2/2011

Datenschutz Nachrichten

34. Jahrgang
ISSN 0137-7767
9,00 Euro

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

Datenschutz-Baustellen

Inhalt

Termine

Montag, 1. August 2011
Redaktionsschluss DANA 3/11
Thema: Datenschutz bei Online-Spielen,
verantwortlich: Frans Jozef Valenta
Fragen und Anregungen bitte an:
valenta@t-online.de

Samstag, 10. September 2011
Demonstration „Freiheit statt Angst“
Berlin.
kontakt@vorratsdatenspeicherung.de

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

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

Samstag, 29. Oktober 2011
DVD-Mitgliederversammlung
Bonn.

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

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

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

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

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

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

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

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

Abbildungen
Frans Jozef Valenta

Datenschutz-Baustellen

Liebe Leserinnen und Leser,

zählt man die Datenschutz-Baustellen, die derzeit in Deutschland und Europa betrieben werden, so beschleichen einen Zweifel an der Kompetenz der Bauherren und der beauftragten Gewerke. Alles wird angefangen, nichts zu Ende gedacht, nichts fertig gestellt. Vorratsdatenspeicherung, Beschäftigtendatenschutz, Bewertung von Geodaten und der Umgang mit sozialen Netzwerken sind nur einige Aufschriften, die auf Baustellenschildern stehen und uns die miserable Straßenlage des Gesetzgebers vor Augen führen.

In diesem Durcheinander kann selbst Professoren schon mal der rechte Maßstab abhanden kommen. Anlässlich des Gesetzgebungsvorhabens zu DE-Mail gab der Präsident des Branchenverbandes BITKOM, Professor August-Wilhelm Scheer, bereits im Februar 2011 eine zustimmende Presseerklärung heraus.. Während die Mehrzahl der Sachverständigen dem vorgelegten Gesetzentwurf in einer Anhörung des Innenausschusses des Deutschen Bundestages große inhaltliche Schwächen und den Machern durch die Blume Protektionismus der profitierenden Provider vorwarf, blieb BITKOM bei seiner Meinung. DE-Mail sei „ein Quantensprung in puncto Sicherheit“. Gemeint war vermutlich das genaue Gegenteil, ist doch ein Quantensprung die kleinste mögliche Änderung innerhalb atomarer und subatomarer (also sehr kleiner) Systeme. Oder wollten uns die Herren etwa darauf hinweisen, dass man weniger als mit diesem Gesetzentwurf eigentlich gar nicht tun kann?

Ein Quantensprung in puncto Beschäftigtendatenschutz wird jedenfalls gerade auch von der EU-Kommission vorbereitet. In der Absicht, die bereits etwas in die Jahre gekommene Richtlinie 95/46/EG zu modernisieren und an heutige Erfordernisse anzupassen, wurde ein Rahmenpapier zur Kommentierung in einem Konsultationsverfahren erstellt. Das Thema Beschäftigtendatenschutz wurde in dieser Vorgabe der Kommission schlichtweg vollständig ausgeklammert. Dies hat die DVD schon in ihrer Stellungnahme vom 15.1.2011 (abrufbar unter dem Stichwort „Themen“ auf der DVD-Website) nachdrücklich kritisiert. Um die Notwendigkeit zu untermauern, Grundregeln zum Schutz von Beschäftigten in die Datenschutzrichtlinie zu integrieren, plant die DVD außerdem, im Oktober eine Veranstaltung im Europäischen Parlament durchführen. Der Vorstand möchte bei diesem Anlass Parlamentarier und Gruppenvertreter mit stichhaltigen Argumenten für die Integration des Beschäftigtendatenschutzes in die Datenschutzrichtlinie versorgen. Auf dass der Datenschutz nicht bei allzu vielen Baustellen über Nacht in der Baugrube versinkt!

Karin Schuler

Autorinnen und Autoren dieser Ausgabe:

Roland Appel
selbständiger Unternehmensberater und Vorsitzender des Internet-Gütesiegelboards der Initiative D21 e.V., Autor und Herausgeber zahlreicher Publikationen zum Thema Bürgerrechte und Datenschutz, ehemaliger Abgeordneter des Landtags NRW für Die Grünen. roland.appel@roaconsult.de

Robert Beens
Geschäftsführer (CEO) von Ixquick und zuständig für Betrieb, Technik, Produktentwicklung, und Finanzen. robert@ixquick.com

Sönke Hilbrans
Rechtsanwalt, Berlin, Stellv. Vorsitzender der Deutschen Vereinigung für Datenschutz. hilbrans@diefirma.net.

Karsten Neumann
Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern a.D., Stralsund. neumann@baltic-privacy-management.eu

Klaus-Jürgen Roth
roth@datenschutzverein.de

Moritz Tremmel
studiert Politikwissenschaften, Soziologie und Rechtswissenschaften an der Universität Tübingen. info@mtmedia.org

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

Karsten Neumann

Es gibt kein belangloses Datum mehr!

Mit der Einführung einer europarechtlich vorgegebenen Geodateninfrastruktur, nicht nur in Deutschland, entsteht eine bisher kaum wahrgenommene Herausforderung für die Diskussion über die rechtliche Ausgestaltung der Informationsgesellschaft. Die standardisierte Georeferenzierung von Navigationsgeräten, mobilen Telefonen, Fotos bis hin zu den Standortdaten moderner Kommunikationsmittel entwickelt sich zur ultimativen Verknüpfungstechnologie. Waren es bisher Name, Wohnanschrift und Geburtsdatum eines Menschen, ist es heute die Steueridentifikationsnummer oder IP-Adresse, so werden es morgen wahrscheinlich Datum, Uhrzeit und Position auf der Erdoberfläche sein, mit deren Hilfe unterschiedlichste Datensammlungen miteinander verschnitten werden können. Es folgt nun der Vermessung der Welt die Vermessung des Menschen; nicht in seinem medizinischen, sondern in seinem sozialen Beziehungsgeflecht.

Damit wird die Diskussion akut, ob der rechtliche Anknüpfungspunkt „Personenbezug" die reale Gefährdungssituation für das Recht auf informationelle Selbstbestimmung noch adäquat widerspiegelt oder ob der Personenbezug – bei einem negativen Befund – nicht vielleicht „ausgedient hat" und das Datenschutzrecht durch ein Informationsrecht abgelöst werden muss. Ein Informationsrecht, das bereits seine freiheitsgewährende Wirkung entfaltet, wenn noch kein personenbezogenes Datum entstanden ist.

Der Datenschutz schützt keine Daten, sondern Menschen und deren verfassungsgemäßen Anspruch auf freie Entfaltung ihrer Persönlichkeit (Art. 2 Abs. 1 Grundgesetz) bei bedingungsloser Achtung der Würde des Menschen. Es stellt sich heute immer wieder die gleiche Frage, wie sie im Jahr 1983 dem Bundesverfassungsgericht gestellt wurde: welcher Zusammenhang besteht zwischen personalen Rechten und objektiven Daten? Und: welche gesetzlichen Schlussfolgerungen müssen sich aus dem Befund ergeben?

„Die Verfassungsbeschwerden geben keinen Anlass zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses" Datum mehr." (Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15. Dezember 1983 - 1 BvR 209/83 u.a. - sog. Volkszählungsurteil)

Damit machte bereits das Bundesverfassungsgericht die **Möglichkeit** der Verwendung und Nutzung der Daten zum Anknüpfungspunkt der Bewertungen. Es wird zu Recht weder eine konkrete oder bereits realisierte Gefahr des Missbrauchs unterstellt, sondern allein die theoretische Möglichkeit des Eingriffs in Freiheitsrechte als ausreichender Anlass für die Ergreifung von Schutzmaßnahmen angesehen. Bereits 1983 sah das Bundesverfassungsgericht dabei den besonderen Einfluss, den die „der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten" auf das Ergebnis der Risikobewertung haben.

Eben diese erahnten Verknüpfungsmöglichkeiten haben sich in den letzten Jahren erst dramatisch erweitert. Nach „Data-Warehouse" und „Data-Mining" ermöglicht die allgegenwärtige Geolokalisation Gerätestandorten eine dynamische Verknüpfungsmöglichkeit, indem eine Person jederzeit an (noch fast) jedem Ort identifiziert werden kann und dieser Person damit andere Daten aus ihrer Umgebung zugeordnet werden können. Damit besteht die Möglichkeit der Erstellung eines Bewegungsprofiles, das ohne Weiteres mit anderen Datensammlungen über die jeweilige Umgebung des Aufenthaltsortes oder andere Personen, die sich dort zum gleichen Zeitpunkt aufhalten, verknüpft werden kann und so die Erstellung von Persönlichkeitsprofilen ermöglicht.

Erst die Verknüpfung macht aus Daten Informationen. Der Vergleich zu den im Berg schlummernden Rohstoffen liegt nahe. Im Gegensatz zum Bergbau soll „Datamining" aber nicht nur die jeweils relevanten Daten zu Tage fördern, sondern bisher unbekannte Zusammenhänge zwischen Einzeldaten aus der Gesamtheit eines Datenbestandes erkennen, um aus diesen – die Aussagekraft der einzelnen Angaben meist deutlich übersteigenden – Informationen vor allem wirtschaftliche Vorteile für die speichernde Stelle erzielen zu können. Es geht also nicht nur um das „Auffinden" der jeweils richtigen Daten, sondern es geht um das Generieren, das Schmelzen und Gießen, das Legieren und chemische Herstellen von Informationen. Und wie die industrielle Revolution von den Technologien getrieben, aber erst durch Standardisierung zur Massenproduktion fand, so ist es auch in der Informationsgesellschaft die Verabredung von gemeinsamen Standards, die neuen Technologien erst zu ihrer Massenwirksamkeit verhilft. Ein solcher neuer Standard scheint sich aus der Georeferenzierbarkeit zu entwikkeln.

Neue Infrastruktur für Profilbildung

Mit den Vorgaben der Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft,

der sog. INSPIRE-Richtlinie, soll eine Geodateninfrastruktur in der Europäischen Gemeinschaft geschaffen werden. Für die Umsetzung dieser Vorgaben sind in allen Ländern entsprechende Rechtsgrundlagen geschaffen[1].

Georeferenzierte Informationen sind Informationen, die einen Bezug zu einem fest definierten Punkt auf der Erdoberfläche aufweisen. Dieser Bezug ist inzwischen – dank der INSPIRE-Richtlinie – einheitlich bestimmt und damit auch unabhängig vom jeweiligen Bezugssystem jederzeit reproduzierbar. Nicht mehr nur Satelliten- und Luftbildaufnahmen, kartografische Karten oder Bauleitplanungen, sondern auch Fotos, Handystandorte und IP-Adressen sowie mittels RFID-Chips gekennzeichnete Chemietransporte, Sondermüll, der Dienstwagen oder die 12jährige Tochter sind heute georeferenzierbar. Durch Nutzung von Informations- und Kommunikationstechnik sind sie ortbar, jederzeit und auch ohne Willen und Kenntnis des Betroffenen.

Sowohl der europäische wie der nationale Gesetzgeber wurden sich der Problematik noch rechtzeitig bewusst, weshalb die INSPIRE-Richtlinie als mögliche Ausnahme von dem allgemeinen Grundsatz des unbeschränkten Zugangs in Artikel 13 Nummer 1 formuliert: „...Mitgliedstaaten [können] den Zugang der Öffentlichkeit zu Geodatensätzen und –diensten ... beschränken, wenn dieser Zugang nachteilige Auswirkungen hätte auf ... (f) die Vertraulichkeit personenbezogener Daten und/oder Akten über eine natürliche Person, sofern diese der Bekanntgabe dieser Informationen an die Öffentlichkeit nicht zugestimmt hat und sofern eine solche Vertraulichkeit nach einzelstaatlichem oder gemeinschaftlichem Recht vorgesehen ist.“

Erklärtes Ziel und Ausgangspunkt aller Initiativen war es, den brachliegenden „Digitalen Rohstoff Geoinformation“ zu erschließen. Dabei richten sich die gesetzgeberischen Initiativen vor allem auf die Zugänglichmachung „aller bei der öffentlichen Hand vorhandenen geobasierten Informationen“. Diese sollen unter den Wettbewerbsregeln des Informationsweiterverwendungsgesetzes diskriminierungsfrei und zu einheitlichen Kosten allen Marktteilnehmern in einer technischen Form zur Verfügung gestellt werden, die deren Verknüpfung und Verwertung ermöglichen. Hierfür werden zentrale Portale geschaffen, nachdem die Datensammlungen entsprechend standardisiert wurden. Die einfachere verwaltungsübergreifende Nutzungsmöglichkeit ist dabei nur ein marginaler Nebeneffekt, auch wenn dieser gern unter der Überschrift der Entbürokratisierung daher kam.

Umfangreiche Datensammlungen wurden in Jahrzenten durch die kommunalen Vermessungsämter erhoben, gepflegt und durch die öffentliche Hand genutzt. Diese Daten wurden zu einem großen Teil auf der Basis einer gesetzlichen Ermächtigung zwangsweise aus einem hoheitlichen Sonderverhältnis heraus erhoben, durch die Grundstückseigentümer auch noch bezahlt, aber mit einer strengen öffentlich-rechtlichen Zweckbindung unter dem „Schutzmantel“ des öffentlichen Datenschutzrechtes und der strafrechtlich sanktionierten Amtsverschwiegenheit. Diese strenge Zweckbindung wird nunmehr durch Gesetz nicht nur aufgehoben, sondern in ihr Gegenteil verkehrt: die öffentliche Hand muss die Daten jeglicher privater Verwendung, Nutzung und Verschneidung zur Verfügung stellen. Diese Durchbrechung des Zweckbindungsgrundsatzes wäre noch vor zwei Jahren eine Straftat gewesen, mit der gesetzgeberischen Deckung ist es heute Dienstpflicht.

Wie wurde dieser Paradigmenwechsel begründet? Im Gesetzentwurf der Landesregierung von Mecklenburg-Vorpommern vom 26. Mai 2010 liest sich dies wie folgt: „In den letzten Jahren haben sich die Anforderungen von Staat und Gesellschaft an das öffentliche Vermessungswesen erheblich verändert. Das amtliche Raumbezugssystem, die Geotopographie und das Liegenschaftskataster haben sich inzwischen innerhalb und außerhalb der staatlichen Aktionslinien zu wesentlichen Basiskomponenten des gesamten Geoinformationswesens entwickelt. … In den öffentlichen Stellen liegen zahlreiche verschiedene Geodaten (Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geographischen Gebiet) vor. Diese Daten wurden mit erheblichen Kosten erhoben. Für eine effiziente und nachhaltige Nutzung der Geodaten sind gemeinsame Strategien sowie einheitliche Normen, Standards und Technologien notwendig. Es besteht Bedarf an konkreten Leitlinien sowie an einer funktionierenden Geodateninfrastruktur.“

Ob eine erhebliche Veränderung der Anforderungen von Staat und Gesellschaft innerhalb und außerhalb von staatlichen Aktionslinien geeignet ist, diese Zweckänderung wirksam zu rechtfertigen, wird sicher unbeantwortet bleiben müssen, denn eine verfassungsrechtliche Prüfung wird es wohl nicht geben. Die Umsetzung der INSPIRE-Richtlinie vollzog und vollzieht sich in allen Ländern nahezu geräuschlos, obwohl sich – verglichen mit dieser Preisgabe der bei der öffentlichen Hand vorhandenen Daten – beispielsweise das mit viel öffentlicher Resonanz bedachte Projekt „google street view“ als nahezu harmlos ausnimmt. Es merkt eben keiner, noch nicht.

Die Konflikte sind jedoch vorprogrammiert und werden mit den ersten Nutzungen dieses Rohstoffes durch die Wirtschaft sicher zu Tage treten. Bekannt wurden bereits die Nutzung von mit Luftaufnahmen verschnittenen Katasterdaten zur Berechnung und Gebührenerhebung von Abwassergebühren auf der Basis des Anteils der versiegelten Grundstücksflächen. Es braucht keine Vor-Ort-Besichtigung mehr: die Luftaufnahmen und die Vermessungsdaten reichen aus, um den Anteil der Grundstücksflächen zu berechnen. Die Nutzung von Geländereliefs zur Herstellung von Schokoladentafeln touristisch bedeutsamer Regionen[2] hat sicher ein geringes Gefährdungspotential für personenbezogene Daten der betroffenen Grundstückseigentümer, bei der Feststellung von Überflutungsgefährdungen, Bodenkontaminationen oder der Denkmalseigenschaft kann dies jedoch schon ganz anders aussehen.

Geodaten und Datenschutz

Deshalb hat die GIW-Kommission, eine Kommission des Bundesministeriums für Wirtschaft und von Wirtschaftsverbänden zur Förderung der Geoinformationswirtschaft, schon frühzeitig beim Unabhängigen Landeszentrum für Datenschutz Schleswig-

Holstein Gutachten in Auftrag gegeben, um die datenschutzrechtlichen Rahmenbedingungen der Verwendung geobasierter Daten untersuchen zu lassen. Mit der Studie „Geoinformation und Datenschutz“ wurde 2007 die nationale Rechtssituation hinsichtlich datenschutzrelevanter Aspekte analysiert. Die „Ampelstudie“ der GIW-Kommission folgte im Jahre 2008. In ihr werden die Datenwünsche der deutschen Wirtschaft (188 Datencluster) mit Ampelfarben entsprechend der jeweiligen datenschutzrechtlichen Situation versehen. Hiermit sollten zentrale Fragen nach der datenschutzrechtlichen Sensibilität kombinierter Geoinformationen und dem Zeitpunkt der Verschneidung zu personenbeziehbaren Informationen beantwortet werden.

Die sog. Ampelstudie[3] hat die begrüßenswerte Arbeit geleistet, die unterschiedlichen, bei der öffentlichen Hand vorhandenen Datenarten zu erheben und die meist landesrechtlichen Rahmenbedingungen auszuwerten. Dass letztere nicht durch Detailliertheit und Begründetheit überzeugten, mag aufgrund der eingangs beschriebenen Ausgangssituation der Erhebung und vorgesehenen eingeschränkten Verwendung der Daten nicht überraschen. Der Versuch, die Datenkategorien mit den Ampelfarben rot – gelb – grün zu versehen und damit den Grad der erforderlichen datenschutzrechtlichen Prüfung abstrakt zu bestimmen, lässt jedoch den wichtigsten Aspekt dieser Datenherausgabe unberücksichtigt: deren unbestimmten Verwendungszusammenhang und die Verschneidbarkeit der Datensätze. Entgegen der Farbenlehre kann nämlich die Zusammenführung von zwei „grünen“ Datensätzen auch mal ein klares Rot ergeben. Auch wenn die Studie selbst vor einer solchen Schlussfolgerung warnt, bedient sie doch in unverantwortlicher Weise die Erwartungshaltung der Nutzer, eine „klare Antwort“ zu bekommen.

Jede Nutzung von Datenbeständen muss sich vor dem Hintergrund der konkreten Verwendung einer datenschutzrechtlichen Prüfung stellen, in der mögliche Gefährdungen für das Persönlichkeitsrecht der Betroffenen erkannt und Maßnahmen getroffen werden, um diesen entgegenzuwirken. Hierfür gibt es inzwischen genügend Managementinstrumente, nicht zuletzt das Verfahrensverzeichnis des § 4e BDSG. Aber nicht erst die Zusammenführung der Datenbestände, also die Nutzung, löst eine solche Prüfpflicht aus, sondern bereits die Zur-Verfügung-Stellung der Datensätze durch die öffentliche Hand.

Zweimal Grün in der falschen Konstellation führt zu unerwünschten Situationen..

Freie Geodaten?

Die Vertraulichkeit personenbezogener Daten ist sowohl nach gemeinschaftlichem Recht, als auch nach dem nationalen Recht gewährleistet. Deshalb heißt es „konkretisierend“ in § 15 Absatz 2 Satz 2 Geoinformations- und Vermessungsgesetz (GeoVermG) M-V: „Soweit durch den Zugang zu Geodaten personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden, ist der Zugang zu beschränken, es sei denn, die Betroffenen haben eingewilligt“. Hier hat also vor Herausgabe der Informationen eine Prüfung stattzufinden, ob (a) durch den Zugang personenbezogene Daten offenbart würden und wenn ja, ob (b) dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden. In § 15 Absatz 4 heißt es weiter: „Die Bereitstellung von Geodaten und Geodatendiensten hat insbesondere unter Beachtung der im Landesdatenschutzgesetz und im Bundesdatenschutzgesetz festgelegten Grundsätze des Schutzes personenbezogener Daten zu erfolgen.“ Damit wird der gesamte Katalog des Datenschutzrechtes eröffnet: von den Anforderungen an eine informierte Einwilligung bis hin zur Durchsetzung von Löschansprüchen. All diese Anforderungen werden durch technisch-organisatorische Maßnahmen zum Beispiel durch eine Beauflagung oder Lizensierung abzubilden sein.

Standard-Lizenzen oder gar „Klick“-Lizenzen dürften angesichts dieser rechtlichen Situation ausgeschlossen sein. Vielmehr ergibt sich die Notwendigkeit der Vorabkontrolle jeder vorgesehenen Übermittlung auf der Basis des jeweiligen Verwendungszusammenhangs der Daten, um dann hieraus das erforderliche Schutzprogramm zu ermitteln. Dieser Befund ergibt sich nicht nur gleichermaßen in Bayern, Berlin, Brandenburg, Niedersachsen, Saarland, Sachsen, Sachsen-Anhalt sowie Thüringen, sondern angesichts der Rechtslage auch im Bund.

Nach dem Geodatenzugangsgesetz (GeoZG) vom 10.02.2009 gelten die „Zugangsbeschränkungen nach § 8 Absatz 1 sowie § 9 des Umweltinformationsgesetzes vom 22. Dezember 2004 (BGBl. I S. 3704) entsprechend“; damit ist ein Antrag auf Informationszugang abzulehnen, soweit „durch das Bekanntgeben der Informationen personenbezogene Daten offenbart und dadurch Interessen der Betroffenen erheblich beeinträchtigt würden,“ es sei denn, „die Betroffenen haben zugestimmt oder das öffentliche Interesse an der Bekanntgabe überwiegt“. Den unglücklichen, weil sachfremden, Bezug zum Umweltinformationsgesetz wählten auch die Länder Bremen, Nordrhein-Westfalen und Schleswig-Holstein.

Hier tritt also neben den oben erwähnten Schwierigkeiten noch das besondere Abwägungsrisiko eines eventuell überwiegenden öffentlichen Interesses hinzu. Diese Schwelle ist nicht so leicht zu überwinden, wie man annehmen mag: das Abwägungsprogramm wird nämlich durch ein Grundrecht bestimmt,

dessen Einschränkung nur im überwiegenden Allgemeininteresse auf der Basis eines verhältnismäßigen und normenklaren Gesetzes verfassungsrechtlich zulässig ist (Volkszählungsurteil). Hier versucht nun also der Gesetzgeber, die aus guten Gründen allein ihm übertragende Abwägung des Grundrechtes der öffentlichen Verwaltung zu überantworten. Diese gesetzgeberische Arbeitsverweigerung ist schon bemerkens- und überprüfungswert.

Konsequenter ist nur das Land Hessen, wo der Öffentlichkeit der Zugang zu Geodaten über Geodatendienste zu beschränken oder zu versagen ist, „wenn durch diesen Zugang personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt", es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse an dem Zugang überwiegt die Beeinträchtigung. Ergänzend enthält das Hessischen Vermessungs- und Geoinformationsgesetz eine Auslegungsregel, wonach das öffentliche Interesse an dem Zugang zu personenbezogenen Daten immer überwiegt, „wenn die Geodaten keine Angaben über persönliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person und über das räumliche Umfeld von einer bestimmten oder bestimmbaren natürlichen Person enthalten, die dazu verwendet werden können, diese zu bewerten oder zu beurteilen, in einer bestimmten Art und Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen." Doch auch hier bleibt die Frage, wie eine solche mögliche Verwendung wirksam geprüft und/oder ausgeschlossen werden kann.

Das Landesgeodatenzugangsgesetz Baden-Württemberg senkt die Schwelle hingegen weiter ab, indem der Zugang zu personenbezogenen Daten nur unzulässig ist, wenn „dadurch Interessen der Betroffenen erheblich beeinträchtigt würden". Wie diese Erheblichkeitsschwelle zu definieren ist, wird der Rechtsprechung sicher genügend Arbeit bereiten.

Eine differenzierende Regelung findet sich im Landesgeodateninfrastrukturgesetz Rheinland-Pfalz, wonach der „Zugang zu Angaben über den Namen und das Geburtsdatum von Eigentümerinnen, Eigentümern und Erbbauberechtigten von Grundstücken sowie von sonstigen natürlichen Personen" nur für öffentliche Stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, und Personen und Stellen außerhalb des öffentlichen Bereichs eröffnet werden darf, soweit diese ein berechtigtes Interesse an der Kenntnis dieser Geodaten darlegen und überwiegende schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden. Dieser Beschränkung der Verwendungsmöglichkeit einer Gruppe von personenbezogenen Daten folgt eine problematische Erweiterung für die „sonstigen" personenbezogenen Daten: „Der Zugang zu sonstigen personenbezogenen Geodaten darf eröffnet werden, es sei denn, bei einer Eröffnung des Zugangs für Personen und Stellen außerhalb des öffentlichen Bereichs werden **im Einzelfall erkennbare überwiegende** schutzwürdige Interessen der Betroffenen beeinträchtigt." Hier soll also einerseits die Prüftiefe gesenkt (im Einzelfall erkennbar) und anderseits das Abwägungsergebnis nur bei einem Überwiegen der schutzwürdigen Interessen greifen.

Ampelstudie konkret

Die Ampelstudie fand nur in einem Bundesland gesetzgeberische Resonanz: gemäß § 11 Absatz 3 Geodateninfrastrukturgesetz für das Land Schleswig-Holstein **kann** die „in § 8 Abs. 2 UIG-SH für eine Offenbarung von personenbezogenen Daten vorgeschriebene einzelfallbezogene Abwägung des öffentlichen Interesses an der Bekanntgabe von Geodaten gegen den Schutz privater Belange" „durch eine daten- und nutzungsspezifische Kategorisierung von Geodaten ersetzt werden, wenn schutzwürdige private Belange nur geringfügig beeinträchtigt werden. Die Kategorisierung ist von der jeweiligen geodatenhaltenden Stelle im Einvernehmen mit dem Unabhängigen Landeszentrum für Datenschutz durchzuführen und von der Koordinierungsstelle nach § 9 öffentlich verfügbar bereitzustellen." Die Kategorisierung von Geodaten nimmt – genauso wie die Kategorisierung von personenbezogenen Daten in Rheinland-Pfalz – Unschärfen bewusst in Kauf, solange schutzwürdige Belange „nur geringfügig" beeinträchtigt werden. Statt dem „Verbot bei schwerwiegenden Beeinträchtigungen" steht hier eine „Erlaubnis für geringfügige Beeinträchtigungen": kein wirklicher Fortschritt.

Der einzige, aber deshalb nicht zu unterschätzende, innovative Ansatz der Regelung aus Schleswig-Holstein steckt in der Verantwortungsübernahme durch das Unabhängige Landeszentrum für Datenschutz: dieses beteiligt sich mithin selbst an der Kategorisierung und damit an der Verantwortung für eine pauschalierte Bewertung ohne Kenntnis der konkreten Anwendungssituation. Damit wird der Landesbeauftragte für den Datenschutz selbst zum Akteur und fällt bedauerlicherweise als Kontroll- und Petitionsinstanz aus. Ob dieser Preis nicht zu hoch für den Gewinn einer vermeintlichen Rechtssicherheit für die datenverwendende Industrie ist, wird der Gesetzgeber in Schleswig-Holstein zu bewerten haben. Die Anforderungen an die Prüfprozesse werden sich aber in den einzelnen Ländern wohl kaum unterscheiden: § 9 BDSG bzw. die jeweiligen Landesnormen werden den Rahmen vorgeben und die Betroffenenrechte den Inhalt, denn es gibt (bald) kein belangloses Datum mehr!

Das Bundesverfassungsgericht setzte diese Erkenntnis im Jahr 2008 in seiner wegweisenden Entscheidung zur Begründung des Rechtes auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme um. Dort stellte das Gericht fest:

„Das Recht auf informationelle Selbstbestimmung geht über den Schutz der Privatsphäre hinaus. Es gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (vgl. BVerfGE 65, 1 <43>; 84, 192 <194>). Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeits**gefährdung** [alle Hervorhebung d.d. Autor] beginnen lässt. Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art

und Weise genutzt und verknüpft werden **können**, die der Betroffene weder überschauen noch verhindern kann. Der Schutzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. **Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben** (vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 <2466>).“

Fazit

Landes- und Bundesgesetzgeber sind beim Thema Geodaten an der Größe der Aufgabe gescheitert, die Quadratur des Kreises zu bewältigen: Daten werden erst in ihren konkreten Zusammenhängen zu Informationen. Scheinbar belanglose Daten können sich in konkreten Anwendungen zu freiheitsgefährdenden Informationen verbinden. Diese Gefahr kann nicht abstrakt, sondern immer nur konkret bestimmt werden. Wenn aber der Schutz erst mit der Verschneidung beginnt, weil erst dann der Personenbezug hergestellt ist, kommt er zu spät. Datenschutzrecht ist immer präventives Recht. Diese Prävention muss bereits **vor der Schwelle der Personenbeziehbarkeit** beginnen. Damit wird die Diskussion akut, ob der rechtliche Anknüpfungspunkt „Personenbezug“ die reale Gefährdungssituation für das Recht auf informationelle Selbstbestimmung noch adäquat widerspiegelt oder ob der Personenbezug – bei einem negativen Befund – nicht vielleicht „ausgedient hat“ und das Datenschutzrecht durch ein Informationsrecht abgelöst werden muss. Ein Informationsrecht, das bereits seine freiheitsgewährende Wirkung entfaltet, wenn noch kein personenbezogenes Datum entstanden ist.

Egal ob soziale, oder welche Netzwerke auch immer unsere Zukunft bestimmen werden: sie vergessen nichts und vergeben selten. Ist eine rechtliche Regulierung denkbar, die die hieraus erwachsenen Gefahren für die persönliche Freiheit begrenzt, ohne die Chancen zu untergraben? Oder muss sich vielleicht eher unser gesellschaftliches Verhältnis zu Informationen wandeln und vom Diktat des scheinbar „objektiven“ frei machen? ´Forget Privacy´ ist keine Kampfansage, sondern eine Kapitulation vor der Aufgabe, technologische und gesellschaftliche Entwicklung in Einklang zu bringen. Wir brauchen eine Ethik der Informationsgesellschaft, die die Verwertung von Jugendbildern in Stellenbesetzungsverfahren nicht verbietet, sondern ächtet. Und wie die Demokratie Demokraten braucht, braucht die Informationsgesellschaft kreative und verantwortliche Akteure, die sich ihrer Verantwortung rechtzeitig bewusst werden. Bedauerlicherweise gehören die Gesetzgeber gegenwärtig nicht dazu.

1 Übersicht unter www.geobusiness.org, einer Präsentation der GIW-Kommission beim Bundesministerium der Wirtschaft.

2 Einer der Finalisten des GeoBusinessAward überträgt die Geländeprofile auf eine Tafel Schokolade, die dann in der Region als Werbemittel genutzt werden kann. Der Grad der Auflösung dürfte gering genug sein, um jede Personenbeziehbarkeit auszuschließen.

3 Rahmenbedingungen für die Bereitstellung von Geodaten für die Wirtschaft.

Die Abbildung zeigt eine Aufnahme eines Autobahnabschnittes. Die Daten wurden aus verschiedenen Datensammlungen zusammengefügt und mit den Daten aus einer satellitengestützten Geschwindigkeitsmessung der Fahrzeuge verknüpft. Dabei zeigen die Dreiecke die jeweilige Fahrtrichtung und die Geschwindigkeit an. Im Original gut zu erkennen sind so Gefährdungen des Fahrzeugverkehrs durch stehende Fahrzeuge (schwarz), ebenso wie durch Geschwindigkeitsüberschreitungen (weiß).

Quelle: „Was die Technik schon kann“, Vortrag von Holger Maass, Deutsches Fernerkundungsdatenzentrum, Deutsches Zentrum für Luft- und Raumfahrt Neustrelitz auf der Datenschutz-Fachtagung des Landesbeauftragten für Datenschutz Mecklenburg-Vorpommern, Neustrelitz, 25. Juni 2009, http://www.datenschutz-mv.de/dschutz/veransta/privat/vortraege/Maass.pdf

Roland Appel

Volkszählung 2011 – Anlass zur Kritik am Überwachungsstaat?

Unter dem Motto „Wissen, was morgen zählt“ findet derzeit in Deutschland die erste Volkszählung seit 1987 statt. Vom Frühjahr bis in den Herbst werden zehn Prozent der Bürgerinnen und Bürger in Deutschland von Zählern oder via Internet befragt. Anlass genug, der Frage nachzugehen, was die Situation im Frühjahr 2011 von 1987 grundsätzlich unterscheidet. Den Organisatoren des Volkszählungsboykotts 1987 ging es keineswegs um die Verhinderung der Volkszählung, sondern darum, den ausufernden Datensammlungen des Staates über seine Bürger Einhalt zu gebieten. Heute geht es um dieselben Themen: Mehr Bürgerrechte, mehr Selbstbestimmung. Bürgerinnen und Bürger wollen nicht befragt werden, sondern aktiv an Entscheidungen teilhaben, wie zuletzt bei Stuttgart 21.

Die politischen Rahmenbedingungen der 80er unterscheiden sich grundsätzlich: Es gab noch Berufsverbote für Lokführer mit DKP-Parteibuch oder friedensbewegte Lehrer. Die RAF hatte in den siebziger Jahren eine Welle von Antiterrorgesetzen herbeigebombt. Verfassungsschutz und Polizei spitzelten in Bürgerinitiativen, verdeckte Ermittler provozierten mit Steinwürfen Gewalt. In Brokdorf flogen BGS-Hubschrauber CS-Gasangriffe auf Menschen und in Hamburg wurden fünftausend Demonstranten von der Polizei stundenlang eingekesselt, so dass viele ihre Notdurft aufs Straßenpflaster verrichten mussten. Im Klima des Misstrauens war die Ankündigung einer flächendeckenden staatlichen Personendatensammlung eine schiere Provokation. Viele Menschen sahen Bürgerrechte wie die Demonstrationsfreiheit gefährdet. Die Volkszählung war der Tropfen, der das Fass zu überlaufen brachte. So entstand die Bewegung 1983 spontan innerhalb weniger Wochen und Monate und auf die Aussetzung durch das Verfassungsgericht folgte am 15. Dezember das legendäre Volkszählungsurteil, dessen zwei wichtigste Kerngedanken fortgelten: Erstens: Unter den Bedingungen moderner Datenverarbeitung gibt es kein belangloses Datum mehr. Zweitens: Eine Gesellschaft, in der der Mensch nicht mehr weiß, wer, wann, was und warum über ihn weiß, wäre mit einer freiheitlichen Gesellschaft, wie sie das Grundgesetz will, nicht vereinbar.

Die Volkszählung 1987 war der ideale Anlass für die größte Datenschutzkampagne in der Geschichte Deutschlands, zwei Jahre vorher auch von uns Kritikern geplant. Sie hat die informationelle Selbstbestimmung letztlich in die Verfassungswirklichkeit umgesetzt.

Der Zensus 2011 wird auch deshalb kein Anlass für Massenproteste sein, weil eine wichtige Forderung der damaligen Volkszählungsgegner erfüllt wurde, wenige Stammdaten aus dem Melderegistern zu ziehen und nur eine Stichprobe zu befragen. Zudem gehen heute große Gefahren für die informationelle Selbstbestimmung nicht nur vom Staat, sondern mehr von wirtschaftlicher Macht aus. Das soll nicht heißen, dass der Zensus 2011 keinen Anlass zur Kritik gibt. Aber es geht weder darum, sich auf aussichtlose Verfassungsklagen einzulassen, noch darum, sich an den statistischen Ämtern abzuarbeiten, sondern um Politik und Sensibilisierung der Bürgerinnen und Bürger gegenüber Datenübergriffen von Staat und von Privaten.

Die Volkszählung „Zensus“ 2011: Gebäude- und Wohnungszählung

Die meisten Personen, die mit dem Zensus in Kontakt kommen, sind die Haus- und Grundeigentümer mit Auskunftspflicht. Die ersten Pannen sind entstanden, weil die der Zählung zugrunde liegenden Eigentümerdaten aus den nicht aktuellen Verzeichnissen der Gemeinden über Grundsteuerpflichtige kommen. Diese Register können gar nicht aktuell sein, denn wenn der Eigentümer stirbt, erfolgt die Umschreibung von Grundeigentum erst nach Erteilung eines Erbscheins. Die Grundsteuerpflicht geht sogar meist erst im auf den Eigentümerwechsel folgenden Jahr auf den neuen Eigentümer über. So ist zu erklären, dass zahlreiche Verstorbene angeschrieben werden und Datenerhebungen auch bei Personen versucht werden, die ihre Immobilie schon länger verkauft haben. Ein erheblicher Anteil an Fehlantworten ist zu erwarten, da die Statistikbehörden nicht vom Eigentümerwechsel erfahren, wenn die Angeschriebenen dies nicht mitteilen.

Da ein nachträglicher Abgleich dieser Registerdaten natürlich nicht zulässig ist, wird auch keine Verbesserung der kommunalen Datenbasis erreicht – umso fragwürdiger erscheinen dann Fragen nach den Namen der Bewohner. Missverständnisse und Verwirrung sind vorprogrammiert, weil in größeren Wohnanlagen sowohl die Eigentümer, als auch die Verwalter angeschrieben werden. Wohnungseigentümer sind nicht verpflichtet, den Verwaltungsgesellschaften mitzuteilen, an wen sie ihre Wohnung vermieten. Dort, wo es darüber Erkenntnisse gibt, sind diese nicht auf dem neuesten Stand. Wie und auf welche Weise die Statistik damit umgehen wird, ist bisher nicht erkennbar. Damit werden also Datenfriedhöfe angelegt. Zu welchem Zweck die Namen erhoben werden, wurde nicht plausibel erläutert, denn über die Namen Rückschlüsse auf Familienzusammenhänge zu ziehen, ist beim geltenden Namensrecht mehr als fragwürdig.

Schwerer wiegt, dass hier Dritte über Personen Auskunft geben, ohne dass die Betroffenen hierzu ihre Zustimmung geben. Das Vorgehen widerspricht dem Kerngedanken des Volkszählungsurteils,

dass Daten grundsätzlich bei den Betroffenen zu erheben sind. Ob die allgemeine Mitteilung ausreicht, dass gerade eine Gebäudezählung stattfindet, ist mehr als zweifelhaft. Und spätestens hier hat sich der Autor bei der Abwägung zwischen dem möglichen Verstoß gegen die Persönlichkeitsrechte der Mieter und dem schlimmsten Fall der Androhung eines Zwangs- oder Bußgeldes von ein paar hundert Euro für die Wahrung des Datenschutzes entschieden und keinen Namen, sondern seine Datenschutzbedenken in den Fragebogen eingetragen.

Dies fiel auch nicht schwer, weil im Unterschied zur Stichprobe der Fragebogen per Post zugestellt wird. Ach ja, die Post: Zwar werden die Befragten gebeten, den Rückumschlag mit Porto zu versehen, aber erste Erfahrungen mit dem Zensus zeigen, dass die Erhebungsstellen sich so sehr über Datenrückläufe freuen, dass sie selbstverständlich auch unfrankierte Umschläge in Empfang nehmen.[1]

Erkenntniswert: Schlicht und bescheiden!

Die Fragen der Gebäudezählung zeigen im Übrigen das ganze Ausmaß der politischen Fragwürdigkeit des Zensus. Wenn angesichts der Notwendigkeit, die mit dem Atomausstieg zu gestaltende Energiewende einzuleiten etwa nach der Größe und Ausrichtung von Dachflächen gefragt würde, ob Photovoltaik installiert oder nicht, wenn nicht nur nach Baujahr, sondern nach Daten des Energiepasses gefragt würde, um Isolierungsbedarf zu ermitteln, könnten sogar Anhaltspunkte für die zukünftige Gestaltung von Förderprogrammen zur Energieeinsparung gewonnen werden. Auch könnte die Frage nach einer möglichen Asbestbelastung dazu führen, die Ausmaße eines volkswirtschaftlich noch zu bewältigenden Problems im Gebäudebestand zu ermitteln...leider Fehlanzeige!

Auch die Frage nach dem Energieträger, ob Gas, Kohle, Holz, Erdwärme oder Strom, ob erneuerbare Energien bereits genutzt werden, oder nicht, wäre sinnvoll, um Erkenntnisse über den Verbrauch verschiedener Energiearten und über Einsparpotenziale zu gewinnen – erneut Fehlanzeige! Stattdessen beschränkt sich der Zensus auf die Frage nach Vorhandensein eines Klos und einer Dusche oder Badewanne[2], um dies dann im Europäischen Vergleich vielleicht an Bulgarien zu messen - willkommen in Europa!

Grundsätzlich falsche Erwartungen

Die Erhebung erweckt den Eindruck, als ob in Deutschland Wohnraum und das Entstehen von Gebäuden strategisch geplant würde. Die Praxis unserer Städte sieht jedoch völlig anders aus. So werden Planungsentscheidungen über Flächennutzungs- und Bebauungspläne zumeist in Einzelverfahren, nicht aber strategisch oder gar langfristig aufgestellt. Das Angebot von Wohnraum hängt wesentlich stärker vom Grundstücksmarkt und örtlichen Parametern ab, als von Daten, die in so allgemeiner Form ermittelt werden, wie beim Zensus 2011. Zur Verwirklichung generationengerechten Wohnens in den Städten, zur Vermeidung von Ghettostrukturen, dem Aufbau einer lebendigen Einzelhandelsstruktur oder zur Versorgung mit öffentlichen Nahverkehrsmitteln bedarf es ausreichender kommunaler Finanzmittel ebenso wie wirtschaftlicher Anreize für private Investoren. Hierzu kann der Zensus viel weniger Beiträge leisten, als eine aktive und wirkungsvolle Beteiligung der Bürger an den Entscheidungen in ihrer Stadt mit Planungswerkstätten, Stadtteilprojekten und Bürgerentscheiden. Aber hierfür fehlt es den Kommunen an Geld.

Die Stichprobe

Wer nicht selbst zur Stichprobe von 9,6% der Bevölkerung zählt[3],, hat es nicht leicht, einen Zählbogen auf Papier zu erlangen, denn die pdf- Dateien auf der offiziellen Homepage der statistischen Ämter sind nicht druckfähig, aber dem kann mit der Erstellung eines Screenshot mit frei im Netz verfügbarer Software http://cropper.codeplex.com/ abgeholfen werden. Im Folgenden sollen nur die wichtigsten Probleme angerissen werden. Weiterführende Argumente finden sich im Netz unter www.humanistische-union.de, der ältesten Bürgerrechtsorganisation Deutschlands und unter www.zensus11.de des AK Vorratsdatenspeicherung.

Was kommt da auf manche von uns zu?

Wer jedoch als Teilnehmerin oder Teilnehmer der Stichprobe per Zufallsprinzip ausgesucht wird, ist auskunftspflichtig. Dies ist allein schon deshalb zu kritisieren, weil eine Stichprobe, wie sie der Zensus vorsieht, zum einen die Möglichkeit lässt, Menschen, die nicht befragt werden wollen, nicht zu belästigen, zum anderen Freiwilligkeit grundsätzlich die Qualität von Umfragen optimiert. Zudem ist eine Stichprobe von etwa 10% so groß, dass repräsentative Aussagen selbst bei einer hypothetischen Verweigererquote von 20% noch problemlos getroffen werden könnten. Es ist also zu vermuten, dass die Statistiker diesmal – und damit handeln sie weitaus klüger als ihre Kollegen vor dreiundzwanzig Jahren – eine augenzwinkernde Zahl von Verweigerern von vornherein berücksichtigt haben. Anwälte vermuten, dass Verweigerer analog zu 1987 realistischerweise mit bis zu dreihundert Euro Bußgeld rechnen müssen – wenn die Verweigerung überhaupt verfolgt wird.

Im Unterschied zur Volkszählung 1987 kommt in jedem Fall ein Erhebungsbeauftragter, – so heißen nun die Zähler – ins Haus, der den Fragebogen persönlich übergeben muss. Wie 1987 muss niemand diesen Zähler in die Wohnung lassen oder gar gemeinsam mit ihm die Fragen beantworten. Allerdings erhält der Zähler als Vergütung pro interviewter Person 7,50 EUR, bei schlicht abgegebenem Fragebogen jedoch nur 2,50 EUR. Das monetäre Interesse des Zählers ist daher nicht von der Hand zu weisen. Es ist zwar unwahrscheinlich, dass die NPD bei der Zählerbewerbung sehr erfolgreich war, aber auszuschließen ist es nicht. Schon deshalb sollte der Zählbogen nur freundlich entgegengenommen, dann aber unbedingt auf dem Postweg zurückgesandt werden.

Der Papst zählt zweimal mit!

Wer den Haushaltsbogen aufschlägt, wird spätestens bei der siebten Frage stutzen. Wer der Werbung glaubt, die Frage

nach der Religion sei freiwillig, wird eines Besseren belehrt. Frage sieben nämlich lautet: Welcher Religionsgesellschaft gehören Sie an? Schon die Reihenfolge verwundert, die römisch-katholische Kirche kommt doch im Alphabet nicht vor der evangelischen Kirche oder jüdischen Gemeinden? Die Evangelischen tauchen dann als „Freikirchen" nochmals auf; ebenso „sonstige öffentlich-rechtliche Religionsgemeinschaften" – wer soll das sein – und „keine öffentlich-rechtliche Religionsgemeinschaft" – als Pflichtantwort – was geht das den Staat an? 1987 war Religion noch Privatsache und die EU schreibt so etwas gewiss nicht vor. Noch schlimmer kommt es mit der – freiwilligen – Frage 8: „Zu welcher der folgenden Religionen, Glaubensrichtungen oder Weltanschauungen bekennen Sie sich?" Dass dann nach „Christentum", „Judentum" und „Islam" mit den Unterkategorien „sunnitischer" „schiitischer" und „alevitischer" gefragt wird, „Buddhismus", „Hinduismus", „Sonstige" und „keine Religion, Glaubensrichtung oder Weltanschauung?" – das ist ernst gemeint! Der nordrhein-westfälische Datenschutzbeauftragte Ulrich Lepper hat bei Frage Nummer sieben inzwischen „erhebliche Datenschutzbedenken" angemeldet.[4] Abgesehen davon, dass möglicherweise die Mehrzahl der Aleviten gar nicht mit dem Islam in Verbindung gebracht werden möchte[5], weil sich diese Religion auf ältere Quellen in Mesopotamien gründet, muss man sich hier doch ernsthaft die Frage stellen, ob wir es uns im 21. Jahrhundert leisten können, die Kernfragen des Mittelalters auf die Tagesordnung zurückzuholen? Was ist, möchte man fragen, angesichts dieser Fragestellung, die Steigerungsform von verfassungsfeindlich? Und in welcher mentalen Verfassung müssen Abgeordnete des Deutschen Bundestages gewesen sein, als sie einem solchen Gesetz zustimmten?

Fragen 14 bis 22 lauten: „Aus welchem Staat sind Sie oder Ihre Eltern nach 1955 in das heutige Gebiet der Bundesrepublik Deutschland zugezogen?" Soll damit die lange vernachlässigte Migrationsforschung nun eine neue Datenbasis bekommen? Ernsthafte Kritiker sehen hier die Gefahr, dass diskriminierende Daten erhoben werden[6]. Dem können Antwortpflichtige natürlich entgegenwirken: Wer als Herkunftsstaat San Marino angibt und bei Frage 44 als Berufsgruppe Land- und Forstwirtschaft ankreuzt, entgeht garantiert jeder Diskriminierung. Vielleicht ergibt sich ja, dass etwa 2 Mio. Förster seit 1955 aus San Marino eingewandert sind. Das würde endlich erklären, warum dieser Zwergstaat nur etwa 31.000 Einwohner hat!

Sondergruppen bei der Volkszählung

Wesentlich ernsthafter muss allerdings die Kritik an der Methode ausfallen, wie Menschen in besonderen Einrichtungen wie Internaten, Studentenwohnheimen oder Altenheimen registriert werden und wie die Insassen von Obdachlosenunterkünften, psychiatrischen Kliniken oder im Strafvollzug erfasst werden. Während in Internaten, Klöstern und Studentenwohnheimen die Einwohner selbst befragt werden, geschieht die Beantwortung der Fragen in der Psychiatrie und im Strafvollzug durch die Heim- bzw. Anstaltsleiter. Zwar wird im Falle der Vollzugsanstalten auf die Erhebung von Ausbildungs- und Berufstätigkeitsdaten verzichtet, allerdings stellt sich gleichwohl die Frage, wieso es überhaupt notwendig ist, hier eine namentliche Erfassung durchzuführen, zumal sowohl die Zahl der Haftplätze, als auch der Belegungsquoten den Justizbehörden der Bundesländer aktuell bekannt ist. Da kein Melderegisterabgleich stattfinden darf, ist auch das Argument des Statistischen Bundesamtes, hier käme es zu besonders erheblichen Abweichungen von den Melderegistern, obsolet.

Auch im Falle der Altenheime scheint die Methode des Zensus, Personen namentlich zu erfassen, keinen Erkenntnisgewinn zu bringen. Die wirklichen Probleme ergeben sich aus der von der Politik durchaus gewollten und inzwischen weit verbreiteten Praxis, dass Menschen so lange wie möglich in ihrer gewohnten Umgebung verbleiben. Ganz viele Altenheime sind daher in einer vergleichbaren Situation, wie sie ein Leiter einer AWO- Einrichtung charakterisierte: „Bei uns nähert sich die durchschnittliche Aufenthaltsdauer inzwischen nur noch wenigen Monaten, weil die Menschen erst kommen, wenn es zu Hause mit ambulanter Pflege überhaupt nicht mehr geht. Wir sind mehr Hospiz als Pflegeheim." Genau diese Situation würde eigentlich einen anderen Personalschlüssel in den Einrichtungen erfordern, wird jedoch bei der namentlichen Zählung der Bewohner mitnichten abgefragt.

Ohne Nutzwert – Chancen verpasst!

Die wenigen genannten Kritikpunkte zeigen, dass sich Zensus2011 und Volkszählung 1987, was den statistischen Wert der Aussagen betrifft, im gleichen bescheidenen Rahmen bewegen werden. Ob dies einen Aufwand von 710 Millionen Euro rechtfertigt, darf getrost in Frage gestellt werden. Denn natürlich verfügt das Gemeinwesen mit den verschiedenen öffentlichen Datenregistern bereits über erhebliche Anhaltspunkte, um die Bevölkerungszahl, die im Übrigen ja eine dynamische Größe ist, zu ermitteln. Da sind zum Einen die Einwohnermelderegister, da ist aber auch der Datenbestand der 2006 bis 2008 durch das eigens dafür geschaffene, 910 Beschäftigte schwere Zentrum für Informationsverarbeitung und Informationstechnik ZIVIT beim Bundesfinanzministerium. Hier werden bereinigte Personendaten vorgehalten, die zusammengeführt und genutzt wurden, um die einheitliche Steuernummer zu generieren, die wir alle von der Wiege bis zur Bahre als einheitliches und verfassungsrechtlich fragwürdiges Personenkennzeichen zugeteilt bekommen. Um kein Missverständnis zu erzeugen: Hier sollen keine Daten genutzt werden, aber zur anonymisierten Erstellung einer einzigen Zahl, - der aktuellen Bevölkerungszahl - sollte diese Behörde eigentlich fähig sein.

Der angeblich so wichtige Wert des Zensus ist auch 2011 nicht zu erkennen

Da sollen angeblich die Wahlkreise neu zugeschnitten werden, wofür man die Volkszählungsdaten braucht. Dafür sind Grundlage zunächst einmal die Melderegister, die ja nicht bereinigt

werden und wer sich die Mühe macht, Drucksachen und Debatten in Landtagen und Bundestag zu verfolgen, wenn es um den Wahlkreiszuschnitt geht, wird schnell erkennen, dass hier mehr Parteiengerangel um „Hochburgen“ den Ausschlag gibt, als amtliche Statistik.

Die Verteilung des Bund-Länder-Finanzausgleichs und die Zuweisungen an die Kommunen sollen ein wichtiger Grund für den Zensus sein. Das ist zwar nicht völlig falsch, aber die Erfahrung mit der letzten Volkszählung hat gezeigt, dass auch relativ frische Daten die damalige schwarz-gelbe Politik nicht daran hindern konnten, zugunsten von Steuerleichterungen für Unternehmen die öffentlichen Haushalte, insbesondere der Kommunen Anfang der 90er Jahre in einem historisch einmaligem Kahlschlag zu plündern, der bis heute fortdauert. Wenn selbst angesichts von sensationellen 3% Wachstum und Hochkonjunktur in Deutschland 2011 die Steuerschätzung weiterhin steigende Defizite von Bund, Ländern und Gemeinden ergibt, dann liegt das sicher nicht an fehlendem Datenmaterial. Es bedarf keines Zensus, sondern einer anderen Steuerpolitik, um den Kommunen endlich wieder Handlungsmöglichkeiten zurückzugeben!

Wenn in Deutschland inzwischen die Zahl der Analphabeten bei mindestens 3 Mio. liegt, wenn bis zu 40% der Hauptschüler die Schule ohne Abschluss verlassen, wenn gleichzeitig der Fachkräftemangel immer größer wird und nach wie vor Unterricht ausfällt und es keine flächendeckende Ganztagsschulen gibt, dann ist zu befürchten, dass Zensusdaten im äußerten Fall zur besseren Verwaltung des Mangels herangezogen werden, anstatt das zu tun, was Schwellenländer wie Malaysia schon vor einem halben Jahrzehnt getan haben, indem sie ihre Bildungsinvestitionen verdoppelt haben.

Auch das Schulsystem hätte angesichts von Pisa durchaus interessante statistische Informationen bereitgehalten: Wie groß sind die Klassen in den verschiedenen Bundesländern wirklich, wie ist ihre Ausstattung mit moderner IT-Technik, wie viele Lehrer verfügen über IT-Grundkenntnisse, die sie ihren Schülern auch vermitteln können? Wie viel Ganztagsangebote gibt es, wie viele Schulen bieten ein Mittagessen an und wie viele verfügen über Sozialpädagogen und wie viele Verletzungen der Schulpflicht hat es im vergangenen Jahr gegeben? Wo gibt es vorschulische Sprachförderung und wo nicht? Aber danach fragt der Zensus nicht.

Ist Zensuskritik 2011 ein Popanz?

Nein. Die Volkszählung 2011 ist anders als die Volkszählung 1987 nicht geeignet, um eine politische Kampagne zu führen. Sie ist allerdings nicht Grund, aber ein geeigneter Anlass, sich über den Umgang mit personenbezogenen und personenbeziehbaren Daten zu informieren.

Bürgerrechte sind nicht auf Dauer gewährt

Das Misstrauen gegen den Sicherheitsstaat ist nach wie vor gerechtfertigt. Denn Bürgerrechte, dies zeigt die jahrzehntelange Auseinandersetzung über neue Antiterrorgesetze, die „Sicherheitspakete“ und „Otto-Kataloge“ nach dem 9. November 2001, werden durch die Sicherheitsbehörden immer wieder auf den Prüfstand gestellt. Jedes Mal, wenn ein Terroranschlag oder auch nur der Versuch unternommen wird, ein besonders medienwirksames Verbrechen die Zuschauer in seinen Bann schlägt, melden sich die professionellen „Warner“ und „Terrorpropheten“ wie z.B. BKA-Präsident Ziercke in den Medien. Und zugleich oder kurz darauf wird ein neues Allheilmittel zur Bekämpfung des allfälligen Bösen gekürt. Dies wird dann alsbald, meist flankiert von den Apologeten des armen, wehrlosen Rechtsstaats – früher der Bayrische Innenminister Günter Beckstein, dann Otto Schily, - heute Dieter Wiefelspütz (SPD) und Wolfram Bosbach (CDU) in Gesetze gegossen. Und in den letzten 10 Jahren werden diese regelmäßig, aber auch begleitet von einer schon bewundernswerten Lernunfähigkeit der Initiatoren, vom Bundesverfassungsgericht aufgehoben. Vom Großen Lauschangriff, für den 1996 die Verfassung geändert wurde, über das Luftsicherheitsgesetz als „Lizenz zum Töten“ zum Abschuss von Passagiermaschinen, die 2008 vom Verfassungsgericht gestoppte „Online-Durchsuchung“ bis zur 2010 aufgehobenen Vorratsdatenspeicherung: Die Liste vorläufig beendeter Angriffe auf Bürgerrechte ist lang. Allerdings lässt der jüngste Vorstoß des NRW-Innenministers Ralf Jäger (SPD) auf Einführung einer „sorgenfreien Mindestdatenspeicherung“ erahnen, dass auch in Zukunft die Kette der Begehrlichkeiten seitens der Ermittlungsbehörden nicht abreißen wird.

Vorratsdatenspeicherung verhindern!

Die Vorratsdatenspeicherung muss dabei ganz oben auf der Liste der abzuwehrenden Gesetze stehen. Das Verfassungsgericht hat sie aufgehoben, aber nicht völlig verworfen. Deshalb muss die Vorratsdatenspeicherung dringend unter dem Eindruck fortschreitender Technik neu bewertet werden. Denn die Verkehrsdaten der Telekommunikation – insbesondere bei Handys, Smartphones oder sonstigen mobilen Geräten, verraten heute anders als vor fünf Jahren nicht nur, wer, wann, mit wem, wie lange kommuniziert hat, sondern auch, wo sich eine Person aufhält und wohin sie sich bewegt. Übrigens gehören zu den Geräten, die derartige Profile generieren auch die Navigationssysteme moderner Fahrzeuge. Mit Einführung der Smartphones und Entwicklung des Ubiquious Computing hat der Grad der möglichen Überwachung aller Bürgerinnen und Bürger eine neue Qualität erreicht. Die Verkehrsdaten lassen nicht nur umfassende Einblicke in persönliche Kommunikation zu, sie geben auch Aufschluss über Verhaltensweisen, Gewohnheiten und Beziehungsnetzwerke und erzeugen permanente Bewegungsbilder sämtlicher Nutzer. Denn moderne Smartphones greifen ständig auf das Internet zu, um sich mit dem Computer ihres Besitzers abzugleichen oder tauschen über so genannte „Apps“ laufend unkontrolliert Datenpakete aus.

Was ist die größere Bedrohung für Freiheitsrechte in der Informationsgesellschaft?

Allgemeine Beschleunigung der Computerisierung hat unsere Gesellschaft gegenüber den 80er Jahren des letzten Jahrhunderts tiefgreifend verändert. Während von der Erfindung des Automobils 1886 bis zum Bau der ersten Autobahn zwischen Köln und Bonn 1926 vierzig Jahre vergingen, haben sich Arbeit, Privatleben, Handel, Produktion, Wissenschaft und Forschung seit der Einführung des Personal Computer in den 80er Jahren und der Nutzung des Internets seit Mitte der 90er Jahre völlig verändert. Es gibt heute keinen der 391 Ausbildungsberufe mehr, der auf Informationstechnik verzichten kann. Weit über 90 Prozent der Bundesbürger hat nach dem (N-)Onliner Atlas der Initiative D21 e.V. privat oder über ihre Arbeitsstätte Zugang zu Computern und Internet. Medienkompetenz und Wissen über Datenschutz- und Sicherheitsprobleme halten jedoch mit dieser rasanten Entwicklung nicht Schritt.

Die Nutzung von Geodaten in Kombination mit Personendaten bedroht die Privatsphäre

Inzwischen sind beim Handel mit Immobilien Bing und Google Earth zu einem alltäglichen Instrument geworden. Die Auflösung der aus Satellitendaten generierten Luftbilder ist auf unter 20 m/Bild gesunken. Entsprechend ist nicht nur zu erkennen, welches Fahrzeug Sie vor Ihrer Haustüre parken, sondern auch, ob Sie vergessen haben, Ihr Schiebedach zu schließen. Dies gilt zumindest theoretisch – denn noch sind diese Daten durchschnittlich etwa zwei Jahre alt.

Damit aber können Bewerber um einen Job bequem einer Durchleuchtung ihres Umfeldes unterzogen werden. Schaue ich mir doch erst einmal anhand der Adresse an, wo der oder die Bewerberin wohnt: Ist das eine Einfamilienhausgegend oder ein verfallenes Viertel mit vielen Sozialhilfeempfängern? Wurde das Haus erst kürzlich renoviert oder bröckelt schon der Putz? Mit Google Streetview alles kein Geheimnis mehr – weder für Arbeitgeber noch den Sachbearbeiter bei der Versicherung oder der Bank. Auch die organisierte Planung von Tageswohnungseinbrüchen wird durch Google Streetview erheblich erleichtert: So sind mit Google Earth leicht die Wohngegenden mit gehobenem Wohnstandard zu identifizieren, die nahe an Autobahnanschlüssen und Fernstraßen liegen. Dank Google Streetview kann nun auch schon einmal ein Blick auf die Standards der Türen und der Sicherheitseinrichtungen geworfen werden, um den nächsten Raubzug generalstabsmäßig zu planen.

Wie sehr die Politik der IT-Technik hinterherläuft, zeigte der Start der Zweitauflage von Streetview im Mai 2011 durch den Microsoft Konzern, genannt Bing Streetside. Und immer noch gibt es kein Gesetz, dies zu unterbinden oder zumindest zu erschweren. Ein Gesetz, das die bildliche Erfassung von Straßenzügen und Straßenzusammenhängen für kommerzielle Zwecke und die damit verbundenen Grundrechtsverletzungen mit einer drastischen Steuer belegt, wäre eine interessante Neuerung. Und der bisher leer laufende Rechtsschutz könnte durch „Rabatte“ bei dieser Gebühr für jene Erfasser verbessert werden, die sich vertraglich verpflichten, sich dem BDSG zu unterwerfen und den Betroffenen vor Veröffentlichung und auf Dauer Widerspruchsrechte einzuräumen.

Soziale Netzwerke im Zwielicht: Intransparente Verwertung, illegale Mitgliederwerbung, heimliches Spähen.

Viele Beobachter stehen heute staunend vor der Tatsache, dass ganz im Gegensatz zu Zeiten der Volkszählung ’87 heute Millionen Jugendliche und Erwachsene Mitglieder in „Facebook“, „Schüler-VZ“ und anderen VZ-Netzwerken wie „Lokalisten“, „Xing“ oder „Stay Friends“ werden und zum Teil persönlichste Dinge über sich offenbaren. Viele denken offenbar, dass ihre Daten in der Vielzahl von Profilen schon verschwinden werden oder zumindest nicht auffallen. Spätestens dann jedoch, wenn die Lehrstelle futsch ist, weil der zukünftige Arbeitgeber das Saufvideo auf Facebook oder YouTube entdeckt hat, schlagen manche hart auf dem Boden der Realität auf.

Warum fallen so viele Menschen auf diese Dienste herein und lassen sich von den Anbietern geradezu einlullen? Facebook greift auf relativ simple psychologische Tricks von Werbefachleuten zurück, um jegliches Misstrauen einzuschläfern. Während etwa das seriöse Netzwerk Xing von „Kontakten“ spricht, nennt Facebook das „Freunde“ und schleicht sich so ins Vertrauen der Klienten. Hinterhältig und illegal geht Facebook bei der Totalerfassung ganzer Mailadressbücher seiner Mitglieder vor: Unter „Freunde suchen“ sollen die User ihr E-Mailkonto und ihr Passwort eingeben. Was normalerweise kein vernünftiger Mensch einem völlig Fremden, der in Kalifornien sitzt, gestatten würde, tun erstaunlich viele: Facebook lädt sich sämtliche E-Mail - Adressen hoch, durchsucht danach seinen Profilbestand und schlägt Personen mit gleich lautender E-Mailadresse als „Freunde“ vor. Facebook geht aber noch weiter und schickt dann auch Personen, die gar keine Facebook- Mitglieder sind, Werbemails mit der Aufforderung zu, sich bei Facebook anzumelden: dort würden sie folgende „Freunde“ treffen können. An keiner Stelle wird darauf hingewiesen, in welchem Umfang sich Facebook Daten aneignet. Stattdessen werden User mit dem Hinweis eingelullt, dass Facebook persönliche Mails und Adressen niemals an Werbekunden weitergeben würden. DAS müssen sie auch gar nicht.

Der Autor des Buches „Die Facebook Falle“, Sascha Adamek, sagte hierzu im März 2011:[7] „Ein brisanter Test mit dem Institut für Internetsicherheit Gelsenkirchen hat ergeben, was aus den Adressbüchern zu Facebook gelangt: Alles. Im Test gaben wir dem Max-Mustermann noch ein paar Notizen bei, er sei geschwätzig und auf Arbeitssuche. Auch fügten wir eine Mobilnummer mit dem Stichwort „sexy Schnitte“ hinzu. Alles landete bei Facebook – und am Schlimmsten: ohne die von Facebook versprochene SSL-Verschlüsselung. Jahrelang haben Menschen so womöglich ihr allerheiligstes Passwort unverschlüsselt an Facebook übertragen und jeder, der wollte, konnte die E-Mail-Passwörter abgreifen. Seit Mai 2010 verschlüsselt Facebook allerdings diese Funktion.“

Vertrauen erschleichen, Benutzer mit Vertraulichkeiten einlullen

Noch einen Schritt weiter geht der „Gefällt mir"-Button auf Facebook-Seiten, der nach Adamek unsere Konsuminteressen und Bedürfnisse genau rastern soll. Und je enger die Plattform dieses Raster unserer Person strickt, desto besser kann sie für die werbetreibende Industrie Anzeigen setzen, die auf uns ganz persönlich zugeschnitten sind. Hinzu kommt der Aspekt des Empfehlungs-Marketings. Denn seien wir ehrlich: den Empfehlungen durch unsere „Freunde" folgen wir allemal lieber als wildfremden Anzeigen. Hier setzt Facebook als moderne Werbemethode das „Virale Marketing" ein. Virales Marketing, auch als „Königsdisziplin des Social Media Marketing" [8] bezeichnet, beruht darauf, dass Freunde bewusst Empfehlungen an ihre Freunde weitergeben und sich diese Nachricht nach dem Schneeballprinzip ausbreitet - an sich legitim, wenn sich die Akteure dessen bewusst sind, was sie tun.

Das muss allerdings im Falle von Facebook lebhaft bezweifelt werden. Zwar weist die Facebook-Datenschutzerklärung, sofern man sie anklickt, auf die Funktionsweise der Buttons hin, aber um diesen Teil der Erklärung zu finden, muss auf der betreffenden Seite schon weit nach unten gescrollt werden und auch hier wird verharmlost, getarnt und getäuscht. So heißt es unter Datenschutz/Werbung: „Wenn du auf der Facebook-Seite, Werbeanzeige oder dem Produkt eines Unternehmens auf „Gefällt mir" klickst: ...Stellst du eine Verbindung zu diesem Unternehmen her und erhältst Aktualisierungen von diesem in Deinen Neuigkeiten... Wird die Meldung über deine Verbindung an deiner Pinnwand angezeigt.... können deine Freunde eine Meldung darüber in ihren Neuigkeiten sehen, dass dir dieses Unternehmen gefällt.[9] Die vollständige Übersetzung dieser Zeilen müsste etwa lauten:

Wenn Sie diesen Knopf drücken, wird ihre E-Mailadresse an das betreffende Unternehmen weitergegeben und Sie erhalten Werbung. Außerdem wird Ihr Profil zum Werbeträger dieser Firma und unsere Software sendet diese Werbung - als persönliche Nachricht und ohne Ihre gesonderte Zustimmung – allen ihren Kontakten. Auch wenn Sie Ihr Profil später löschen, werden Daten, die Dritte erhalten haben, weder zurückgeholt, noch gelöscht.

Systematische Datenenteignung durch Social Engineering

Ein Schelm, der hier an einen Zufall oder gar liebenswerte Naivität glaubt. Es handelt sich bei Facebook um nichts anderes als eine systematisierte und institutionalisierte Form von „Social Engineering". Als „Social Engineering" wird der Versuch bezeichnet, Menschen mittels Vertraulichkeiten und Bruchstücken persönlicher Informationen über sie und ihr Umfeld – man ist ja von „Freunden" umgeben - in eine Stimmung zu versetzen, aufgrund derer es gelingt, unter Ausnutzung von Arglosigkeit Informationen zu erschleichen[10]. Facebook hat damit den systematischen, psychologisch ausgefeilten Datendiebstahl zum Geschäftsmodell erkoren und ist damit weltweit erfolgreich.

So wird verständlich, wie es dazu kommt, dass so viele, eigentlich ganz vernünftige Facebook-Nutzer (davon 19 Mio. in Deutschland[11]) ihre persönlichen Daten auf Facebook preisgeben. Denn gerade Facebook hat es zur Perfektion getrieben, nicht nur Daten über seine Kunden zu sammeln, sondern erhöht den Reiz und Spielwert dadurch, dass neben den „Freundschaften", die gesammelt werden, auf der Pinwand jede Menge Kommunikation stattfindet, die Auskunft über Interessen, Weltanschauungen, politische Meinungen und Vorlieben des Nutzers gibt. Darüber hinaus wird sein Verhalten in Foren, Spielen und Tests aufgezeichnet und kann danach ausgewertet werden, wie leicht oder schwer er oder sie zu manipulieren ist und auf welche digitalen Schlüsselreize Reaktionen erfolgen. Angesichts dieser Fakten ist pikant, dass Facebook-Milliardär Mark Zuckerberg kürzlich forderte, soziale Netzwerke in USA künftig auch für Kinder zu öffnen, die jünger als 13 Jahre sind. Noch verbietet nämlich der Children's Online Privacy Protection Act (COPPA) US-amerikanischen Unternehmen, persönliche Daten von Kindern zu speichern.[12] Allerdings sind nach einer Untersuchung des „Consumer Reports Magazine" 2011 bereits 5 Millionen Kinder unter 10 Jahren in USA Mitglied bei Facebook, zumeist ohne Wissen oder Aufsicht ihrer Eltern. [13]

Demokratiesegen oder freiwillige StaSi?

In den ersten Monaten der arabischen Revolutionen 2011 wurde der Name Facebook immer wieder als die Plattform genannt, auf der sich die kritische, weltoffene Jugend zu Protesten verabredet und Solidarität organisiert hat. Eine politikwissenschaftliche Untersuchung ist darüber allerdings bisher nicht erfolgt. Auch ein anderer Aspekt mahnt zu Vorsicht vor vorschnellen Urteilen über den Stellenwert sozialer Netzwerke im Rahmen der öffentlichen Meinungsbildung: So überschlugen sich während der Zuspitzung des zu Guttenbergschen Fälschungskandals innerhalb weniger Tage auf Facebook die in die Hunderttausende gehenden „Gefällt mir" Bekundungen während sich zu den angekündigten Demonstrationen nur ein paar unentwegte Einzelkämpfer zusammenfanden, die an zwei Händen abzuzählen waren. Der Kabarettist Michael Niavarani nennt Facebook dagegen „StaSi auf freiwilliger Basis."14 bei der jeder seine Akte auch noch selbst anlegt. Diese sensiblen Daten sind, solange sie bei Facebook in den USA gehostet werden, nach der Homeland Security Gesetzgebung bei Terrorismusverdacht den Sicherheitsbehörden FPI, CIA und der NSA zugänglich.

Facebook-Kritiker Adamek hat Details herausgefunden: „Der Segen der schnellen Vernetzung kann zugleich zum Fluch werden. So wurden in Iran 2009 Oppositionelle verhaftet, weil der Geheimdienst ihre Profile mit sämtlichen Aktivitäten und Verbindungen ausgewertet hatte, ja sogar eigene Facebook-Profile angelegt hatte, um Menschen auszuhorchen. Vor dem Sturz von Präsident Ben Ali in Tunesien gelang es der Regierung durch Phishing-Mails, die Facebook-Konten vieler Oppositioneller und Sympathisanten zu knacken. Die Leute gaben ihr Passwort ein und ahnten nicht, dass sie damit di-

rekt auf die Server des Regimes umgelenkt wurden. Facebook selbst reagierte darauf erst viele Wochen später, als sich Oppositionelle beschwerten, dass bestimmte Meinungsäußerungen regelmäßig verschwanden. Das zeigt mir: Die Rolle von Facebook ist janusköpfig und kann auch von autokratischen Regierungen missbraucht werden."[15]

Je größer und detaillierter die Datenmenge, je genauer die Persönlichkeitsprofile, die diese neue Datenindustrie über die Menschen gewinnen kann, desto höher die Gewinne, die durch Werbung und Verhaltenskontrolle generiert werden können. Hinzu kommen die Möglichkeiten der Manipulation durch ungewolltes virales Marketing, und die Möglichkeiten, durch Spiele, Animationen oder „Reality Mining"[16] Verhaltensmuster detailliert zu analysieren und zu manipulieren. Gemeint ist damit die systematische Auswertung der Statusmeldungen, die viele Nutzer in die Rubrik „Was machst Du gerade?" ständig eintragen. Banalitäten wie Kaffeetrinken, Konzertbesuche oder Gang zum Friseur finden Marketingfirmen höchst interessant. Anbieter wie Daytum kleiden derartigen Schwachsinn in Apps, die permanente Selbstbespiegelungen fürs iPhone verarbeiten und für Marketingzwecke aufbereiten. Zum auf dem iPhone gespeicherten Bewegungsbild kommt dann auch noch die freiwillige Beschreibung der Tätigkeit. Dergleichen muss jede Observationsgruppe des Verfassungsschutzes vor Neid erblassen lassen.

Nein, die Volkszählung 2011 ist nicht das Problem. Datenschutz geht in ein neues Jahrhundert und eine neue Dimension. Es gibt viel aufzuklären und viel zu tun.

1 So der Präsident des Landesbetriebs Information und Technik NRW im WDR 2 Hörfunk am 12.5.2011

2 Erhebungsbogen der Gebäude- und Wohnungszählung 2011, S. 3 Fragen W 6 bis W 9

3 Erhebungsbogen der Haushaltsbefragung auf Stichprobenbasis: www.zensus2011.de

4 in der WDR 2 Sendung „Volkszählung – wie viele Daten brauchen wir" vom 12.5.2011

5 http://de.wikipedia.org/wiki/Aleviten

6 http://www.humanistische-union.de/aktuelles/aktuelles_detail/back/aktuelles/article/zensus-2011-der-datenschutz-zaehlt/

7 Sascha Adamek im Interview des Publizisten Reinhard Jellen, Heise Online v. 27.3.2011 http://www.heise.de/tp/artikel/34/34323/1.html

8 Dorothea Reder, Social Media Marketing, a.a.O. S. 31

9 http://www.facebook.com/privacy/explanation.php

10 http://de.wikipedia.org/wiki/Social_Engineering_(Sicherheit)

11 Dorothea Heymann-Reder, „Social Media Marketing", München, San Francisco 2011, S. 29

12 Zitiert nach einer Meldung auf "Heise Online" vom 23.5.2011 12.00 Uhr

13 http://www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/facebook-concerns/index.htm

14 Michael Niavarani http://www.youtube.com/watch?v=v5cZaaRzwGk

15 Sascha Adamek a.a.O., Interview am 27.3.2011 http://www.heise.de/tp/artikel/34/34323/1.html

16 Reality Mining in sozialen Netzwerken: http://www.heise.de/newsticker/meldung/Reality-Mining-im-Social-Network-1240082.html

Pressemitteilung des Arbeitskreises Zensus vom 31.05.2011:

Zensus-Daten in Gefahr

+++ Organisator der britischen Volkszählung gehackt +++

Der mit der Durchführung des britischen Zensus beauftragte Rüstungskonzern Lockheed-Martin wurde am 21. Mai gehackt. Nun fürchten 62 Millionen Briten um ihre Daten. Grundlage des unbefugten Zugriffs bildete der vorhergehende Angriff auf einen weltmarktführenden Anbieter von IT-Sicherheit. Ähnliche Angriffe sind auch bei allen anderen Datenspeicherungen möglich.

Schon im März wurde gemeldet, dass der weltweit mit-führende Anbieter von IT-Sicherheitskomponenten, Verschlüsslungs- und Authentifizierungssoftware, die US-amerikanische RSA Security Inc., Opfer eines professionellen Hackerangriffs geworden ist.[1] In Folge dieses Angriffs erbeuteten Hacker hochsensible Informationen über die zur Sicherheit zahlreicher renommierter Weltkonzerne eingesetzten Rechner-Verschlüsselungssysteme. Damit dürften nach Schätzung von IT-Experten die IT-Systeme der weltweit bedeutendsten Großkonzerne und Rüstungsunternehmen ein ernsthaftes Sicherheitsproblem bekommen haben.[2] Sogar vom Pentagon als RSA-Kunden ist die Rede.

Nun ist der erste Hack eines RSA-Kunden publik geworden:[3] Der amerikanische Rüstungskonzern Lockheed-Martin meldete den erfolgreichen Hacker-Einbruch in ihre Rechnersysteme. Der Konzern konnte zunächst nicht sagen, ob und welche Daten von Diebstahl und/oder Manipulation betroffen waren.

Besonders brisant ist dabei die Tatsache, dass Lockheed-Martin an der Durchführung der britischen Volkszählung maßgeblich beteiligt ist und unter anderem die Zensusfragebögen der Briten erfasst.[4] Der Vorfall zeigt, dass die von den Kritikern der deutschen Volkszählung vorgebrachten Warnungen vor unsicheren Daten ernstzunehmen sind.

„Selbst Hochtechnologiekonzerne wie Lockheed-Martin oder Sony sind nicht in der Lage, ihre Rechnersysteme zuverlässig zu schützen," sagt Michael Ebeling von der Bürgerinitiative Arbeitskreis Zensus. „Das überrascht uns nicht. Wir sind der festen Überzeugung, dass auch die Volkszählungsdaten bei den hiesigen Statistikämtern nie sicher sein können. Deswegen halten wir die Sammlung von sensibelsten Daten wie Auskunftssperren, Migrationshintergrund oder die namentliche Markierung aller Bewohner von psychiatrischen Anstalten, Gefängnissen, Behindertenwohnheimen, Flüchtlingslagern, Frauenhäusern u.v.m. für völlig untragbar. Das ist und bleibt skandalös."

Diese und andere Merkmale der in Deutschland durchgeführten Volkszählung kritisieren die Datenschützer in ihrer „Gemeinsamen Erklärung zum Zensus 2011".[5] Auf ihrem Internetportal „www.zensus11.de"[6] stellen die in der Bürgerinitiative versammelten Kritiker unabhängige Informationen und Hilfestellungen[7] zur Verfügung, sammeln Beschwerden und Klagen[8] und fordern den sofortigen Stopp dieser ihrer Meinung nach unverhältnismäßigen Erfassungsmaßnahme.

Die Schwachstellen bei der Datensicherheit wirken sich nicht nur auf den Zensus aus, sondern haben ebenfalls erhebliche Auswirkungen auf alle anderen gespeicherten vertraulichen Daten. Dies betrifft neben den Gefahren für die Wirtschaft unter anderem auch Datensammlungen wie die erneut geplante Vorratsdatenspeicherung, die Fluggastdatenspeicherung, ELENA u.v.m.

Broschüre des Arbeitskreises Vorratsdatenspeicherung zum Thema Datensicherheit:

http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten.pdf

[1] http://heise.de/-1210245
[2] http://gizmodo.com/5806485/lockheed-martins-security-networks-were-hacked
[3] http://heise.de/-1251902
[4] http://www.lockheedmartin.com/news/press_releases/2008/0828_lmuk-2011-census.html
[5] http://wiki.vorratsdatenspeicherung.de/images/B%C3%BCndnisaufruf.pdf
[6] http://zensus11.de/
[7] http://zensus11.de/hilfestellungen/
[8] http://zensus11.de/beschwerden/

Sönke Hilbrans

Konfliktlinien auf dem Weg zu einem Beschäftigtendatenschutzgesetz

Die DVD- Position in der Anhörung im Innenausschuss des Deutschen Bundestages

Es war etwas stiller geworden um die Gesetzgebung zum Beschäftigtendatenschutz, nachdem die Bundesregierung im Jahr 2010 noch eine stürmische und von der Fachöffentlichkeit vehement kritisierte Entwurfstätigkeit entfaltet hatte[1]. Sah es zwischenzeitlich fast so aus, als ob das Projekt einer Vollkodifizierung des Arbeitnehmerdatenschutzes in neuen Paragraphen 32 – 32l BDSG ganz zum Stillstand kommen würde, so trat die Bundesregierung mit einem deutlich bereinigten Gesetzentwurf vom 15.10.2010 (Bundestags-Drucksache 17/4230) an die Öffentlichkeit. Dieser Entwurf stand dem Innenausschuss des Deutschen Bundestages am 23.05.2011 zur Auswertung in einer Sachverständigenanhörung an. Er stand dabei nur noch scheinbar in Konkurrenz zu dem älteren und wegen der Mehrheitsverhältnisse nicht durchsetzungsfähigen Gesetzesentwürfen der Fraktion der SPD (BT-Drucks. 17/69) und dem sehr lesenswerten jüngeren Entwurf aus der Fraktion Bündnis 90/Die Grünen vom 22.02.2011 (BT-Drucks. 17/4853)[2]. Zusätzliche Bewegung kam dadurch in die Sache, dass die Ausschussberichterstatter der Koalitionsfraktionen ein Arbeitspapier in die Runde warfen, welches offenbar jüngere Kritik an dem Gesetzentwurf der Bundesregierung aufgriff[3]. Nur: diese Kritik kann offensichtlich nicht aus den Reihen von Datenschützern gekommen sein.

Die DVD hat ihre bis heute in wesentlichen Punkten der Bundesregierung widersprechende Haltung zur Regelung des Arbeitnehmerdatenschutzes in Deutschland bereits frühzeitig in die Diskussion eingebracht und mit einer aktualisierten Stellungnahme auch im Innenausschuss des Bundestages vertreten[4]. Auch der Entwurf der Bundesregierung vom 15.12.2010 weist danach nicht in eine Zukunft des Arbeitnehmerdatenschutzes. Er soll zwar das Ziel verfolgen, praxisgerechte Regelungen für die Verarbeitung von Beschäftigtendaten zu schaffen, Datenverarbeitung auf das zu Zwecken des Beschäftigungsverhältnisses Erforderliche zu beschränken, Beschäftigte wirksam vor Bespitzelungen am Arbeitsplatz zu schützen und gleichzeitig Arbeitgebern verlässliche Grundlagen für die Erfüllung von Compliance-Anforderungen und den Kampf gegen Korruption an die Hand zu geben. Diese Ziele verfehlt der Entwurf allerdings, weil

- er keine klare gesetzliche Differenzierung zwischen den verschiedenen mit personenbezogenen Daten von Beschäftigten verfolgten Zwecken trifft,
- daher informationelle Gewaltenteilung im Betrieb und Unternehmen nicht geschaffen wird,
- der Vorrang der offenen Direkterhebung personenbezogener Daten weiträumig aufgehoben wird,
- schutzwürdige Interessen von Beschäftigten im Wesentlichen nur mittels in der Praxis nicht abgrenzungsscharfer Generalklauseln geschützt werden sollen,
- effektive Verfahrensregelungen und Sanktionen zum Schutz der Beschäftigten vor Datenschutzverstößen (Zustimmungsvorbehalte für den betrieblichen Datenschutzbeauftragten, Verwertungsverbote usw.) nicht geschaffen werden.

Dagegen zielt der vorgelegte Entwurf etwa mit der Legalisierung der betriebsinternen Rasterfahndung darauf, eine Überwachung und Ausforschung von Beschäftigten rechtlich abzusichern, die nach geltendem Recht unzulässig wäre. Datenschutzverstöße, die noch in jüngster Zeit als Skandale gewertet wurden, würden dadurch legalisiert. Demgegenüber werden Innovationen, welche Beschäftigte vor sachlich nicht angezeigten Eingriffen in ihre Persönlichkeitsrechte wirksam schützen könnten, nicht aufgegriffen. So verzichtet er etwa auf die im Entwurf der Fraktion Bündnis 90/ Die Grünen beschriebene Verbandsklagebefugnis im Beschäftigtendatenschutzrecht, auf obligatorische betriebliche Mitbestimmung bei der Auswahl der betrieblichen Datenschutzbeauftragten und eine unabhängige Kontrolle von eingriffsintensiven heimlichen Datenerhebungen gerade im Compliance-Bereich. Auch bleiben etliche Baustellen zurück: So fehlen etwa Anpassungen des Beschäftigtendatenschutzes an den gesetzlichen Schutz besonderer Arten personenbezogener Daten (§ 3 Abs. 9, § 28 Abs. 6 – 9 BDSG u. a.) ebenso wie eine Lösung für die (auch) private Nutzung betrieblicher Telekommunikationseinrichtungen[5]. Gegenüber früheren Fassungen drängt sich der Eindruck auf, dass das Gesetz Standardlösungen für Fallgestaltungen verfolgt, in denen Arbeitgeberinteressen bislang an den Persönlichkeitsrechten der Beschäftigten zu scheitern drohen. So sind etwa Entwurfsregelungen für ärztliche Untersuchungen in Eignungstests (§ 32c Abs. 3 BDSG-E) wohl nur mit dem Bedürfnis vieler Arbeitgeber zu erklären, auch während des laufenden Beschäftigungsverhältnisses grundlegende Einstellungsvoraussetzungen immer neu zu bewerten und die Belegschaft nach medizinischen und anderen scheinbar objektiven Kriterien gleichsam zu

optimieren. Die arbeitsrechtliche Praxis kann dagegen mit den bestehenden Regelungen zu den Betriebsärzten und zum Wiedereingliederungsmanagement auskommen. Beibehalten wurde auch die globale Zweckbestimmung für Beschäftigtendaten, welche letztlich jedes von einem Arbeitgeber im Rahmen der Verhaltens- und Leistungskontrolle verfolgbares Interesse zum legitimen Zweck einer Datenverarbeitung macht. Effektive Schranken wenigstens für eingriffsintensive Verarbeitungsschritte wie die Übermittlung an Dritte finden sich auch im aktuellen Gesetzentwurf nicht.

Im Regelungsbereich Compliance will der Entwurf über die erst 2009 eingeführte strenge Regelung von § 32 Abs. 1 S. 2 BDSG hinwegkommen und heimliche Maßnahmen der Arbeitgeberseite auch bei verhältnismäßig geringfügigen mutmaßlichen Pflichtverletzungen der Beschäftigten zuzulassen (Stichwort Maultaschenkündigung). Der im öffentlichen Bereich geläufige Maßstab des Rechtsgüterschutzes soll im Beschäftigtendatenschutz durch arbeitsvertragliche Wertungen ersetzt werden, ohne dass eine verfahrensrechtliche Sicherung vor exzessiver oder unverhältnismäßiger Datenerhebung bestehen soll. Dass die wenigsten Betroffenen den Fortbestand ihres Arbeitsverhältnisses durch eine datenschutzrechtliche Beschwerde oder gar das Beschreiten des Rechtswegs gefährden würden, bleibt unter diesen Umständen ein zentrales Problem, dem sich der Gesetzentwurf ebenfalls nicht stellt.

Es folgen im Stil eines Polizeigesetzes Einzellösungen zu spezifischen Datenerhebungsmethoden wie etwa der Videoüberwachung, biometrischer Verfahren und der Nutzung von Telekommunikationsdiensten. Diese Regelungen sollen die Spielräume, welche die Rechtsprechung den Arbeitgebern im gegenwärtigen Rechtszustand lässt, wesentlich erweitern. Während der Gesetzentwurf damit auf im Einzelfall verfassungswidrige Zustände zusteuert, hat das Arbeitspapier der Berichterstatter der Koalitionsfraktionen bereits einen der wenigen effektiven Vorzüge des Gesetzentwurfs der Bundesregierung zur Disposition gestellt, nämlich das Verbot der heimlichen Videoüberwachung am Arbeitsplatz. Weiterhin unverständlich ist auch, dass der Gesetzentwurf zwar auf eine förmliche Whistleblower-Regelung verzichtet, aber in Anlehnung an eine Tendenz in der Rechtsprechung die Mitteilung von Verstößen des Arbeitgebers gegen Gesetz und Recht an Strafverfolgungs- oder Aufsichtsbehörden (wie die Datenschutzbeauftragten des Bundes und der Länder) davon abhängig macht, dass der Arbeitnehmer den Arbeitgeber informieren und um Abhilfe ersuchen muss.

Es ist nach dem Beitrag der Berichterstatter der Koalitionsfraktionen abzusehen, dass die weiteren Gesetzesberatungen außerdem um zwei in dem Gesetzentwurf vom 15.12.2010 noch unangefochtenen Prinzipien kreisen wird: Dem Verbot einer Benachteiligung der Beschäftigten durch Betriebsvereinbarungen, welche hinter den Schutzstandard des Gesetzes zurückfallen (§ 32l Abs. 5 BDSG-E), und der Kanonisierung der Anwendungsfälle der Einwilligung (§ 32l Abs. 1 BDSG-E). Während der Gesetzentwurf auch von Arbeitgeberseite in der Anhörung an vielen Stellen Kritik erfuhr, zeichnete sich in den mündlichen Beiträgen ab, dass die Frage, ob es nicht doch legitime Anwendungsfälle der datenschutzrechtlichen Einwilligung im Arbeitsverhältnis geben kann und welche dies sind, die Sachverständigenrunde spaltete[6]. Ob die Koalition angesichts der ungelösten inhaltlichen Probleme noch viel Appetit darauf hat, das Beschäftigtendatenschutzgesetz in dieser Legislaturperiode zu vollenden, bleibt abzuwarten. Es hat sich zunächst eine parlamentarische Arbeitsgruppe gebildet, welche das Projekt weiter verfolgt. Die Vertreterinnen der Gewerkschaften waren dagegen in ihrer Haltung eindeutig: Kein Gesetz ist immer noch besser als der vorgelegte Gesetzentwurf der Bundesregierung. Sollte es in dieser Legislaturperiode zu einem Beschäftigtendatenschutzgesetz kommen, werden wir uns an diese Position noch häufiger erinnern.

http://www.datenschutzverein.de/Themen/DVD%20Stellungnahme%20zur%20Anhoerung%20BeschDS%2020110523.pdf

1 s. dazu den Beitrag von Sören Jungjohann, Chronik der Kodifizierung des Arbeitnehmerdatenschutzes, DANA 4/10, S. 147.

2 Alle Gesetzentwürfe, Anträge und schriftliche Äußerungen der Sachverständigen sind auf der Website des Deutschen Bundestages abrufbar unter: http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung08/index.html

3 Gisela Piltz, MdB, FDP und Michael Friser, MdB, CDU

4 Siehe schon die gemeinsame Presseerklärung „Eckpunkte eines Beschäftigtendatenschutzgesetzes“ v. 20.05.2010; die Stellungnahme der DVD zur Anhörung im Bundestag ist abrufbar unter http://www.datenschutzverein.de/Themen/DVD%20Stellungnahme%20zur%20Anhoerung%20BeschDS%2020110523.pdf.

5 Stattdessen erfolgt mit § 32 Abs. 2 BDSG-E eine teilweise Anpassung an das allgemeine Gleichstellungsgesetz und behält § 32i BDSG-E das aus den Vorentwürfen übernommene verfehlte Regelungsmodell bei, s. Hilbrans, Beschäftigtendatenschutz und betriebliche Telefonanlagen, AuR 2010, 424.

6 Das Protokoll der mündlichen Beiträge wird in Kürze vom Innenausschuss veröffentlicht werden. S. auch heute im bundestag hib Nr. 206 v. 23.05.2011.

Ixquick.com und Startpage.com bieten anonyme Websuche

Wir haben den CEO von Ixquick, Robert Beens, gebeten, uns über Vorzüge und geplante Entwicklungen bei Ixquick zu informieren. Dies ist seine Antwort.

Statement – Robert Beens, CEO:

„Privatsphäre ist fundamentales Menschenrecht und die Basis jeder freien Gesellschaft. Wir bringen die NutzerInnen unserer Suchmaschinen in den Genuss des gesamten Internets ohne diese Rechte anzutasten."

Zusammenfassung:

Ixquick und Startpage sind Suchmaschinen zur Wahrung der Privatsphäre. Startpage präsentiert die Suchresultate von Google, während Ixquick die Aufgabe hat, kombinierte Resultate von vielen anderen Suchmaschinen (Metasuche) darzustellen. Beide übermitteln die Resultate zu den Suchanfragen unter absoluter Wahrung der Privatsphäre.

Datenschutz-Hintergrund:

Suchmaschinen spielen bei der Diskussion um den Datenschutz immer schon eine große Rolle. Das Internet enthält immense Mengen von Informationen, die uns einen beispiellosen Zugang zu Einkaufsmöglichkeiten, Nachrichten, Unterhaltung und vielen anderen Dingen ermöglichen. Suchmaschinen helfen uns dabei, durch all diese Daten zu navigieren, um das, was wir suchen, schnell und effizient zu finden.

Sie sind Zugangspunkte zum Internet. Ihnen werden viele – vertrauliche – Informationen über das Privatleben der Nutzer anvertraut, die diese durch ihre Internet-Surf-Gewohnheiten preisgeben. Wer sucht wann nach was – und wohin gehen die Benutzer dann letztlich? Zeit und Häufigkeit, Suchbegriffe, IP Adressen, besuchte Webseiten usw.: alles wird aufgezeichnet und gespeichert.

Die meisten Benutzer sind sich immer noch nicht dessen bewusst, dass Suchmaschinen ihre Daten sammeln, die sie persönlich identifizieren. IP-Adressen sind die primäre Methode, mit der an Suchmaschinen übergebene Informationen persönlich identifizierbar gemacht werden. Eine weitere wichtige Methode ist die Verwendung von „einmaligen ID-Cookies". Diese „einmaligen ID-Cookies" werden auf Ihrem Computer gespeichert und dienen als Bindeglied zwischen den kleinen Datenpaketen aus den verschiedenen Internet-Services. Das Cookie fügt die Teile des Puzzles zusammen. IP-Adressen können sich ändern – einmalige ID-Cookies nicht. Einen noch viel größeren Einbruch in unsere Privatsphäre bringen die so genannten LSO- oder Supercookies mit sich. Es gestaltet sich nämlich vor allem für Laien als sehr schwierig, diese Cookies wieder von der Festplatte zu entfernen.

Natürlich ist es nicht einfach zu verstehen, dass jeder Zugriff und jede Frage die wir in unsere Lieblingssuchmaschine eingeben, einen Teil im Puzzle unseres Persönlichkeitsprofils ergänzt. Und nutzen wir diese Suchmaschine regelmäßig, ergibt sich aus diesen Teilen irgendwann ein Gesamtbild. Die Suchmaschine hat nun gelernt, welchen Hobbys wir nachgehen, sie kennt unsere berufliche Ausrichtung, unseren Familienstand, unsere politischen Interessen, unsere sexuelle Orientierung, unsere medizinische Vergangenheit und somit unsere gesamte Lebensplanung.

Auch wir begrüßen neue Technologien, die uns Menschen mehr Komfort bieten. Doch gegenwärtig produziert das Verhalten der Wirtschaft und der Politik einen Einheitsbrei. Unser Denken wird durch personalisierte Ergebnisse in den Suchmaschinen gesteuert und kann sich so nicht mehr frei entwickeln. Dies verändert unser gesamtes Verhalten nachhaltig. Denn wir orientieren uns, ohne es zu merken, nur noch an den Interessen der Vergangenheit. Die Weiterentwicklung unseres Denkprozesses aufgrund von Lebenserfahrung kommt zum Stillstand.

„Ich habe nichts zu verbergen", ist wohl das häufigste Argument der sogenannten Post-Privacy-Generation. Wenn aber personalisierte Daten über einen Menschen vorhanden sind, werden sie früher oder später verwendet werden. Die reichhaltigen Datensammlungen der Suchmaschinenbetreiber sind die eine Seite. Telekommunikationsbetreiber speichern den Zeitpunkt und den Ort, sowie die Gesprächspartner unserer Telefonate oder unsere Verbindungsdaten im Internet. Das wiederum ruft die Staaten auf den Plan. Diese erhalten dank dieser Technologien und bereits gespeicherter Daten die volle Kontrolle; Stichwort: Vorratsdatenspeicherung. Und nicht zu vergessen sind auch die riesigen Hackercommunitys. Der jüngste und auch vom Umfang her größte Datendiebstahl bei Sony hat gezeigt, wie sicher unsere Daten sind. In Anbetracht dieser Fakten sollte jedem Menschen klar sein, dass gesammelte Daten immer gegen einen selbst verwendet werden können. Somit haben wir alle etwas zu verbergen.

Zwischenstatement:

„Ihre gespeicherten Daten werden früher oder später zu Datenmissbrauch führen. Die einzige Lösung diesem Problem zu begegnen ist, diese Daten erst gar nicht zu speichern."

Die Lösung

Ixquick wurde 1998 in New York entwickelt und in Betrieb genommen. Im Jahr 2000 wurde das Ixquick von Surfboard Holding B.V., einem im Privatbesitz stehenden niederländischen Unternehmen übernommen, dessen einzige Aktivität im Betrieb von Ixquick und Startpage besteht. Seit der Gründung im Jahr 1998 ist Ixquick konstant gewachsen, in erster Linie durch Mundpropaganda.

Im Jahr 2005 führte das Management von Ixquick eine Überprüfung durch, um mögliche Verpflichtungen des Unternehmens festzustellen. Ein schok-

kierendes Ergebnis bestand darin, dass wir enorme Mengen von sensiblen, die Privatsphäre betreffenden Informationen über unsere Benutzer gesammelt hatten. Wie andere Suchmaschinen hatten wir Dinge wie die verwendeten Suchbegriffe, die Zeiten und Tage ihrer Besuche, welche Links sie angeklickt haben, ihre IP-Adressen und ihre Benutzer-ID-Cookies gespeichert. Die technischen Gründe für die Sammlung der Daten waren simpel und sind im heutigen IT-Umfeld leider sehr verbreitet: Es kostet nicht viel, es lässt sich sehr einfach durchführen, und die Daten könnten in der Zukunft nützlich sein.

Als wir uns den Berg dieser Daten betrachteten, erschien uns dieser jedoch mehr wie eine Datenschutzbelastung denn als geschäftlicher Aktivposten. Wir hatten die Informationen niemals verkauft oder kommerziell verwendet. Da Ixquick ein unabhängiges Unternehmen ist, das sich ausschließlich auf die Suche konzentriert, waren wir nicht daran interessiert, die Benutzerdaten mit anderen Services zu kombinieren, die wir anbieten. Kurz und gut: Wir hatten eine Datenbank voller Benutzerdaten, die wir weder brauchten noch wollten. Wir fragten uns, warum wir all diese sensiblen Informationen speicherten und erkannten, dass es keinen guten Grund dafür gab.

Diese Erkenntnis veranlasste uns, eine kühne neue Richtung einzuschlagen, und von diesem Augenblick an machten wir den Schutz der Privatsphäre unserer Nutzer zu unserer obersten Priorität.

Im Juni 2006 bereinigten wir unsere Datenbank und löschten rückwirkend alle IP-Adressen und andere gespeicherte Suchdaten. Wir begannen damit, alle neuen IP-Adressen innerhalb von 48 Stunden zu löschen. Und ab Januar 2009 verzichteten wir völlig darauf, IP-Adressen zu speichern.

Inzwischen haben wir unsere Suchprozesse optimiert, um den Schutz Ihrer Privatsphäre zu garantieren und sicherzustellen, dass wir niemals persönliche Daten unserer Benutzer sammeln. Außerdem arbeiten wir daran, sicherzustellen, dass die Suchdaten der Benutzer nicht von anderen Parteien gesammelt werden. Ixquick war die erste führende Suchmaschine, die SSL- (Secure Socket Layer) oder HTTPS-Verschlüsselung angeboten hat, um zu verhindern, dass Suchanfragen von Internet Service Providern (ISP) oder skrupellosen WiFi-Providern und Hackern „belauscht“ werden.

Hervorragende Suchergebnisse

Ixquick ist eine leistungsfähige Meta-Suchmaschine, die gleichzeitig mehrere beliebte Suchmaschinen und Internet-Datenbanken durchsucht, um die umfassendsten und genauesten Ergebnisse aus dem Internet zu sammeln und anzuzeigen. Anders als Einzel-Suchmaschinen wie Google, Yahoo oder Bing kann Ixquick größere Bereiche des Internets abdecken als jede Suchmaschine für sich alleine. Durch die Kombination von Suchergebnissen kann Ixquick den Benutzern dabei helfen, die kommerzielle Manipulation bestimmter Websites zu vermeiden. Diese als „Cloaking“ bezeichnete Praxis sorgt dafür, dass diese Seiten bei einzelnen Suchmaschinen einen künstlich hohen Stellenwert erhalten.

Ixquick bietet weiterhin neue Funktionen, um die Nützlichkeit und Leistungsfähigkeit seiner Suchmaschine zu verbessern. Hierzu zählen unter anderem eine Hervorhebungsfunktion, um die Suchbegriffe auf der Ergebnisseite deutlicher sichtbar zu machen, Universal Power Search, eine globale Suche (Global Search) und Power Refinement. Über unser Internationales Telefonverzeichnis bieten wir auch Telefonnummern und Adressen aus aller Welt, und mit unserer Video-Suche können die Benutzer 18 Millionen Stunden Videoinhalte durchsuchen.

2008 führten wir den Namen Startpage.com in den USA ein, da uns dieser leichter merkbar erschien. Startpage bietet heute Google Suchresultate unter absoluter Wahrung der Privatsphäre. Wenn man mit Startpage sucht, werden vor der Weiterleitung der Anfrage an Google alle Identifikationsmerkmale gelöscht. Die erhaltenen Resultate werden unter Wahrung der Privatsphäre an den User übermittelt. Die IP-Adresse wird zu keinem Zeitpunkt aufgezeichnet, der Besuch wird nicht indexiert und es werden keine Spionage-Cookies im Browser installiert. Die Datenschutzrichtlinien von Ixquick und die erstklassige technische Umsetzung sorgen für hervorragende Suchergebnisse und absolute Anonymität.

Mit Startpage liefern wir Google-Ergebnisse. Damit ist Startpage definitiv mit Google gleichzusetzen. Aber viele unserer NutzerInnen ziehen die Ergebnisse von Ixquick vor, da diese mehr in die Tiefe gehen. Hier kombinieren wir die Resultate verschiedener wichtiger Suchmaschinen und filtern diese nochmals nach der jeweiligen Relevanz bei den einzelnen Anbietern.

Gegenwärtig befinden wir uns in der glücklichen Situation keinen Mitbewerber zu haben. Nur Ixquick und Startpage wurden nach einer ausführlichen Überprüfung aller Prozesse und Angaben mit dem europäischen Datenschutzsiegel ausgezeichnet. Und beide Suchmaschinen haben das Alleinstellungsmerkmal, die europäischen Datenschutzrichtlinien zur Gänze zu erfüllen.

Beide, Ixquick und Startpage offerieren den Erhalt der Privatsphäre im selben Ausmaß:

- Keine Aufzeichnung von IP Adressen
- Keine Aufzeichnung Ihrer Suchanfragen
- Sichere SSL Verschlüsselung verfügbar

- Kostenfreier Proxyservice
- Empfohlen von Datenschutzexperten weltweit
- Seit 12 Jahren erfolgreich
- Ausgezeichnet mit dem europäischen Datenschutzsiegel

European Privacy seal

Als Anerkennung für diese einzigartigen Funktionen überreichte der europäische Datenschutzbeauftragte, Peter Hustinx, Ixquick im Juli 2008 das erste Europäische Datenschutz-Gütesiegel. Denn für unseren Dienst war ein unabhängiges Gutachten enorm wichtig, um zu zeigen, dass wir zu unseren Versprechen stehen.

EuroPriSe überprüft gnadenlos und garantiert heute allen Ixquick- und StartpagenutzerInnen die Wahrung der Privatsphäre bei Nutzung der Dienste.

Die Überprüfung wurde Anfang 2011 erneuert und abermals erhielten beide Suchmaschinen das begehrte Siegel.

Rechtliche Verpflichtungen

Natürlich wäre Ixquick, wie alle anderen, verpflichtet, einzelnen Staatsorganen auf Anforderung Userdaten zur Verfügung zu stellen. Da Ixquick aber keine Daten loggt und somit auch nicht speichern kann, existieren zu keinem Zeitpunkt Userdaten. Vielleicht ist das auch ein Grund, warum Ixquick bislang keine einzige Anfrage von Staat oder Exekutive erhalten hat.

Finanzen

Ixquick ist ein privatwirtschaftlich geführtes Projekt. Wir sind also nicht verpflichtet, Informationen über unseren Finanzstatus zu veröffentlichen. Aber wir freuen uns darüber, dass Ixquick seit fünf Jahren Profit abwirft und wir so in der Lage sind, aus eigenen Mitteln die Weiterentwicklung unserer Werkzeuge im Interesse der Gesellschaft voranzutreiben.

Wie viele andere Websites und Internetservices finanziert sich Ixquick über gesponserte Werbeeinschaltungen. Aber anders als andere Websites gibt Ixquick über die Werbemittel keinerlei persönliche Daten (IP-Adressen, Cookie-Informationen, u.ä.) an die Betreiber dieser gesponserten Einschaltungen weiter. Das wäre auch gar nicht möglich, da diese Daten weder erfasst noch aufgezeichnet werden.

Die Zukunft

Ixquick wird auch in Zukunft innovative Funktionen und Dienstleistungen für verbesserten Datenschutz bieten. Mit unserem demnächst eingeführten Proxy-Service können die Benutzer Websites von Drittanbietern anonym über die Server von Ixquick aufrufen, ohne von diesen Websites erfasst zu werden.

Der Datenschutz bei Suchmaschinen ist ein wichtiges Thema, das weiter an Bedeutung gewinnen wird. Wir sind überzeugt, dass unser Dienst weiter wachsen wird und die Nachfrage stark ansteigen wird. 2011 und 2012 sollen weitere Dienste an den Start gehen.

In jüngster Zeit entdeckten wir auch den Bedarf an einem E-Mailservice, der es möglich macht, E-Mails einfach und bequem ohne großartiges Know-how verschlüsselt zu empfangen und zu senden und den Inhalt nicht ohne Einverständnis aufzubewahren. Deshalb haben wir in die Planung und Entwicklung eines solchen Dienstes investiert. Ein großes Entwicklerteam ist gerade fieberhaft mit der Umsetzung beschäftigt. Wir sind zuversichtlich, dass der Dienst noch in diesem Jahr bereitgestellt werden kann. Denn Websuche mit Privatsphäre war für uns nur der erste Schritt in eine sichere Zukunft.

Während sich das Internet ständig weiterentwickelt, wird Ixquick an seinem Engagement für den Schutz der Privatsphäre festhalten und nach weiteren Möglichkeiten suchen, um der Privatsphäre auch in der digitalen Zukunft einen festen Platz zu reservieren und für den Erhalt einer freien Gesellschaft Sorge zu tragen.

Thilo Weichert

Datenschutz und Transparenz in Russland

I. Einführung

Ende Februar 2011 war der Widerstand gegen die Herrscher und Regierungen in vielen arabischen Staaten entbrannt. Das russische Fernsehen sendete hierzu wenige Berichte und Bilder. Wer sich in Moskau zu dieser Zeit über diese die Welt bewegenden Ereignisse informieren wollte, musste schon westeuropäische Kanäle im Fernsehen ansteuern. Der Umbruch in der arabischen Welt hatte die russische Gesellschaft nicht wirklich erreicht. Auch wenn die russische Regierung keine vergleichbaren Aufstände im eigenen Land befürchten musste, äußerte sie sich kritisch zur westlichen Reaktion hierauf: Die westlichen Regierungen würden die Unruhen schüren, um islamistische Bestrebungen zu stärken, die auch den Widerstand gegen die russische Zentralregierung betreiben. Nicht zur Kenntnis genommen wird im offiziellen Russland, dass dieser Umbruch auch etwas zu tun hat mit einem bürgerrechtlichen Aufbegehren einer informationsgesellschaftlich beeinflussten Jugend gegen autoritäre Herrschaftsstrukturen.

Derartige auch in Russland bestehende Strukturen stehen dort noch nicht zur Disposition. Dennoch: Das Goethe-Institut lud mich zu einem Vortrag zum Thema „Datenschutz“ nach Moskau ein. Gemeinsam mit einem Vertreter einer Open-Data-Initiative und einer Verlagschefin als Moderatorin diskutierte ich über Persönlichkeitsschutz in einer sich digitalisierenden Gesellschaft, über Freiheitsrechte, Privatsphäre, gesellschaftliche Transparenz - und Überwachung. In Einzelgesprächen tauschte ich mich zudem mit einer Menschenrechtsaktivistin und mit der Leiterin des Öffentlichkeitsarbeit des Sacharow-Zentrums aus, das historische Aufklärungsarbeit, aber auch aktuelle Bürgerrechtsarbeit leistet.

Mein viertägiger Trip nach Moskau war nicht geeignet, einen umfassenden Überblick über Datenschutz und Transparenz in Russland zu bekommen. Er konnte nur - zweifellos eindrucksvolle - vereinzelte Einblicke geben. Dennoch halte ich diese für so berichtenswert, dass ich diese hier festhalte, nicht zuletzt, weil es zum Thema „Datenschutz in Russland“ - soweit mir erkennbar - bisher keine deutschsprachigen Veröffentlichungen gibt.

II. Tradition Repression

So sehr die heutige Rezeption des Datenschutzes in Deutschland von dessen Geschichte geprägt ist, so sehr trifft dies für Russland - mit seinen völlig anderen politischen und gesellschaftlichen Erfahrungen - zu: Die Geschichte Russlands war über weite Strecken für viele Menschen grausam und ist bis heute nur begrenzt gut. Überwachung, Repression, Willkür und Menschenverachtung bis hin zur Menschenvernichtung hatten schon während der vielhundertjährigen Zarenzeit eine persistente, wenngleich wechselhafte Tradition. Nach den Wirren der Oktoberrevolution 1918 hat sich diese Tradition mit der 25jährigen Schreckensherrschaft Stalins bis zu dessen Tod 1953 noch verbreitert und vertieft. Die danach erfolgenden leichten Liberalisierungen unter Chruschtschow, Breschnew und schließlich Gorbatschow erfolgten ohne revolutionäre Umwälzungen graduell. Dies gilt auch für den erklärten Wechsel vom Kommunismus zum Kapitalismus und das Aufkommen und der Entwicklung einer Konsumgesellschaft unter Jelzin, Putin und heute Medwedjew.

Mit dem Konsum kam auch die Meinungsfreiheit. Doch diese bleibt weitgehend in gesellschaftliche Nieschen gebannt, da die öffentlichen Medien von der russischen Oligarchie, einem teilweise korrupten bis mafiösen Geldadel, beherrscht werden. Es gibt weiterhin mehr oder weniger versteckte politische Unterdrückung, wenig öffentliche und/oder parlamentarische Kontrolle, wenig Transparenz in der Politik, noch weniger in der Verwaltung, und es gibt praktisch keinen Datenschutz.

III. Datenschutz

Dies soll nicht heißen, dass es keine Datenschutzregelungen gäbe. Am 07.11.2001 unterzeichnete Russland das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarats von 28.01.1981. Eine Ratifizierung und ein Inkrafttreten konnte nicht festgestellt werden. Mehrere relativ neue Regelungen orientieren sich mit ihrem normativen Inhalt weitgehend an westeuropäischen Standards. Es finden sich Festlegungen zur Einwilligung und zur vertraglichen Verarbeitungsbefugnis, zum Schutz sensitiver Daten, zur Datensicherheit, zur Übermittlung ins Ausland, zum Auskunftsanspruch und sonstigen Betroffenenrechten. Sogar eine – zweifellos wachsweiche – Zweckbindungsvorschrift besteht. Folgende Regelungen sind bekannt:

- Konvention zum Schutz von Personen im Hinblick auf die automatisierte Verarbeitung persönlicher Daten, ratifiziert von der Russischen Föderation am 19.12.2005,
- Gesetz der Russischen Förderation „über persönliche Daten“ vom 27.07.2006 (Nr. 149 od. Nr. 152-FZ),
- Regeln zur Sicherung in Personendatenbanken verarbeiteter persönlicher Daten, in Kraft gesetzt durch Verordnung der Russischen Regierung vom 17.11.2007 (Nr. 781) mit spezifischen Sicherheitsanforderungen,
- Gesetz der Russischen Förderation „über Werbung“ vom 13.03.2006 (Nr. 38-FZ) mit Regeln zum Versenden von E-Mail- und SMS-Werbung,
- Gesetz über Verwaltungsverstöße vom 30.12.2001 (Nr. 195-FZ).

Als Behörden zuständig sind die regionalen Niederlassungen des „Russischen förderalen Dienstes zur Überwachung

von Massenkommunikation, Telekommunikation und der Bewahrung des kulturellen Erbes“ (künftig Föderaler Telekommunikaktionsdienst – FTD). Wer auf russischem Territorium persönliche Daten verarbeiten will, muss sich beim FTD registrieren. Wer Werbung versenden möchte, müsste sich eigentlich vom FTD eine spezifische Erlaubnis besorgen. Die Verfahren für diesen Zweck sind aber noch nicht eingerichtet. Der FTD hat auch die Befugnis, im Fall eines Datenschutzverstoßes einen Datenverarbeiter zu verklagen und Bußgelder zu verhängen. Über eine entsprechende Praxis ist nichts bekannt.

Das Goethe-Institut führt gemeinsam mit dem Verlag „Nowoje Literaturnoje Obosrenie“ eine Gesprächsreihe „Gegenwart der Zukunft“ durch. Im Rahmen dieser Gesprächsreihe fand am 24.02.2011 im Polytechnischen Museum in Moskau eine Vortrags- und Diskussionsveranstaltung mit dem Thema „Datenschutz der Zukunft. Was bleibt vom Privaten?“ statt. In Vorbereitung dieser Veranstaltung organisierte das Goethe-Institut im Internet eine Veröffentlichungsfolge mit Informationen, Interviews und Berichten zum Thema aus deutscher wie russischer Sicht – in deutscher wie in russischer Sprache.

Bei der spannenden Podiumsdiskussion vor ca. 300 v.a. jungen Besucherinnen und Besuchern meinte der russische Referent und Counterpart, Iwan Begtin, Generaldirektor des „Labors für intellektuelle Datenanalyse“, der wirksamste Datenschutz werde in Russland über die Korruption durch die geldgesteuerte Abweichung von der staatlich geplanten und organisierten Überwachung bewirkt. Für Überwachung vorgesehene Gelder würden eben teilweise in dunklen Kanälen landen und so nicht zur Installierung z.B. von Kontrolltechnik genutzt. Korruption bedinge Informationsmonopole, und diese stünden einem übergreifenden Austausch von Überwachungsergebnissen entgegen.

IV. Überwachung und Kontrolle

Die These ist gewagt: Wissen wir doch nur sehr wenig über die staatliche Überwachung in Russland. Diese geschieht, unzweifelhaft, durch den Geheimdienst FSB (Federalnaia Slushba Bezopasnosti), die Nachfolgeorganisation des ehemals berüchtigten KGB, durch die Polizei und weitere Sicherheitsbehörden, auch wenn von ihr wenig sichtbar ist. Natürlich haben sich die Überwachungstechnologien der ehemals sozialistischen Geheimdienste weiterentwickelt, von deren Stand wir im Jahr 1989 durch die Öffentlichmachung der Akten der DDR-Staatssicherheit (Stasi) einen sehr guten, aber inzwischen nicht mal mehr ansatzweise übertragbaren Einblick erhalten haben. Während der deutschen Stasi aber weitgehend schonungslos der Mantel des Schweigens heruntergerissen werden konnte, weil die herrschenden Eliten durch Menschen aus dem Westen und durch bisherige Oppositionelle fast vollständig ersetzt wurden, gibt es in Russland, mehr als 20 Jahre nach der politischen Wende, immer noch sehr wenig Aufarbeitung. Diese wird in einem mühevollen Kampf von Bürgerrechtlern und Journalisten vorgenommen und findet keine staatliche Unterstützung, so wie dies mit der deutschen Stasi-Unterlagenbehörde, geleitet von Joachim Gauck, dann Marianne Birthler und nun Roland Jahn, möglich war und ist. Diese Tradition hat zur Folge, dass die informellen Mitarbeiter des KGB immer noch im kollektiven wie im individuellen Bewusstsein vieler Menschen präsenter sind, als die heutige elektronische Aufklärung des FSB.

Es darf vermutet werden, dass der FSB die politische Opposition nicht so lückenlos und systematisch überwacht und verfolgt, wie dies z.B. im Iran oder in China der Fall ist und in Russland zu KGB-Zeiten der Fall war. Aber Überwachung findet statt und zwar, so eine russische Bürgerrechtlerin, mit modernster aus China importierter Überwachungstechnologie. Während meines Besuches konnte mir niemand meiner Gesprächspartner einigermaßen gesicherte Informationen über staatliche Überwachung mitteilen. Ich erhielt einen Hinweis auf einen zivilgesellschaftlichen Ausschuss in der Provinz Perm, der sich des Themas staatlicher Überwachung angenommen hat. Aber diese Informationen liegen nur in Russisch vor - also in einer Sprache, die für die globale Zivilgesellschaft schwer erreichbar ist. Englisch spricht immer noch nur eine kleine intellektuelle und die ökonomische Elite. Viele aus der intellektuellen Elite sind aus Russland, vorrangig in den Westen, ausgewandert. Diese haben weiterhin Bindungen nach Russland, wie auch zur demokratischen Kultur ihrer neuen Heimat. Dass dies aber im Hinblick auf den Datenschutz in Russland Auswirkungen zeigen würde, konnte ich nicht feststellen.

Über die allgemeinen Medien ist zur Überwachung in Russland wenig zu erfahren. So berichtet Evgeny Morozow, dass die russische Regierung, ähnlich wie in vielen anderen autoritären Staaten, Blogger dafür bezahlt, regierungsfreundliche Online-Propaganda zu verbreiten. Um die möglicherweise schwer zu überwachenden westlichen sozialen Netzwerke zu neutralisieren, fördert Russland - ähnlich China - eigene nationale Konkurrenzmedien. Eine Onlinegruppe, die sich den Umsturz der russischen Regierung zu Ziel gesetzt hätte, könnte auf der russischen Facebook-Alternative Vkontakte leicht kontrolliert und abgeschaltet werden. Es sind russische Angebote, die in der Onlinewelt der meisten ehemaligen Sowjetrepubliken dominieren. Als sich im Dezember 2010 nach umstrittenen Wahlen in Weißrussland Protestgruppen formierten, verschwand eine Onlinegruppe, die einen Oppositionskandidaten unterstützte und für die Organisation der Proteste wichtig geworden war, über Nacht aus Vkontakte.

In Russland werden Internet-Anbieter gesetzlich verpflichtet, Hardware zu installieren, durch die der FSB verfolgen kann, wer welche Web-Seiten besucht und welche E-Mails geschrieben werden. Immerhin verlangt das Gesetz eine richterliche Genehmigung.

V. Meldungen aus Russland

2009 sollen 45 Mio. von den 142 Mio. Russen das Internet genutzt haben. Für 2010 wird schon eine Zahl von 60 Mio. genannt. Medwedjew präsentiert sich in der Öffentlichkeit als Internetfan, der einen eigenen Blog betreibt und twittert und über diese Kanäle schon auch „Offenheit auf allen Kanälen“ fordert. Er nannte die Informationstechnologie einen „Schlüssel zur Entwicklung der Demokratie“ und das Internet als „wich-

tige Ressource“ zur Modernisierung des Landes.

Doch dabei handelt es sich nicht um eine konsistente Politik, sondern um einzelne Signale, die von entgegengesetzten politischen Signalen begleitet werden. So unterschrieb er im Sommer 2010 ein umstrittenes Gesetz, das dem 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 Journalisten und verdächtige Bürgern 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 Bürger 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 Medwedjews 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“.

Tatsächlich scheint die Macht des Inlandsgeheimdienstes FSB mit seinen ca. 100.000 Mitarbeitern größer zu sein, als dies in der westlichen Öffentlichkeit wahrgenommen wird. Er ist zuständig für die Spionageabwehr im militärischen und zivilen Bereich, die Bekämpfung von Terrorismus und die Aufklärung von Organisierter Kriminalität. In bestimmten Fällen ist der FSB auch befugt, Auslandsaufklärung zu betreiben. Neben anderen Informationsbeschaffungsmaßnahmen werden auch fremde Staatsangehörige observiert und abgeschöpft. Im April 2010 wurde bekannt, dass die uralte Praxis des Einsatzes von schönen Frauen zur Kompromittierung und Erpressung von wirtschaftlich oder politisch wichtigen Ausländern weiterhin praktiziert wird. Die Überwachung des Internets spielt beim FSB eine immer bedeutender werdende Rolle.

Kurz nach meinem Besuch in Moskau kündigte Medwedjew sehr konkret an, in fünf Jahren eine Bürgerkarte einzuführen, die alles ist und enthält: Identitätsnachweis, Krankenversicherung, Patientenakte, Banknachweis. Dass dies eher der Überwachung und Kontrolle dienen soll, als der Inanspruchnahme digitaler Freiheiten, muss angesichts der wolkig bleibenden Überlegungen zu Transparenz und Bürgerrechten im Netz vermutet werden.

VI. Eindrücke und Silberstreifen

Die Hoffnung für digitale Bürgerrechte liegt bei den jungen Menschen, die zu der Diskussionsveranstaltung in Moskau in großer Zahl erschienen. Die Qualität der Debatte stand der einer öffentlichen Diskussion irgendwo in Deutschland in nichts nach. In ihr kamen staatliche Überwachung ebenso vor, wie die durch Private, also z.B. Google oder Facebook. Diese beiden US-Firmen sind auf dem russischen Markt präsent, haben aber z.B. in den Bereichen Suchmaschinen oder Soziale Netzwerke mehr russische Konkurrenz als es in Deutschland deutsche Konkurrenz, gibt. Diese Konkurrenz hat aber keine bürgerrechtlichen oder Datenschutz-Gründe, sondern v.a. sprachliche, kulturelle und historische Ursachen. Eine Datenschutzdiskussion, wie wir sie am 24. Februar führten, wird - so mein Eindruck - ansonsten in Russland noch nicht offen geführt.

Nach Ansicht meines russischen Gesprächspartners bei der Podiumsdiskussion steht das russische Datenschutzrecht nur auf dem Papier und hat weder etwas mit der Realität zu tun, noch passt es zu den sonstigen geltenden Gesetzen. Datenschutz werde oft nicht als Schutz der Bürgerinnen und Bürger vor dem Staat oder vor mächtigen Unternehmen verstanden, sondern als Schutz des Staates vor den Menschen. So berichtete eine Mutter, dass ihr die Aushändigung der Röntgenbilder ihres Kindes mit dem Argument „Datenschutz“ verweigert wurde. Eine unabhängige Datenschutzkontrolle gibt es nicht; der zuständige Föderale Telekommunikationsdienst (FTD, s.o.) hat andere, wohl als wichtiger bewertete Aufgaben. Transparenz der Datenverarbeitung gibt es erst recht nicht. Transparenz ist ein Thema, für das sich eine kleine intellektuelle Minderheit, die sich weder in den offiziellen Medien, noch in der organisierten Politik wiederfindet, und eine kleine Gruppe jugendlicher technikbegeisterter und kritischer Journalisten erwärmen können.

Dieses Bild hinterließ bei mir, mit meinem aufgeklärt preußisch-deutschen Blick und mit dem Sozialisationshintergrund deutscher autoritärer Vergangenheit, einen irgendwie Unbehagen einflößenden Eindruck. Für meine Gesprächspartnerinnen und -partner schien dieses Bild dagegen eher positiv und von Hoffnung geprägt angesichts der repressiven, oft brutalen Vergangenheit, auf der Russland aufbaut. Es gibt da z.B. eine kleine, größer werdende und feine Open-Data-Community. Eine internationale Organisation mit dem Namen frontlinedefenders bietet im Internet für Bürgerrechtsaktivisten Selbstschutzmöglichkeiten im Internet an. Es gibt in Moskau ein kleines Büro der Human Rights Watch. Und es gibt die preisgekrönte Initiative Memorial, die sich vor allem der Aufarbeitung der russischen Geschichte verschrieben hat und deren Aktivitäten sich zwar nicht vorrangig im Netz abspielen, die dort aber wohl präsent sind.

Es sind, so wurde mir berichtet, vor allem russische Emigranten in Westeuropa, die ihre neuen Beziehungen mit denen ihrer Herkunft und Heimat verbinden - auch im Hinblick auf Bürgerrechte. Von der vom Kommunismus wenig geliebten und nun von der Regierung gehätschelten Kirche können sich Bürgerrechtsorganisationen offensicht-

lich nur wenig erhoffen; Entsprechendes gilt für die etablierte Politik und die staatlichen Einrichtungen. Aber neben viel Armut und einer explodierenden Konsumgesellschaft scheint ein kleines Pflänzchen einer bürgerrechtlich engagierten Intelligenzia heranzuwachsen, für die Informationstechnik und Rechtsstaatlichkeit keine Fremdworte sind. Transparenz steht als erstes auf der Agenda – als die wirksamste Therapie gegen eine korruptionsdurchtränkte Oligarchie. Ein Hinweis hierauf gibt der studierte Jurist und Blogger Alexej Nawalny in Moskau, dessen Popularität darauf beruht, dass er Daten publik macht, die seines Erachtens öffentlich sein sollten. Zwar gibt es in Russland inzwischen viele Blogger, die stärker vielleicht als klassische Medien Skandale aufdecken und Missstände anprangern. Doch anders als in den arabischen Staaten gibt es keine Anzeichen dafür, dass sich hieraus eine umfassendere Bewegung für mehr Demokratie und Menschenrechte entwickelt.

Vom Orga-Team der FIfF-Jahrestagung

Dialektik der Informationssicherheit

Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit

Die diesjährige FIfF-Jahrestagung wird von Freitag, den 11. November, bis Sonntag, den 13. November 2011, an der Hochschule München in der Lothstr. 64 stattfinden. Folgendes ist bisher geplant:

- Freitag: Hauptvortrag von Thomas Petri und eine Podiumsdiskussion zum Tagungsthema „Dialektik der Informationssicherheit – Interessenskonflikte bei Anonymität, Integrität und Vertraulichkeit“
- Samstag: am Vormittag und Nachmittag jeweils Workshops mit einem Zeitblock von 2 bis 2,5 Stunden, Vortrag von Monika Hansmeier zu „Konflikte der IT-Sicherheit in Unternehmen“, die FIfF-Studienpreis-Verleihung mit kurzen Laudatios und ein Filmabend zum Thema Fair IT
- Sonntag: Vortrag von Philipp W. Brunst „Anonymität, Integrität und Vertraulichkeit vs. Strafverfolgung“ (er bekam letztes Jahr vom FIfF den ersten Studienpreis verliehen). Anschließend wird die Mitgliederversammlung stattfinden.

Die diesjährige Tagung zählt auch als Hochschulveranstaltung, weswegen die Vorträge und Workshops für die Studierenden der Hochschule eine besondere Bedeutung haben. Wir rechnen mit etwa 70 Teilnehmer/-innen.

Podiumsdiskussion

Angefragt sind: Constanze Kurz, Rainer Gerling (siehe Workshop „Krypto auf Reisen“), und dann wünschen wir uns noch jemand vom LKA oder Verfassungsschutz und jemanden aus der Wirtschaft. Thomas Petri (siehe Hauptvortrag am Freitag) hat bereits zugesagt. Roter Faden sollen die diversen Konflikte zwischen Staat(en), Bürgern und Unternehmen in allen denkbaren Kombinationen dieser Beteiligten sein (Staat-Staat: Spionage; Staat-Bürger: Terrorismusabwehr, Vorratsdatenspeicherung; Staat-Unternehmen: Spionage; ...)

Arbeitsgruppen, Poster-Session, Stände

Auch dazu gibt es erste Anfragen: „Chaos macht Schule“ (CCC), „Krypto auf Reisen“ (zu Integrität und Vertraulichkeit im Konflikt mit Staat und Unternehmen), Infrastruktur-Themen, IPv6 security extensions, INDECT, Internationalisierung, Web 2.0, vielleicht auch eine Arbeitsgruppe mit Overnight-Contest zum Aktualisieren eines Datenschutz-Planspiels, kurz: Ideen hat das Programmkomitee richtig viele. Wer macht mit?

Wir sind auch bei Themen fündig geworden, die nicht unmittelbar im Zusammenhang mit dem Tagungsthema stehen, beispielsweise die internationale Zusammenarbeit (wenigstens im deutschsprachigen Raum), AK Ruin (Rüstung und Informatik); Redaktionsarbeit FIfF-Kommunikation, Fair IT mit einem Workshop zum Film, ... Für nicht in den AGs abgedeckte Themen wird Platz in einer Poster-Session sein, beispielsweise zu Torservers.net oder dem Crypto-Chip der Privacy Foundation. Stände soll es dieses Mal auch von Firmen geben, von einer Unternehmerin, die eine (teil-)Fair-IT-Maus herstellt, von Foebud und vom FIfF.

Über weitere Ideen und Angebote von Mitgliedern der DVD und Lesern der DANA freuen wir im Orga-Team uns natürlich sehr, Kontakt für inhaltliche Beiträge: jt-orga@lists.fiff.de.

Moritz Tremmel

Die panoptische Vorratsdatenspeicherung

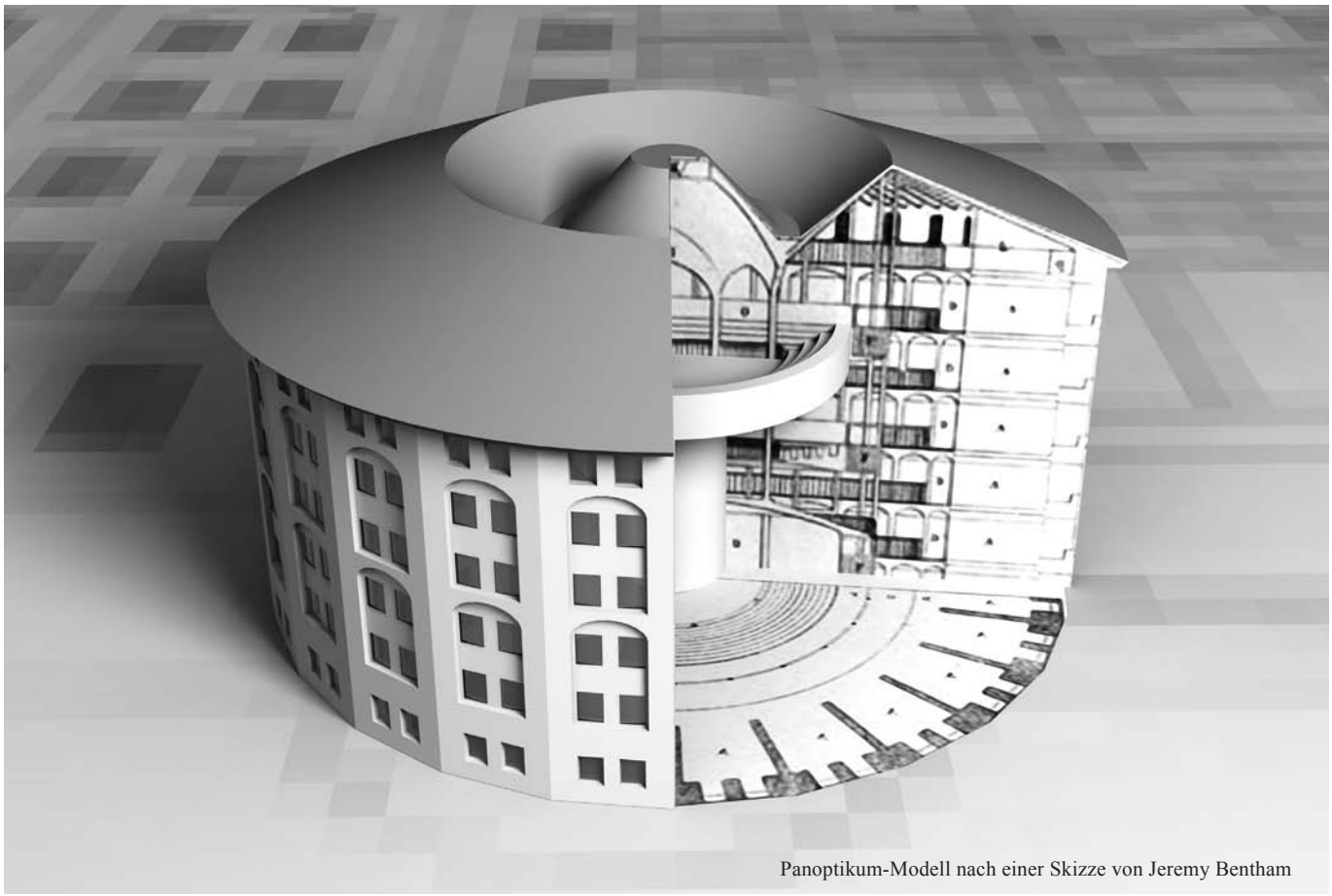
Am 2. März 2010 hat das Bundesverfassungsgericht das Gesetz zur Vorratsdatenspeicherung in Deutschland für nichtig erklärt, dennoch hielt es die Vorratsdatenspeicherung an sich nicht für verfassungswidrig – vielmehr hat es nur die bisherige Umsetzung der EU-Richtlinie kritisiert, es erläutert aber gleichzeitig in seinem Urteil die Vorgaben für eine verfassungsgemäße Umsetzung.[1]

Seitdem tobt eine Diskussion ob, und wenn ja in welcher Form, die Vorratsdatenspeicherung erneut eingeführt werden soll. Die Diskussion wird dabei häufig polemisch geführt. Welche Wirkungen die konkrete Überwachungsmaßnahme auf die Menschen oder eine Gesellschaft hat, oder haben kann, bleibt dabei allzu oft außen vor. Eine wissenschaftliche Aufarbeitung des Themenkomplexes scheint dadurch umso wichtiger.

Aufbauend auf den Erfahrungen der bisherigen Vorratsdatenspeicherung und den Vorgaben des Bundesverfassungsgerichts sollen die (Macht-)Wirkungen der Vorratsdatenspeicherung im folgenden Artikel mit Hilfe des panoptischen Prinzips von Michel Foucault analysiert werden. Dieses basiert auf der Gefängnisarchitektonik des Panoptikum von Jeremy Bentham. Das Gefängnis besteht aus einem ringförmigen Gebäude, in dem Zellen eingelassen sind, welche durch die ganze Tiefe des Gebäudes reichen und zum Mittelpunkt hin einsehbar, aber untereinander abgeschirmt sind. Genau in der Mitte der Anlage befindet sich ein Turm in dem der Wächter postiert wird. Dieser Turm ist so beschaffen (Jalousien, Trennwände), dass er für die Häftlinge nicht einsehbar ist, gleichzeitig aber die Überwachung der Zellen perfekt gewährleistet.[2]

Der Insasse muss von einer stetigen Überwachung ausgehen, obgleich diese nicht gewährleistet sein muss, ja sogar überflüssig sein kann. Die Überwachung muss dabei sichtbar, aber uneinsehbar sein – „der Häftling [darf] niemals wissen [...], ob er gerade überwacht wird, aber er muss [sich] sicher sein, daß er jederzeit überwacht werden kann.“[3] Durch den Überwachungsdruck können den Insassen Verhaltensweisen aufgezwungen werden.

Foucault leitet aus der Architektur und ihrer Wirkungsweise das dahinterstehende panoptische Prinzip ab. Mit Hilfe dieses Prinzips soll im Folgenden die Vorratsdatenspeicherung im Hinblick auf ihre panoptischen Züge ana-



Panoptikum-Modell nach einer Skizze von Jeremy Bentham

lysiert werden. Hierfür wurden die wichtigsten Elemente des panoptischen Prinzips abgeleitet und geordnet. Diese werden nun im Hinblick auf die Vorratsdatenspeicherung diskutiert.

Sichtbarkeitsbereiche

Eine sehr wichtige Rolle spielt beim Panoptikum die Sichtbarkeit. Das Gefängnis ist so angelegt, dass es eine perfekte Einsehbarkeit der Zellen gewährleistet – mit nur einem Blick ist es möglich, viele Insassen zu sehen und ihr Verhalten auf Konformität zu prüfen. Dabei darf der Überwachte keinen Hinweis darauf bekommen, ob er gerade überwacht wird oder nicht.

Uneinsehbarkeit der Überwachung

Die Speicherung der Daten findet bei verschiedenen privaten Unternehmen statt. Ob auf sie zugegriffen wird, wird dem Betroffenen, wenn überhaupt, nur im Nachhinein mitgeteilt. Das Max-Planck-Institut zog Akten-Stichproben vergangener Verkehrsdatenabfragen und wertete diese aus. Laut dieser Studie konnten ein Drittel der Beschuldigten über die Akteneinsicht Wissen über die Nutzung der Verkehrsdaten erlangen. Nur 4% wurden per Aktenbeschluss informiert. Eine Vernichtung der Daten konnte den Akten nur in 3% der Verfahren entnommen werden.[4] Eine rechtliche Aufklärungspflicht besteht nicht, obgleich das BVerfG in einer zukünftigen Umsetzung eine Benachrichtigungspflicht fordert. Diese setzt dennoch erst nach der Überwachung ein.

Welche Informationen aus den Vorratsdaten abgeleitet werden, mit welchen Daten sie verknüpft werden und welche Verdachtsmomente und Schlüsse aus ihnen gezogen werden, bleibt weiter unklar. Selbst Verfahrensregeln über die Auswertung der Daten, die nach dem Urteil des BVerfG zu erlassen sind, lassen kaum Schlüsse zu, unter welchen Umständen die Überwachung stattfindet.

Es können mittels sogenannter ‚Stiller SMS' sogar Verkehrsdaten ohne das Wissen des Überwachten erzeugt werden. Dem Überwachten können beispielsweise vom BKA ‚Stille SMS' im Fünfminutentakt gesendet werden. Diese sind im Prinzip ganz normale SMS, die aufgrund einer Information in der SMS aber vom empfangenden Gerät nicht angezeigt werden. Dadurch werden Verkehrs- und Standortdaten erzeugt, die wiederum über eine Verkehrsdatenabfrage abgerufen werden können.[5]

Der Überwachte kann also grundsätzlich nur im Nachhinein nachvollziehen, ob er überwacht wurde. Eine Einsicht in die Funktionsweise des Systems kann er nicht erlangen.

Sichtbarkeit der Überwachten

Die Inhaltsanalyse von Kommunikation ist sehr aufwendig, teuer und fehleranfällig. Die Analyse der Verkehrsdaten hingegen kann vollautomatisiert stattfinden und ist häufig deutlich aufschlussreicher als die Inhaltsanalyse.[6] Im Folgenden sollen die Möglichkeiten der Informationsgenerierung aus den Vorratsdaten und etwaige Umgehungsmöglichkeiten skizziert werden.

Extraktion von Wissen aus Verkehrsdaten

Beziehungen zu anderen Personen und Verhalten

In den Verkehrsdaten nur einer Person spiegeln sich nahezu alle sozialen Kontakte wieder. Es können aber auch Beziehungsintensitäten abgeleitet werden: „Mit wem kommuniziert die Person wann, wie oft, über welche Kommunikationsart, wie lange und in welchem zeitlichen Kontext zu bestimmten Ereignissen?"[7]

Aus langer und häufiger Kommunikation lässt sich eine engere soziale Bindung ableiten. Es kann zwischen geschäftlichen Kontakten, die innerhalb üblicher Geschäftszeiten stattfinden, und privaten differenziert werden. Beziehungspartner können anhand der Intensität der Kommunikation, welche auch während üblicher Geschäftszeiten und Auslandsaufenthalten anhält, identifiziert werden. Ebenso kann eine Affäre aus den Daten herausgelesen werden. Auch spielen die Orte der eingebuchten Handys eine zentrale Rolle bei der Analyse der Beziehungen. Durch die Verknüpfung mit weiteren Daten entsteht ein noch klareres Bild. Wurde zum Beispiel einige Zeit zuvor ein Hotel gebucht, an dessen Ort sich die beiden Telefone treffen? Die Daten können aber auch mit externen Quellen abgeglichen werden, z.B. mit dem Bankkonto, Buchungsinformationen von Verkehrsmitteln (Mietwagen, Bahn etc.) oder Hotels.[8]

Rückschlüsse auf persönliche Lebenssituation

Rückschlüsse auf die momentanen Lebensumstände von Personen sind vielfältig:

„So ließe sich beispielsweise aus einem E-Mail-Kontakt mit einem auf Familienrecht spezialisierten Anwalt, gefolgt von telefonischen Anfragen bei Wohnungsmaklern eine Scheidungsabsicht prognostizieren. Kontakte zu Konflikt- und Schwangerschaftsberatungen, spezialisierten Ärzten, Prostituierten, Telefonsex-Hotlines, spezialisierten Versandhändlern, Kreditvermittlern, Jobcentern, Umzugsservices, Interessenverbänden etc. ergäben aus einer minimalen Datenmenge jeweils umfangreiche Rückschlüsse auf das Privatleben eines Betroffenen."[9]

Netzwerkanalyse

Die Analyse der Vorratsdaten beginnt mit einem Datenabruf der Kommunikationsdaten einer bestimmten Person. Daraufhin werden die Daten der (wichtigsten) Kontaktpersonen abgerufen und auf Verbindungen untereinander untersucht. Menschen, die innerhalb eines Sozialgefüges eine zentrale Rolle spielen, lassen sich identifizieren. Es lässt sich des Weiteren feststellen, ob es sich um eine lose Gruppe, um eine familiäre oder eine hierarchische Struktur handelt. Es können ähnliche Kommunikationsketten erkannt werden, die von bestimmten Kontakten ausgelöst werden. Es können dabei Annahmen getroffen werden, welches Ereignis diese hervorrief. So kann beispielsweise eine Person als sehr bedeutend für eine Umweltschutzgruppe erkannt werden, ohne dass dies dieser bewusst sein muss. „Durch Beeinträchtigung der Handlungsfähigkeit einer einzelnen Person kann dann mit minimalem Aufwand die Wirksamkeit einer ganzen Gruppe oder Bewegung behindert werden."[10]

Beschränkungen beim Abruf der Daten

Die oben genannten Schlüsse können logischerweise erst nach Abruf der Daten bei den verschiedenen Providern erfolgen. Dem Abruf der Daten sind aber verschiedene Schranken seitens des Gesetzgebers und des Bundesverfassungsgerichts gesetzt worden. Bei den meisten Abfragen gilt ein Richtervorbehalt, welcher die Einhaltung der entsprechenden Normen gewährleisten soll. Diese Kontrolle findet aber in der Realität nur bedingt statt. Eine Aktenauswertung des Max-Planck-Institutes ergab, dass nur ganz selten Anordnungen zum Datenabruf abgelehnt bzw. Änderungen (in 1,7% der ausgewerteten Fälle) am Antrag durchgeführt werden. Eine darüberhinaus durchgeführte Expertenbefragung erhärtete den Eindruck, dass der Richtervorbehalt seine Kontrollfunktion nur bedingt erfüllt.[11] Dennoch stellt er eine gewisse Hürde dar. Mit der Einführung der Vorratsdatenspeicherung durften die Daten nahezu in jedem Fall abgerufen werden. Die Gefahrenabwehr, alle Straftaten sogar bis hin zu Ordnungswidrigkeiten rechtfertigten das Mittel. Das Bundesverfassungsgericht erließ daraufhin im März 2008 eine einstweilige Anordnung, welche die Maßnahme nur noch bei schweren Straftaten gestattet.[12] In ihrem darauffolgenden Urteil zur Vorratsdatenspeicherung im März 2010 verlangen die Richter eine Liste mit Straftaten, für die die Daten verwendet werden dürfen und generelle Ausnahmen für Kommunikationsdaten, die bei Beratung im sozialen oder kirchlichen Bereich entstehen.

Diese Strenge gilt allerdings nicht für die Zuordnung von Bestandsdaten zu IP-Adressen, da diese das Gericht für weniger schützenswert hält. Des Weiteren gilt sie nicht für die herkömmliche Abfrage der zu Abrechnungszwecken gespeicherten Verkehrsdaten, auf die ein Zugriff seit 2002 möglich ist.[13]

Umgehung der Vorratsdatenspeicherung

Anonymer Internetzugriff

Über sogenannte Anonymisierungsdienste kann die IP-Adresse verschleiert werden. Diese Dienste schalten einen oder mehrere Server zwischen Client und angefragten Server. Der angefragte Server bekommt nur die IP-Adresse des zwischengeschalteten Rechners. Die Verbindung zwischen den Rechnern findet meist verschlüsselt statt. Die zwischengeschalteten Computer dürfen kein Logging (das Mitprotokollieren der Verkehrsdaten) betreiben.[14] Eine Rückverfolgung mittels der IP-Adresse endet so immer bei einem der zwischengeschalteten Server. Die Vorratsdatenspeicherung sah auch eine Protokollierung bei diesen Anonymisierungsdiensten vor und führte diese so ad absurdum. Allerdings waren von dieser Regelung nur Rechner in Deutschland betroffen.

Bei mobilem Internet mittels UMTS werden die IP-Adressen momentan für mehrere Anschlüsse verwendet, eine Zuordnung ist nicht möglich. Das surfen ist faktisch anonym.[15]

Anonyme Kommunikation

Die Vorratsdatenspeicherung kann beim Telefonieren über die Benutzung von öffentlichen Telefonzellen, durch die Benutzung von anonymen Prepaid- oder ausländischen Mobiltelefonen umgangen werden. Letztere müssen logischerweise aus Ländern stammen, die keine Vorratsdatenspeicherung praktizieren – diese können auch in Deutschland problemlos genutzt werden. Wechselt man die Geräte und Karten häufig, kann ein relativ hoher Anonymisierungsgrad erreicht werden.[16]

Die Kommunikation per E-Mail kann über sogenannte Remailer komplett anonymisiert werden. Diese funktionieren ähnlich wie die oben beschriebenen Anonymisierungsdienste. Weitere Möglichkeiten sind die Nutzung ausländischer E-Mailanbieter oder Wegwerf-E-Mail-Adressen, welche nur kurze Zeit genutzt werden können. Alternativ dazu kann auch auf Webforen oder Nachrichtendienste innerhalb von Webseiten zurückgegriffen werden.[17] Es können natürlich auch offene W-LAN-Spots oder Internetcafés benutzt werden, hierbei kann aber zumindest eine Lokalisierung bis zum Ausgangspunkt und somit eine Zeit-Ort-Bestimmung stattfinden.

Problem: Redundanz der Daten

Die Daten werden redundant gespeichert, sie fallen immer bei beiden Kommunikationsteilnehmern an. Daher müssen auch beide Anonymisierungsstrategien verfolgen, da ansonsten zumindest teilweise, wenn nicht alle, Daten rekonstruiert werden können. Für die organisierte Kriminalität oder Terroristen sollte es ein Leichtes sein, diese Kommunikationsmittel in ihren Netzwerken zu nutzen. Für den Privatmensch gestaltet sich die Nutzung aber schwierig, da zum Einen das Wissen über die Möglichkeiten fehlt, zum Anderen auch die Kommunikationsteilnehmer mitziehen müssten. Eine staatliche Interventionsmöglichkeit bietet das Verbot derartiger Dienste oder der Zwang zur Mitprotokollierung der Vorratsdaten. Da das Internet aber nur bedingt Grenzen kennt, ist eine Umgehung mit dem entsprechenden Know-how praktisch immer möglich.[18]

Sichtbarkeit und Überprüfung der Konformität

Die Beispiele zeigen deutlich, dass eine Sichtbarkeit bis in die privatesten Räume möglich ist, gleichzeitig die Vorratsdatenspeicherung aber auch mit relativ einfachen Mitteln umgangen werden kann. So ist weniger die organisierte Kriminalität oder der Terrorismus von der Überwachung betroffen, da diese sich normalerweise im Klandestinen bewegen. Das Entdeckungsrisiko wird dabei einkalkuliert und möglichst weit abgesenkt.[19] Vielmehr kann Kontrolle nur über die ausgeübt werden, die sich entweder nicht zu schützen wissen und / oder in (Beziehungs-) Netzwerke eingebettet sind, die eine geschützte Kommunikation nicht beherrschen. Deren Verhalten ist minutiös nachvollziehbar und darüber auch auf Konformität prüfbar. Die einzig verbliebenen (Zugriffs-)Schranken sind die des Bundesverfassungsgerichts bzw. des Gesetzes.

Dabei wird die Datenmenge in Zukunft tendenziell zunehmen. Mobile Dienste und Geräte erobern immer weitere Bereiche. Als Beispiele seien hier Bezahldienste per Handy, Mautsysteme oder Gesundheitsmonitoring zu nennen – dabei muss den Betroffenen nicht

unbedingt klar sein, dass sie gerade Verkehrsdaten erzeugen.[20]

Die bewusste Überwachung

Auf die Trennung der Sichtbarkeit des Überwachten und der Unsichtbarkeit des Überwachenden baut die Sichtbarkeit des Überwachungssystems auf. Der Überwachte muss sich stets überwacht fühlen, sich bewusst sein, dass er jeden Moment überwacht werden kann. Daraus ergibt sich eine kontinuierliche Wirkung der Überwachung, obwohl ihre Durchführung nur sporadisch ist oder gar unterbleiben kann.

Die Sichtbarkeit der Überwachung findet vor allem über die Aufklärung der Medien statt, da die Vorratsdatenspeicherung selbst komplett verdeckt abläuft. Die Berichterstattung wurde dabei vor allem durch den Streit der Befürworter und Gegner hervorgerufen. Die Berichterstattung in Deutschland ist hauptsächlich ereignisbasiert. Die Medien verlieren sehr schnell das Interesse an einem Thema, wenn sich keine Nachrichten mit Neuigkeitswert ergeben. Es ist davon auszugehen, dass die Berichterstattung abebbt, sobald der Streit beigelegt ist. Nur bei bedeutungsvollen Ereignissen in Bezug auf die Vorratsdatenspeicherung (möglicherweise auftretenden Datenskandalen, Ermittlungserfolgen, der Einführung oder Verwendung von weiteren andersartigen Überwachungsmaßnahmen etc.) ist wieder mit einer Berichterstattung zu rechnen.[21]

Der Streit zwischen den Befürwortern und Gegnern der Vorratsdatenspeicherung hat dieser einen immensen Bekanntheitsgrad unter den Menschen beschert. Dies kann zum einen mit dem medialen Hype, der beispielsweise auch um die knapp 35.000 Verfassungsbeschwerden und deren Verhandlung entstanden ist,[22] zum Anderen aber auch mit Umfragen belegt werden. Nach einer repräsentativen Forsa-Umfrage im Auftrag des Arbeitskreises Vorratsdatenspeicherung vom Mai 2008 wissen 73% der Bundesbürger von der Speicherung der Verbindungsdaten.[23]

Dieser hohe Bekanntheitsgrad, verknüpft mit der vermuteten, deutlich geringeren Berichterstattung in der Zukunft, ergibt zumindest eine teilweise Erfüllung der stetigen Sichtbarkeit. Sicher ist diese nicht mit der Stetigkeit des panoptischen Turmes zu vergleichen, dennoch ist davon auszugehen, dass die Vorratsdatenspeicherung in den Köpfen ist und durch eine gelegentliche Auffrischung durch oben genannte Ereignisse auch bleibt.

Verknüpft mit den weiteren Überwachungsmaßnahmen ist es denkbar, dass ein Eindruck des stetigen Überwachtseins aus der Vielzahl der Instrumente entsteht und auch das Internet nicht (mehr) als rechtsfreier Raum, sondern vielmehr als besonders überwachter Raum, wahrgenommen wird.

Kontinuität der Überwachungswirkung

Die Provider sind gesetzlich verpflichtet, die Daten über den Zeitraum von sechs Monaten zu speichern und in Reaktion auf eine legitime Anfrage an die entsprechende Stelle auszuhändigen. Eine Auswertung der Daten ist also über das komplette vergangene halbe Jahr möglich, kann aber ebenso in die Zukunft gerichtet sein. Sie findet also nicht nur in diesem Moment statt, sondern ist auch vergangenheitsbezogen und in die Zukunft gerichtet.

Der Überwachte muss folglich davon ausgehen permanent überwacht zu werden bzw. überwacht werden zu können.

Verhaltensanpassung und -änderung

Ob durch die Vorratsdatenspeicherung eine Verhaltensanpassung stattfindet, ist umstritten. Laut einer repräsentativen Forsa-Umfrage haben 11% der Bundesbürger in den ersten 5 Monaten der Vorratsdatenspeicherung in Deutschland aufgrund dieser in bestimmten Fällen auf die Kommunikation mittels E-Mail, Telefon oder Handy verzichtet. Zu sensiblen Einrichtungen (Drogenberatung, Psychotherapeut etc.) würden 52% der Befragten seit der Speicherung der Verbindungsdaten keinen Kontakt mehr per Telefon, E-Mail oder Handy suchen. 6% haben den Eindruck, dass seit dem weniger Menschen Kontakt mit ihnen über diese Medien aufnehmen.[24]

Leider gibt es keine weiteren Studien, die sich explizit auf eine mögliche Verhaltensänderung durch die Vorratsdatenspeicherung beziehen. Hier besteht dringend Forschungsbedarf.

Betroffen ist auch die Presse und darüber letztlich auch das demokratische Prinzip der vierten Gewalt. Ein Informantenschutz kann mit einer Vorratsdatenspeicherung kaum noch gewährleistet werden. Offen bleibt inwieweit Systeme wie Wikileaks diese Lücke füllen können.

Ob ein sogenannter ‚chilling effect' (Nichtgebrauch von Freiheitsrechten) durch die Vorratsdatenspeicherung herbeigeführt wird, ist mangels Studien bisher empirisch nicht nachweisbar, dennoch ist es sehr wahrscheinlich.[25] Das Bundesverfassungsgericht stellt in seinem Urteil zur Vorratsdatenspeicherung fest, dass diese ein „besonders schwere[r] Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt"[26], ist. Da die Verwendung der Daten unbemerkt stattfindet, ist sie „geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann."[27]

Findet eine Verhaltensänderung statt, muss diese, bei einer derartig abstrakten Überwachung, internalisiert werden, d.h. der Überwachte beginnt sein Verhalten und letzen Endes sich selbst zu überwachen – als Reaktion auf die Überwachung und aus Angst vor etwaigen Negativfolgen.

Da der Betroffene sein Verhalten nur auf der Annahme des Überwachtwerdens ändert, ohne genau zu wissen, ob dies wirklich stattfindet, folgt daraus in logischer Konsequenz eine Unabhängigkeit der Verhaltensänderung von einer wirklichen Überwachung.

Fazit

Foucault's Panoptismus eignet sich sehr gut als Analysewerkzeug für die komplex-abstrakte Überwachungstechnik. Mit der Trennung des Paares ‚sehen und gesehen werden' lässt sich die Vorratsdatenspeicherung sehr gut erklären. Eine panoptisch-präventive Wirkung lässt sich zwar empirisch mangels Studien nicht nachweisen, dennoch zeigt die Analyse mittels des panoptischen Prinzips, dass eine Machtwirkung vorhanden ist, und diese verhaltensän-

dernd wirkt. Eine Forsa-Umfrage gibt auch erste empirische Hinweise.

Die Erklärungen und Ergebnisse überzeugen. Die Vorratsdatenspeicherung lässt sich besser verstehen und enthält Funktionselemente, die tatsächlich wie die panoptische Maschine, die Foucault beschreibt, funktionieren. Durch die ähnliche Struktur ergibt sich während der Analyse auch eine ähnliche Wirkungsweise. Die Vorratsdatenspeicherung kann daher auch nie als reine Strafverfolgungstechnik gesehen werden, da immer auch die Machtwirkungen einer Überwachungstechnik mitschwingen.

Insgesamt kann die Vorratsdatenspeicherung als panoptisches System betrachtet werden, welches in seiner Implementierung einige Schwächen aufweist. Weiterer Forschungsbedarf besteht insbesondere auch über die Wechselwirkungen der unterschiedlichen Überwachungstechniken. Werden Schwächen und Probleme der einen Überwachungstechnik mit einer anderen Technik beseitigt? Wird die Überwachung mittels der verschiedenen Techniken von den Überwachten schon als umfassend wahrgenommen? Lassen sich panoptisch wirkende Überwachungstechniken überhaupt mit der Idee von Demokratie verbinden?

1 BVerfG (2010):Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß. http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html

2 Foucault, Michel (1994): Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt/Main: Suhrkamp

3 ebd.

4 Albrecht, Hans-Jörg / Grafe, Adina / Kilchling, Michael (2008): Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Forschungsbericht im Auftrag des Bundesministeriums der Justiz. http://www.bmj.bund.de/files/-/3045/MPI-GA-2008-02-13%20Endfassung.pdf

5 Schaar, Peter (2009): Stellungnahme zum Fragenkatalog. http://www.bfdi.bund.de/cae/servlet/contentblob/952738/publicationFile/62213/StellungnahmeVorratsdaten100609.pdf

6 Engling, Dirk (2008): Vorratsdatenspeicherung. In: Gaycken, Sandro / Kurz, Constanze (Hrsg.) (2008): 1984.exe.Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: Transcript

7 Kurz, Constanze / Rieger, Frank (2009): Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung. http://ccc.de/de/vds/VDSfinal18.pdf

8 ebd.

9 ebd.

10 ebd.

11 Albrecht, Hans-Jörg / Grafe, Adina / Kilchling, Michael (2008)

12 Schröder, Burkhard (2008): Bitte bevorraten Sie sich. http://www.heise.de/tp/r4/artikel/27/27544/1.html

13 ebd. BVerfG (2010)

14 Kubieziel, Jens (2007): Anonym im Netz. Techniken der digitalen Bewegungsfreiheit. München: Open Source Press

15 Vetter, Udo (2010): Anonym über UMTS. http://www.lawblog.de/index.php/archives/2010/04/19/anonym-uber-umts/

16 Engling, Dirk (2008)

17 ebd. Kubieziel, Jens (2007)

18 Engling, Dirk (2008)

19 Albrecht, Hans-Jörg / Grafe, Adina / Kilchling, Michael (2008) Kurz, Constanze / Rieger, Frank (2009)

20 Kurz, Constanze / Rieger, Frank (2009)

21 Hickethier, Knut (2003): Einführung in die Medienwissenschaft. Stuttgart: J. B. Metzler

22 Heise Online (2010): Vorratsdatenspeicherung: Zivilgesellschaft fordert endgültige Abschaffung. http://www.heise.de/newsticker/meldung/Vorratsdatenspeicherung-Zivilgesellschaft-fordert-endgueltigeAbschaffung-981313.html

23 Forsa (2008): Meinungen der Bundesbürger zur Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

24 Forsa (2008)

25 Maras, Marie-Helen (2009): From targeted to mass surveillance: is the EU Data Retention Directive a necessary measure or an unjustified threat to privacy? In: Goold, Benjamin J. / Neyland, Daniel (Hrsg.) (2009): New Directions in Surveillance and Privacy. Cullompton: Wallan

26 BVerfG (2010)

27 ebd.

Der Artikel basiert auf einer Magister-Zwischenprüfungsarbeit. Die komplette Arbeit kann unter http://moritztremmel.de/veroffentlichungen/die-vorratsdatenspeicherungund-der-panoptismus/ abgerufen werden.

Sönke Hilbrans

Von Baustelle zu Baustelle…

Schlaglichter der deutschen Big Brother Awards 2011

Nein, es waren (fast) keine Aprilscherze, die bei der Verleihung der 11. Big-Brother-Awards am 1. April 2011 in Bielefeld zum Besten gegeben wurden. Wieder traf die Verleihung der populären Negativ-Preise acht um Datenschutzfehlleistungen hoch verdiente PreisträgerInnen, unter ihnen prominente Szenegrößen: den deutschen Zoll (für ein Zertifizierungsverfahren „Zugelassene Wirtschaftsbeteiligte“ und den Abgleich von personenbezogenen Daten mit Anti-Terror-Listen), die Zensuskommission (für den Zensus 2011), die Daimler AG (für Bluttests bei MitarbeiterInnen), Facebook (für Facebook), Apple (für die Nutzung von I-Phone-Nutzerdaten für Werbung und durch Dritte) und – als Wiederholungstäter – den niedersächsischen Innenminister Schünemann (dieses Mal für den Einsatz von Überwachungsdrohnen bei Versammlungen). Ein weiterer Preisträger schaffte streng genommen den Spurt über die Ziellinie nicht: Der stellvertretend für die oftmals viel zu guten Informationsbeziehungen zwischen Schulen und werbender Wirtschaft prämierte Verlag für Wissen und Innovation wird keine Freude mehr an der Preisträgerschaft gehabt haben. Er hatte bereits kurz vor der Preisverleihung seine Geschäftstätigkeit eingestellt.

Prof. Wedde startet den Prämierungsreigen und präsentierte zunächst ein Zertifizierungssystem „Sicherer Export-Diensteanbieter“ (SED), welches der deutsche Zoll in Zusammenarbeit mit den russischen Sicherheitsbehörden zur Umsetzung eines russischen Verfahrens zur Importkontrolle implementiert habe. Das durch Weddes Vortrag und eine aufwändig präsentierte Website www.sed-easy.bmf.bund.de beeindruckte Publikum dürfte kalte Füße bekommen haben, als es erfuhr, dass unter anderem Zugriffe des russischen Inlandsgeheimdienstes FSB auf Unternehmensdaten erfolgen sollten. Erleichterung machte sich breit, als Prof. Wedde den Aprilscherz „SED“ offen legte. Bitter blieb, wofür der Deutsche Zoll letztlich doch einen Award erhielt: das real existierende Zertifizierungsverfahren für „Zugelassene Wirtschaftsbeteiligte“ erleichtert die Überwachung von europäischen und amerikanischen Anti-Terror-Listen bis hinein in die Prüfung, ob auch ArbeitnehmerInnen auf diesen Listen verzeichnet sind.

Demgegenüber wenig überraschend gibt es auch der Welt der allgegenwärtigen Datenverarbeitung gleich mehrere Preisträger hervorzuheben. So belobigte padeluun die Modemarke „Peuterey“ dafür, dass sie allen Ernstes noch heute Kleidungsstücke auf den Markt bringt, in denen sich ein verdeckter RFID-Chip befindet. Verdeckt von einem Aufnäher im Innenteil der Kleidung. Dort, wo die Kunden vielleicht sinnvolle Informationen oder auch nur modischen Schnickschnack erwarten, warnt der Satz „Don´t remove this label“ eindrucksvoll davor, Manipulationen an Kleidungsstücken vorzunehmen. Offensichtlich sollen die Kunden nie auf die Idee kommen, die eindeutige, unerkannt und berührungslos auslesbare Seriennummer des Kleidungsstückes unlesbar zu machen. Der Datenkraken-Dauerbrenner RFID war – einmal mehr – abzustrafen (vgl. auch die Beiträge von Hansen, DANA 3/10, S. 100 ff.; Weichert, DANA 4/10, S. 140 ff. und Hansen, DANA 1/11, S. 9 ff.).

Anwendungen des ubiquitous computing greifen auch außerhalb der schlichten Warenwelt weiter Platz, wie die Preisverleihungen an Facebook Deutschland und an Apple in der Wettbewerbsklasse „Kommunikation“ belegen. Die Laudatio von Andreas Bogk/ Frank Rosengart (beide CCC) scholt Apple für die „Geiselnahme“ der iPhone-Kunden durch die Geschäfts- und Datenverarbeitungsbedingungen des Konzerns, welche eine unkontrollierbare Vermarktung von Kundendaten an Dritte erlaube. Wer der Laudatio von Rena Tangens lauschte, sah vor sich aufwändig recherchierte neue Welten der Verarbeitungen und Verknüpfungen von Daten des elektronischen Alltags entstehen. Wenig beruhigend, dass die Gründer und Betreiber von Facebook in den Medien sowohl der Nähe zur rechtskonservativen Zusammenschlüssen, als auch zum US-amerikanischen Geheimdienst gescholten werden. Die Funktionalitäten von Facebook ergaben in der Laudatio zusammen genommen eine elektronische gated community ohne Ausstiegsmöglichkeit. Das Publikum zollte der Preisverleihung an die beiden Global Player im Kommunikationsbusiness nachhaltigen Applaus. Fast erleichtert konnten man schließlich aus dem Munde des routiniert wort- und witzmächtigen Rolf Gössner der Laudatio der Experimente der niedersächsischen Landespolizei mit fliegenden Überwachungskameras (Drohnen) lauschen. Die wenigstens sind noch mit bloßem Auge zu erkennen…

Die Jury des BBA 2011 hat sich gegenüber den Vorjahren verändert: Neben dem Ausscheiden von Prof. Frederic Roggan ist der Einstieg von Prof. Peter Wedde in die Jury zu verzeichnen. Für die DVD übernimmt Sönke Hilbrans die Jurymitgliedschaft der im Oktober 2010 zur DVD-Vorsitzenden gewählten Karin Schuler. Auch für die Datenschutznachrichten ändert sich mit diesem Jahr etwas: wir werden kein Heft mit allen Laudationes zu den Big-Brother-Awards mehr machen. Die vollständigen Laudationes finden Sie auf der Website www.bigbrotherawards.de. Noch besser, Sie schauen sich die nächste Preisverleihung selbst an – im Bielefeld oder im live stream.

Prof. Peter Wedde hielt die Laudationes für die Kategorien „Arbeitswelt 1“ (Deutscher Zoll) und „Arbeiswelt 2“ (Daimler AG).

Werner Hülsmann übergibt den BigBrotherAward an Prof. Dr. Gerd G. Wagner in der Kategorie „Behörden und Verwaltung“ für die als „Zensus 2011“ bezeichnete Vollerfassung der Bevölkerung Deutschlands.

Prof. Dr. Martin Haase mit einem Beitrag in der Sonderkategorie „Neusprech“ zum Begriff „Mindestspeicherdauer“.

Padeluun war der Laudator für den Negativpreis in der Kategorie „Technik“ (Modemarke Peuterey).

Sönke Hilbrans informierte über die Verbraucherschutzfeindliche Datensammlung des Verlages für Wissen und Innovation.

Rena Tangens beklagte in der Kategorie „Kommunikation 1“ den Umgang mit der Privatsphäre bei Facebook.

Andreas Bogk sprach in der Kategorie „Kommunikation 2“ über Apple und problematische Datenschutzbedingungen.

Dr. Rolf Gössner verurteilte Innenminister Uwe Schünemann wegen Überwachungsdrohnen in der Kategorie „Politik“.

Klaus-Jürgen Roth

Internet-Pöbelseiten von Jugendlichen für Jugendliche

Der Fall „iShareGossip“

Beleidigungen, Verleumdungen, üble Nachrede: Pöbelseiten im Internet verunsichern zunehmend SchülerInnen, Eltern und Lehrkräfte. Nach einer durch Veröffentlichungen auf der Webseite „iShareGossip“ ausgelösten Prügelei unter SchülerInnen ist die Diskussion in der Öffentlichkeit angekommen. Der Name der Seite auf deutsch übersetzt: „Ich teile Klatsch und Tratsch.“ Ende März 2011 hatten 20 Jugendliche in Wedding einen 17jährigen Berliner krankenhausreif geprügelt, weil er seine Freundin wegen einer regelrechten Hetzjagd auf iShareGossip verteidigen wollte. Vor dem Überfall wollte der Schüler den Konflikt zwischen seiner 18jährigen Freundin und deren Mitschülerinnen wegen der Mobbing-Beiträge schlichten, was scheiterte, nachdem sich weitere Jugendliche einmischten. Die Polizei nahm vier Jungen und zwei Mädchen im Alter zwischen 14 und 18 Jahren vorläufig fest.

„E. S. aus der Klasse 9c ist die größte Schlampe der Schule. Sie schläft mit jedem Jungen der Oberstufe und ist dumm wie Brot.“ Dieses und in der Tonalität noch viel schlimmere Pamphlete finden sich öffentlich und für jeden lesbar im Internet. Die Frage nach dem „beschissesten Lehrer“ ist noch harmlos. SchülerInnen bezeichnen sich unter voller Namensnennung als „Schlampen“ und „Fotzen“. Nach Bundesländern sortiert, sind auf der betreffenden Seite alle Schulen aufgeführt. Mit einem Mausklick landen Kinder und Jugendliche auf der eigenen Schulseite - und sehen die dort eingetragenen Pöbeleien.

Der Auftritt ist Facebook nachempfunden. In der oberen Eingabezeile der Pinwand wird man aufgefordert, seine „Neuigkeiten, Gerüchte und Lästereien“ einzutragen, es gibt wie bei Facebook einen „Gefällt mir“- Daumen, mit dem man andere Beiträge bewerten kann, und neuerdings die Möglichkeit, Fotos einzustellen. Das alles ist angeblich anonym, man benötigt nicht einmal eine Anmeldung. Und auf diese Anonymität verweist der Seitenbetreiber nachdrücklich: Man speichere keine IP-Adressen, beantworte keine Anfragen, auch nicht von Polizisten, Lehrern, Direktoren. „Ihr seid 100 Prozent anonym. Wer etwas anderes behauptet, ist ein Lügner und will Euch Angst machen.“

Allein bei der Staatsanwaltschaft Frankfurt am Main gingen innerhalb kurzer Zeit Anfang 2011 mehr als 50 Strafanzeigen ein. Am Schadow-Gymnasium in Zehlendorf und am Spandauer Hans-Carossa-Gymnasium kam es zu einer Amokdrohung auf der Plattform. Der Unterricht wurde abgesagt. Die Amokläufe fanden glücklicherweise nicht statt. Günter Wittig, von der ermittelnden Generalstaatsanwaltschaft Frankfurt am Main meinte: „Die Betreiber haben sich von Anfang an bewusst konspirativ verhalten und ihre wahre Identität verschleiert.“ Die hessische Zentralstelle für Internetkriminalität ermittelt nach den Verantwortlichen. Herbst 2010 hatte ein anonymer Nutzer in einem Forum erstmalig auf das „Projekt“ hingewiesen und schrieb einen Wettbewerb aus: Wer am meisten „authentischen Inhalt“ in seiner Rubrik zusammenbekommt, solle 100 Euro bekommen und „WICHTIG“: „Je kontroverser ein Post ist, desto eher kommt ihr auf die Startseite und desto mehr Leute werden eurer Kategorie folgen.“

Das Impressum von iShareGossip verweist auf ein lettisches Unternehmen, das aber auf Anfragen nicht reagierte. Das Stadtmagazin „Journal Frankfurt“ hat ein Interview mit einem vermeintlichen Verantwortlichen veröffentlicht, in dem dieser erklärte, die Webseite stamme von einer Gruppe von Freunden. Der Server steht nach eigenen Angaben bei dem schwedischen Internet-Provider PRQ. Der Name der Mobbing-Plattform zielt offensichtlich auf eine Assoziation zu der auf ProSieben laufenden und unter Jugendlichen äußerst beliebten US-Serie „Gossip Girl“. Als Betreiber der Seite wird der Name Alexander Liepa genannt. Über diesen ist bisher nur eine öffentliche Äußerung bekannt. Der Erfolg des Forums, so wird Liepa zitiert, käme in erster Linie dadurch zustande, dass es die Rachegefühle und die Feigheit der Nutzer bediene. Auf die Frage, was er tun würde, wenn jemand sich wegen iShareGossip umbringen würde, soll er kaum etwas zu sagen gehabt haben: „Eine Katastrophe wäre das, absolut katastrophal. Aber so spontan kann ich dazu nichts sagen. Da müsste ich ausführlicher drüber nachdenken.“

Pöbelseiten

Pöbelseiten sind ein großes Thema in Schulen und auf Elternabenden. Nach einer repräsentativen Befragung des Marktforschungsunternehmens Forsa sind 98% der deutschen Kinder und Jugendlichen im Alter von 10 bis 18 Jahren online im Netz, selbst bei den bis zu Zwölfjährigen sind es 96%. Drei Viertel von ihnen nutzen aktiv soziale Netzwerke. Die positiven Erfahrungen überwiegen. Aber ein Drittel der Jugendlichen beklagt sich über Belästigungen. Das müssen nicht besagte Pöbelseiten mit anonymem Zugriff wie iShareGossip sein, sondern das betrifft auch die sozialen Netzwerke wie Schüler- und Studi-VZ oder Facebook, wo man sich in der Regel mit seinem realen Namen anmeldet. Uwe Maerz, Vorsitzender der Landelternschaft in Nordrhein-Westfalen, berichtet, dass an vielen Schulen inzwischen Mobbing-Attacken über das Internet stattfinden, initiiert „vor allem von Mädchen“. Das Phänomen ist relativ neu, aber es ist international. Die Schülerin Megan Meier aus dem US-Bundesstaat Missouri hat

sich wenige Wochen vor ihrem 14. Geburtstag im Jahr 2006 erhängt wegen Cybermobbing, Anfeindungen und übler Nachrede im Netz.

Viele Eltern mit wenig Medienerfahrung meinen immer noch, das Internet sei generell gefährlich. Wie kann man Kinder vor Belästigungen, „Schmutz und Schund", Pornographie und sonstigen Übergriffen schützen? Der Ruf nach staatlichen Kontrollen steht im Raum. Die Debatte über das Sperren von Kinderpornografie-Seiten im Internet hat aber gezeigt, dass technische Verfahren den Zugang zu indizierten Seiten nur begrenzt unterbinden können und äußerst unerwünschte Nebeneffekte haben. Neue Eingriffsbefugnisse in Fällen von Beleidigung oder übler Nachrede im Netz wären wegen der damit verbundenen Eingriffe in die grundgesetzlich garantierten Rechte auf Meinungs- oder Informationsfreiheit äußerst heikel.

Der Vorsitzende des Berliner Landeselternausschusses Günter Peirisch forderte die Abschaltung der „unsäglichen Mobbing-Seite". Unabhängig von dem Übergriff in Berlin untersuchte schon die Bundesprüfstelle für jugendgefährdende Medien die Indexierung von iShareGossip. Folge dieser innerhalb kürzester Zeit erfolgreichen Indexierung ist, dass die Internetseite nicht mehr über die gängigen Suchmaschinen auffindbar ist.

Nach Ansicht von PsychologInnen führen Seiten wie iShareGossip zu einer Verschärfung des Mobbings an Schulen, da sich die UrheberInnen in der Anonymität sicher wähnen und die Beschimpfungen u.U. dauerhaft erhalten bleiben. Mobbing im Netz ist weltweit öffentlich, erreicht auch Eltern und Lehrkräfte, und wird daher als besonders gravierend erlebt. Ist der Beitrag zugleich anonym, so löst dies bei dem Opfer oft ein Gefühl der Hilf- und Hoffnungslosigkeit aus: Wer war das, vielleicht meine Nebensitzerin, meine beste Freundin? Die Beiträge versuchen sich zu übertrumpfen – das schlimmste Foto, das brutalste Video, das geilste Nacktfoto – und genau nach solchen Kriterien selektieren auch die AdressatInnen das Angebot. Etwa 30% der Jugendlichen berichten von schwerwiegenden Fällen des Cyber-Mobbing, dass z.B. Gerüchte über sie verbreitet wurden. Etwa 5% gaben an, dass sie massiv bedroht wurden.

In der Wöhlerschule in Frankfurt am Main, das sich als „Medienkompetenz-Schule" bezeichnet, ging Schulleiter Norbert Rechner durch die Klassen und sprach das Thema des „Internet-Mobbing offensiv an. Ein Schüler schmuggelte sich daraufhin als Moderator bei iShare-Gossip ein und löschte die Lästerbeiträge über seine MitschülerInnen. Andere SchülerInnen fluteten die Webseite mit massenhaften Nonsense-Einträgen, so dass die Betreiber mit dem Löschen nicht mehr hinterherkamen. Eine weitere Folge der intensiven Beschäftigung mit iShareGossip in dieser Schule war, dass die Webseite für die SchülerInnen uninteressant wurde und sich danach fast keine Mobbing-Beiträge zu dieser Schule mehr fanden.

Auch in der jüdischen Oberschule in Berlin-Mitte reagierte diese mit einer Vielzahl unterschiedlicher Maßnahmen: Lehrerkonferenzen, Vorträge eines Datenschützers, Befassung durch die Schulpsychologin, Strafanzeigen durch die Eltern. Einige SchülerInnen entwickelten einen Sticker und ein Plakat mit dem Motto „I never share gossip". Die Schulleiterin Barbara Witting hatte sämtliche Kommentare über ihre SchülerInnen ausgedruckt und stieß dabei auch auf folgenden Kommentar: „Der Mensch, der diese Seite geöffnet hat, ist einfach nur genial und wisst ihr, wieso? Weil ihr Vollidioten mit dieser Seite zeigt, dass ihr auf eure `Freunde´ scheißt. Genau das ist das, worüber ihr nachdenken solltet."

Technische Kindersicherungen

Die Idee, dass die Eltern das Heft selbst in die Hand nehmen und mit Schutz-Software den Zugriff auf bedenkliche Inhalte blockieren, führt wenig weiter. Bei diesen sog. „Kindersicherungen" wird oft mehr versprochen, als gehalten werden kann: Sie schützten vor den Gefahren im Internet und verhinderten, dass Kinder auf Seiten gelangen, die nicht für sie bestimmt seien. Wer in diese Richtung denkt, findet schon auf der Ebene des Betriebssystems etliche Optionen in Verbindung mit den Benutzerkonten. Bei Windows 7 und dem aktuellen Mac OS X kann man mit Bordmitteln Kindersicherungen und Zeitkonten sowie Zugriffsbeschränkungen für einzelne Programme einrichten. Ferner bieten handelsübliche WLAN-Router wie etwa die Fritzboxen von AVM eine rudimentäre Kindersicherung, die zwar nicht die Inhalte kontrolliert, aber die Zugriffszeiten für einzelne PCs. Andere Techniken implementieren Inhaltskontrollen im Router. Mit spezieller Kinderschutz-Software soll der Zugriff auf die dunklen Seiten des Netzes gesperrt werden. Diese Pakete greifen ins Betriebssystem und den Browser ein. Keines der Angebote funktioniert perfekt, wie unlängst eine Vergleichsstudie der EU gezeigt hat. Sie blockieren nur acht von zehn der für Kinder nicht geeigneten Seiten, vor allem Erotikangebote. Weniger „bildlastige" Seiten werden kaum erfasst und Inhalte mit besonders kindgerechten Angeboten fälschlich blockiert. Kaum ein Filter ist in der Lage, Inhalte in sozialen Netzwerken, Foren oder Blogs zu durchforsten. Beim Instant-Messaging sowie bei Chat-Anwendungen ist die Fehlerrate ebenfalls hoch. Hinzu kommt, dass je tiefer ins Betriebssystem eingegriffen wird, desto leichter es zu Störungen und Fehlfunktionen bei unbedenklichen Seiten oder Standardprogrammen kommen kann.

Kindersicherungen sind kein Allheilmittel. Sie dürfen in jedem Fall keine Beruhigungspille für das elterliche Gewissen sein, weil sie ein möglicherweise trügerisches und lückenhaftes Versprechen von Sicherheit geben. Selbst wenn man zu Hause alle Rechner zu einer festen Burg aufgerüstet hat, kann niemand Kinder und Jugendliche daran hindern, bei FreundInnen und Bekannten das zu tun, was daheim nicht funktioniert. Mit den internetfähigen Smartphones der Kids, die als mobile Surf- und Chatstationen immer wichtiger werden, eröffnen sich neue offene Scheunentore. Sperren signalisieren vor allem, dass man seinem Kind in Sachen Medienkompetenz nicht über den Weg traut.

A und O: Kommunikation mit den Kindern

Vernünftige Eltern werden nicht umhinkommen, mit ihren Kindern über sicheres Surfen und ein angemessenes Verhalten im Netz zu reden, auch über

den Umgang mit persönlichen Daten und Bildern. Eltern sollten wissen, wofür sich ihre Kinder im Netz interessieren, und sie sollten die ersten kompetenten Ansprechpartner in allen Zweifelsfällen und bei Belästigungen sein. Meist braucht man den erhobenen Zeigefinger nicht, denn Kinder und Jugendliche sind in Sachen Netzkompetenz oft klüger, als ihre besorgten Mütter und Väter denken.

In den Gesprächen - vor allem an der Schule - sollten die Pöbelseiten und Belästigungen in sozialen Netzwerken offen thematisiert werden. Aufklärung an dieser Stelle betrifft auch die tatsächlich dann doch nicht bestehende perfekte Anonymität im Netz, die ein wesentliches Lebenselixier solcher Seiten ist. Oft ist es möglich, durch die Art des Mobbings auf die UrheberInnen Rückschlüsse zu ziehen.

Es gibt seriöse und weniger seriöse Webangebote. Bei seriösen Telemedienanbietern ist es regelmäßig einfach, Cyber-Mobbingattacken zur Löschung zu bringen, indem einfach auf die inakzeptable Seite hingewiesen wird. Daran haben die Betreiber insofern auch ein Interesse, da, wenn Sie im Fall von eindeutigen Rechtsverstößen nicht tätig werden, Gefahr laufen, sich selbst haftbar zu machen.

Rechtsverfolgung

Das Internet ist kein rechtsfreier Raum, sondern ein Medium. Pöbeleien und andere Übergriffe können strafbar sein, und diese Straftaten werden, sofern eine Seite in Deutschland aufrufbar ist oder Deutsche betroffen sind, nach deutschem Recht geahndet. In jedem Fall sollten die Angriffe im Netz per Ausdruck von Screenshots dokumentiert werden. Eltern der Opfer oder diese selbst können auf eigene Faust herauszubekommen suchen, wer hinter einer Mobbing-Aktion steckt. Sie können sich unter Decknamen in dem betreffenden Netzwerk anmelden und versuchen, der TäterIn auf die Spur zu kommen oder ihr eine Falle zu stellen.

Gibt es durch Veröffentlichungen im Internet Anhaltspunkte auf Straftaten wie Verleumdung oder üble Nachrede, so sollten Eltern, wenn es Hinweise auf die möglichen TäterInnen gibt, im Zweifelfall zur Polizei gehen und Anzeige erstatten. Die Polizei ist verpflichtet, solchen Anhaltspunkten nachzugehen, und sie wird es umso besser können, je konkreter die Verdachtsmomente gegen einzelne Personen sind. Hat beispielsweise jemand in der Clique, also vor anderen Klassenkameraden, mit seiner Schreiberei in einem Forum geprahlt und deuten weitere Indizien auf diese eine SchülerIn hin, kann die Polizei aktiv werden. In extremen Fällen kann diese sogar eine Hausdurchsuchung vornehmen, Computer im Haushalt beschlagnahmen und durch Sachverständige auswerten lassen, wo sich dann fast immer Spuren finden lassen.

Die Polizei kann zudem bei den Internet-Providern vorstellig werden, und das tut sie verstärkt auch. Mit einem Gerichtsbeschluss können Provider und soziale Netzwerke zur Herausgabe aller Daten einer NutzerIn verpflichtet werden, die sich auf den Servern befinden. Hierzu gehören unter Umständen nicht nur die sogenannten Bestandsdaten (Benutzerkonto, Login-Daten), sondern auch Inhalte, die sich in den Mailboxen und auf Profilseiten befinden. Alle großen Anbieter arbeiten mit den deutschen Behörden zusammen, auch wenn sie (offiziell) gar keinen Sitz in Deutschland oder der EU haben. Wer also denkt, seine Daten bei ausländischen Diensten seien vor dem Zugriff deutscher Behörden geschützt, irrt. Gerade die Global Player des Internet ignorieren einen deutschen Gerichtsbeschluss nicht.

Mit Cybermobbing-Veröffentlichungen gehen regelmäßig auch Datenschutzverstöße einher. Daher kann anstelle und ergänzend zu einer Strafanzeige auch die örtlich zuständige Datenschutzaufsichtsbehörde des Landes eingeschaltet werden. Auch diese kann ermittelnd tätig werden. Anders als die Polizei unterliegt sie nicht dem Legalitätsprinzip und kann evtl. auch zwischen Tätern und Opfern vermittelnd tätig werden, evtl. unter Einschaltung der Schule, des Vereins oder einer Jugendeinrichtung.

IShareGossip und andere Pöbelseiten mögen ihren juristischen Sitz im Ausland haben. Dies ist Teil der Verunsicherungsstrategie der Betreiber. Wenn eine Seite deutschsprachig ist und sich gezielt an deutsche SchülerInnen richtet, spielt es keine entscheidende rechtliche Rolle, wenn die Server tatsächlich im Ausland stehen. Dessen ungeachtet können auch bei ausländischen Seiten Beschwerden gegenüber den nationalen zuständigen Aufsichtsbehörden zur Beseitigung der Störung finden. So wandten sich Datenschützer in Deutschland wegen des US-amerikanischen Angebots Rottenneighbor.com an die in den USA zuständige Verbraucherschutzaufsichtsbehörde Federal Trade Commission (FTC). Dies scheint dazu geführt zu haben, dass diese Seite als deutschsprachiges Angebot und mit deutscher Landkarte im Netz nicht mehr erreicht werden kann.

Befinden sich der Betreiber oder die Infrastruktur in Deutschland oder wendet sich ein Angebot an deutsches Publikum, so ist deutsches Recht oder in jedem Fall ein sonstiges europäisches Recht anwendbar mit Zugriffsmöglichkeiten durch Polizei, Staatsanwaltschaft und Gerichte. Das Versteckspiel mit ausländischen Adressen wird oft sehr dilettantisch betrieben. Kann dies aufgedeckt werden, so haben die Verantwortlichen Probleme - wegen der Foren- und Störerhaftung nach dem Telemediengesetz und wegen ihrer datenschutzrechtlichen Verantwortlichkeit. Auch die Eltern von betroffenen Jugendlichen können diese zivilrechtlich zur Rechenschaft ziehen. Umgekehrt können aber auch die Eltern der jugendlichen Schmierfinken ein Problem bekommen. Bei übler Nachrede oder Verleumdung lassen sich nicht nur strafrechtliche, sondern auch zivilrechtliche Ansprüche durchsetzen, etwa auf Unterlassung oder gar Schadenersatz und Schmerzensgeld. Drei Zeilen auf einer Pöbelseite können zu vierstelligen Kosten führen.

Dessen ungeachtet: Jugendliche wissen zunehmend, dass sie selbst das nächste Opfer werden können, wenn sie in der vermeintlichen Anonymität des Netzes gegen andere pöbeln. Außerdem: So belastend solche Angriffe aus dem Dunklen auch sein mögen, sollte man Souveränität und Gelassenheit zeigen. Das fällt einer Elterngeneration vielleicht besonders schwer, die in einer Kindheit und Jugend ohne Internet aufgewachsen ist. Nun gibt es Bedrohungen und Rechtsverletzungen in einem neuen Medium. Aber Konflikte und Auseinandersetzungen in der Schule hat es schon immer gegeben, und das wird

auch so bleiben. Mit oder ohne Internet. Schulen waren noch nie eine heile Welt. Nicht für SchülerInnen, nicht für Eltern und nicht für Lehrkräfte.

Ausgewertete Quellen: Spehr www.faz.net 07.03.2011; Conradi SZ 24.03.2011, 11; SZ 25.03.2011, 21; SZ 31.03.2011, 9; Bartsch/Becker/Brandt/Rosenbach Der Spiegel 13/2011, 44 f.; siehe auch Interview mit Katzer in www.spiegel.de 23.03.2011; Brautlecht www.welt.de 23.03.2011.

Udo Jürgens: „Du bist durchschaut“

Der 76jährige Udo Jürgens ist seit Jahrzehnten eine beständige Größe im deutschen Schlagergeschäft. Er versucht mit seinen Themen auf der Höhe der Zeit zu bleiben und macht immer wieder mit gesellschaftskritischen Texten Kasse („Lieb Vaterland magst ruhig sein“). Nun hat er den Datenschutz entdeckt und in seinem Anfang 2011 präsentierten neuen Album ein Lied aufgenommen, das von der Süddeutschen Zeitung (SZ) absolut verkürzend als „Anti-Internet-Lied“ beschrieben wird.

Nun ist, so Jürgens freimütiges eigenes Bekenntnis, der Grandseigneur des deutschen Schlagers im Internet nicht unterwegs, ja er gab gar an, keinen Computer zu haben, wohl aber zwei Smartphones. Er habe nichts gegen das Internet: „Ich erkenne das Internet und seine Möglichkeiten. Google und Twitter sind politisch gesehen ein Segen für die Welt. Kein Diktator kann machen, was er will. Über das Netz steht er ständig unter Beobachtung. ... Sich im Internet entblößen, mag bisweilen lustig sein – dass diese Informationen nie mehr verschwinden, kann zu einem grausamen Bumerang werden.“ Schon seit 10 Jahren läge das Thema in seiner Schublade. Und da habe er sich mit seinem Liedermacher Wolfgang Hofer hingesetzt und nach etwas Zeitgemäßem gesucht. Hofer sei dann eingefallen „Die Welt ist eine Google.“ Die SZ sah sich dann aber veranlasst klarzustellen, dass dieser Satz nicht von Hofer stammte, sondern vom Schriftsteller Peter Glaser. Sie war am 13.04.2005 Überschrift eines Eintrags seines „Glaserei“-Blogs. Doch Peter Glaser zeigte sich gegenüber Jürgens versöhnlich: „Wir müssen freundlich zu Udo sein, weil meine Mutter ein großer Udo-Fan ist.“ Schon vor ihm sei jemand auf dieses Wortspiel gekommen. Und für alle Fälle stellte er noch ein paar Zeilen für alle Textschmieden der Welt zum freien Zitat zur Verfügung: Unverpixelte Gesichter – Fressefreiheit. Unfall auf der Datenautobahn – zwei Schwervernetzte. Wörter zu Fluchscharen. Sag zum Abschied leise Service“ (Riedl SZ 23.03.2011, 24; SZ 31.03.2011, 11).

> Sehr geehrter Herr Valenta,
>
> vielen Dank für Ihre Anfrage vom 5. Juli d.J.
>
> Nach Rücksprache sowohl mit dem Udo Jürgens Management als auch mit dem Textdichter müssen wir Ihnen mitteilen, dass wir Ihnen KEINE Genehmigung erteilen können. Den Text darf weder in einer komprimierten Fassung noch als vollständige Textversion abgedruckt werden. Aus diesem Grund müssen wir Sie auffordern, von dem geplanten Vorhaben Abstand zu nehmen.
>
> Wir gehen des Weiteren davon aus, dass sich somit auch eine Veröffentlichung des genannten Artikels erledigt hat.
>
> Mit freundlichen Grüßen
> Hans Mai
> - Copyright Manager -
>
> Melodie der Welt - GmbH & Co. KG

Wir wollten eigentlich zeigen, dass auch Udo Jürgens das Thema „Datenschutz“ entdeckt hat, aber die Veröffentlichung dieses Artikels sollte mit der Verweigerung einer Genehmigung zum Abdruck des Textes verhindert werden. Dabei ist der Text im Internet frei zugänglich und kann über den Browser ausgedruckt werden.
Den Link finden Sie hier: http://www.udojuergens.de/lied/du-bist-durchschaut

Bildkomposition mit Textfragmenten.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Chinese wegen Spionage angeklagt

Die Bundesanwaltschaft in Karlsruhe hat gegen einen 62jährigen Chinesen Anklage wegen Spionage erhoben. Ihm wird vorgeworfen, von Mitte 2005 bis November 2009 die uigurische Gemeinschaft in Deutschland ausgespäht zu haben – insbesondere in München. Seine Erkenntnisse soll er an einen chinesischen Nachrichtendienst weitergegeben haben (HmbAbendbl. 19./20.03.2011, 4).

Bund

Offizieller Widerstand gegen libysche Spitzeltätigkeit

Am 13.04.2011 wurde der libysche Botschafter ins Auswärtige Amt einbestellt. Ihm wurde mitgeteilt, dass fünf libysche Diplomaten ausgewiesen werden und in sieben Tagen Deutschland verlassen müssen, weil diese Landsleute in Deutschland kontrollierten und unter Druck setzten. Die Ausweisung sei, so das Auswärtige Amt, ein „letztes Mittel" und werde selten eingesetzt. Ausweisungen von Diplomaten in diesem Umfang sind aus der jüngeren Vergangenheit nicht bekannt. Den Ausgewiesenen wurde vorgehalten, dass sie Druck auf libysche Studenten ausübten, sich nicht für die Opposition in der Heimat einzusetzen: Im Verfassungsschutzbericht für das Jahr 2009 heißt es dazu: „In Deutschland entfalten der Auslandssicherheitsdienst und die Revolutionskomitees illegale nachrichtendienstliche Aktivitäten. Diese gehen vorrangig von den Residenten der Dienste am Libyschen Volksbüro (Botschaft) in Berlin aus." Der libysche Auslandssicherheitsdienst pflege in Deutschland zahlreiche Verbindungen zu libyschen Asylsuchenden mit islamistischem Hintergrund und führe Informanten und Quellen in diesen Bereichen. Aus Furcht vor Repressionen gegen in Libyen lebende Familienmitglieder stoße der Dienst „meist auf geringen Widerstand".

Kurz vor Ausbruch der Unruhen in Libyen fand vor dem Berliner Kammergericht ein Prozess gegen einen 46jährigen Libyer statt, dem von der Bundesanwaltschaft vorgeworfen wurde, in Berlin und Halle oppositionelle Landsleute ausgespäht zu haben. Der Angeklagte legte ein Geständnis ab, seinem Führungsoffizier Informationen über einen Landsmann beschafft und dafür 3.000 Dollar kassiert zu haben. Als angeblicher Regimekritiker wollte sich der Elektronikingenieur demnach weiter in oppositionelle Kreise einschleichen (SZ 02.02.2011, 8; 14.04.2011, 8).

Bund

Transparentere Nebeneinkünfte von MdBs

Mitglieder des deutschen Bundestags (MdBs) sollen nach einer Einigung der Rechtsstellungskommission des Bundestags ihre Einkünfte künftig transparenter machen. Abgeordnete mit einem jährlichen Zusatzeinkommen von mehr als 10.000 Euro müssen die Höhe ihrer Nebeneinkünfte genauer als bisher angeben. Statt wie bisher 3 soll es künftig 7 Stufen geben. Bislang werden alle Einkünfte über 7.000 Euro pauschal ausgewiesen. Künftig sollen die Nebeneinkünfte gestaffelt von 10.000 Euro bis über 150.000 Euro im Jahr veröffentlicht werden. Der Bundestag muss dieser Absprache noch zustimmen (SZ 15.04.2011, 5).

Bund

HIS - Neue Auskunftei für Versicherer

Die deutschen Versicherungsunternehmen starteten am 01.04.2011 ein neues „Hinweis- und Informationssystem" (HIS), das das alte, von den Datenschutzbehörden seit einigen Jahren als „Schwarze Liste" stark kritisierte HIS bzw. „Uniwagnis" ablöst. Ziel des Auskunftssystems ist es gemäß dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV), Betrugsbekämpfung und Risikoprüfung effizienter machen. In der Auskunftei werden Meldungen zu Versicherten gemacht, bei denen es zu atypischen Schadenhäufigkeiten oder Auffälligkeiten im Leistungsfall gekommen ist. Aber auch gefährliche Berufe oder Vorerkrankungen können im HIS aufgelistet werden. Gesundheitsdaten sollen nicht in das System eingetragen werden. Das neue HIS betreibt die informa Insurance Risk and Fraud Prevention GmbH (Rheinstr. 99, 76532 Baden-Baden, Tel. 07221/5040-3700, Fax 07221/5040-3701, E-Mail info@informa.de). Das Unternehmen wurde für den Betrieb der neuen Auskunftei gegründet. Es ist ein rechtlich selbstständiges Tochterunternehmen von arvato infoscore, einem Unternehmen des Medien- und Kommunikationsdienstleisters Bertelsmann AG. Alleiniger Geschäftszweck ist der Betrieb des HIS.

Gemäß dem Vorsitzenden der Hauptgeschäftsführung des GDV, Jörg von Fürstenwerth, sollen die HIS-Einträge nicht zu Ablehnungen von Verträgen führen: „Eine Meldung im HIS führt nicht zur Ablehnung einer Leistung oder eines Vertrages. Das System hilft, die Risikoprüfung schneller und effizienter zu gestalten sowie Versicherungsbetrug und -missbrauch aufzudecken." Das System erfülle, so der GDV, die aktuel-

len Anforderungen des Datenschutzes. Es werde keine Gesamtprofile von Personen geben; das HIS arbeitet getrennt nach Versicherungssparten. Die Meldung der Versicherten in das System erfolge nach einheitlichen Kriterien. In der Privathaftpflicht-, Hausrat- und Wohngebäudeversicherung werden KundInnen gemeldet, wenn sie ihrem Versicherer in 24 Monaten drei Schäden melden. In der Kfz- und Rechtsschutzversicherung liegt die Schwelle bei vier Schäden in 12 Monaten. In der Autoversicherung wird jeder Fahrzeugdiebstahl und jeder Totalschaden gemeldet. Außerdem gibt es eine Eintragung, wenn der Geschädigte auf Basis eines Sachverständigengutachtens sein Geld fordert. Maßgeblich ist die Höhe der Entschädigung. Peter Phillipp, beim GDV für Sach-Kriminalität zuständig, meinte: „Damit wollen wir die Betrugsabwehr verstärken." Ab welcher Schadenshöhe eine Meldung erfolgt und nach welchen sonstigen Kriterien eine Aufnahme ins HIS erfolgt, will der GDV geheim halten. Thomas Lämmrich, Leiter der Kriminalitätsbekämpfung beim GDV erläutert: „Wenn wir diese Kriterien veröffentlichten, würden wir den Tätern eine Betrugsanleitung liefern." Die Kriterien sind mit Punkten bewertet. Ab 60 Punkten darf auch einE KundIn, die erstmalig einen Schaden meldet, ins HIS eingemeldet werden. 20 Punkte gibt es z.B., wenn innerhalb von drei Monaten nach Vertragsschluss bereits ein Schaden gemeldet wird. Weist z.B. ein Laptop mehrere Schäden auf, die nicht mit der Schilderung des Schadensverlaufs übereinstimmen, so ist die 60-Punkte-Schwelle erreicht.

Eintragungen ins HIS erfolgen zudem beim Abschluss einer Lebens- und Berufsunfähigkeitsversicherung. Es wird die versicherte Summe gemeldet, damit sich KundInnen nicht weit über ihre wirtschaftlichen Verhältnisse absichern. Das gilt in der Lebensversicherung ab 100.000 Euro und in der Berufsunfähigkeitsversicherung ab 9.000 Euro versicherte Jahresrente. Gemeldet werden weiterhin KundInnen, die auf Grund von Vorerkrankungen oder wegen eines gefährlichen Hobbys als erhöhtes Risiko gelten. Damit wollen die Versicherungsunternehmen verhindern, dass man sich in betrügerischer Absicht bei anderen Anbietern als gesund meldet. Im Schadenfall kann das Versicherungsunternehmen über Arztauskünfte die Falschangaben meist später noch aufdecken. Ist der KundIn ein Fehler unterlaufen, darf der Versicherer innerhalb von 5 Jahren nach Vertragsabschluss die Leistung verweigern. Kann Betrug nachgewiesen werden, verlängert sich die Ausstiegszeit der Assekuranz auf 10 Jahre.

Etwa 60% der gespeicherten Daten betreffen Autos. Die Einspeisung der Informationen erfolgt anhand eines Leitfadens, der gemäß den Angaben des GDV von den Datenschutzbehörden freigegeben wurde. Die Betroffenen würden über den Eintrag benachrichtigt und könnten sich über eine unentgeltliche Selbstauskunft informieren. Die seit 1993 betriebene Datensammlung wurde jahrelang von KritikerInnen wegen der damit verbundenen Geheimniskrämerei kritisiert. Im Jahr 2007 wurde dann dessen Funktionsweise gemeinsam vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein und dem GDV veröffentlicht (https://www.datenschutzzentrum.de/wirtschaft/20070703-his.htm). Das HIS umfasst laut GDV derzeit rund 9 Mio. Einträge (www.banktip.de 25.03.2011; SZ 25.03.2011, 29; Schmidt-Kasparek SZ 01.04.2011, 18).

Bund

Feldpostleistelle öffnete Soldatenbriefe

Ein Sprecher der Staatsanwaltschaft bestätigte einen Rundfunkbericht, dass sich im Fall der Öffnung von Feldpostbriefen von SoldatInnen in Afghanistan der Verdacht auf Straftaten erhärtet hätte (vgl. DANA 1/2011, 16 f.). 30 bis 40 Briefsendungen seien anscheinend doch in der Feldpostleitstelle Darmstadt geöffnet worden. Dies könnte möglicherweise auch unbeabsichtigt geschehen sein. Gleichzeitig wurde auch der Weg ausgehender Postsendungen geprüft. Im Januar wurde die Öffnung von Briefen und Paketen aus Pakistan öffentlich bekannt (SZ 19./20.02.2011, 6).

Bund

„Datenschutz in Redaktionen" des Deutschen Presserats in 2. Auflage

Der vom Deutschen Presserat 2003 erstmalig herausgegebene Leitfaden „Datenschutz in Redaktionen" ist nun in einer überarbeiteten 2. Auflage erhältlich und kann im Internet herunter geladen oder in der Geschäftsstelle des Presserats bestellt werden. Er bietet auf 61 Seiten eine Hilfestellung für den Umgang mit persönlichen Daten im Redaktionsalltag. Neben grundsätzlichen Erläuterungen zu Datenschutz und Datensicherheit wurden die einschlägigen Regelungen des Pressekodex, des Bundesdatenschutzgesetzes und des Rundfunkstaatsvertrags zusammengestellt und kommentiert. Antworten auf häufig gestellte Fragen, ein Glossar und ausführliche Textauszüge komplettieren die Broschüre. Katrin Saft, Vorsitzende des Beschwerdeausschusses zum Redaktionsdatenschutz, erläuterte, dass der Leitfaden sich v.a. an JournalistInnen und VerlegerInnen richtet und das Ziel verfolgt, „die Freiheit der Presse und gleichzeitig die Belange des Datenschutzes" zu sichern. „Datenschutz in Redaktionen" ist unter http://www.presserat.info/inhalt/dokumentation/publikationen.html im Internet erhältlich oder zum Selbstkostenpreis von 3,50 € (inklusive Porto und Versand) in der Geschäftsstelle des Presserats zu bestellen. Bestellungen bitte per E-Mail an: info@presserat.de (PI Presserat 06.04.2011).

Bund

Telekom entschädigt Spitzelopfer

Aus Kreisen des Telekom-Konzerns sickerte heraus, dass der Journalist Reinhard Kowalewsky vom Konzern ein Schmerzensgeld in Höhe von „erheblich" mehr als 30.000 Euro erhält. Konzernmitarbeitende waren in sein Privatleben eingedrungen, um festzustellen, mit welchem Aufsichtsrat der

damalige Redakteur des Magazins Capital telefoniert hatte. Er hatte über Jahre hinweg bestens informiert über geschäftliche Vorgänge im Vorstand berichtet. Im Zug der Affäre hatte der Bonner Konzern 2005 und 2006 Tausende Telefondatensätze erhoben und auswerten lassen, um ein mögliches Leck aufzuspüren. Die als „Telekomgate“ in die Analen eingegangene Schnüffel-Attacke, die ca. 60 besonders beobachtete Opfer hatte, war durch die Berichterstattung von Kowalewsky ausgelöst worden. Rund ein Jahr lang waren sein Dienstttelefon, sein Handy, sein Privatanschluss und - für kurze Zeit - ein weiteres seiner Telefone von der Sicherheitsabteilung des Konzerns überwacht worden. Selbst die Verbindungsdaten des Handys seiner Frau, die Lehrerin ist, sowie einiger ihrer Bekannten waren von der illegalen Aktion betroffen. Neben Kowalewsky waren weitere vier Journalisten ins Visier der Schnüffler geraten. Mit ihnen wird angeblich auch über die Zahlung von Schadenersatz verhandelt, wobei die angepeilten Beträge unter dem von Kowalewsky liegen sollen. Telekom-Chef René Obermann hatte sich bereits 2008 für den „ungeheuerlichen und zutiefst beschämenden Vorgang“ in „aller Form“ entschuldigt. Inzwischen soll der Konzern mehr als eine Million Euro in einer Fonds für die Spitzelopfer eingezahlt haben, unter denen sich auch viele Gewerkschafter und Betriebsräte befinden. Mehrere Institutionen, die sich um Erhaltung der Pressefreiheit oder des Datenschutzes kümmern, haben zudem von der Telekom 1,7 Mio. Euro als Spende erhalten. Viele Details des Schnüffel-Skandals konnten bis heute nicht aufgeklärt werden (Leyendecker SZ 25.03.2011, 17).

Baden-Württemberg

Datenschutz aus einer Hand beim LfD

Nur wenige Tage nach der Landtagswahl in Baden-Württemberg, die dort erstmals eine grün-rote Mehrheit hervorbrachte, wurden die Aufgaben der Datenschutzaufsicht im nicht-öffentlichen Bereich vom Innenministerium des Landes auf den Landesbeauftragten für Datenschutz (LfD) übertragen. Noch der alte Landtag hatte zwecks Umsetzung des Urteils des Europäischen Gerichtshofes zur Unabhängigkeit der Datenschutzaufsicht vom 09.03.2010 (DANA 2/2010, 85) eine Neuordnung der Datenschutzkontrolle beschlossen. Dies wurde vom LfD Baden-Württemberg Jörg Klingbeil wie folgt erläutert: „Meine Dienststelle wird dem Landtag zugeordnet und ist dann nicht mehr nur für die Datenschutzkontrolle im öffentlichen Bereich, sondern auch für die Datenschutzaufsicht im nichtöffentlichen Bereich zuständig, also zum Beispiel bei Auskunfteien, Banken und Versicherungen. Ein gewisser Wermutstropfen ist allerdings die beschränkte Durchschlagskraft; für die Verfolgung von Ordnungswidrigkeiten wegen Verstößen gegen das Datenschutzrecht ist künftig allein das Regierungspräsidium Karlsruhe zuständig.“

Im Hinblick auf die Zusammenlegung der Datenschutzaufsichtsbehörden in Baden-Württemberg bat der Landesdatenschutzbeauftragte zugleich die BürgerInnen um Verständnis für vorübergehend längere Bearbeitungszeiten bei Eingaben: „Die organisatorischen Veränderungen werden in den nächsten Wochen und Monaten unsere Personalkapazitäten in erheblichem Umfang binden, zumal meine Dienststelle umziehen muss und noch einige Stellen neu zu besetzen sind; hierunter wird die Leistungsfähigkeit der Behörde unweigerlich leiden. Ich bin aber zuversichtlich, dass wir nach einer gewissen `Durststrecke´ kompetente Beratung und Datenschutzkontrolle aus einer Hand bieten können“ (PM LfD Baden-Württemberg 31.03.2011).

Baden-Württemberg

Polizisten-DNA-Datenbank

Die Polizei Baden-Württemberg sammelt ab sofort DNA-Proben von MitarbeiterInnen der Spurensicherung und der Kriminaltechnik. Damit sollen künftig Tatortspuren abgeglichen und so Fehlermittlungen vermieden werden. Gemäß den Angaben des Landesinnenministeriums werden zunächst in dieser sog. Eliminationsdatenbank in anonymisierter Form die DNA von rund 700 BeamtInnen gespeichert. Die Abgabe der DNA-Probe ist freiwillig. Landespolizeipräsident Wolf Hammann weist in einem internen Schreiben auf Folgendes hin: „Selbst umfangreiche Schutzmaßnahmen bieten keine absolute Gewahr dafür, dass nicht doch eine unbeabsichtigt verursachte Trugspur am Tatort oder an einem Beweismittel hinterlassen wird. Wir können uns aber in dem äußerst wichtigen Prozess der DNA-Spurensicherung und -Analyse keine Schwachstelle leisten.“ Fast vier Jahre nach dem Mord an einer Polizistin in Heilbronn zieht das Ministerium damit eine weitere Konsequenz aus der Panne um das „Phantom“: Knapp zwei Jahre lang hatte die Polizei nach einer Serientäterin gesucht, die es gar nicht gab. Die Ermittelnden waren rund 40 Trugspuren gefolgt, die durch verunreinigte Wattestäbchen entstanden waren (Der Spiegel 15/2011, 12, vgl. DANA 1/2009, 26).

Bayern

Wanzen beim ADAC

Beim ADAC Nordbayern sind über Monate, wenn nicht Jahre hinweg MitarbeiterInnen und ehrenamtliche Funktionäre mit Hilfe von Wanzen bespitzelt worden. Ein Anwalt des gut 930.000 Mitglieder zählenden Autofahrerverbandes bestätigte diese Presseinformationen. Auch Telefone in der ADAC-Niederlassung in Nürnberg sollen abgehört worden sein. Sogar im Dienstfahrzeug des Geschäftsführers soll sich eine Wanze befunden haben. Wer wen bespitzeln ließ und zu welchem Zweck, konnte noch nicht festgestellt werden. Die amtierende Spitze des ADAC hegte den angeblich „begründeten Verdacht“, dass ein ehemaliger Mitarbeiter hinter den Abhörmaßnahmen steckt. Der Mann sitzt seit Ende September 2010 in Untersuchungshaft, weil er verdächtigt wird, seit 2005 mehr als 400.000 Euro veruntreut zu haben. Dessen Anwalt wies derweil diese Vorwürfe zurück: „In diese Richtung wird von der Staatsanwaltschaft überhaupt nicht er-

mittelt.“ Der Ex-Mitarbeiter solle offenbar zum Sündenbock für Missstände beim ADAC in Nordbayern gemacht werden. Der Pegnitzer Rechtsanwalt und langjährige ADAC-Funktionär Herbert Gabler macht dem Vorsitzenden Herbert Behler den Vorwurf, er habe diesen „schon vor Monaten“ über die Lauschangriffe in Kenntnis gesetzt. Er vermutet, „ein hochrangiges Vorstandsmitglied des ADAC Nordbayern“ habe veranlasst, „dass in bestimmten Bereichen Tonaufzeichnungen gemacht wurden“, weil ihm auf normalem Wege „nicht alle geforderten Informationen zugängig waren.“ Ziel der Lauschangriffe soll u.a. ein Mitarbeiter gewesen sein, der sich seit Wochen schweren Vorwürfen ausgesetzt sieht, weil sich langjährige Mitarbeiterinnen über Sexismus und Mobbing beklagten (Ritzer SZ 17.03.2011, 38).

Hamburg

ECE zeichnete heimlich Kundenanrufe auf

Wer im Einkaufszentrum Hamburger Meile anrief, wurde beim Telefonat automatisch aufgezeichnet und der Anruf gespeichert, ohne dass die Betroffenen dies wussten. Die Gruppe ECE, die zum Hamburger Otto-Konzern gehört und deutschlandweit 93 große Shoppingcenter betreibt, erläuterte ihre Abhöraktion als reine Vorsichtsmaßnahme. Die Aufzeichnungen hätten ausschließlich dazu gedient, bei Drohanrufen wie z.B. Bombendrohungen „eine effektive Ermittlungsmöglichkeit für die Polizei“ zu haben. Der Datenschutzbeauftragte von Hamburg (HmbBfDI) Johannes Caspar monierte, dass nicht alle Anrufer unter Generalverdacht gestellt werden dürften, nur wenn sich ein Unternehmen bedroht fühlt: „Man darf nicht vorratsmäßig Anrufe aufzeichnen, ohne dass die Betroffenen dies wissen.“ Caspar stellte Strafanzeige gegen ECE wegen der Verletzung des „nicht öffentlich gesprochenen Wortes“ - ein Verstoß gegen § 201 StGB. Es steht der Verdacht im Raum, dass ECE ganz grundsätzlich alle Kundenanrufe in mehreren Centern in Sachsen und Hamburg aufgezeichnet und gespeichert hat. Der Konzern wehrt sich mit dem Argument, die Aufzeichnungen wären „gegen unbefugten Zugriff gesichert“ gewesen und wären lediglich „im Fall von eingegangenen Drohanrufen“ ausgewertet worden. „Dabei ist man in einigen Centern über das eigentliche Ziel technisch hinausgeschossen“ und entschuldigte sich „ausdrücklich“.

Die Datenschützer sind auf die Abhörgeräte aufmerksam geworden, als sie wegen Videoüberwachungsmaßnahmen recherchierten. Allein im Alstertal Einkaufszentrum (AEZ) in Hamburg setzte die ECE-Gruppe 75 Überwachungskameras ein; Caspar hatte das Unternehmen aufgefordert, mindestens 24 davon wegen Verstößen gegen das Bundesdatenschutzgesetz abzubauen. ECE teilte im April 2011 mit, die beanstandeten Kameras abzubauen. Entsprechende Kameras in den anderen deutschen Einlaufszentren von ECE sollten folgen. Caspar begrüßte dies und wies darauf hin, dass damit „ein zeit- und kostenintensives Verfahren vor den Gerichten“ vermieden werde (vgl. DANA 1/2011, 19 f.; Läsker SZ 01.04.2011, 20; PM HmbBfDI 19.04.2011).

Mecklenburg-Vorpommern

Neues Polizeirecht strapaziert Datenschutz

Mit den Stimmen der rot-schwarzen Regierungskoalition ist das Sicherheits- und Ordnungsgesetz (SOG) von Mecklenburg-Vorpommern novelliert worden. Es räumt den Ordnungshütern mehr Befugnisse ein und entfristet einige Regelungen, die nur für den G8-Gipfel gedacht waren. Innenminister Lorenz Caffier (CDU) erklärte im Landtag: „Mit dem Inkrafttreten dieses Änderungsgesetzes am 31.03.2011 wird Mecklenburg-Vorpommern wieder über ein aktuelles und modernes, an die Rechtsprechung des Bundesverfassungsgerichts angepasstes Polizeigesetz verfügen.“ Gegen das neue Gesetz votierte die Linksfraktion, z.B. deren innenpolitischer Sprecher Peter Ritter: „Trotz erheblicher verfassungsrechtlicher Zweifel hält die Koalition an der Videoüberwachung öffentlicher Orte fest, ohne einen konkreten Bedarf darzulegen. So können einen Vielzahl von Menschen beobachtet werden, die in keinem Bezug zu Gefahren stehen, die abgewehrt werden sollen.“ Diesen Punkt hatte auch Ina Schäfer vom Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) gegenüber dem Innenausschuss sowie vorab in einer Stellungnahme bemängelt: „Wir wollten die im Zuge des G8-Gipfels eingeführte polizeiliche Videoüberwachung eingrenzen.“ Mit einem derartigen Großereignis sei so schnell ja nicht wieder zu rechnen. Die ursprünglich bis Mitte 2010 befristete Überwachung wird durch das neue SOG entfristet. Schäfer: „Die gewählte Formulierung, ein die öffentliche Sicherheit schädigendes Ereignis ist wohl kaum für eine an einem öffentlichen Ort einzurichtende Videobeobachtung ausreichend“.

Dem hielt Innenminister Caffier entgegen: „Mit abgehobenen und weltfremden juristischen Diskussionen kann man die Sicherheit unserer Bürgerinnen und Bürger nicht gewährleisten. Wenn einige behaupten, manche Vorschriften seien unnötig, weil sie angeblich zu wenig angewendet werden, liegen sie falsch.“ Als nicht notwendig erachtet die Linksfraktion etwa die Entfristung der präventiven Telefonüberwachung sowie der automatischen Erfassung von Auto-Nummernschildern. Ritter: „Für ein Festhalten am automatisierten Erfassungen von Kfz-Kennzeichen gibt es weder rechtliche noch fachliche Gründe.“ Andere Bundesländer, darunter Schleswig-Holstein, hätten sich nach einem Bundesverfassungsgerichtsurteil vom März 2008 zur ersatzlosen Streichung entschieden. Damals hatten mehrere Autofahrer Verfassungsbeschwerde gegen das KfZ-Scanning eingelegt – die Karlsruher Richter erklärten die in Hessen und Schleswig-Holstein anlassunabhängig praktizierte Kennzeichenerfassung für unzulässig (DANA 1/2008, 55). Caffier hält am Scanning fest: „Einige Vorschriften stellen wegen ihrer Eingriffsqualität zu Recht sehr hohe Voraussetzungen an ihre Anwendung. Wenn aber in nur einem Falle die körperliche Unversehrtheit oder gar ein Leben geschützt werden kann, hat sich diese Vorschrift bewährt.“

Im neuen SOG ist außerdem die Erhebung sensibler Daten etwa zur politischen Meinung, zur ethnischen Herkunft, zum Sexualleben oder zur Gewerkschaftszugehörigkeit geregelt. Caffier: „Die polizeiliche Datenerhebung dient nicht einem Selbstzweck, sondern allein der Sicherheit und dem Schutz der Bürgerinnen und Bürger. Sie nützt also jedem von uns“ (Kreutzträger www.taz.de 20.03.2011).

Datenschutznachrichten aus dem Ausland

Weltweit

Hacker stehlen über 100 Millionen Sony-Kundendaten

- Playstation-Netzwerk und Qriocity

Bei Hackerangriffen u.a. auf das Onlinespiele-Netzwerk von Sony sind Daten von über 100 Millionen NutzerInnen gestohlen worden. Zunächst wurde bekannt, dass die NutzerInnen des Playstation Network (PSN) und des Video- und Musikservices Qriocity weltweit betroffen sind. Das Unternehmen hatte die beiden Angebote Mitte April 2011 zunächst ohne Angaben von Gründen vom Netz genommen. Eine unbekannte Person habe sich Zugang zu persönlichen Daten wie Name, Adresse, E-Mail oder Geburtsdatum verschafft, schrieb Sony am Abend des 26.04.2011 in Firmenblogs und informierte die Betroffenen. Firmensprecher Patrick Seybold erklärte in einem Blogbeitrag, die Täter hätten sich Zugang zu einer unverschlüsselten Datenbank verschafft. Auch Logins und Passwörter seien nach derzeitigem Kenntnisstand ausgespäht worden, möglicherweise auch die Liste der Käufe: „Obwohl es derzeit keine Anzeichen dafür gibt, dass auf Kreditkarteninformationen widerrechtlich zugegriffen wurde, können wir diese Möglichkeit nicht gänzlich außer Betracht lassen.“ Die KundInnen sollten nun besonders wachsam sein, um keinem Betrug aufzusitzen, und ihr Konto kontrollieren.

Das in 59 Ländern genutzte Playstation Network und der Qriocity-Service haben weltweit etwa 77 Millionen KundInnen, viele davon in Deutschland (36 Mio. USA, 32 Mio. Europa, 9 Mio. Asien). Über das Playstation-Netzwerk können NutzerInnen miteinander spielen, chatten und Filme ansehen. Immer mehr Spiele für die Konsole Playstation 3 und auch die mobile Playstation Portable haben inzwischen Online-Komponenten. Unter dem Namen Qriocity vertreibt der Konzern Musik und Videos.

- Erste Reaktionen von Sony

Die Hacker waren gemäß der Erklärung des Konzerns vom 17. bis zum 19.04 in die Kundendatenbanken eingedrungen. Am 20.04. hatte Sony daraufhin den Betrieb des Online-Netzwerks komplett abgeschaltet. Die Expertenanalyse, welchen Umfang das Datenleck habe und welche Bereiche betroffen seien, habe sich über mehrere Tage hingezogen, hieß es in einer weiteren Erklärung des Konzerns am 20.04. Das Unternehmen habe eine Sicherheitsfirma mit der Untersuchung des Vorfalls beauftragt. Sony ging zunächst davon aus, dass Unbefugte Zugriff auf folgende Daten erlangen konnten: Name, Adresse (Stadt, Bundesland, Postleitzahl), Land, E-Mail-Adresse, Geburtsdatum, PlayStation Network/Qriocity Passwort und Login PSN Online ID. Möglich sei außerdem, dass Rechnungsanschrift, Sicherheitsfrage zum Passwort und Kaufhistorie abgerufen werden konnten. Es seien Schritte eingeleitet worden, um das System zu erneuern und um einen besseren Schutz persönlicher Daten zu ermöglichen.

Wer hinter der folgenschweren Attacke steht, blieb zunächst unklar. Eine Vermutung war, dass der Angriff ein Racheakt aus der Szene gewesen sein könnte, nachdem Sony den Playstation-Hacker GeoHot verklagte. Der 21-Jährige, der schon Apples iPhone geknackt hatte, manipulierte auch den Schutzmechanismus der Konsole. Mit seinem Jailbreak war es möglich, Software auf der Konsole zu installieren, welche die Prüfinstanzen von Sony nicht durchlaufen hat. Die Anleitung dazu veröffentlichte er im Internet. Nach der Klage einigten sich der Konzern und der Hacker außergerichtlich. Er musste versprechen, die Software nicht mehr zu vertreiben und schrieb daraufhin in einem Blog, er schließe sich einem Boykott von Sony-Produkten an. Sonys Hightech-Konsole galt bis dahin als relativ sicher. Die Internet-Guerilla Anonymous hatte Mitte April 2011 als Reaktion auf das juristische Vorgehen gegen GeoHot und einen weiteren Hacker zum Sturm auf die Sony-Server aufgerufen. Mit massenhaften Zugriffen sollte das Playstation-Netzwerk am 16.04. lahmgelegt werden. Der Versuch gilt allerdings als gescheitert. Eine Verantwortung für den offenbar später erfolgten massiven Datendiebstahl weisen die InternetaktivistInnen von sich: „Diesmal waren wir es nicht“, heißt es in einem Blogeintrag, in dem Sony als „inkompetent“ beschimpft wird.

Trotz der präventiven Leugnung, hinter den Angriffen zu stecken, versuchte Sony am 04.05.2011, Anonymous diese in die Schuhe zu schieben, indem auf die vorangegangenen DDoS-Attacken verwiesen wurde (Distributed Denial of Service). Diese DDoS-Attacken hatten nicht nur Sony betroffen, sondern viele Finanzfirmen und Internetdienstleister, die ihre Geschäftsbeziehungen zur Enthüllungsplattform Wikileaks aufgekündigt hatten. Konkrete Verdächtige, räumte Sony in einem Brief an US-Abgeordnete ein, seien aber bisher noch nicht festgestellt worden.

- Die Reaktionen der Anderen

Der IT-Sicherheitsspezialist Holger Heimann von der Firma it.sec in Ulm kritisierte, dass Sony offenbar die Passwörter der Nutzerkonten nicht verschlüsselt gespeichert hatte: „Das ist ein deutlicher Hinweis auf ein mangelndes Sicherheitsmanagement – ein elementarer Lapsus.“ Die Passwort-Panne hätte Sony möglicherweise vermeiden

können, etwa mit Penetrationstests, bei denen Fachleute einen Angriff simulieren.

NutzerInnen zeigten sich aufgebracht und warfen dem Konzern eine miserable Informationspolitik vor: „Ihr habt eine ganze Woche gewartet, bis ihr uns wissen lasst, dass unsere privaten Informationen in Gefahr sind?“, empörte sich ein User in einem Sony-Blog. In den USA gab ein Unterausschuss des Repräsentantenhauses eine Untersuchung des Falles in Auftrag, mehrere US-Staatsanwälte haben begonnen, sich mit der Angelegenheit zu befassen, das FBI wurde von Sony eingeschaltet. Der New Yorker Generalstaatsanwalt Erich Schneidermann ließ verlauten, dass er von Sony Informationen erzwingen wolle, wie das Unternehmen Kundendaten absichert.

In Großbritannien untersucht das Büro des „Information Commissioners“, der dortige Datenschutzbeauftragte, den Fall für Europa. Man habe Sony kontaktiert und prüfe derzeit, ob das Verhalten des Unternehmens britische Gesetze zum Datenschutz verletzt habe. Zuständig für den Datenschutz in Europa ist nach den Einschätzungen auch der deutschen Datenschutzbehörden die Europazentrale von Sony in London.

Auch deutsche Politiker und Datenschützer sind empört. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Peter Schaar, hat als Konsequenz aus dem riesigen Datenklau schärfere internationale Datenschutz-Standards gefordert. „Ich glaube, wir brauchen hier in diesem Zusammenhang keine anderen Gesetze. Wir brauchen aber stärkere internationale Instrumente, um den Datenschutz zu gewährleisten.“ Notwendig sei also ein sehr hohes internationales Datenschutzniveau. Der Leiter des Unabhängigen Datenschutzzentrums Schleswig-Holstein (ULD), Thilo Weichert, sieht das anders: „Die Bundesregierung sollte den Fall Sony zum Anlass nehmen, das deutsche Datenschutzrecht endlich auf die Höhe der Zeit zu bringen.“ Weltkonzerne wie Facebook, Google oder Sony seien in Deutschland faktisch nicht für Versäumnisse beim Datenschutz haftbar zu machen. Schaar hält es für durchaus möglich, Sony in Deutschland für mögliche Schäden zur Verantwortung zu ziehen: „Der Konzern muss haften, wenn hier Schäden eingetreten sind.“ Abgesehen von Fällen, in denen KundInnen nachweislich ein Schaden entstanden ist, könnte Sony möglicherweise auch gegen deutsches Recht verstoßen haben, indem das Unternehmen KundInnen erst eine Woche nach dem Einbruch über den Datendiebstahl informierte. Der japanische Konzern habe mit dieser verzögerten Bekanntgabe „ein extrem unseriöses und rechtswidriges Verhalten an den Tag gelegt“, meinte der Fachanwalt für Informationstechnologierecht Peter Heyers. Das sei ein Rechtsverstoß. „Nach § 42a des Bundesdatenschutzgesetzes hätte Sony dies sofort veröffentlichen müssen.“ Deshalb müsse das Unternehmen auch für Schäden haften, die nun möglicherweise dadurch entstanden seien, dass die NutzerInnen nicht rechtzeitig gewarnt und informiert worden seien, so der Experte.

Die Union ließ es sich nicht nehmen, empört zu fordern, Sony müsse für mögliche finanzielle Schäden durch den Datenklau haften. So z.B. der rechtspolitische Sprecher der Unions-Bundestagsfraktion, Stephan Mayer (CSU): „Ich sehe hier Sony klar in der Haftung.“ Die Fraktionschefin der Grünen im Bundestag, Renate Künast, forderte die Regierung zum Handeln auf: „Der Fall Sony ist auch ein Fall schwarz-gelber Untätigkeit, die jetzt Millionen Betroffene in Deutschland mit ihren Daten bezahlen.“ Nach dem „größten Hackerangriff aller Zeiten“ sei die Bundesregierung in der Pflicht, endlich das Datenschutzrecht zu ändern. Die Ministerien für Justiz und Verbraucherschutz forderten von Sony eine schnelle Aufklärung, z.B. ein Sprecher von Justizministerin Sabine Leutheusser-Schnarrenberger (FDP): „Es ist äußerst bedenklich, dass das Unternehmen erst nach einigen Tagen die massive Panne eingeräumt hat.“

In einer Umfrage im Auftrag der Deutsche Presseagentur kurz nach dem Bekanntwerden des Datendiebstahls erklärten nur 4% der befragten deutschen Online-Nutzenden, dass sie als Konsequenz aus dem Vorfall gänzlich auf Einkäufe im Netz verzichten würden; 84% meinten, dass der Vorfall nichts daran ändern werde, dass sie online einkaufen. 23% meinten jedoch in einer repräsentativen Befragung des Kölner Meinungsforschungsinstituts YouGov mit 1020 Befragten im Alter über 16 Jahren, dass sie sich jetzt unsicherer bei der Nutzung von Online-Diensten fühlten. Doch auch dort kündigten nur 21% an, ihre Einkäufe im Internet einzuschränken; 61% verneinten eine entsprechende Frage. 94% sahen die Betreiber der Online-Dienste in der Pflicht, für mehr Sicherheit zu sorgen. 73% erwarteten dies auch von der Regierung.

- Sony Online Entertainment und Gewinnspiel

Anfang Mai räumte dann das Unternehmen ein, dass das Datenleck noch größer als bisher bekannt ist: Hacker hätten schon früher weitere 25 Mio. Nutzerkonten gekapert. Die Daten beziehen sich auf den mittlerweile abgeschalteten Dienst Sony Online Entertainment, wo Computerspieler über das Netz gegeneinander antreten können, z.B. in Rollenspielen wie „Everquest.“ Diesmal waren in 12.700 Fällen auch Kreditkarten- und in 10.700 Fällen Bankkontodaten betroffen, die in einer Datenbank aus dem Jahr 2007 mit KundInnen aus Deutschland, Österreich, den Niederlanden und Spanien gespeichert waren. Entwendet worden sind außerdem Name, Adresse, E-Mail-Adresse, Geburtsdatum und Telefonnummer der KundInnen. Festgestellt wurde dieser Angriff erst am 02.05.2011. Der Konzern schloss nicht aus, dass noch mehr Daten geklaut worden sind bzw. werden können, so eine Sprecherin: „Es sind Hacker am Werk. Wir wissen nicht, wo sie als nächstes zuschlagen werden. Von dem Datendiebstahl sind, so ein Schreiben der von Sony beauftragten internationalen Anwaltskanzlei Baker & McKenzie, mindestens 3,23 Mio. Nutzende betroffen. „Von dieser Zahl haben bislang 366.000 Nutzer ihre Kreditkarte zu Bezahlzwecken benutzt.“

Die Kreditkartenunternehmen Mastercard und Visa stellten zwar noch keine unzulässigen Abbuchungen im größeren Stil fest, versicherten aber, dass die Kontobewegungen von ihnen kontinuierlich auf mögliche Unregelmäßigkeiten hin beobachtet würden.

Kurz darauf musste Sony bekanntgeben, dass Namen und Adressen von 2.500 KundInnen und Teilnehmenden eines Gewinnspiels aus dem Jahr 2001 in einer Internetdatenbank aufgetaucht sind. Eine Unternehmenssprecherin erklärte, man habe die Kundendaten umgehend aus dem Netz entfernen lassen. Kreditkartendaten und Passwörter sollen nicht darunter gewesen sein. Weitere Informationen, auf welche Weise die Daten verfügbar waren und wie sie gefunden und entfernt wurden, gab Sony nicht preis.

- Finanzielle Konsequenzen

Für Sony erweist sich der Vorgang als ein ökonomisches Desaster. Deren Konsole erreichte schon zuvor nicht den Marktanteil von Microsoft und Nintendo. Schon in der ersten Woche nach Bekanntwerden des Lecks hatte der japanische Elektronikkonzern 2,5 Mrd. Euro an Aktienwert verloren. Im Jahr 2010 trug Sonys Spielesparte mit umgerechnet 6,1 Mrd. Euro mehr als ein Zehntel zum Umsatz des gesamten Konzerns bei. Der Anteil der Playstation-Plattform am Umsatz von Sony wurde mit 500 Mio. Dollar angegeben. Der Analyst bei der Investmentfirma Mizuho Investors Securities, Nobua Kurahashi, schätzte, dass das Datendesaster den Konzern 1,24 Mrd. Dollar kosten werde.

Im Rahmen der ersten Entschuldigungsaktion bot Sony seinen KundInnen an, einige Dienste in Anspruch nehmen zu dürfen, etwa einen Monat lang kostenfrei das Premiumangebot des Online-Services. Anwaltskanzleien in Kalifornien und Kanada brachten umgehend Sammelklagen gegen Sony mit einem Streitwert von 1 Mrd. Dollar auf den Weg. Vor einem Gericht in San Francisco verklagte der Playstation-Besitzer Kristopher Johns Sony auf Schadenersatz. Bei einem Schuldspruch in einer Sammelklage hätten alle 100 Millionen Inhaber von Nutzerkonten Ansprüche gegenüber Sony, auch wenn sie selbst nicht geklagt haben sollten. Johns verlangt Schadenersatz für den Fall des Missbrauchs von Kreditkartendaten sowie für den Ausfall der Online-Dienste nach dem Hacker-Einbruch. Außerdem fordert er die Verhängung einer Geldstrafe gegen Sony.

Am 01.05.2011 hatte der Konzern noch erklärt, das Nutzende innerhalb einer Woche wieder auf den Service zugreifen könnten. Diese Prognose erwies sich als zu optimistisch. Am 07.05. betonte dann eine Sprecherin, es sei nicht möglich, einen Zeitpunkt für die Freischaltung der Online-Dienste zu nennen, die seit dem Datendiebstahl gesperrt waren. Es solle ein verbessertes Sicherheitssystem installiert werden. Sony-Sprecher Shigenori Yoshida meinte, voraussichtlich könnten die Dienste erst wieder am 31.05.2011 im Netz verfügbar gemacht werden.

Investoren zeigten sich erbost über das Konzern-Krisenmanagement. Einige forderten den Rücktritt von Konzernchef Howard Stringer, der sich auch zwei Wochen nach dem Datenklau hierzu noch nicht öffentlich geäußert hatte. Vor die Presse geschickt wurde zunächst die Nr. 2 im Konzern, der designierte Nachfolger von Stringer Kazuo Hirai. Der entschuldigte sich für die Pannen und verbeugte sich tief und lang. Am 05.05. meldete sich dann auch Stringer. In einem per Blog verbreiteten Brief erklärte er: „Wir als Firma - und ich persönlich - entschuldigen uns für die Unannehmlichkeiten und Sorgen, die durch die Attacke entstanden sind." Das Unternehmen werde alle Ressourcen nutzen, um „jedes Detail" über die Art und die Auswirkungen des Angriffs herauszufinden. Singer versprach, dass Sony seine Sicherheit verbessern werde: „Falls es also wieder zu so einer Attacke kommen sollte, wird unsere Verteidigung noch besser sein."

Um die finanziellen Risiken einzugrenzen, gab Sony bekannt, zunächst die US-amerikanischen KundInnen von PSN und Qriocity mit einer Identitätsdiebstahl-Versicherungspolice über je 1 Mio. US-Dollar pro NutzerIn zu schützen. Vergleichbare Programme sollten dann für andere Regionen folgen (www.spiegel.de 27.04.2011; www.tagesschau.de 27.04.2011; www.spiegel.de 28.04.2011; www.zeit.de 28.04.2011; Bernau/Kuhn/Riedl SZ 28.04.2011, 1, 4, 17; Bernau SZ 29.04.2011, 19; Bernau SZ 04.05.2011, 17; SZ 05.05.2011, 20; www.heise.de 05.05.2011 u. 06.05.2011; Der Spiegel 19/2011, 116; www.heise.de 07.05.2011; SZ 09.05.2011, 17; www.faz.net 09.05.2011).

Weltweit

Apple speichert Lokalisierungsdaten auf iPads und iPhones

Alasdair Allan und Pete Warden stellten auf einem Vortrag auf der IT-Konferenz „Where 2.0" in San Francisco und dann im Internet ihre Feststellung vor, dass iPhones und mobilfunkfähige iPads (3G), die mit dem Betriebssystem iOS 4 ausgestattet sind, ständig ihre Aufenthaltsorte aufzeichnen. Die NutzerInnen wurden hierüber bis dahin nicht informiert, geschweige denn um Erlaubnis gefragt. Anhand dieser Informationen können hochpräzise Bewegungsprofile der Geräte und damit ihrer Nutzer erstellt werden. Die beiden hatten die Datei namens „consolidated.db" eher zufällig entdeckt. Darin finden sich die Angaben zu Längen- und Breitengraden, die jeweils mit einem Zeitstempel versehen sind. Diese Informationen seien „nicht immer ganz korrekt, aber recht detailliert". Die Ortsdaten seien vermutlich mithilfe der Funkzellen des Mobilfunknetzes errechnet worden und stammten nicht vom GPS-Empfänger der iGeräte. Ein fester Rhythmus, in dem die Aufzeichnungen erfolgten, sei nicht zu erkennen. Die Speicherungen fänden völlig unregelmäßig statt, so Allan und Warden. Die von den beiden Forschern gefundenen Aufzeichnungen reichen zum Teil knapp ein Jahr zurück - bis zu dem Zeitpunkt, als Apple das Betriebssystem iOS 4 veröffentlichte. Es scheinen nur Geräte mit dieser Version betroffen zu sein.

Die Datei „consolidated.db" wird nicht nur auf dem mobilen Gerät gespeichert, sondern über iTunes im Zuge von Sicherungskopien auch auf dem Desktop-Rechner der Nutzenden - und zwar unverschlüsselt. Dort ist es regelmäßig sehr einfach, auf die gespeicherten Daten zuzugreifen. Warden hat ein Tool dafür geschrieben, mit dem jeder die Datei auf seinem Rechner auslesen kann (http://petewarden.github.com/iPhoneTracker/). Unbefugte könnten das natürlich auch.

Sicher bestand immer die Möglichkeit, im Optionsmenü bei „iPhone-Backup verschlüsseln" einen Haken setzen; aber

dies hatte bis dahin wohl niemand getan. In jedem Fall sind die Daten langlebig – denn sie werden nach Erkenntnissen von Allan und Warden auch nach einem Gerätewechsel weiterverwendet. Verbindet man sein jungfräuliches neues iPhone das erste Mal mit iTunes, wird auch die bereits bestehende Datenbank überspielt und dann weiter gepflegt. Was die Informationen in „consolidated.db“ bedeuten, zeigten die Experten auf einfache Weise: Sie haben die gespeicherten Ortsinformationen auf einer Landkarte eingetragen. Wie eine Ameisenstraße zog sich das Beispiel-Bewegungsprofil von Baltimore über Philadelphia bis nach New York. Solche Muster lassen sich für jeden bilden. So lässt sich feststellen, wo wir uns wann aufgehalten haben. Allan meinte: „Die Mobilfunkanbieter haben diese Daten schon immer gehabt - aber man benötigt einen Richterentscheid, um auf sie zuzugreifen. Und jetzt liegen diese Daten offen in der Gegend herum.“

Was Apple mit diesen Daten vorhatte, war zunächst unbekannt. Das Unternehmen hatte weder auf die Fragen der beiden Experten noch auf die von JournalistInnen geantwortet. Erst fünf Tage nach Beginn der „Geodaten-Affäre“ meldete sich Steve Jobs persönlich zu Wort. In einer E-Mail an einen Kunden dementierte er die international geäußerten Vorwürfe, der Konzern würde seine NutzerInnen ausspionieren. „Wir überwachen niemanden“, erklärte er in einer nicht verifizierten E-Mail, die das Apple-Portal MacRumors veröffentlichte. Die Informationen, die derzeit im Umlauf sind, seien schlichtweg falsch.

Obwohl die Daten nicht an Apple versendet werden, sind Datenschützer darüber beunruhigt, dass die Daten unbegrenzt und in einem unverschlüsselten Format abgespeichert werden. Somit könnten die Ortungsdaten mit einer entsprechenden Software ausgewertet werden. Tests haben ergeben, dass die Datenspeicherung auch erfolgt, wenn entsprechende Lokalisierungsfunktionen wie GPS und WLAN-Ortsmarkierung abgeschaltet sind. Dies bestätigt, dass die Koordinaten über die Position der Mobilfunkmasten festgestellt werden und dass über die Abschaltung der Ortungsfunktionen iPhone-BesitzerInnen keine Möglichkeit haben, die Speicherung der Ortsdaten zu verhindern.

Statt detailliert auf solche Datenschutz-Fragen einzugehen, erhob Apple-Gründer Jobs in seiner E-Mail-Antwort den Vorwurf gegen Google, mit seinem Betriebssystem Android ebenfalls Standortdaten zu sammeln. Der von Jobs öffentlich angemailte Kunde hatte erwogen, auf das Google-Betriebssystem Android umzusteigen, weil dieses „mich nicht überwacht“. Jobs‘ Antwort: „Doch, sie tun es.“ Dem widersprach umgehend Google: Android-Handys speicherten Ortsdaten nur, wenn die NutzerInnen hierfür vorher die Einwilligung gegeben hätten. Zudem sichere das System einzig die letzten 50 Mobilfunkmasten und 200 WiFi-Netzwerke, die das Handy anpeilt. Die Daten würden anonym an die Firmenserver gesendet und seien keinem Handynutzer zuordenbar. Dessen ungeachtet haben zwei Android-Nutzende im US-Staat Michigan eine Sammelklage eingereicht, in der sie monieren, dass die Software ihre Standortdaten aufzeichne, Schadenersatz und das Ende der Speicherung fordern. Auch Smartphones mit dem Microsoft-Betriebssystem Windows Phone 7 speichern nach einem Fachpressebericht Standortdaten, allerdings laut Angabe des Unternehmens nicht direkt auf dem Gerät.

Am 27.04.2011 nahm dann Apple auf seiner Internetseite Stellung zu den Vorwürfen: Es bestätigte, dass die Positionsdaten über Mobilfunkzellen und WLAN-Router erfasst würden. Diese Funktionsweise hatte Apple schon im Juli 2010 in einem Brief an zwei US-Abgeordnete erklärt, jedoch ohne Erwähnung des Zeitstempels, der die Erstellung von Bewegungsprofilen ermöglicht. In dem Brief wurde fälschlich behauptet, die Datenbank sei gesichert und nur Apple zugänglich, bei abgeschalteten Ortungsdiensten würden keine Updates erfolgen. Apple räumte nun Fehler ein: Das Backup der Daten auf den PC des Nutzers werde künftig unterbunden und das Fortschreiben sei ein „Bug“. Beides wollte Apple mit einem zukünftigen iOS-Update beheben. Die Datenbank solle auf die Einträge der letzten sieben Tage beschränkt und beim Ausschalten der Ortungsdienste komplett gelöscht werden, auch die Einträge vor dem Ausschalten. Im nächsten größeren iOS-Update solle die Datenbank auf dem iPhone zusätzlich verschlüsselt werden.

Einen weiteren Tag später schoben Firmenchef Steve Jobs, Marketingboss Phil Schiller und iOS-Softwareleiter Scott Forstall in Interviews weitere „Informationen“ hinterher. Es handele sich bei den fraglichen Daten um „anonyme Informationen“, die Apple über ein Crowdsourcing-Verfahren erhalten hat. „Das haben die Leute auf ihren Telefonen gesehen und es für Ortsdaten gehalten.“ Damit verriet Apple nebenbei ein weiteres Detail: den Aufbau einer Verkehrsdatenbank für Staumeldungen. Die Bewegungsdaten der iPhones will Apple anonymisiert sammeln, um Aussagen über die Verkehrsdichte zu treffen, ein Dienst, der „in the next couple of years“ freigeschaltet werden soll. Ähnliches machen auch andere Anbieter wie Google mit Android und schon länger Navigon und Tomtom (siehe S. 486). Mehrere Stellen für Entwickler von Navi-Apps hatte Apple voriges Jahr ausgeschrieben.

Die Apple-Funktionäre bekräftigten, die Datei sei im System geschützt, sie sei ein Root-File und vor anderen Apps in einer „Sandbox“ versteckt. „Wenn nun aber jemand sein Telefon hackt und einen Jailbreak durchführt, kommt er an sie heran.“ Die Datei sei aber „komplett anonym“ und könne nicht individuellen Personen oder Geräten zugeordnet werden. Dass diese Zuordnung unnötig ist, weil die Datei ja auf einem individuellen Gerät sitzt, ist jedeR wenig versierten iPhone-NutzerIn klar.

Zitiert werden muss dann noch ein Zitat von Jobs anlässlich dieses Vorgangs: „Wenn eine neue Technik gesellschaftlich eingeführt wird, bedarf es einer Zeit der Anpassung und der Erziehung. Wir als Industrie haben bei der Erziehung der Leute keinen guten Job gemacht. Ich meine, wenn es um komplizierte Dinge geht. So sprangen Leute auf eine Menge falscher Schlussfolgerungen.“

In den USA haben nach einem Bericht der US-Nachrichtenagentur Bloomberg

bereits zwei Nutzer Sammelklage gegen Apple eingereicht. Der demokratische Senator Edward Markey will in einem offenen Brief von Apple-Chef Steve Jobs wissen, zu welchem Zweck die Daten gesammelt werden und ob die Funktion abzuschalten ist. In Deutschland forderte ein Sprecher von Verbraucherschutzministerin Ilse Aigner (CSU) Apple auf, sich zu äußern; eine heimliche Standorterfassung wäre ein „grober Eingriff in die Privatsphäre". Der Leiter des Bayerischen Landesamtes für Datenschutzaufsicht, Thomas Kranig, forderte Apple Deutschland auf, bis zum 10.05. Stellung zu beziehen und drohte mit einem Bußgeld von 300.000 Euro. Auch italienische und französische Datenschutzbehörden nahmen Ermittlungen auf.

Am 05.05. kündigte Apple dann ein Update an, mit dem die Ortung ausgeschaltet werden kann. Damit wird die Größe der Datei mit den Ortsdaten reduziert. Zudem würden, so Apple, die Informationen bei der Synchronisierung nicht mehr auf den Computer übertragen. Die Nutzenden könnten es selbst verhindern, dass die Daten auf den mobilen Geräten überhaupt gespeichert werden: „Der Zwischenspeicher wird vollständig gelöscht, sobald die Ortungsdienste abgeschaltet sind." Die Software wird über iTunes verfügbar gemacht. D.h. die Nutzenden müssen ihr mobiles Gerät, also iPhone oder iPad, an den Computer anschließen und die Synchronisation starten.

Das PR-Desaster traf Apple hart, nachdem der Konzern noch eine Woche zuvor auf einer Erfolgswelle ritt: Apple veröffentlichte Unternehmensergebnisse, nach denen der Elektronikhersteller den Absatz seines iPhones im vergangenen Quartal mehr als verdoppeln konnte. Dank seines iPhones konnte Apple im ersten Quartal den Umsatz auf 24,7 Mrd. Dollar steigern. Der Gewinn lag mit knapp sechs Milliarden Dollar deutlich über den Markterwartungen (Sander www.stern.de 20.04.2011; Martin-Jung SZ 23.-25.04.2011, 1, 2, 4; www.heise.de/mobil/ 27.04.2011; www.heise.de 28.04.2011, SZ 30.04./01.05.2011, 26; Schmundt Der Spiegel 18/2011, 116 ff.; SZ 06.05.2011, 19).

Weltweit

Unescos BewerberInnendaten ungeschützt im Netz

Die UN-Organisation für Bildung, Wissenschaft und Kultur (Unesco) hat über Jahre hinweg Bewerbungsunterlagen für jeden einsehbar ins Internet gestellt. Die Dokumente enthielten Informationen über den Bildungsweg, die bisherigen Arbeitgeber und zum Teil auch Angaben über Jahresgehälter. Betroffen waren zwei Datenbanken, eine mit Bewerbungen um Praktikumsplätze, die andere für reguläre Posten innerhalb der Organisation. Eine Unesco-Sprecherin bestätigte die Sicherheitslücken, die inzwischen aber geschlossen worden seien. Betroffen waren zehn-, womöglich hunderttausende von Bewerbungsunterlagen – inklusive Anschreiben und Adressen. In den Bewerbungen finden sich genaue Angaben, z.B. wie viel ein leitender Mitarbeiter im diplomatischen Dienst Pakistans verdient (einen sechsstelligen Dollar-Betrag) und welche Angestellten der Weltbank zur Unesco wechseln wollten. Die BewerberInnen kamen aus aller Welt. Unter ihnen waren DiplomatInnen und WissenschaftlerInnen. Die von Presseorganen stichprobenweise eingesehenen Bewerbungen stammten aus den Jahren 2006 bis 2011.

Die Unterlagen von Praktika-BewerberInnen waren völlig ungeschützt über die Eingabe einer bestimmten URL abrufbar. Um zu einem anderen Bewerber zu springen, genügte es, die Kennziffer in der URL zu verändern. Die Bewerbungen für reguläre Unesco-Stellen waren nur einsehbar, wenn man sich als BewerberIn bei der Unesco registriert hatte – dazu reichte aber eine Mail-Adresse. Zu anderen BewerberInnen war man wiederum über die Veränderung der Kennziffer in der Adresszeile gekommen. Die Unesco hatte zunächst wochenlang nicht auf Hinweise auf das Sicherheitsproblem reagiert. Ein Unesco-Bewerber hatte das Problem mehr als einen Monat vor der Veröffentlichung in den Medien entdeckt und die Organisation schriftlich darüber informiert.

Die 1945 in London gegründete Unesco ist in der breiten Öffentlichkeit vor allem für ihre Welterbeliste bekannt. Die mehr als 2.000 Mitarbeiter in der Pariser Zentrale und den 65 Außenbüros kümmern sich aber auch um Bildungsprojekte in Entwicklungsländern, den Schutz von Ökosystemen oder Wissenschaftsprogramme. Deutschland ist seit 1951 Mitglied und nach den USA und Japan drittgrößter Beitragszahler (Lischka www.spiegel.de 28.04.2011; www.heise.de 28.04.2011).

Europa/USA

USA greift ungebremst auf SWIFT-Bankdaten zu

Ein aktueller Bericht der Gemeinsamen Kontrollinstanz (GKI) von Europol zur Umsetzung des umstrittenen Terrorist Finance Tracking Programme (TFTP) kritisiert, dass Europol die Anfragen von US-Behörden nach den Bankdaten von EU-BürgerInnen beim Finanzdienstleister SWIFT einfach durchwinkt. Die als Kontrollinstanz vorgesehene zentrale Polizeibehörde Europol hat danach die Anfragen zu lax geprüft. Die Anfragen des amerikanischen Finanzministeriums seien schlicht so vage, dass Europol kaum fundiert entscheiden könne, ob die Daten weitergegeben werden müssten. Dennoch habe Europol weiterhin alle Anfragen akzeptiert und durchgewunken. Die GKI empfahl, Europol müsse das US-Finanzministerium kontaktieren und darauf drängen, dass „alle künftigen Anfragen nach Swift-Daten mit den im TFTP-Abkommen festgelegten Kriterien übereinstimmen".

Bis zur Verabschiedung dieses Abkommens, um das beide Seiten hart gekämpft hatten, hatten sich die amerikanischen Behörden an den Daten praktisch völlig ungehindert selbst bedient. Dann hatte das Europäische Parlament eine Reihe von Kontrollmechanismen erstritten – darunter das Recht, Europol die Anfragen auf Notwendigkeit und Verhältnismäßigkeit prüfen zu lassen.

Der Bundesdatenschutzbeauftragte Peter Schaar sieht durch den öffentlichen Teil des Kontrollberichts sei-

ne schlimmsten Befürchtungen bestätigt und erklärte: „Es bestehen massive Defizite. Die politisch Verantwortlichen auf europäischer und nationaler Ebene müssen umgehend dafür sorgen, dass die festgestellten Mängel beseitigt werden.“ Schaar kritisierte, dass der größte Teil des Berichts als geheim eingestuft wurde - diese Passagen seien auch dem EU-Parlament nicht mitgeteilt worden.

Der Grünen-Abgeordnete Jan Philipp Albrecht forderte nun die EU-Kommission auf, das Abkommen mit den USA aufzukündigen. Albrecht warnte, dass nach wie vor millionenfach Daten europäischer BankkundInnen an die US-Terrorfahnder weitergegeben würden: „Dabei geht es auch um rein europäische Überweisungen“. Das habe kürzlich Innenkommissarin Cecilia Malmström bestätigt. Eine fristlose Kündigung des Abkommens wäre im Falle des Vertragsbruchs einer Partei theoretisch möglich. Der liberale Abgeordnete Alexander Alvaro, der als Berichterstatter für das SWIFT-Abkommen gestimmt hatte, beurteilte eine Kündigung als Ultima Ratio. Zunächst gelte es, Europol in die Verantwortung zu nehmen: „Ich bin stinksauer.“ Die Liberalen hätten dem Abkommen „schweren Herzens zugestimmt“ und sich um eine Balance zwischen den Datenschutzinteressen der europäischen BürgerInnen und den Sicherheitsinteressen bemüht. „Wenn jetzt die Maßnahmen nicht nur etwas lax umgesetzt, sondern komplett ignoriert werden, müssen wir Europol wohl daran erinnern, dass sie an EU-Recht gebunden sind.“ Das Vorgehen der USA überrasche kaum: „Wenn man dem Kind die Keksdose vor die Nase hält, wird es sich auch bedienen.“ Alvaro wollte zunächst Rob Wainwright, den Europol-Direktor einbestellen. Im August 2010 hatte im Deutschen Bundestag die CDU/CSU und FDP das neue Abkommen noch als „respektabler Verhandlungsergebnis“, das „deutliche Verbesserungen“ beim Daten- und Rechtsschutz bringe, gefeiert (BT-Drs. 17/2431).

Europol-Sprecher Sören Petersen war hingegen der Meinung, alle Anfragen seien nach professionellen Grundsätzen geprüft worden: „In vier Fällen haben wir von den US-Behörden zusätzliche Informationen verlangt.“ Übrigens werde man ja keineswegs „zugespamt“ mit Anfragen – seit vergangenem August waren es gerade einmal sieben. Zwar seien Verbesserungen bei der Umsetzung eines so neuen Abkommens immer möglich und Kritik willkommen. „Wir verwahren uns aber gegen die Kritik, dass die Grundlage, auf der die Transfers bewilligt wurden, unzureichend sei.“ Wie viele Datensätze aus welchen Ländern übermittelt wurden, dazu könne er keine Angaben machen: „Das Abkommen regelt Massenabfragen.“ Das EU-Parlament hatte ein System, bei dem nur Treffer von Ermittlungen an die Amerikaner weitergegeben würden, seit Langem gefordert. Bislang hatte sich die US-Seite allerdings immer erfolgreich dagegen gewehrt. Offiziell wurden dafür bislang mangelnde Kapazitäten oder Kompetenzen der EU-Strafverfolger angegeben.

Auch das deutsche Innenministerium hatte Anfang Februar die Informationspolitik von Europol scharf kritisiert, nachdem Europol sich geweigert hatte zu sagen, wie viele Daten deutscher BürgerInnen bereits übermittelt worden sind. Martin Kotthaus, der Sprecher der deutschen Vertretung in Brüssel, meinte allerdings, der deutschen Kritik sei inzwischen „teilweise“ entsprochen worden. Ein eintägiger Workshop etwa solle bald die Fragen von Kommission, Europol und Mitgliedsstaaten klären. Daher lautet es jetzt aus dem Ministerium, man befände sich „mit der Kommission über Fragen im Rahmen der Umsetzung des EU-US-TFTP-Abkommens im Gespräch“. Mit Blick auf die Statistik warten alle Seiten gespannt auf die erste gemeinsame Prüfung der Umsetzung des TFTP durch die EU-Kommission und das US-Finanzministerium.

Diese soll laut Artikel 13 des TFTP Aufschluss über die Anzahl der übertragenen Transaktionsdaten und daraus erfolgten Maßnahmen oder gar Verfahren bringen. Gleichzeitig soll dieser Bericht auch die Fälle auflisten, in denen die US-Terrorermittler den EU-Mitgliedsstaaten, Europol und Eurojust sowie Nicht-EU-Staaten Erkenntnisse mitgeteilt haben, die sie auf der Basis der Swift-Daten gewonnen haben. Auch die Einhaltung der Datenschutzgarantien sowie Umsetzung und Effektivität stehen dabei insgesamt auf dem Prüfstand. Die BürgerInnen haben zwar formal ein Recht zu erfahren, was in den USA über sie gespeichert wird. Dieses Recht gilt inzwischen aber in der Praxis als kaum durchsetzbar (Ermert www.zeit.de 10.03.2011; www.spiegel.de 09.03.2011; PM BfDI 08.03.2011).

Europa

EU-Kommission billigt RFID-Framework

Die Kommission der Europäischen Union (EU) hat eine Selbstverpflichtung der Wirtschaft zur Sicherung der Privatsphäre bei Funketiketten, also beim Einsatz von RFID-Chips, abgesegnet. Der Datenschutz soll möglichst von Anfang an gemäß dem Konzept „Privacy by Design“ in die Produkte integriert werden. Laut der Vereinbarung, die die für die Digitale Agenda zuständige Kommissarin Neelie Kroes am 06.04.2011 gemeinsam mit führenden IndustrievertreterInnen aus der EU und den USA sowie VertreterInnen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und des Datenschutzes unterzeichnet hat, sollen Unternehmen die Risiken für das informationelle Selbstbestimmungsrecht der VerbraucherInnen durch RFID-Anwendungen umfassend bewerten und vor der Markteinführung minimieren. Das „Privacy Impact Assessment Framework“ bietet anhand eines Entscheidungsbaums einen Rahmen zur Datenschutz-Folgenabschätzung. Es soll Anwendenden in der Industrie helfen, Auswirkungen auf die Privatsphäre der vielfach als Barcode-Ersatz verwendeten und auch bei elektronischen Bezahlverfahren, in Pässen oder auf Tickets eingesetzten kontaktlos auslesbaren Chips von vornherein zu bedenken und technisch zu adressieren. Das Dokument beschreibt die Ziele und methodische Vorgehensweise eines „Privacy Impact Assessment“ (PIA), die zu berücksichtigenden Teile einer RFID-Anwendung sowie die Struktur und den Inhalt von Überprüfungsberichten.

Kroes begrüßte, dass die vorab von der „Artikel-29“-Gruppe der EU-Datenschutzbeauftragten in einer Stellungnahme befürworteten Leitlinien die Privatsphäre der Verbraucher „als zentralen Aspekt der RFID-Technologie“

anerkennen und gewährleisteten, dass der Datenschutz vor dem Einsatz der Produkte berücksichtigt werde. Die Niederländerin lobte, dass die Industrie hier mit Verbrauchern, Datenschutzbehörden und anderen Gremien zusammenarbeite. Der PIA-Rahmen biete für die darauf bauenden Unternehmen Rechtssicherheit. Sarah Spiekermann, Leiterin des Instituts für Betriebswirtschaftslehre und Wirtschaftsinformatik an der Wirtschaftsuniversität Wien, unterstrich, dass während der Verhandlungen „gänzlich verschiedene Sichtweisen europäischer und amerikanischer Unternehmen auf den Datenschutz" zutage getreten seien. Umso erfreulicher sei es, dass der finale Text dem Bedürfnis der EU-BürgerInnen nach informationeller Selbstbestimmung Rechnung trage. Die beteiligten Firmen würden künftig mindestens sechs Wochen vor Markteinführung einer neuen Anwendung den Aufsichtsbehörden eine Datenschutzabschätzung übermitteln, versicherte Heinz Paul Bonn, Vizepräsident des IT-Verbands Bitkom. Die Privatsphäre zu sichern liege im Eigeninteresse der Wirtschaft. Die Technik werde nur flächendeckend akzeptiert, wenn Verbraucher ihr vertrauten. Die Industrie setzt mit dem Selbstregulierungskodex eine RFID-Datenschutzempfehlung der Kommission vom Mai 2009 um. Demnach müssen die Anwender von „Smart Tags" prüfen, ob und inwieweit personenbezogene Daten gespeichert und verarbeitet werden. Der deutsche Bundesrat hatte auf die Umsetzung der Hinweise aus Brüssel gedrängt. Nach Ansicht der Länder sollten Produkte mit Funkchips auch klar nach europaweit einheitlichen Standards gekennzeichnet und die Etiketten einfach deaktivierbar sein (Krempl www.heise.de 06.04.2011).

Niederlande

TomTom verkauft anonymisierte Bewegungsprofile an Polizei

Der große holländische Navigationsgerätehersteller TomTom hat seine gespeicherten Verkehrsdaten an die niederländische Regierung verkauft. Die Regierung hat die erworbenen Daten nicht, wie von TomTom angeblich angenommen, zur Verbesserung des Straßennetzes verwendet, sondern um Temposünder zur Kasse zu bitten. Der Firmenchef von TomTom, Harold Goddijn, entschuldigte sich öffentlich für diesen Vorfall. In den Geschäftsbedingungen bittet TomTom die Nutzenden um Zustimmung für die anonyme Nutzung der Daten „zum Zweck der Produktverbesserung", wobei damit wohl kaum jemand an Polizeiprodukte denken dürfte. TomToms Verkehrsinformationsdienst HD Traffic wertet unter anderem Bewegungsprofile von Navigationsgeräten mit Internetanbindungen und von Smartphones mit TomTom-App aus, um beispielsweise verlangsamten Verkehr oder Staus möglichst früh zu erkennen. Hierbei werden auch Daten wie Fahrgeschwindigkeitswerte anonymisiert übermittelt. Die niederländische Polizei nutzte diese Werte, um nachzuvollziehen, an welchen Stellen besonders viele Gerätenutzer sich nicht an das Tempolimit halten. An diesen Stellen wurden dann Radarfallen aufgestellt. Etwa die Hälfte aller Polizeidienststellen des Landes kauften diese Daten. Nach Angaben von TomTom nutzen mehr als 1 Mio. KundInnen die modernen Navis mit Live-Diensten. Die Geräte bekommen dabei über das Mobilfunknetz von Vodafone Informationen und senden gleichzeitig Daten zur Fahrsituation an einen Unternehmensserver. Navis der Konkurrenten Garmin, Medion oder Navigation arbeiten ähnlich.

TomTom versichert, dass es sich bei den gespeicherten Verkehrsdaten um anonymisierte Daten handelt, die mit Einwilligung der Nutzer gespeichert werden. Die Speicherfunktion kann jederzeit vom Benutzer per Klick abgestellt werden, was allerdings auch Auswirkungen auf die Genauigkeit der zukünftigen Routenberechnung hat. Um eine Nutzung der Kundendaten wie durch die niederländische Polizei künftig zu vermeiden, prüft TomTom nun Änderungen bei den Lizenzbestimmungen. Der Verkauf der Verkehrsdaten sei an sich legal, von TomTom in den Nutzungsbedingungen angekündigt und solle auch weiterhin erfolgen. Das Angebot besteht auch in Deutschland; bislang ist aber, so ein Unternehmenssprecher, noch kein vergleichbarer Fall bekannt. TomTom sucht derzeit neue Nischen auf dem Navi-Markt, ohne dabei auf die klassischen Geräte zu setzen, die auf dem Armaturenbrett angebracht werden. Das Unternehmen erwartet, dass der Markt für solche Navigationsgeräte 2011 um mindestens 15% schrumpfen wird, weil verstärkt Tablet-Computer und Smartphones genutzt werden, die in vielen Fällen mit der entsprechenden Software als Navigationsgeräte genutzt werden können.

Der niederländische Automobilclub ANWB äußerte durch seinen Sprecher Markus van Tol Kritik: „TomTom muss seine Kunden darüber informieren, was mit den Daten geschieht, die über Autofahrer gesammelt werden. Wer als Autofahrer ein TomTom-Navi nutzt und es programmiert, der weiß nicht, dass er damit gleichzeitig auch die Polizei darüber informiert, wohin er fährt." Ähnliche Kritik äußerte die auf Informationstechnik spezialisierte Jura-Professorin Corin Prins: „Auch der Staat hat die Pflicht, die Autofahrer zu informieren, wenn er ihr Bewegungsprofil nutzt."

(www.heise.de 28.04.2011; NOZ 28.04.2011, 2; SH-Z 29.04.2011, 8; www.spiegel.de 28.04.2011).

Großbritannien

„News of the World" bittet wegen Abhöraktion um Verzeihung

Rupert Murdochs Zeitungskonzern News International, die Mutterfirma der News corp (Sun, Wall Street Journal) hat sich öffentlich bei acht von 24 Opfern der Abhöraffäre des englischen Boulevard-Blatts „News of the World" (NoW) entschuldigt und bot einigen der Kläger gegen das Revolverblatt eine Entschädigung an. Die britische Boulevardzeitung wird bezichtigt, in mehreren Fällen zwischen 2004 und 2006 Telefone und Mailboxen von Politikern und prominenten Persönlichkeiten illegal abgehört zu haben. Gemäß Presseberichten wurden bei dem von NoW beschäftigten Privatdetektiv Glenn Mulcaire Beweise gefunden, die von über 3.000

abgehörten Opfern zeugen. 24 der vermutlich Betroffenen, darunter unter anderem Schauspielerin Sienna Miller und die ehemalige britische Kultusministerin Tessa Jowell, reichten Klage gegen das Blatt, das von der News-Corp-Tochter News International verlegt wird, ein. Das Murdoch-Unternehmen habe sich bei acht der 24 Kläger entschuldigt und ihnen Entschädigungszahlungen angeboten. Nach Presseberichten soll sich die Gesamthöhe der angebotenen Zahlungen auf rund 100.000 Pfund belaufen. Gegen andere Klagen, die unter anderem von dem Comedian Steve Coogan und dem Jockey Kieren Fallon stammen, wolle sich der Konzern dagegen weiterhin auf juristischem Wege zur Wehr setzen.

In der von News International veröffentlichten Entschuldigung räumte das Unternehmen erstmals öffentlich ein, dass die Abhör-Praktiken in der NoW weit verbreitet waren. Kurz danach druckte NoW folgenden Text: „Hier und heute entschuldigen wir uns öffentlich und uneingeschränkt bei allen Betroffenen. Was Ihnen passiert ist, hätte nicht passieren dürfen. Es war und bleibt inakzeptabel." Noch zu Beginn des Jahres 2011 hatte das Blatt generelle Verfehlungen bestritten und auf Eigenmächtigkeiten des Privatdetektivs zurückgeführt. Die öffentliche Abbitte kam in einer Phase, in der sich die Beweislast gegen das Blatt zunehmend verdichtete. Der Oberste Gerichtshof Großbritanniens hatte zuletzt verfügt, dass News International interne E-Mails über die beiden möglichen Betroffenen Sienna Miller sowie den Sport-Agenten und ehemaligen Tennisspieler Sky Andrew vorlegen müsse. Diese könnten dokumentierern, welche Geschäftsführer des Boulevardblatts von Mulcaires Bespitzelungen Kenntnis gehabt hätten. Außerdem wurden der NoW-Chefredakteur Neville Thurlbeck und der Mitherausgeber Ian Edmondson, der im Januar 2011 seines Postens enthoben worden war, von Scotland Yard befragt.

Einer der Betroffenen ist der Fußballer Wayne Rooney von Manchester United. Über eine Internet-Plattform bestätigte er, dass Scotland Yard ihm entsprechende Dokumente übergeben hat. Einige der Betroffenen haben auf den Vorstoß von NoW abweisend reagiert. Schauspielerin Sienna Miller ließ per Anwalt ausrichten, dass sie keine Vergleichszahlungen angenommen habe. Die frühere Parlamentarier George Galloway wies die Entschuldigung ebenfalls zurück. Andere würden die Offerte hingegen in Erwägung ziehen, hieß es ohne Nennung von Quellen. Rechtsanwalt Rod Dadak stellte unterdessen die Vermutung in den Raum, dass die Entschuldigung gegenüber seinem Mandanten Lewis Slikin nur der Anfang von weiteren Entschädigungsansprüchen sein könnte. Der Jurist rechnet mit Schadensersatzforderungen in Höhe von mehr als 40 Millionen Pfund, weil nun wahrscheinlich weitere potenzielle Opfer Ansprüche stellen könnten. Lord Prescott, dessen ehemalige Beraterin Joan Hammell ebenfalls Opfer der Abhöraffäre ist, hatte wiederholt gefordert, dass Murdochs Übernahmepläne von BSkyB blockiert werden müssten, bis die Abhörvorwürfe komplett aufgeklärt sind. Im Jahr 2007 war ein Reporter des Blattes zu einer Haftstrafe verurteilt worden, weil er Mailboxen der Königsfamilie abgehört hatte. 2009 wurde bekannt, dass auch PolitikerInnen, SportlerInnen und SchauspielerInnen belauscht worden waren. Zu der Entschuldigung habe man sich, so das Blatt, nun aufgrund interner Recherchen entschieden (www.digitalfernsehen.de 11.04.2011; SZ 12.04.2011, 15; SZ 30.04./01.05.2011, 38).

USA

Schüler werden mit GPS überwacht

Im Schulbezirk Änaheim in Südkalifornien müssen SchülerInnen der 7. und 8. Klasse ein GPS-Tracking-Gerät mit sich tragen, wenn sie mehr als dreimal unentschuldigt gefehlt haben. Ein automatischer Anruf erinnert die SchülerInnen morgens an den Schulbesuch. Auf ihrem Schulweg und während des Tages werden sie von der Schulbehörde über das Gerät geortet. Ein Anfang 2011 gestarteter Pilotversuch dauert 6 Wochen. Pro Tag geben die Schulen für die Überwachung 8 Dollar je SchülerIn aus. Auch im US-Bundesstaat Texas testeten einige Schulen den Schulschwänzer-Alarm (SZ 24.02.2011, 10).

Technik-Nachrichten

E-Mail-Fingerabdrücke zur Schreiberidentifikation

Einem Team der Concordia University in Montreal/Kanada ist es gelungen, den Autor einer E-Mail mit 80 bis 90% Trefferwahrscheinlichkeit aus einer Gruppe von Verdächtigen herauszufischen. Diese Methode soll Beweisprobleme vor Gericht lösen, um etwa Verfasser von Viren-Mails oder kinderpornografischen Mails zu fassen. Eine Software sucht hierfür z.B. nach spezifischen Tipp- und Grammatikfehlern, wie sie nicht bei anderen Verdächtigen auftauchen - also eine Art Fingerabdruck der Schriftsprache. In einem Test durchsuchten die Forschenden über 200.000 E-Mails von 158 Mitarbeitenden des Energiekonzern Enron. Zehn Probe-Mails pro Person reichten meist, um die Autorenschaft unter 10 Verdächtigen zu identifizieren (Der Spiegel 11/2011, 120).

Dreidimensionale Gesichtsbilder

Die japanische Firma Tohto C-Tech hat eine Lösung entwickelt, wie sich aus den mit einer Stereo-Kamera gefilmten Gesichtsbildern ein dreidimensionales Modell (3D-Modell) des Kopfes errechnen lässt. Die Rechenleistung einer Grafikkarte soll dafür ausreichen. Zweck und vorrangiges Anwendungsfeld die-

ser Technik ist für das Unternehmen die Identifikation von Personen (WIK 2/2011, 8)

iPhone-Apps spähen Nutzende aus

Gemäß einer aktuellen Studie von Manuel Egele von der Technischen Universität (TU) Wien und weiteren KollegInnen verletzt mehr als die Hälfte von 1.400 untersuchten Apps ohne Rückfrage die Privatsphäre der Nutzenden, indem sie die Identifikationsnummer des iPhones - eine 40stellige Hexadezimalzahl - versendet. In Verbindung mit Facebook- oder Google-Konten lassen sich daraus Nutzungsprofile erstellen und Namen zuordnen. Fünf der geprüften Apps durchsuchten zudem das Adressbuch; 36 gaben ungefragt die aktuellen Geodaten weiter (Lemos, www.heise.de 02.02.2011 - Technology Review; WIK 1/2011, 7, Download der Studie unter http://www.iseclab.org/papers/egele-ndss11.pdf).

Russen und NATO entwickeln gemeinsam Sprengstoff-Detektor

Russland und die NATO wollen gemeinsam eine neue Sprengstoffabwehr entwickeln, um sich wirksamer vor Terroranschlägen zu schützen. Ein Sensor mit dem Projektnamen „Standex“ (Stand-off Detection of Explosives) soll die Enttarnung von SelbstmordattentäterInnen ermöglichen. An der wissenschaftlichen Kooperation nimmt u.a. auch das deutsche Fraunhofer-Institut für Chemische Technologie bei Karlsruhe teil. Standex soll eingesetzt werden, um große Menschenansammlungen mit unauffälligen, festinstallierten Geräten auf Sprengstoff zu scannen. Damit sollen Selbstmordattentate wie der Anschlag auf dem Moskauer Flughafen Domodedowo verhindert werden, wo sich Ende Januar ein Angreifer mit 37 weiteren Menschen in die Luft sprengte und tötete. Standex soll ohne auffällige Sicherheitsschleusen auskommen, die TerroristInnen warnen könnten. Ein hochrangiger russischer Diplomat erklärte, die Scanner könnten noch im Laufe des Jahres 2011 bei Tests in der Pariser U-Bahn erprobt werden: „Bis zu deren endgültiger Fertigstellung dauert es aber wohl noch drei Jahre.“ 2014 finden im russischen Sotschi die Olympischen Winterspiele statt (Der Spiegel 12/2011, 87).

Intelligente Videoüberwachung „Smart Eyes“

Ein neues Videoerkennungssystem des Fraunhofer-Instituts für Angewandte Informationstechnik soll zu mehr Sicherheit bei Großveranstaltungen führen. Die lernfähige Software kann Auffälligkeiten in einer Menschenmenge entdecken und etwa aufspringende Fans von passiven ZuschauerInnen unterscheiden. Im März wurde das System „Smart Eyes“ erstmals während des Zweitliga-Spiels Fortuna Düsseldorf gegen den VfL Osnabrück getestet. Smart Eyes eignet sich auch für andere Lebensbereiche, etwa um Verstöße im Straßenverkehr festzustellen. Die Fraunhofer-Gesellschaft koordinierte im Rahmen des EU-Projektes „Searise“ die Entwicklung von Smart Eyes. Die deutsche Bundesregierung fördert ähnliche Projekte zu Videoüberwachungen mit insgesamt rd. 12 Mio. Euro (Der Spiegel 10/2011, 19).

Nutzerkontrolle per Eye-Tracking

In dem Laptop des chinesischen Computerherstellers Lenovo steckt die von schwedischen Spezialisten entwickelte Technologie des Eye Trackings. Der Computer kann die Blicke der BetrachterIn verfolgen, indem eine Kamera zweimal pro Millisekunde den Grad der Lichtreflexion misst, die je nach Ausrichtung der Pupille unterschiedlich ausfällt. Eye Tracking war bislang vor allem ein Werkzeug in der Marktforschung. Entwickler meinen, die Technik könne in wenigen Jahren Bestandteil unseres Alltags werden. Ein Blick könne dann genügen, um am PC eine unliebsame E-Mail im Papierkorb verschwinden zu lassen oder um einen Kartenausschnitt heran zu zoomen (Bernau SZ 09.03.2011, 22).

USA bietet fliegendes Kommunikationsnetz gegen Diktaturen

Wenn, wie in Ägypten, in Libyen oder 2009 nach den Wahlen im Iran Diktatoren das Internet abschalten, sind die USA offenbar in der Lage, es wieder anzuschalten. Die US-Airforce hat einige ihrer Propellermaschinen vom Typ EC-130 „Hercules“ so technisch aufgerüstet, dass sie in ihrem Überfluggebiet einen Internet- und Handyzugang ermöglichen können. Damit wollen die USA oppositionellen Bewegungen helfen, sich gegen den Willen der betreffenden Regime zu organisieren. John Arquilla, Spezialist für Militärtechnologie, erläuterte: Wir verfügen sowohl über stalliten- als auch über nichtsatellitengestützte Anlagen, damit die Menschen vor Ort wieder online gehen können.“ Details verriet der Rüstungsexperte jedoch nicht. Rundfunk- und Fernsehdienste der „Commando Solo“-Flugzeuge sind bereits früher genutzt worden, z.B. 1997 in Bosnien-Herzegowina oder 2001 während des Afghanistan-Einsatzes „Enduring Freedom“. Damals wurden auf diesem Weg Nachrichten an die Bevölkerung übermittelt (Der Spiegel 10/2011, 76).

Lockheed EC-130 „Hercules“

Quelle: Wikipedia, US Airforce
http://www.af.mil/shared/media/photodb/photos/990101-F-5502B-002.jpg

Rechtsprechung

BVerfG

Kein Verwertungsverbot nach polizeilicher Alkoholkontrolle

Eine Kammer des 2. Senats des Bundesverfassungsgerichts hat mit Beschluss vom 24.02.2011 entschieden, dass die Ergebnisse einer Blutprobe zur Feststellung des Blutalkoholgehalts selbst dann vor Gericht verwertbar sein kann, wenn der Test von einem Polizisten angeordnet wurde, der dafür eigentlich nur bei „Gefahr im Verzug" zuständig ist (Az. 2 BvR 1596/10 u. 2346/10). Blutproben müssen grundsätzlich von einem Richter angeordnet werden. Mit dieser Entscheidung gerät dieser viel kritisierte Richtervorbehalt weiter unter Druck. Im entschiedenen Fall hatte ein Beamter einen betrunkenen Radfahrer nachts zur Blutprobe geschickt, weil beim zuständigen Amtsgericht keine Nachtbereitschaft existierte. Das begründet noch keine „Gefahr im Verzug". Trotzdem erklärte das BVerfG den Promilletest für verwertbar. Die Mehrheit der Bundesländer und der Richterbund halten den Einsatz von Richtern bei diesem massenhaften Routineeingriff für überflüssig (SZ 16.03.2011, 8).

BGH

Deutsche Gerichtszuständigkeit nur bei inhaltlichem Inlandsbezug

Der Bundesgerichtshof (BGH) hat in einem Urteil vom 29.03.2011 entschieden, dass deutsche Gerichte bei der Verletzung von Persönlichkeitsrechten im Internet (nur) dann zuständig sind, wenn die Inhalte einen Inlandsbezug haben (Az. VI ZR 111/10). Dies sei der Fall, wenn die Interessenkollision zwischen Persönlichkeitsrecht und Berichterstattung tatsächlich im Inland eintritt. Der BGH wies die Klage eines russischen Geschäftsmanns mit Wohnsitz in Deutschland ab. Der hatte bei einem Klassentreffen in Moskau eine Bekannte getroffen, die mittlerweile in den USA lebt. Die Frau hatte darüber einen wohl wenig netten Bericht geschrieben und ihn in russischer Sprache und kyrillischer Schrift auf dem Internetportal www.womanineurope.com veröffentlicht. Der Betreiber des Portals hat seinen Sitz in Deutschland. Das reiche nicht aus, entschied der BGH. Weder der Serverstandort noch die Möglichkeit, den Text auch in Deutschland abzurufen, begründeten die Zuständigkeit deutscher Gerichte (www.sueddeutsche.de 30.03.2011).

KG Berlin

Google Street View-Aufnahmen nicht zu beanstanden

Der 10. Zivilsenat des Kammergerichts (KG) Berlin hat mit Beschluss vom 25.10.2010 die Beschwerde der Eigentümerin eines Einfamilienhauses zurückgewiesen, die vor dem Landgericht (LG) erfolglos versucht hatte, der Google Inc. die Aufnahme ihres Hauses im Umfeld von Berlin zu untersagen (Az. 10 W 127/10). Sie befürchtete, dass sie und ihre Familie sowie der private Bereich ihres Vorgartens und der Wohnung auf den Fotos erkennbar sein könnten. Soweit keine Fotos unter Überwindung einer Umfriedung gefertigt werden oder die Fotos eine Wohnung darstellen, sei es, so das KG, rechtlich nicht zu beanstanden, wenn für die Internetseite Google Street View Aufnahmen eines Hauses von der offenen Straße aus gefertigt werden. Die bloße Abbildung von Häuserzeilen oder Straßenzügen sei rechtlich nicht relevant, so zuvor das LG. Eine hinreichende Wahrscheinlichkeit für die Fertigung darüber hinausgehender unerlaubter Aufnahmen habe die Antragstellerin jedoch nicht dargelegt. Sie könne daher nicht bereits die Untersagung von Fotos im Wege des vorbeugenden Rechtsschutzes verlangen. Außerdem lasse Google die Gesichter von Personen anonymisieren und räume die Möglichkeit ein, Gebäudeaufnahmen vor ihrer Veröffentlichung gleichfalls unkenntlich zu machen (Vorinstanz LG Berlin, B. v. 13.09.2010, Az. 37 O 363/10; PM Die Präsidentin des Kammergerichts 15.03.2011).

BAG

Kein Abberufung eines internen bDSB zwecks Bestellung eines Externen

Das Bundesarbeitsgericht (BAG) hat am 23.03.2011 entschieden, dass die Bestellung zur betrieblichen Datenschutzbeauftragten (bDSB) nicht mit der Begründung widerrufen werden kann, dass die Aufgaben zukünftig von einem externen Dritten wahrgenommen werden sollen oder dass der Beauftragte Mitglied im Betriebsrat sei (Az. 10 AZR 562/09). Die seit 1981 bei dem beklagten Unternehmen beschäftigte Klägerin war im Jahr 1992 zur Datenschutzbeauftragten des Unternehmens und deren 100%iger Tochtergesellschaft berufen worden. Für die Aufgabe waren ca. 30% ihrer Arbeitszeit vorgesehen. Seit 1994 ist die Klägerin auch Mitglied im Betriebsrat des beklagten Unternehmens. Am 12.08.2008 beschlossen das Unternehmen und deren Tochtergesellschaft, die Aufgaben des Beauftragten für den Datenschutz zukünftig konzernweit einheitlich durch einen externen Dritten wahrnehmen zu lassen und widerriefen deshalb die Bestellung der Klägerin. Das Unternehmen sprach zudem gegenüber der Klägerin eine Teilkündigung dieser Aufgabe aus. Hiergegen wendete sich die Klage, der die Vorinstanzen stattgegeben hatten. Auch die Revision des beklagten Unternehmens vor dem BAG hatte keinen Erfolg.

Gemäß dem BAG gewährt die § 4f Abs. 3 Satz 4 BDSG und § 626 BGB dem Beauftragten für den Datenschutz einen besonderen Abberufungsschutz. Damit solle dessen Unabhängigkeit und die weisungsfreie Ausübung des Amtes gestärkt werden. Eine Abberufung sei nur aus wichtigem Grund möglich, wenn eine Fortsetzung des Rechtsverhältnisses für den Arbeitgeber unzumutbar sei. Zwar sei der Arbeitgeber bei der erstmaligen Bestellung frei, ob er einen internen oder externen Datenschutzbeauftragten bestelle. Habe er hingegen einen internen Beauftragten bestellt, könne er nicht dessen Bestellung allein mit der Begründung widerrufen, er wolle nunmehr einen Externen konzernweit mit dieser Aufgabe beauftragen. Allein in einer solchen Organisationsentscheidung liege kein wichtiger Grund. Ebenso wenig rechtfertige die bloße Mitgliedschaft im Betriebsrat, die Zuverlässigkeit eines Beauftragten für den Datenschutz in Frage zu stellen. Auf konkrete Pflichtenverstöße hätten sich die Beklagten nicht berufen.

LAG Hessen

Entschädigung wegen illegaler Videoüberwachung

Das Landesarbeitsgericht (LAG) Hessen entschied mit Urteil vom 25.10.2010, dass ein Arbeitgeber einer Mitarbeiterin eine Entschädigung in Höhe von 7.000 Euro bezahlen muss, weil er diese mindestens seit Juni 2008 an ihrem Arbeitsplatz permanent mit einer Videokamera überwacht hatte (Az.: 7 Sa 1586/09). Die 24-jährige kaufmännische Angestellte arbeitete in einer hessischen Niederlassung eines bundesweit tätigen Unternehmens. Gegenüber der Eingangstür des Büros hatte der Arbeitgeber eine Videokamera angebracht, die nicht nur auf den Eingangsbereich, sondern im Vordergrund auch auf den Arbeitsplatz der Klägerin gerichtet war. Mit der im Oktober 2008 eingegangenen Klage machte die Mitarbeiterin Schadensersatzansprüche wegen Persönlichkeitsverletzung geltend. Das Arbeitsgericht Wetzlar hatte den Arbeitgeber zur Zahlung einer Entschädigung von 15.000 Euro verurteilt (Urteil vom 01.09.2009 – 3 Ca 211/08).

Die gegen dieses Urteil eingelegte Berufung hatte nur zum Teil Erfolg. Weder das Arbeitsgericht noch das Landesarbeitsgericht ließen die Einwendungen des Arbeitgebers gelten. Der Arbeitgeber hatte sich im Prozess damit verteidigt, dass die Kamera nicht ständig in Funktion gewesen und nur zur Sicherheit der Mitarbeiter angebracht worden sei, weil es in der Vergangenheit schon zu Übergriffen auf Mitarbeiter gekommen sei. Nach Ansicht des LAG war der Eingriff in das allgemeine Persönlichkeitsrecht der Mitarbeiterin dennoch unverhältnismäßig. Eine Ausrichtung der Kamera nur auf den Eingangsbereich des Büros wäre möglich gewesen. Es sei auch unerheblich, dass die Kamera nicht ständig in Funktion war. Allein die Unsicherheit darüber, ob die Kamera tatsächlich aufzeichne oder nicht, habe die Mitarbeiterin einem ständigen Anpassungs- und Überwachungsdruck ausgesetzt, den sie nicht hinnehmen musste, nachdem sie sich bereits früh gegen die Installation der Videokamera gewandt hatte. Das LAG Hessen hielt die Überwachung für „eine schwerwiegende und hartnäckige Verletzung des informationellen Selbstbestimmungsrechts“. Nach Abwägung aller Umstände sei die Verurteilung zu einer Entschädigung von 7.000 Euro gerechtfertigt. Die Zubilligung einer Geldentschädigung im Falle einer solchen schweren Persönlichkeitsrechtsverletzung beruhe auf dem Gedanken, dass ohne einen Entschädigungsanspruch Verletzungen der Würde und Ehre des Menschen häufig ohne Sanktionen blieben mit der Folge, dass der Rechtsschutz der Persönlichkeit verkümmern würde. Bei der Entschädigung stehe regelmäßig der Gesichtspunkt der Genugtuung des Opfers im Vordergrund (beck-aktuell. beck.de; WiK 2/2011, 8).

Buchbesprechung

Martin Zilkens,
Datenschutz in der Kommunalverwaltung - Recht-Technik-Organisation,
3. Aufl. Erich Schmidt Verlag,
Berlin 2011, 680 S.

tw Die Rechtsgebundenheit personenbezogener Datenverarbeitung ist vor allem in Kommunen, also bei Gemeinden, Städten und Landkreisen, ein Problem, weil dort die auf lokaler Basis erfolgenden Aufgabenerledigungen aus den unterschiedlichsten Bereichen zusammenlaufen, hierbei der Einsatz von Informationstechnik inzwischen Selbstverständlichkeit ist und Datenschutz- und Datensicherheits-Know-how oft nicht vorausgesetzt werden kann. Insofern ist das Thema von Zilkens von höchster Relevanz. Ein Handbuch zum Datenschutz in der Kommunalverwaltung kommt der Quadratur des Kreises gleich. Es muss sein: umfassend und zugleich einfach verständlich, auf dem aktuellen Stand der Praxis und der Wissenschaft und Technik und zugleich geeignet für die SachbearbeiterIn in einer kommu-

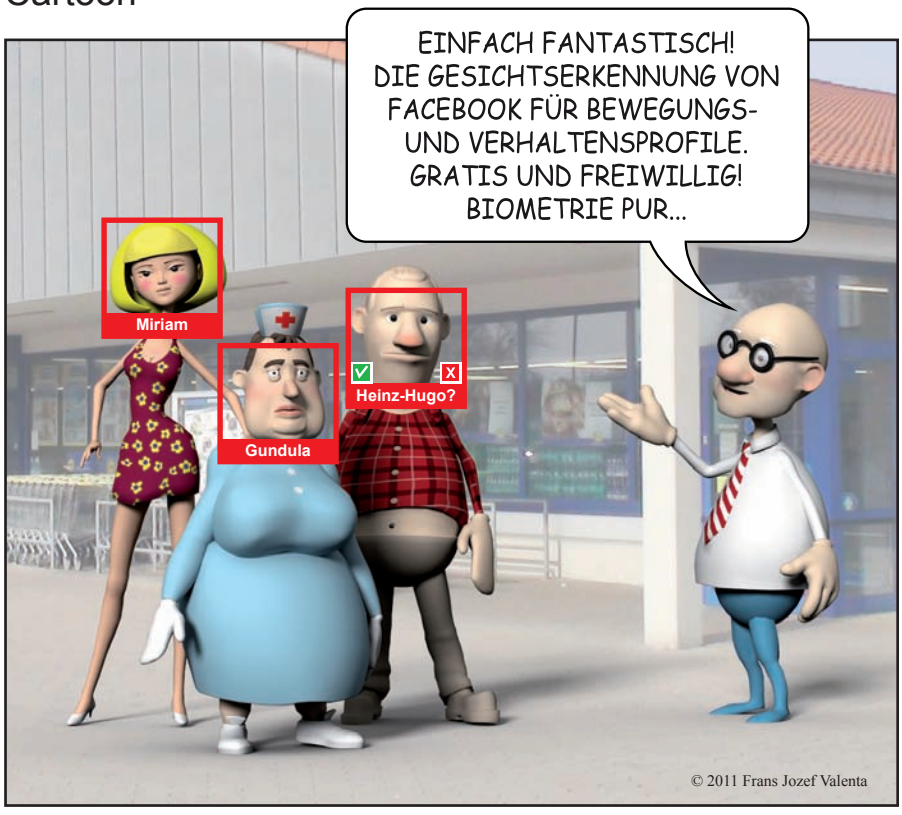
nalen Fachverwaltung, adressiert an die Leiter der Kommunalverwaltung, die Mitglieder der Ratsversammlung, die Bediensteten in dieser Verwaltung und nicht zuletzt die betroffenen BürgerInnen. Es muss die vielfältigen gesetzlichen Grundlagen darstellen und die wissenschaftlichen Diskussionen hierzu wiederspiegeln und zugleich so überschaubar sein, dass auch der Laie sich orientieren kann. Wer meint, diese Quadratur des Kreises sei unmöglich, der oder die kann sich von dem Handbuch von Zilkens eines Besseren belehren lassen. Zilkens schafft es tatsächlich auf 680 Seiten, dieser Quadratur nahezukommen.

Nach einer ersten Auflage im Jahr 1991 und einer zweiten im Jahr 2008 folgte kurzfristig nun die dritte, „völlig neu bearbeitete und erweiterte Auflage". Der als Datenschutzbeauftragter der Landeshauptstadt Düsseldorf tätige Autor weiß auf Basis seiner langjährigen Tätigkeit wie wegen des sehr gewissenhaften Auswertens der vorhandenen Literatur einschließlich Internet-Veröffentlichungen, wovon er schreibt. Und er tut dies als Jurist in einer Art und Weise, die von einem hohen technischen Verständnis zeugt und zugleich von der DatenschutzlaiIn verstanden wird. Für die Letztere liefert er nicht nur praktische Problemlösungen für spezifische Einzelfälle, sondern zugleich eine allgemeine umfassende Einführung in das Datenschutzrecht. Er bearbeitet zudem praktisch alle Themen, die auf kommunaler Ebene relevant sind und werden können: Sozialrecht, öffentliches Gesundheitswesen, betriebsärztlicher Dienst, Ausländerwesen, Melderecht, Personalausweis- und Passwesen, Schule, Ratsarbeit, Straßenverkehrswesen, Beschäftigtendatenschutz, Internetdatenverarbeitung, Kommunalaufsicht, innere Organisation der Verwaltung, Datensicherheit, privatisierte Betriebe..., um nur die wichtigsten Spezialüberschriften zu benennen. Am Ende befasst sich Zilkens dann noch mit der laufenden bzw. notwendigen Modernisierung des Datenschutzes, mit den europarechtlichen Bezügen sowie dem Informationsfreiheits- und sogar dem Verbraucherinformationsrecht.

Der Autor selbst kommt aus Nordrhein-Westfalen, weshalb das dortige Landesrecht, auch bzgl. des teilweise sehr unterschiedlichen Kommunalrechts, zur Grundlage genommen wird. Das Buch ist aber auch in allen anderen Bundesländern gut gebrauchbar, zumal es bei den wichtigen Rechtsquellen im Rahmen des Machbaren auch die relevanten Regelungen der anderen Länder aufführt. Es beschreibt nicht nur die abstrakte Rechtslage, sondern garniert diese mit einer Vielzahl von praktischen Beispielen, die offensichtlich auch teilweise den eigenen Erfahrungen entspringen, aber auch denen der in der Datenschutzkontrolle der Kommunen tätigen Landesbeauftragten, wie sie sich aus deren Tätigkeitsberichten sowie deren Internet-Veröffentlichung ergibt. Dabei zitiert er korrekt und einfach recherchierbar, so dass nicht nur den LaiInnen, sondern auch den ExpertInnen und WissenschaftlerInnen der Griff zu diesem Buch empfohlen werden kann. Natürlich erfolgt insofern keine vertiefte Bearbeitung - das wäre definitiv zu viel verlangt, doch verweist der Autor zu jedem Thema auf relevante Quellen, die eine valide Grundlage für weitere Recherchen abgeben können. Dies ist insbesondere in den spezialgesetzlich geregelten Bereichen besonders erfreulich, bei denen Quellen ansonsten nur in der verstreuten Fachliteratur zu finden sind, während hier alles zwischen zwei Buchdeckel passt.

Die Arbeit von Zilkens ist nicht nur fleißig, aktuell, gut recherchiert und gut les- und verstehbar, sondern auch klar in den Positionen. Dabei vermeidet der Autor oft eine eigene Positionierung, stellt aber, insbesondere wenn bei einem Streit noch keine feste Rechtsmeinung besteht, die unterschiedlichen Sichtweisen dar. Dem Handbuchcharakter kommen zudem eine übersichtliche Strukturierung und Gliederung sowie ausführliche Abkürzungs-, Literatur- und Stichwortverzeichnisse zugute. Es ist also ebenso geeignet für die Lösung eines Einzelproblems, zur Grundausbildung einer DatenschützerIn wie als Suchmittel für die ExpertIn. Die Investition von stolzen 80 Euro für den InteressierteN sowie für eine Bibliothek für Interessierte ist, wem das Anliegen der Verwirklichung des Rechts auf informationelle Selbstbestimmung auf kommunaler Ebene ernst ist, gut angelegt.

Cartoon



Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Pressemitteilung 14/2011 Bonn/Berlin, 16. Mai 2011

Für Elektromobilität, aber gegen gläserne Autofahrer!

Anlässlich der Veröffentlichung des zweiten Berichtes der Nationalen Plattform Elektromobilität fordert der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, Aspekte des Datenschutzes bei der Elektromobilität frühzeitig zu berücksichtigen.

Peter Schaar: „Die neu entstehende Infrastruktur aus Ladesäulen, die Anbindung an intelligente Stromnetze sowie an elektronische Kommunikationsdienste darf nicht zu einer Kontrolle des Fahrverhaltens der Nutzer von Elektromobilen führen. So sehr ich auch nachhaltige Mobilitätskonzepte begrüße, dürfen über den Umweg Elektromobilität keine umfangreichen Bewegungsbilder der Nutzer entstehen, aus denen sich Rückschlüsse auf Gewohnheiten und Aufenthaltsorte der Betroffenen ziehen lassen. Durch frühzeitige Berücksichtigung von Datenschutzbelangen können umweltfreundliche Mobilitätskonzepte ohne Abstriche am informationellen Selbstbestimmungsrecht realisiert werden."

Schaar fordert hinsichtlich der Abrechnung von Fahrstrom und der neuen Ladeinfrastruktur die Datensparsamkeit sowie die Möglichkeit zur anonymen Inanspruchnahme von Elektrofahrzeugen zu berücksichtigen. Auch die Datensicherheit muss gewährleistet werden, schließlich sollen die Elektromobile langfristig als Speicher für Strom dienen und mit den Energiesystemen in Haushalten vernetzt werden. Bedauerlicherweise, so Schaar, wurden die Datenschutzbeauftragten an den entsprechenden Modellprojekten bisher nicht beteiligt.

Schaar signalisiert seine Bereitschaft, an der Entwicklung entsprechender Konzepte ergebnisorientiert und konstruktiv mitzuwirken.