geflissentlich ignorieren. Damit täte man dem Autor jedoch Unrecht. Thüsing ist ein renommierter Rechtswissenschaftler. Ein Teil seiner Thesen mag argumentativ auf schwachen Füßen stehen, ignorieren sollte man sie nicht. Künftig werden sich viele Compliance-Befürworter auf den „Thüsing“ berufen, wenn sie die Rechtmäßigkeit von Überwachungsmaßnahmen rechtfertigen. Datenschützer sind deshalb gut beraten, sich mit Thüsings Thesen und Argumenten auseinanderzusetzen, um in der Diskussion mit den Compliance-Beauftragten nicht den Kürzeren zu ziehen.

Hinzu kommt, dass das Werk mit Sorgfalt erstellt ist. Mehr als 1000 Fußnoten untermauern den Anspruch der Autoren, einen wissenschaftlich ernstzunehmenden Beitrag zur Debatte um Datenschutz und Compliance abzuliefern. Es ist sowohl Thüsing & Co. als auch dem Beschäftigtendatenschutz zu wünschen, dass das Werk viele Leser findet, die Thüsings Argumente kritisch hinterfragen. Unabhängig davon wäre eine vertiefte wissenschaftliche Auseinandersetzung mit dem Werk wünschenswert.

Presseerklärung:

Google Street View: Schaar fordert Schaffung eines Widerspruchsregisters und Profilbildungsverbot

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, hält verbesserte Regelungen zum Datenschutz im Internet für dringend erforderlich und erwartet – nach Ablehnung der Bundesratsinitiative zu Street View – von der Bundesregierung nun die zügige Vorlage eines entsprechenden Gesetzentwurfs. Er spricht sich insbesondere für ein zentrales Widerspruchsregister gegen Veröffentlichungen persönlicher Daten im Internet und für ein ausdrückliches Verbot der Bildung von Persönlichkeitsprofilen aus.

Schaar erklärte dazu: “Es kann nicht angehen, dass Widerspruchsrechte vom Goodwill der jeweiligen Unternehmen abhängen. Nicht akzeptabel wäre es auch, dass die Betroffenen separat gegenüber allen Anbietern entsprechender Dienste der Veröffentlichung widersprechen müssen. Durch ein zentrales Widerspruchsregister könnte sichergestellt werden, dass ein einziger Widerspruch die Betroffenen gegen die Veröffentlichung ihrer personenbezogenen Daten im Internet schützt. Ein solches Widerspruchsregister könnte zum Beispiel bei der im Koalitionsvertrag vorgesehenen Stiftung Datenschutz eingerichtet werden.“

In diesem Zusammenhang wendet sich Schaar auch gegen die Bildung von Persönlichkeitsprofilen: „Ein Verbot der Bildung von Persönlichkeitsprofilen könnte etwa dazu beitragen, dass die Daten über Mieter oder Eigentümer von veröffentlichten Gebäuden nicht mit anderen persönlichen Informationen zusammengeführt und ausgewertet werden. Die Verknüpfung von personenbezogenen Daten sollte nur dann zulässig sein, wenn die Betroffenen damit einverstanden sind oder wenn ein Gesetz dies ausdrücklich vorschreibt.“

Der Bundesrat hatte einen Gesetzentwurf vorgelegt, durch den gesetzliche Rahmenbedingungen für flächendeckende Aufnahmen von Straßenansichten und deren Veröffentlichung im Internet durch Dienste wie Google Street View geschaffen werden sollen. Die Bundesregierung hat den Entwurf in ihrer heute beschlossenen Stellungnahme nicht befürwortet.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Pressemitteilung 35/2010 Bonn/Berlin, 18. August 2010

pressestelle@bfdi.bund.de

FIfF

DVD

Deutsche Vereinigung
für Datenschutz e.V.

Gemeinsame Jahrestagung 2010

Beschäftigten-Datenschutz

5. – 7. November 2010
Alte Feuerwache – Melchiorstr. 3, 50670 Köln
http://www.fiff.de/2010

Eine Veranstaltung des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) in Kooperation mit der Deutschen Vereinigung für Datenschutz e.V. (DVD). Plakatgestaltung: Frans Jozef Valenta, Bonn