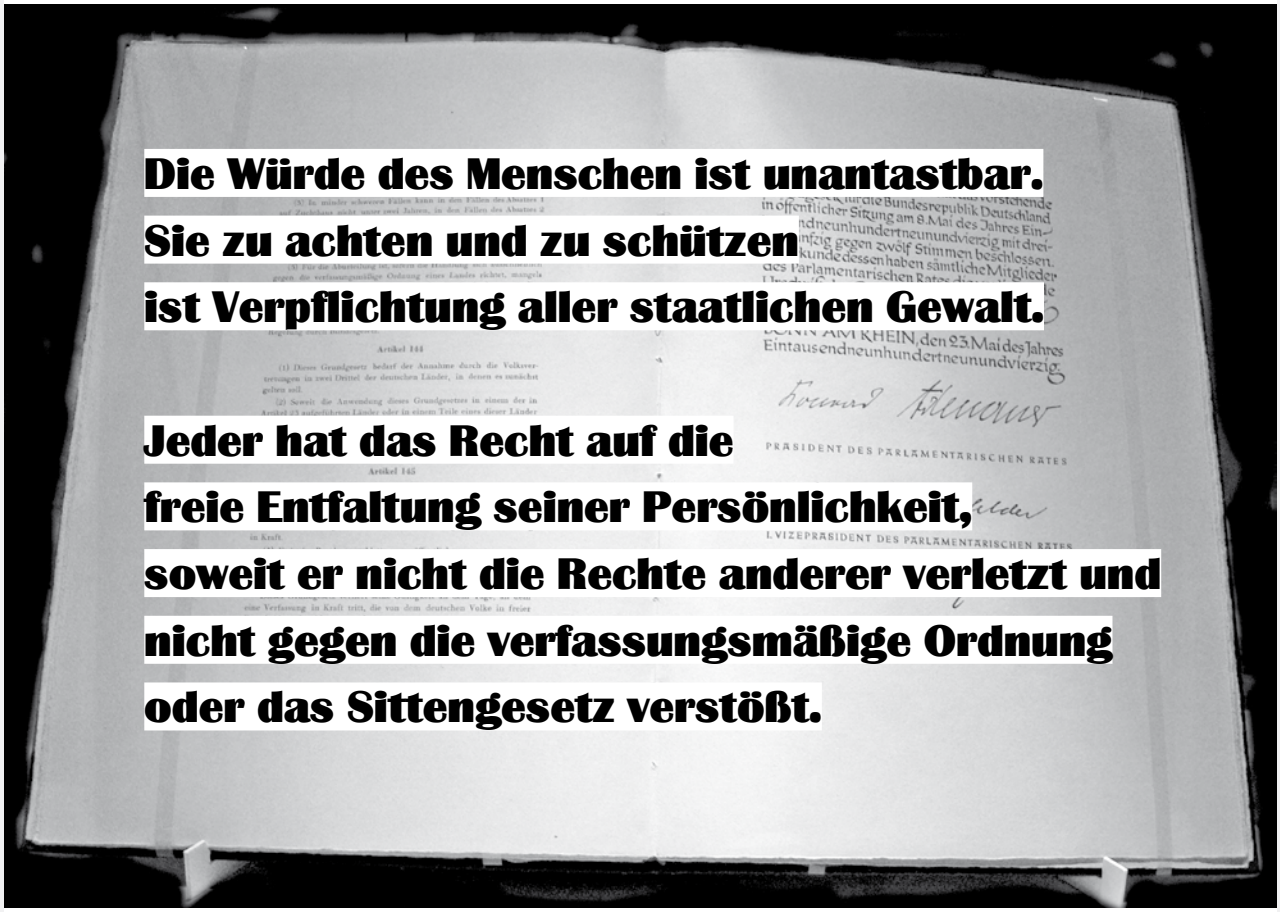
H 7625

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

32. Jahrgang 2015 Einzelpreis: 7 EUR **2/2015 – Juni 2015**

Perspektiven des Datenschutzes



BigBrotherAwards 2015

ISSN 0938-3476

• Cyberpeace-Kampagne • Faire Computer • Kampfdrohnen •

FIfF Kommunikation

Titelbild: Wortlaut von Art. 1 Abs. 1 und Art. 2 Abs. 2 GG über Faksimile des Grundgesetzes von 1949, Foto: Andreas Praefcke

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.

Inhalt

Ausgabe 2/2015

inhaltt

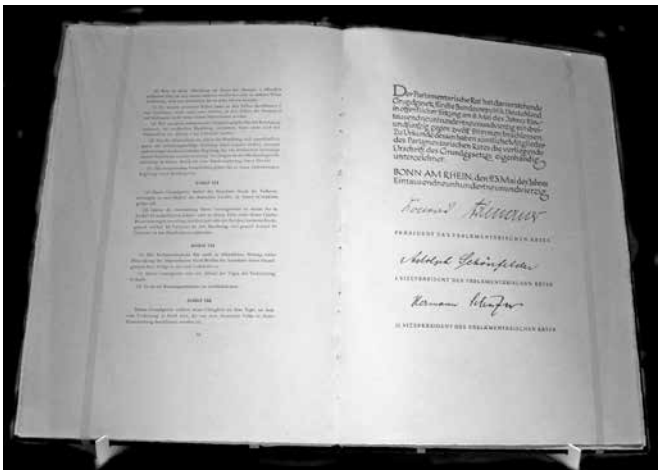
Editorial

Datenschutz – ein Thema, das im Zentrum der Auseinandersetzung mit *Informatik und Gesellschaft* steht und auch das FIfF seit Anbeginn beschäftigt. Als verfassungsmäßiges Grundrecht, abgeleitet durch das Bundesverfassungsgericht als *informationelle Selbstbestimmung* aus dem allgemeinen Persönlichkeitsrecht, ist der Datenschutz ein Grundbaustein der menschengerechten Informationsverarbeitung. 1890 formuliert von Samuel D. Warren und Louis D. Brandeis als „*Right to be let alone*"[1], die „*Geburtsurkunde für den modernen Datenschutz*"[2], in Deutschland erstmals kodifiziert im Hessischen Landesdatenschutzgesetz von 1970. Ulrich Seidel prägte den modernen Datenschutzbegriff 1970 in seinem Aufsatz *Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten*[3], den wir als Retrospektive in dieser Ausgabe nachdrucken; Seidel wurde 1986 mit dem Bundesverdienstkreuz ausgezeichnet.

Im Zentrum unseres Schwerpunkts *Perspektiven des Datenschutzes*, den wir mit einem eigenen Editorial der Schwerpunktredaktion, Eberhard Zehendner und Stefan Hügel, einleiten, stehen zwei Beiträge von und mit dem *Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit*, Lutz Hasse: ein Aufsatz, in dem er selbst seine Arbeit beschreibt, und ein Interview, in dem er Perspektiven des Datenschutzes aus seiner Sicht aufzeigt. Weitere Beiträge des Schwerpunkts stammen von Dagmar Boedicker, Bärbel Heide Uhl, Stefan Ullrich, Jörg Pohle, Angela Meindl und Carsten Seeger.

Obwohl der Datenschutz in Deutschland quasi Verfassungsrang hat, steht er unter Druck. Geschäftsmodelle, die auf der Nutzung privater Daten aufbauen, werden durch einen starken Datenschutz behindert. Auch die Ausspähung der Bevölkerung durch Geheimdienste – Stichwort NSA- und BND-Skandal – und Strafverfolgungsbehörden – Stichwort Vorratsdatenspeicherung – steht dem Datenschutz entgegen. Kein Wunder also, dass sich auch die Gegner eines starken Datenschutzes formieren – aktuell in der Debatte um die EU-Datenschutz-Grundverordnung. Dabei werden zwei Grundprinzipien des Datenschutzes in Frage gestellt: die Datensparsamkeit und die Zweckbindung. In einem offenen Brief an EU-Kommissionspräsident Jean-Claude Juncker, der unter anderem von *European Digital Rights* initiiert wurde, wird an das Versprechen erinnert, dass die Grundverordnung keinesfalls hinter das Datenschutzniveau der Richtlinie 95/46/EG von 1995 zurückfallen werde. 66 Organisationen weltweit, auch das FIfF, haben sich dem Appell angeschlossen; wir dokumentieren den Brief und die Liste der Unterzeichner in dieser Ausgabe.

Datenschutz und Geheimdienste standen auch im Mittelpunkt der diesjährigen *BigBrotherAwards*. Nach einer einleitenden Zusammenfassung dokumentieren wir vier der Laudationes, die im Rahmen der Gala am 17. April 2015 in Bielefeld gehalten wurden: Zu *Hello Barbie* in der Kategorie *Technik*, einer Puppe, die mit Mikrofon, Lautsprecher und WLAN ausgerüstet ist und mit der – selbstverständlich nur zum Zweck der Spracherkennung – bereits Kinder ausspioniert werden können; zum *Bundesnachrichtendienst* in der Kategorie *Behörden & Verwaltung*, der massenweise Telekommunikationsdaten an die NSA übermittelt hat; zu Crowdsourcing-Plattformen wie *Amazon Mechanical Turk* und *Upwork* (vormals *Elance-oDesk*) in der Kategorie *Wirtschaft*, von denen wir nur hoffen können, dass sie nicht künftig unsere gesamte Arbeitswelt prägen werden; und zu Bundesinnenminister *Thomas de Maizière* und seinem Vorgänger *Hans-Peter Friedrich* in der Kategorie *Politik*, die sich offenbar in Brüssel systematisch gegen eine starke Datenschutz-Grundverordnung einsetzen.



Unsere Kampagne *Cyberpeace* führen wir gleichzeitig fort. Am 17.-19. April 2015 fand in Berlin unser Kampagnenwochenende statt, Thomas Reinhold berichtet davon. Auch regional gibt es eine Reihe von Aktivitäten; Hans-Jörg Kreowski und Raffael Rittmeier berichten von der Arbeit der Cyberpeace-Kampagne in Bremen. Einen Vorgeschmack auf unsere diesjährige FIfF-Konferenz am 6.-8. November 2015 in Erlangen – *Kommerzialisierung des Sozialen, Markt und Macht im Zeitalter digitaler Kompletterfassung* – gibt die Ankündigung von Felix Freiling.

Abgerundet wird diese Ausgabe durch die Kolumnen zu *Cyberpeace* – diesmal von Stefan Hügel – und zu *Faire Computer* – wie gewohnt von Sebastian Jekutsch –, und dem *Log*, das in der letzten Ausgabe gefehlt hat und deswegen dieses Mal etwas länger ausfällt.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel
für die Redaktion

Anmerkungen

1 *Das Recht auf Privatheit – The Right to Privacy. Weiterentwicklung des Common Law, dt. Übersetzung von Marit Hansen und Thilo Weichert in FIfF-Kommunikation 2/2012, Seite 45-58, im Original: Harvard Law Review, Vol. IV, No. 5, 15 December 1890,*

2 *So Weichert in seinen Anmerkungen zur Übersetzung, a.a.O., Seite 58*

3 *Ulrich Seidel (1970): Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, Neue Juristische Wochenschrift 1970, Seite 1581-1583*

Der Brief

„Unter eine solche Geschichte lässt sich kein Schlussstrich ziehen“

Die wohlfeilste Art des Stolzes hingegen ist der Nationalstolz … jeder erbärmliche Tropf, der nichts in der Welt hat, darauf er stolz seyn könnte, ergreift das letzte Mittel, auf die Nation, der er gerade angehört, stolz zu seyn: hieran erholt er sich und ist nun dankbarlich bereit, alle Fehler und Thorheiten, die ihr eigen sind, mit Hand und Fuß zu vertheidigen.
(Arthur Schopenhauer)

Und selbst wenn alles scheiße ist, Du pleite bist und sonst nichts kannst
dann sei doch einfach stolz auf Dein Land.
(Kraftklub)

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

in Deutschland brennen wieder Asylbewerberheime.

Am 26. Mai 1993 beschloss der Deutsche Bundestag ein neues Asylrecht. Die uneingeschränkte Garantie in Artikel 16 (ursprünglich in Artikel 16, heute in Artikel 16a) des Grundgesetzes, „*Politisch Verfolgte genießen Asylrecht*“, wurde faktisch beseitigt und durch die „Drittstaatenregelung“ ersetzt. Wir erinnern uns: Zu der Zeit gab es eine Reihe von fremdenfeindlichen Brandanschlägen, denen mehrere Menschen zum Opfer fielen. Auch sonst seriöse Zeitungen berichteten von einer „Asylantenflut“. Einer dieser Anschläge forderte nur wenige Tage nach dem Beschluss den Bundestages, am 29. Mai 1993 in Solingen, fünf Todesopfer. Durch die Änderung des Grundgesetzes wurde den rechtsgerichteten Brandstiftern signalisiert: Politische Gewalt zahlt sich aus.

Europarechtlich fanden die neuen Verfassungsprinzipien später Eingang in das Dubliner Übereinkommen und seine Folgeverträge Dublin II und Dublin III. Sie erlegen den Anliegerstaaten des Mittelmeers durch ihre Randlage eine erhebliche Last auf, während Staaten wie Deutschland bisher versuchten, sich der Verantwortung zu entziehen – kaum ein Flüchtling wird über die Nordsee zu uns kommen. Programme zur Rettung von Flüchtlingen, die auf dem Mittelmeer schiffbrüchig werden und ertrinken, wie *Mare Nostrum*, wurden längere Zeit nicht mehr finanziert. Gleichzeitig sind zigtausende Menschen in den letzten Jahren im Mittelmeer ertrunken. Inwieweit Aufnahmequoten für Flüchtlinge dieser Situation abhelfen, bleibt abzuwarten.

In diesen Tagen begehen wir den siebzigsten Jahrestag des Endes des Zweiten Weltkrieges. Schaltet man den Fernseher ein, sieht man auf vielen Kanälen immer wieder die deutsche Geschichte mit der nationalsozialistischen Herrschaft. Doch es mutet häufig an, als ob es jemand anders wäre, der damals die Verantwortung getragen hat, wir damit überhaupt nichts zu tun haben. „*Der 8. Mai war ein Tag der Befreiung. Er hat uns alle befreit von dem menschenverachtenden System der nationalsozialistischen Gewaltherrschaft*“, so der damalige Bundespräsident Richard von Weizsäcker in seiner zu Recht vielbeachteten und -gelobten Rede zum vierzigsten Jahrestag am 8. Mai 1985. Doch wen hat er wirklich befreit? Die Deutschen vom Nationalsozialismus, oder Europa von den nationalsozialistischen Deutschen?

„*Unter eine solche Geschichte lässt sich kein Schlussstrich ziehen*“, sagte der Historiker Heinrich August Winkler in seiner

Rede zum gleichen Anlass 2015. Doch was bedeutet das? Welche Lehren lassen sich aus 1945 – und aus 1933 – für die heutigen rechtsradikalen Gewalttaten und für die Situation am Mittelmeer ziehen?

Wir sollten uns nochmals die Worte von Bundespräsident Richard von Weizsäcker in Erinnerung rufen: „*Die Bitte an die jungen Menschen lautet: Lassen Sie sich nicht hineintreiben in Feindschaft und Haß gegen andere Menschen, gegen Russen oder Amerikaner, gegen Juden oder Türken, gegen Alternative oder Konservative, gegen Schwarz oder Weiß. Lernen Sie, miteinander zu leben, nicht gegeneinander.*“

Eine Ausgeburt des nationalsozialistischen Deutschlands war die *Abteilung Fremde Heere Ost*, geleitet von Reinhard Gehlen, aus der später die *Organisation Gehlen* und letztendlich der Bundesnachrichtendienst hervorging. Nachdem die Enthüllungen von Edward Snowden zur Massenausspähung durch Geheimdienste bereits wieder in Vergessenheit zu geraten drohten – ohne substanzielle politische Konsequenzen nach sich zu ziehen –, überschlagen sich hier gerade die Ereignisse. Medienberichten zufolge gibt es Hinweise darauf, dass der Bundesnachrichtendienst im Auftrag einer ausländischen Macht nicht nur die deutsche Bevölkerung, sondern auch die deutsche Industrie ausspioniert hat. Auch die Rolle des Bundeskanzleramts und der Bundeskanzlerin selbst wird immer undurchsichtiger. Es ist wenig glaubhaft, dass die Machenschaften des Bundesnachrichtendienstes im Bundeskanzleramt völlig unbekannt waren – und damit ist es auch wenig glaubhaft, dass die Bundeskanzlerin selbst nicht gewusst haben soll, was dort vor sich geht. Gerade entwickelt sich die öffentliche Debatte über das angeblich von den USA 2013 in Aussicht gestellte No-Spy-Abkommen. Sie erschüttert die Glaubwürdigkeit der Bundeskanzlerin und der Bundesregierung – damit weitet sich die Ausspähaffäre endgültig zur Staatsaffäre aus.

Fast nicht mehr überraschend ist dann eine weitere Enthüllung – dennoch macht sie sprachlos: Journalisten, die kritisch über die Defizite des Sturmgewehrs der Bundeswehr, dem G36, berichten wollten, sollten offenbar mit Hilfe des Militärischen Abschirmdienstes (MAD) mundtot gemacht werden. Auch wenn der MAD dies anscheinend abgelehnt und die Bundesministerin der Verteidigung klar dagegen Position bezogen hat: Es ist ein weiteres Beispiel für die Verselbständigung deutscher Behörden und der deutschen Geheimdienste. (Gleichzeitig ist es aber auch erstaunlich, wie offen inzwischen über Defizite der Bundeswehr öffentlich debattiert wird – vor fünfzig Jahren lösten Berichte über deren „bedingte Abwehrbereitschaft" noch die Spiegel-Affäre aus.)

Mit FIfFigen Grüßen

Stefan Hügel

Stefan Hügel

Betrifft: Cyberpeace

Vertrauen und Abwehr

Unsere Gesellschaft basiert auf Vertrauen, diese Bedeutung hat Niklas Luhmann (1968) bereits lange vor dem Siegeszug des Internets herausgearbeitet. Nach Luhmann ist Vertrauen notwendig, um die soziale Komplexität unseres Umfeldes zu reduzieren. Nur so können wir die große Zahl an Entscheidungen treffen, die uns die Realität täglich abverlangt – ohne Vertrauen würde diese Zahl ins unermessliche wachsen, bis wir nicht mehr in der Lage wären, damit umzugehen. Bruce Schneier stellt das an einer Alltagssituation plastisch dar:

> *„Just today, a stranger came to my door claiming he was here to unclog a bathroom drain. I let him into my house without verifying his identity, and not only did he repair the drain, he also took off his shoes so he wouldn't track mud on my floors. When he was done, I gave him a piece of paper that asked my bank to give him some money. He accepted it without a second glance. At no point did he attempt to take my possessions, and at no point did I attempt the same of him. In fact, neither of us worried that the other would. My wife was also home, but it never occurred to me that he was a sexual rival and I should therefore kill him."* (Bruce Schneier 2012)

Wenn wir das Internet nutzten, bauten viele von uns dabei bisher ebenfalls auf Vertrauen auf. Wir nutzten bedenkenlos Web-Dienste, die wir für vertrauenswürdig hielten, und verließen uns dabei auf unsere Intuition. Wir verzichteten häufig darauf, Web-Seiten verschlüsselt aufzurufen, da wir darauf vertrauten, dass niemand unsere aufgerufenen Seiten mitliest. Wir verzichteten auch auf Verschlüsselung unserer E-Mail-Korrespondenz, auch bei vertraulichen Dokumenten – es würde schon keiner mitlesen, und wenn, was sollte schon passieren?

Häufig tun wir das heute noch.

Uns ist natürlich klar, dass dieser Vertrauensvorschuss ein wenig Optimismus erfordert. Wir wissen schon immer, dass es im Internet Kriminelle gibt – unser intuitives Sicherheitsgefühl halten wir dagegen in der Regel für ausreichend. Manche stellen irgendwann fest, dass das zu optimistisch war, aber, hey, das sind Ausnahmen, *mir* kann das nicht passieren. Vertrauen wird zur Vertrauensseligkeit.

Auch der Vertrauensvorschuss, den wir unserem eigenen Staat entgegenbrachten, war optimistisch, wir hätten es wissen müssen. Wir wissen in Deutschland nach zwei Diktaturen, dass eine freie Demokratie keine Selbstverständlichkeit ist. Zumindest in der Bundesrepublik hatte sich eine stabile Demokratie herausgebildet – aber auch deren Behörden missbrauchen unser Vertrauen seit Anbeginn, Josef Foschepoth (2012) hat darauf hingewiesen. Ständige Angriffe von politischer Seite auf Vertraulichkeit und Integrität unserer Kommunikation hätten uns ebenfalls warnen müssen. Genannt sei hier nur die Vorratsdatenspeicherung – eine Maßnahme, die vom Bundesverfassungsgericht und vom Europäischen Gerichtshof zurückgewiesen wurde, aber deren Notwendigkeit, ungeachtet solcher Nebensächlichkeiten, immer wieder gebetsmühlenartig betont wird.

Berechtigt war das Vertrauen also wohl nie, heute ist es zerstört. Die Enthüllungen von Edward Snowden (z. B. in Glenn Greenwald 2014) haben sehr deutlich gemacht, dass unsere Kommunikation umfassend überwacht und diese Überwachung immer weiter perfektioniert wird. Diese Überwachung wird parlamentarisch untersucht, in Deutschland vom *1. Untersuchungsausschuss*, genannt *NSA-Untersuchungsausschuss*, der inzwischen *BND-Untersuchungsausschuss* genannt werden müsste, und den weiteren Gremien des Deutschen Bundestags zur Kontrolle der Geheimdienste. Vergleichbare Einrichtungen gibt es in den USA. Doch es zeigt sich, dass seine Arbeit behindert, Information zurückgehalten, und – folgt man den letzten Medienberichten – auch ihm gegenüber gelogen wird. Inzwischen wird darüber berichtet, dass der Bundesnachrichtendienst ausländischen Diensten dabei geholfen haben soll, gegen deutsche Unternehmen Wirtschaftsspionage zu betreiben; eigentlich ist das kaum zu glauben. Erste Strafanzeigen, auch von großen Wirtschaftsunternehmen, sind bereits angekündigt.

Doch in der Online-Ausgabe der *Frankfurter Allgemeinen Zeitung* lesen wir dazu:

> *„Die Spionage der Vereinigten Staaten in unserer Wirtschaft ist gerechtfertigt, in unserem Interesse und keine Industriespionage. Deutschland ist nun einmal einer der großen Exporteure von Rüstungsgütern, sicherheitskritischen Komponenten und Infrastrukturen nach Russland,*

China und in den arabischen Raum. Wir brauchen diese Exporte leider. Sie sind Teil unseres Wohlstands, unseres Systems und unserer Stärke und Stabilität in Europa. Aber sie sind auch gefährlich. Wir verkaufen schwierigen Kräften bessere Handlungsmächtigkeit. Das kann furchtbare Konsequenzen haben." (Sandro Gaycken 2015)

Wir fassen zusammen:

- Um unseren Wohlstand zu sichern, müssen wir Waffen in alle Welt exportieren.
- Damit stärken wir (auch) Regime, die zu unseren Gegnern werden können.
- Um dies wieder „einzufangen", müssen wir die Spionage der US-Amerikaner akzeptieren (und sogar dankbar dafür sein).

Was auf den ersten Blick wie eine gelungene Satire wirkt, ist wohl ernst gemeint. Es gibt Einblick in eine verquere Logik von Militär und Wirtschaft.

Solchen Institutionen blind zu vertrauen, ist offensichtlich naiv und gefährlich. Doch damit gefährden wir auch die Grundlage unserer Gesellschaft. Ohne Vertrauen funktionieren weder Gesellschaft, noch Wirtschaft, noch Politik.

Was tun?

Grundsätzlich gibt es zwei Möglichkeiten, mit der Situation umzugehen:

1. Wir müssen das Vertrauen wiederherstellen.
2. Wir müssen uns selbst schützen und gegen mögliche Angriffe absichern.

Beginnen wir mit dem zweiten Punkt: *„Hilf Dir selbst, sonst hilft Dir keiner"*, das ist das Credo des Neoliberalismus. Das wäre *Victim Blaming*, würden vielleicht andere ausrufen. Doch offensichtlich müssen wir unsere Absicherung selbst in die Hand nehmen. Auch Privatpersonen sollten sich um den Schutz ihrer Kommunikation kümmern. Wie das geht, zeigt zum Beispiel Karin Schuler (2014).

Unternehmen und Behörden schützen sich, indem sie Informationssicherheits-Managementsysteme implementieren und Ihre Systeme technisch und organisatorisch gegen Angriffe von außen und innen absichern. Hier gibt es, besonders bei sicherheitskritischen Systemen, ständigen Handlungsbedarf, um mit den Angreifern Schritt zu halten; manche Organisationen haben vielleicht auch Defizite, die sie zunächst ausgleichen müssen.

Technische Maßnahmen zur Absicherung können sein:

- Verschlüsselung von E-Mails,
- Verschleierung der Metadaten, zum Beispiel im TOR-Netzwerk,
- Härtung von Anwendungen und Infrastruktur,
- Einsatz von Firewalls und Protokollierung von Angriffen,
- Speicherung von Kommunikationsdaten auf Vorrat.

Wait, what? Aber ja doch, die Vorratsdatenspeicherung ist aus Sicht von Sicherheitsbehörden eine technische Maßnahme zur Absicherung der Kommunikation gegen Cyberangriffe und Kriminalität. Auch hier geht es um Vertrauen – das Vertrauen des Staats gegenüber seinen Bürgerinnen und Bürgern. Und es geht um unsere Grundrechte. Unsere Stellungnahme zum IT-Sicherheitsgesetz und die darauffolgende Debatte zeigen, dass hier eine klare Grenze gezogen werden muss (dazu Ingo Ruhmann 2015).

Allein auf Absicherung zu setzen, greift offensichtlich zu kurz. Es ist der Beginn einer Rüstungsspirale im Cyberspace, bei der Angriffs- und Abwehrmaßnahmen auf allen Seiten immer weiter verfeinert werden – NSA-Programme wie BULLRUN zur Entschlüsselung verschlüsselter Kommunikation zeigen das.

Und: Es ist der zum Scheitern verurteilte Versuch, ein soziales Problem technisch zu lösen. Bruce Schneier bringt es erneut auf den Punkt:

„If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." (Bruce Schneier 2000)

Damit kommen wir zu Punkt 1: Wir müssen das Vertrauen wiederherstellen. Für *Cyberpeace* bedeutet das: Wir müssen darauf vertrauen können, dass potenzielle Gegner uns nicht angreifen. Wir müssen eine strukturelle Nichtangriffsfähigkeit schaffen.

Dazu benötigen wir als erstes Transparenz. Nicht die Form der totalen Transparenz, die die Geheimdienste schaffen wollen, und die Byung-Chul Han kritisiert, wenn er behauptet:

„Die gegenseitige Transparenz kann … allein durch permanente Überwachung erreicht werden, die eine immer exzessivere Form annimmt. Das ist die Logik der Überwachungsgesellschaft." (Byung-Chul Han 2012)

Und:

„Das Vertrauen, das freie Handlungsräume hervorbringt, kann nicht einfach durch die Kontrolle ersetzt werden." (Byung-Chul Han 2012)

Dennoch benötigen wir sie: als Nachvollziehbarkeit politischer Entscheidungen, als Nachvollziehbarkeit der Arbeitsweise von Organisationen, als Nachvollziehbarkeit technischer Systeme. Es muss kontrolliert werden können, wie militärische und geheimdienstliche Organisationen arbeiten – wenn nicht durch die Öffentlichkeit, dann zumindest durch ein gestaffeltes System vertrauenswürdiger Instanzen. *„Die Menschen müssen ihrem Herrscher glauben und vertrauen"*, zitiert Han *Richard Sennett* (2004) – aber das hat offensichtlich nicht funktioniert, auch wenn die Bundesregierung das gerne glauben machen will.

Wir müssen als Gesellschaft in der Lage sein, zu beurteilen, wie es zu politischen Entscheidungen in unser aller Namen kommt. Politische Prozesse müssen in der Öffentlichkeit stattfinden,

ohne dabei Rückzugsräume für Unfertiges völlig zu verschließen. Technische Systeme müssen quelloffen sein, und dabei dennoch legitime Interessen an Geschäftsgeheimnissen wahren. Doch Rückzugsräume und Geschäftsgeheimnisse dürfen nicht dazu missbraucht werden können, Fehlverhalten zu vertuschen. Die Grenze ist nicht leicht zu ziehen und sie bedarf eines gesellschaftlichen Konsenses. Wir haben diese Regierung gewählt, sie handelt in unserem Namen, wir tragen für ihr Handeln eine (Mit-) Verantwortung.

Letztlich wird es ohne Vertrauen nicht gehen. Doch die Institutionen, denen wir vertrauen sollen, müssen sich dieses Vertrauens würdig erweisen. Die Medienberichte der vergangenen Tage, Wochen und Monate zeigen, dass dafür viel zu tun ist.

Referenzen

Josef Foschepoth (2012): Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik. Göttingen, Bristol: Vandenhoek & Ruprecht

Sandro Gaycken (2015): Spionage? Kein Grund zur Aufregung! Frankfurter Allgemeine Zeitung, http://www.faz.net/aktuell/politik/inland/bnd-affaere-spionage-unter-freunden-kein-grund-zur-aufregung-13564435.html

Glenn Greenwald (2014): Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München: Droemer

Byung-Chul Han (2012): Transparenzgesellschaft. Berlin: Matthes & Seitz

Niklas Luhmann (1968): Vertrauen. 4. Auflage 2000. Stuttgart: Lucius & Lucius

Ingo Ruhmann (2015): Schutz von Grundrechten nicht in Sicht. FIfF-Kommunikation 1/2015, Seite 10

Bruce Schneier (2000): Secrets & Lies. Digital Security in a Networked World. Indianapolis: John Wiley & Sons

Bruce Schneier (2012): Liars & Outliers. Enabling the Trust that Society needs to Thrive. Indianapolis: John Wiley & Sons

Karin Schuler (2014): Wer nicht kämpft, hat schon verloren. FIfF-Kommunikation 1/2014, Seite 34

Richard Sennett (2004): Respekt im Zeitalter der Ungleichheit. Berlin: Berliner Taschenbuch-Verlag

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Faires Silber.

Ach, die EU. Hauptsache der Euro rollt. Die USA hatten ein Gesetz zur Regulierung von Geschäften mit Konfliktmineralien geschaffen, das nicht perfekt war, aber innovativ und anspruchsvoll. Die EU wollte nachziehen, was die Kommission aber vorlegte, war schwach: Während in den USA alle börsennotierten Endproduktanbieter – also all die Apples, HPs, Ciscos und Intels, die wir kennen – Berichtspflichten auferlegt bekommen haben, sollen in der EU nur die paar Rohstoffimporteure berichten, die niemand kennt, und noch schlimmer: nur wenn sie wollen, denn verpflichtend soll es auch nicht sein. Die Hoffnung der Zivilgesellschaft – auch das FIfF war Teil dieser NGO-Koalition – ruhte daher auf dem EU-Parlament. Das Komitee für Entwicklungspolitik des Parlaments stimmte für eine verbindliche Berichtspflicht. Federführend ist aber leider das Parlamentskomitee für Internationalen Handel, und das hat den Kommissionsentwurf ohne viele Änderungen durchgewunken und Mitte Mai dem gesamten Parlament zur Abstimmung vorgelegt.

Im EU-Parlament war die Stimmung dann jedoch eine ganz andere. In einer kaum für möglich erscheinenden Wende wurde nun ein Gesetzentwurf geschmiedet, der sogar über das hinaus geht, was in den USA verlangt wird: Importeure müssen sich von der EU zertifizieren lassen, und alle Hersteller, die diese Rohstoffe in ihren Produkten haben – in der EU immerhin gut 800 000 meist mittelständische Unternehmen – müssen ihre Sorgfaltspflicht nachweisen, und das nicht nur für Zentralafrika, sondern für alle (noch zu definierenden) Konfliktgebiete. Vielleicht hat ja das Lobbying der vielen NGOs doch gefruchtet? Als nächstes muss das Gesetz allerdings durch den Europäischen Rat, wo es bestimmt wieder abgeschwächt wird.

In den USA steht unterdessen bald schon die zweite Runde der Pflichtberichte an, diesmal für die Geschehnisse im Jahr 2014. Überrascht hat Apple, denn sie veröffentlichten ihren Bericht schon im Februar. Die anderen dann wohl wieder kurz vor knapp. Amnesty International und Global Witness haben sich die letztjährigen Berichte angeschaut und mussten feststellen: Fast 80 % der Unternehmen haben sich gar nicht vollständig an die Vorgaben gehalten und klagen lieber dagegen. Ach, die Multis. Hauptsache der Dollar rollt.

Samsung bleibt von all dem befreit, da aus Südkorea. Aber sie sollten schauen, was in Taiwan mit RCA passierte: Der inzwischen Thomson Multimedia gehörende US-Veteran muss über 30 Jahre, nachdem Mitarbeiter Belastungen durch Chemikalien im Herstellungsprozess ausgesetzt waren, einige Millionen Entschädigung zahlen. Dem versucht Samsung, um auf diesen aktuellen Hersteller von LCDs, CPUs u.v.a. zurück zu kommen, zuvorzukommen, indem sie freiwillig (und ohne Schuldeingeständnis natürlich) erkrankten Mitarbeitern Gelder in Aussicht stellen, natürlich offiziell nicht als Entschädigung, sondern als Fürsorge für ihre Mitarbeiter. Wir berichteten schon davon; neu ist aber, dass es „*not our final plan*“ ist. Da kommt also noch was.

Was gibt es Neues bei den beiden Graswurzelprojekten der fairen Elektronik? Nager-IT möchte, solange es z. B. kein faires Lötzinn gibt – FairLötet ist noch im Entstehen – zum Ausgleich aus dem Verkauf der Mäuse Gelder für ein Unterstützungsprojekt in Indonesien bereitstellen, dort wo vieles des in Elektronik eingesetzten Zinns herkommt, und zwar auf illegale, Gesundheit und Umwelt gefährdende Weise. Außerdem sind die Holzscrollräder

inzwischen serienreif; die bisherigen Plastikräder kamen nämlich aus China unter unbekannten Arbeitsbedingungen.

Fairphone hat einen Audit-Bericht über ihren neuen Fertigungsbetrieb Hi-P in China veröffentlicht, den man so zusammenfassen könnte: Das Übliche, aber nichts Übles, insbesondere ähnlich dem vorherigen Kontraktfertiger. Fairphone hält zudem an der Absicht fest, Fairtrade-zertifiziertes Gold in ihre Smartphones zu bringen, genauer: Komponentenhersteller sollen eine ausgleichende Menge Fairtrade-Gold anschaffen und dem konventionellen Gold zufügen, um dann die Mischung zu verarbeiten. Wir kennen das vom Einspeisen von Ökostrom in die ansonsten konventionellen Netze.

In China treten die ArbeiterInnen zunehmend für bessere Arbeitsbedingungen ein, auch ohne ernst zu nehmende Gewerkschaft, selbst Samsungs Installateure organisieren sich im eher Streik-unfreudigen Südkorea. Ich bin überzeugt, dass das ein wichtiger Faktor hin zu faireren Geräten ist, und ich wünschte, wir könnten dies unterstützen. Aber vielleicht sollten wir bei uns selbst anfangen und zum Beispiel die richtigen EU-PolitikerInnen wählen.

Sebastian Jekutsch *ist Sprecher der AG Faire Computer des FIfF. Wer sich für die Quellen oder das Thema überhaupt interessiert kann gerne Kontakt aufnehmen per sj@fiff.de.*

Humanistische Union – Pressemitteilung

Entwicklung von Kampfdrohnen

Ein faules Osterei der Rüstungsministerin

2. April 2015 – Die jüngste Erklärung von Bundesministerin von der Leyen, Deutschland werde gemeinsam mit Frankreich und Italien eine kampffähige Drohne entwickeln, bezeichnete der Vorsitzende der Humanistischen Union, Werner Koep-Kerstin, als „ein faules Osterei, das Bundesministerin von der Leyen unter Missachtung der ethischen Problematik unbemannter Kampfdrohnen präsentiert hat."

Die Humanistische Union lehnt die Anschaffung und den Einsatz von Kampfdrohnen ab, denn:

- Die Hemmschwelle zum Einsatz von Gewalt sinkt, wenn Waffen eingesetzt werden können, ohne das Leben eigener Soldaten zu riskieren.

- Die Automatisierung und Verselbständigung von Kampfdrohnen und anderen Waffensystemen ist absehbar, da Computer Informationen wesentlich schneller verarbeiten können als Menschen. Am Ende werden Entscheidungen über Leben und Tod an Computer abgegeben, den Krieg führen Roboter. Es droht der Kontrollverlust über die Kriegführung.

- Die Zahl der zivilen Opfer von Drohneneinsätzen, sog. „Kollateralschäden", ist – wie sich am Beispiel von US-Drohnen in Pakistan u. a. nachweisen lässt – erschreckend hoch; Kampfdrohnen sind nicht die Präzisionswaffen, als die sie ausgegeben werden.

Es sei zudem eine Illusion, wenn Bundesministerin von der Leyen meine, das Parlament könne jederzeit den zukünftigen Einsatz von Kampfdrohnen einhegen, erklärte Koep-Kerstin.

Mit großer Sorge betrachtet die Humanistische Union die zunehmende Aufweichung des sogenannten Parlamentsvorbehaltes, den das Bundesverfassungsgericht seinerzeit für Auslandseinsätze geltend gemacht hatte. Demnach ist die Bundesregierung verpflichtet, „für einen Einsatz bewaffneter Streitkräfte die grundsätzlich vorherige Zustimmung des Deutschen Bundestages einzuholen". Inzwischen mehren sich Stimmen, die den Parlamentsvorbehalt grundsätzlich problematisieren hinsichtlich der Effizienz von Entscheidungen und damit verbunden der Bündnisfähigkeit Deutschlands. Mit Bedauern wird konstatiert, dass Deutschland und die Niederlande zu den Ländern gehören, deren Regierungen auf Billigung des Parlaments bei der Entscheidung über bewaffnete Auslandseinsätze ihrer Streitkräfte angewiesen sind.

Die Art und Weise, wie der Deutsche Bundestag die inzwischen mehr als fünfzig Anträge der jeweiligen Bundesregierungen für bewaffnete Auslandseinsätze der Bundeswehr noch stets gebilligt hat – beispielsweise bei den Afghanistan-Mandaten – kann realistisch nur als „Genehmigungs-Automatik" beschrieben werden. Der Parlamentsvorbehalt bietet „keine Sicherheit dafür, dass die deutschen Streitkräfte strikt nach Maßgabe der Vorgaben des Grundgesetzes und der UNO-Charta verwendet werden", erklärte der Verfassungsrechtler Prof. Martin Kutscha, zugleich Vorstandsmitglied der Humanistischen Union.

Wenn jetzt die Erwartung geäußert wird, Bundesministerin von der Leyen könne nun – nach einer Serie von Rüstungsbeschaffungs-Skandalen ihrer Vorgänger – beweisen, wie man effektiv und kostengünstig Großprojekte wie die Kampfdrohne bewältige, so ist dies der falsche Maßstab. „Von der Leyen sollte sich eher die Forderung der fünf Friedensforschungsinstitute im jährlichen Friedensgutachten zu eigen machen und für die weltweite völkerrechtliche Ächtung von Kampfdrohnen plädieren und sich zumindest für die dringend notwendige Rüstungskontrolle bei diesen Waffensystemen einsetzen", meinte der HU-Vorsitzende.

Quelle: Pressemitteilung der Humanistischen Union e. V.

Arbeitskreis Vorratsdatenspeicherung – Pressemitteilung

AK Vorrat kritisiert Referentenentwurf zur Vorratsdatenspeicherung scharf

17. Mai 2015 – Der Arbeitskreis Vorratsdatenspeicherung weist den veröffentlichten Referentenentwurf zur Vorratsdatenspeicherung[1] scharf zurück. Der Entwurf greift laut AK Vorrat tief in die Grundrechte ein und verstößt ebenfalls gegen die Urteile des Bundesverfassungsgerichts und des Europäischen Gerichtshofs. Denn nach wie vor handelt es sich um eine anlasslose Speicherung der Kommunikationsdaten aller Bürgerinnen und Bürger.

Der Gesetzentwurf führt verschiedene Speicherpflichten für Standort- und Verkehrsdaten ein, die Regierungsparteien berufen sich dabei auf das „absolut Notwendige" und objektive Kriterien. „Absolut notwendig ist es hingegen, dass die Regierungsparteien endlich anerkennen, dass unsere Grundrechte mit dieser anlasslosen Überwachung mit Füßen getreten werden und solche Überwachungsmethoden in einem Rechtsstaat nichts zu suchen haben", so Kai-Uwe Steffens vom AK Vorrat.

Weder im Rahmen der Evaluierung der Europäischen Kommission noch während der Verfahren vor dem Bundesverfassungsgericht und dem Europäischen Gerichtshof konnten Beispiele für einen effektiven Nutzen bei der Verfolgung schwerer Straftaten vorgelegt werden, geschweige denn eine Notwendigkeit nachgewiesen werden.

Der Gesetzentwurf fordert die Speicherung sämtlicher Standorte der Kommunikationsteilnehmer für vier Wochen, der Metadaten zu Telefongesprächen, SMS-Nachrichten, Messenger-Nachrichten und der IP-Adressen aller Internet-Zugriffe für zehn Wochen. Dabei ist sehr unklar geregelt, wann diese Daten verwendet werden dürfen, laut Gesetzentwurf auch dann, wenn eine Straftat „mittels Telekommunikation" begangen wurde und wenn die „Erforschung des Sachverhalts auf andere Weise aussichtslos wäre." Das macht es Strafverfolgungsbehörden einfach, auf diese Daten zuzugreifen. „Damit kann auch gegen Filesharer und Trickbetrüger auf Ebay vorgegangen werden", so Steffens weiter. „Ein tiefer Eingriff in die Grundrechte für die Verfolgung solch vergleichsweise geringer Delikte ist mit dem Rechtsgrundsatz der Verhältnismäßigkeit nicht vereinbar."

Die Vorratsdatenspeicherung wurde bereits zweimal von Verfassungsgerichten abgeschafft. Vor wenigen Wochen noch lehnte Justizminister Heiko Maas die Vorratsdatenspeicherung strikt ab, die SPD ist gespalten. Nun soll der jetzige Gesetzentwurf im Eilverfahren durch den Bundestag gebracht werden und noch vor der Sommerpause in Kraft treten. „Ein solches Vorgehen verhindert bewusst jeglichen zivilgesellschaftlichen Dialog, der einer Demokratie für so einen schweren Grundrechtseingriff notwendig wäre", ergänzt Rena Tangens vom AK Vorrat. „Offenbar will die Regierung keine Argumente mehr hören, sondern ein weiteres Mal ein verfassungswidriges Gesetz beschließen."

Quelle: Pressemitteilung des AK Vorratsdatenspeicherung

Anmerkung

1 https://netzpolitik.org/wp-upload/2015-05-15_BMJV-Referentenentwurf-Vorratsdatenspeicherung.pdf

European Digital Rights – Joe McNamee

Citizens' groups from around the world call on EC to defend privacy

The institutions of the European Union are completing a reform of Europe's Data Protection framework. Recognising the huge significance of the reform, the European Commission made an unequivocal promise when it launched the process. As an "absolute red line", the level of protection of individuals' data would not fall below existing levels. However, leaks show that this promise is not being kept.

Sixty-six NGOs from the European Union, North, Central and South America, Africa, Asia and Australia have joined forces to ask for a confirmation from European Commission President Jean-Claude Juncker that the promise will be respected.

> *"Without leadership from President Juncker, the right to privacy, not just in Europe but around the globe will be undermined", said Joe McNamee, Executive Director of European Digital Rights, the organisation that initiated the letter. "We hope and expect that the Commission President will uphold the integrity and independence of his institution. We expect a short, rapid response to our question."*

In 2012, the European Commission made an initial legislative proposal to modernise and reform European privacy legislation. The proposal was amended by the European Parliament in 2014. This update is urgently needed, due to the challenges of new technology, the need to harmonise the law and ensure its effective enforcement in Europe. Faced with profiling, digitisation of health data and online tracking, every corner of our lives is increasingly being invaded by "big data". Due to the amount of data being collected, businesses and governments increasingly know more about us than we know about ourselves – about our preferences, our health, our relationships and our politics. Without credible regulation citizens lose, businesses lose, society loses.

21 April 2015

By email:
To: President Juncker
CC: First Vice-President Timmermans, Vice-President Ansip

Dear President Juncker,

The undersigned organisations, NGOs from the European Union and around the globe are deeply concerned at the changes to the data protection reform package being made in the Council of the European Union. Europe's data protection framework is not just important for the protection of European citizens, it is not just important for building trust in European businesses, it is also crucial as an international gold standard for data protection and privacy on a global level.

On behalf of the College of Commissioners, former European Commission Vice-President Viviane Reding promised European citizens and businesses stronger, unified data protection rules, "bringing them into the digital age without compromising the high level of data protection which has been in place in Europe since 1995".[1] Dropping below the levels of protection in the 1995 Directive would be an "absolute red line" for the Commission, she promised.[2] The Council has retreated beyond this line and is disappearing into the distance, as our recently published analysis demonstrates.[3]

A failure of the European Commission to maintain levels of data protection in the 1995 Directive would be a breach of the promise made by the European Commission, it would be a breach of the promise of treaty-level protection of the right to personal data enshrined in Article 8 of the Charter of Fundamental Rights and it would be a crushing breach of trust for this, in your words, "last chance" Commission.[4]

We write this letter with one simple question – will you take responsibility for ensuring that the Commission's legal and political promise will be kept?

We look forward to your timely answer, before the Council completes its discussions ahead of the trialogue negotiations on this proposal.

Yours sincerely,

Joe McNamee

European Digital Rights – EDRi (Europe)[5] 20 Rue Belliard, 1040 Brussels, Belgium *brussels@edri.org*

INTERNATIONAL:
Access (International); Association for Progressive Communications – APC (International); **Privacy International (International)**; World Wide Web Foundation (International)

EUROPE:
ALES - Alumni of European Studies (Croatia); Aktion Freiheit statt Angst e. V. (Germany)[6]; AKVorrat.at – Arbeitskreis Vorratsdaten Österreich (Austria); Arbeitskreis Vorratsdatenspeicherung (Germany); Asociatia pentru Tehnologie si Internet – ApTI (Romania); BEUC – The European Consumer Organisation (Europe); **Bits of Freedom (Netherlands)**; Consumentenbond (Netherlands); Danish Consumer Council (Denmark); Deutsche Vereinigung für Datenschutz e. V. (Germany); DFRI (Sweden); Digitalcourage (Germany); Digitale Gesellschaft e. V. (Germany); EU-Logos Athèna (Belgium); European Information Society Institute – EISi (Slovakia); FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (Germany); Forum Datenschutz (Austria); Fundamental Rights European Experts Group – FREE (Europe); GeneWatch UK (United Kingdom); GreenNet (United Kingdom); Hungarian Civil Liberties Union (HCLU); Initiative für Netzfreiheit (Austria); International Modern Media Institute (Iceland); Iuridicum Remedium (Czech Republic); IT-Pol (Denmark); Liberty – NCCL (United Kingdom); medConfidential (United Kingdom); Norwegian Consumer Council (Norway); One World Platform (Bosnia Herzegovina); **Open Rights Group (United Kingdom)**; **Panoptykon Foundation (Poland)**; SHARE Foundation (Serbia); #StopWatchingUs Cologne (Germany); VZBV – Federation of German Consumer Organisations (Germany); VIBE - Verein für Internet-Benutzer Österreichs (Austria)

AFRICA:
JONCTION (Senegal); KICTANet (Kenya); Unwanted Witness Uganda (Uganda)

ASIA:
Bytes for All (Pakistan); CIS India (India); Digital Rights Foundation (Pakistan); Foundation for Media Alternatives (Philippines)

AUSTRALIA:
Australian Privacy Foundation (Australia)

CENTRAL AMERICA:
Asociación para una Ciudadanía Participativa – ACI-Participa (Honduras); Fundación Acceso (Costa Rica); IPANDETEC – Instituto Panameño de Derecho y Nuevas Tecnologías (Panama)

NORTH AMERICA:
British Columbia Civil Liberties Association (Canada); Center for Digital Democracy (United States); Consumer Federation of America (United States); Consumer Watchdog (United States); Electronic Privacy Information Center – EPIC (United States); Horizontal (Mexico); Open Government Project (Canada); Red en Defensa de los Derechos Digitales – R3D (Mexico); Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic – CIPPIC (Canada)

SOUTH AMERICA:
ADC - Asociación por los Derechos Civiles (Argentina); DATA (Uruguay); Fundacion Karisma (Colombia); Fundación Vía Libre (Argentina); Hiperderecho (Peru); TEDIC (Paraguay)

Anmerkungen

1 *http://europa.eu/rapid/press-release_MEMO-13-140_en.htm*
2 *http://europa.eu/rapid/press-release_SPEECH-13-514_en.htm*
3 *https://edri.org/broken_badly/*
4 *http://www.euractiv.com/video/juncker-will-be-last-chance-commission-309405*
5 *This letter was initiated by the NGOs whose names are in bold below*
6 *Hinweis der Redaktion: Zur Aktion Freiheit statt Angst bestehen bei einigen Organisationen in Deutschland erhebliche Vorbehalte (zu den Hintergründen siehe z. B. https://netzpolitik.org/2009/aktion-fsa-aktionsbuendnis-freiheit-statt-angst/). Dennoch dokumentieren wir selbstverständlich auch deren Unterschrift.*

Thomas Reinhold

Kampagnen-Wochenende der Cyberpeace-Kampagne

Kurzbericht

Vom 17. bis zum 19. April haben sich FIfF-Aktive in Berlin getroffen, um über den aktuellen Stand und die weiteren Schritte im Rahmen der Cyberpeace-Kampagne zu beraten. Da seit der Kickoff-Veranstaltung auf der FIfF-Konferenz 2014 auch personell neue Gesichter zur Kampagne dazu gestoßen sind und sich das Team ansonsten größtenteils nur über wöchentliche Telefonkonferenzen koordiniert, war das Treffen auch eine gute Gelegenheit, sich von Angesicht zu Angesicht kennen zu lernen. Leider waren einige Teilnehmer durch Krankheit kurzfristig verhindert, sodass es am Ende eine kleinere Runde als erwartet war, die in Berlin zusammen kam.

Als Ziel für das Wochenende hatte sich das Kampagnen-Team zwei wichtige Punkte gesetzt. Zum einen sollten die inhaltlichen Fragen der Kampagne diskutiert werden, um die Fülle an Forderungen und gesteckten Zielen zu kondensieren und das Kern-Thema zu definieren, auf das wir uns mit der Kampagne für die kommenden Monate konzentrieren wollen. Zum anderen sollte es auch um praktische Dinge gehen, wie den Fragen nach konkreten und öffentlichkeitswirksamen Aktionen, der Entwicklung von geeignetem Informationsmaterial, der Zusammenarbeit mit den FIfF-Regionalgruppen sowie der Kooperation mit Partnerorganisationen und dem Fundraising. Für die professionelle Begleitung an dem Wochenende hatten wir uns dank Unterstützung der *bridge*-Stiftung einen Moderator ins Boot geholt, der seit langem friedensbewegte Initiativen bei ihrer Kampagnen-Entwicklung anleitet und betreut.

Zu unserer großen Freude war das Wochenende für alle ein großer Erfolg. Nach einer Einstimmung durch unseren Moderator und einem Einführungsvortrag in das weite Themengebiet ist die Gruppe rasch zusammengewachsen und war mit Freude bei der Sache. So ist es gelungen, die gesteckten Ziele für das Wochenende zu erreichen und die wichtigen Programmpunkte gemeinsam zu bearbeiten. In einem ersten Schritt haben wir uns nochmals damit auseinandergesetzt, wie Kampagnen funktionieren und dass nicht primär die aufgestellten Forderungen, sondern ein Kern-Thema im Vordergrund stehen sollte. Dieses wird bei gesellschaftlichen oder politischen Ereignissen oder anlässlich von Aktionen immer wieder aufgegriffen, um auf bestehende Probleme hinzuweisen, Lösungsmöglichkeiten aufzuzeigen und anschlussfähig Mitstreiter.innen zu gewinnen. Für die kommenden Monate haben wir daher als Thema der Kampagne *Keine militärische Offensive im Cyberspace* ausgewählt, das sich aus den ursprünglichen Kampagnen-Forderungen I, II und IV zusammensetzt. Diese Auswahl fügt sich passend in die aktuellen nationalen und internationalen Debatten über den Aufbau und die Befugnisse von militärischen Cyber-Einheiten und die Entwicklung von Cyber-Offensivmitteln ein. Dabei wollen wir nicht den digitalen Selbstschutz als Lösungsansatz propagieren, sondern uns, im Gegenteil mit politischen Anliegen an jene Entscheider richten, deren demokratische Aufgabe und Verantwortung ist, uns als Bürger zu schützen und die friedliche und nichtmilitärische Gestaltung des Internets zu fördern. Das mindestens ebenso wichtige Thema der Abrüstung im Cyberspace wird dahingegen politisch und zeitlich einen sehr viel längeren Atem benötigen, wie die vergangenen Jahrzehnte und das Ringen wider die ABC-Waffen gezeigt haben. Es soll aus diesem Grund zu einem späteren Zeitpunkt wieder aufgegriffen werden.

Das zweite große Ziel des Wochenendes war die Konkretisierung von Vorhaben, mit denen wir die Kampagne in die Öffentlichkeit tragen wollen, um Menschen zu sensibilisieren und politischen Druck aufzubauen. Neben den Möglichkeiten, verstärkt mit Partnerorganisationen wie *campact* oder der Humanistischen Union zu kooperieren, wurden auch erste Aktionen geplant. Dazu jedoch zu einem späteren Zeitpunkt mehr. Darüber hinaus möchten wir als Kampagnen-Team mit dem Cyberpeace-Thema wieder verstärkt an Regionalgruppen herantreten, um dort eigenständige Aktivitäten anzuregen. Für diesen Zweck werden wir in den nächsten Monaten thematisch passendes Aktionsmaterial zusammenstellen, das wir für Vor-Ort-Aktionen zur Verfügung stellen können. Darüber hinaus werden wir euch auch dort aktiver mit Rat und Tat, Besuchen bei Regionalgruppen-Treffen und Vorträgen unterstützen, wo ihr wirkt, Hilfe benötigt oder aktiv werden wollt. Schließlich haben wir die Aktionen, den bereits in Organisation befindlichen Workshop im Rahmen der IS4IS Tagung in Wien, einem Cyberpeace-Dossier in der Zeitschrift *Wissenschaft & Frieden* und die weiteren Aktivitäten über die kommenden Monate hinweg auf einem Zeitstrahl verteilt. Damit wollen wir uns immer wieder vor Augen

führen, wo wir stehen, was geschafft wurde und was wir noch erreichen wollen. Denn auch das war Thema des Wochenendes: dass wir realistisch einschätzen lernen, welche Kapazitäten im Team verfügbar sind und wo die Grenzen jedes einzelnen sind. Um es mit den Worten unseres Moderators zu formulieren: „Wir dürfen nicht das Opfer unser eigenen Kampagne werden".

Als kleine und sehr wirksame Dreingabe haben wir am Samstag Nachmittag spontan als Teilnehmer der Demo im Rahmen des weltweiten Aktionstages gegen das TTIP-Abkommen mitdemonstriert und medienwirksam mit unserem Friedenstauben-Banner vor der amerikanischen Botschaft in der Menschenkette gestanden. Das rege Interesse bei Mit-Demonstranten, Presse und Passanten hat uns deutlich gezeigt, wie groß der Aufklärungsbedarf rund um das Thema Cyberpeace und wie wichtig unsere aktuelle FIfF-Kampagne ist.

Wissenschaft & Frieden 2/2015 – „Technikkonflikte"

und Dossier „Zivilklauseln"

Technik beeinflusst, wie Menschen handeln und interagieren, und Technik ist auch in vielfältiger Weise in Konflikte involviert, sei es als Konfliktgegenstand, aufgrund ihrer (oft unerwünschten oder nicht vorhergesehenen) Folgen oder als Waffe. Technik bzw. ihr Einsatz ist kaum zu trennen von unserem Wirtschaftssystem und der industriellen „Mega-Maschine", die dieses hervorgebracht hat. Die Artikel in W&F werfen Schlaglichter auf unterschiedliche Aspekte von Technik – von ihrer kleinsten Ausprägung, der Nanotechnik, bis zum weltumspannenden Cyberspace, und von der Militanz kapitalistisch geformter Technik bis zu Überlegungen zu deren Rückbau in Richtung angepasster Technologien.

Zum Schwerpunktthema schreiben in W&F 2/2015 Jürgen Scheffran über „Technikkonflikte in der vernetzten Welt", Wolfgang Neef über *Die Mega-Maschine – Zur strukturellen Militanz kapitalistisch geformter Technik*, Regina Hagen über *Dual-use als Strategie – Europa, der Weltraum und die Sicherheit*, Roland Reimers: *Drohnen – Eine unaufhaltsame Entwicklung?*, Kathryn Nixdorff und Jürgen Altmann über *Krieg im Kleinen? – Die Verschmelzung von Bio- und Nanotechnik*, Daniel Leisegang über *Der cyber-militärische Komplex – Die dunkle Seite des Silicon Valley*, Thomas Reinhold über *Militarisierung des Cyberspace – Friedens- und sicherheitspolitische Fragen*, Daniel Hiß über *Fracking – Keine Technik die begeistert*, Niko Paech und Björn Paech über *Wachstum, Fortschritt, Frieden*.

Außerhalb des Schwerpunktes schreiben Robert Lindner über *Syrien nicht im Stich lassen!*, Matthias Englert, Moritz Kütt und Andreas Löpsinger über *Oslo, Nayarit und Wien – Humanitäre Aspekte in der nuklearen Abrüstungsdebatte*, Hans-Joachim Schmidt über *Der lange Abschied Russlands von KSE*, Thomas Nauerth über *Liebe statt Güte – Warum am Wort »gewaltfrei« festzuhalten ist* sowie Jürgen Nieth die kommentierte Presseschau zum Atom-Deal mit dem Iran.

W&F 2/2015 liegt ein 24-seitiges Dossier *Zivilklauseln – Lernen und Forschen für den Frieden* bei**:** Vor etwa sechs Jahren wurden Zivilklauseln wieder zum Thema. Seither bildete sich unter Beteiligung aller universitärer Statusgruppen eine neue Zivilklausel-Bewegung; sie macht sich dafür stark, dass an wissenschaftlichen Einrichtungen ausschließlich für zivile Zwecke geforscht, gelehrt und gearbeitet wird. An mehr als zwanzig Universitäten wurden vorhandene Zivilklauseln reaktiviert oder neue Regelungen durchgesetzt. Sogar in zwei Landeshochschulgesetzen konnten Zivilklauseln verankert werden, in weiteren Bundesländern wird darüber diskutiert. In diesem Dossier ziehen einige Beteiligte eine Zwischenbilanz.

Wissenschaft & Frieden 2/2015 **Technikkonflikte**, € 7,50 + Porto.

W&F erscheint vierteljährlich. Jahresabo 30 €, ermäßigt 20 €, Ausland 35 €, ermäßigt 25 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F, Beringstr. 14, 53115 Bonn,
E-Mail: *buero-bonn@wissenschaft-und-frieden.de,*
www.wissenschaft-und-frieden.de

Hans-Jörg Kreowski und Raffael Rittmeier

Bericht zur Cyberpeace-Kampagne in Bremen

In Bremen hat sich eine kleine Gruppe Interessierter zusammengefunden, die den Bremer Zweig der Cyberpeace-Kampagne bildet. Wir wollen kurz über den Stand der Arbeit berichten.

Ausgangspunkt war die *Weihnachtsvorlesung* des ersten Autors zum Thema *Cyberpeace – für eine friedensstiftende Informatik*, in deren Einladung es hieß:

> *Die Vorzeichen des größten Teils der Informatikforschung sind inzwischen zivil. Das war in der Anfangszeit des Faches anders, und auch heute noch kann nicht vernachlässigt werden, dass Informatik und Militär äußerst eng verflochten sind. Killerdrohnen und Cyberattacken sind nur die medial stark rezipierten Erscheinungen dieser unheilvollen Liaison. Was sich unter dem Begriff Cyberkrieg subsumieren lässt – und das heißt Krieg mit den Mitteln und dem Know-how der Informatik –, bedroht alle zivilen Infrastrukturen, Recht und Freiheit und letztlich sogar die menschliche Existenz. Der Gegenentwurf ist eine friedensstiftende Informatik.*

Es gibt auch eine Videoaufzeichnung der Weihnachtsvorlesung [1].

Seit Januar hat sich der Bremer Zweig der Cyberpeace-Kampagne alle drei bis vier Wochen getroffen und dabei begonnen, eine Reihe von Veranstaltungen zum Thema *Cyberpeace: Für eine friedliche Entwicklung der digital vernetzten Welt* zu planen. In einer Pressemitteilung ist die Idee so beschrieben:

> *Spätestens durch die Enthüllungen von Edward Snowden ist einer breiten Öffentlichkeit bewusst geworden, dass Geheimdienste weltweit und in horrendem Ausmaß die digitale Kommunikation ausspähen und überwachen und so Grund- und Menschenrechte wie den Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung außer Kraft setzen. Darüber hinaus zeigen die fast täglichen Meldungen von Hackerangriffen und Cyberattacken auf Konzerne, Banken, staatliche Einrichtungen und zivile Infrastrukturen, dass im Internet nicht nur Wirtschaftsspionage im großen Stil betrieben wird, sondern sogar die Funktionsfähigkeit von Wirtschaft, Staat und Gesellschaft bedroht ist. Die Versorgung unserer Lebensgrundlagen wie Trinkwasser und Energie ist abhängig von digitaler Steuerung. Sabotage und Hackerangriffe können lebensbedrohlich für jeden Einzelnen werden. Schließlich belegt nicht zuletzt der tausendfache tödliche Einsatz von Killerdrohnen in Afghanistan, Jemen und in Pakistan, dass schon jetzt die Anwendung von Informationstechnik zum „Kriegsalltag" in vielen Teilen der Welt gehört. Es findet zurzeit – teilweise ganz offen, teilweise verdeckt – eine gigantische Cyberaufrüstung statt. Die digitale Kriegsführung (Cyberwar) eröffnet den Konfliktparteien neue anonyme Möglichkeiten der Vernichtung. Unser Anliegen ist es, die Öffentlichkeit hierüber zu informieren und dafür zu gewinnen, eine Weichenstellung für den digitalen Frieden (Cyberpeace) zu unterstützen.*

Die erste Veranstaltung hat am 14. April 2015 im *Haus der Wissenschaft* in der Bremer Innenstadt unter dem Motto *Stoppt die digitale Ausspähung – Maßnahmen gegen Datensammelwut und Überwachungswahn* stattgefunden. Referenten waren der Rechtsanwalt Dieter Dette aus Bremen zum Thema *Deutsches Datenschutzrecht* und Prof. Dr. Klaus-Peter Löhr aus Berlin zum Thema *Selbstdatenschutz*. Dieter Dette ist zunächst auf die Entstehung des Datenschutzes in Deutschland eingegangen (u. a. Unzulässigkeit von Langzeit-/Querschnittprofilen). Er hat hervorgehoben, dass bisher der Gerichtsstand hinsichtlich der EU-Datenschutzrichtlinie ungeklärt ist. Zu der Möglichkeit der „Selbstzertifizierung" von US-Firmen durch das *Safe-Habour*-Abkommen wurde eine Studie von Galexia zitiert (siehe dazu z. B. [2] und [3]).

Ein Fazit dabei war, dass beim Datenschutz leider eine wirksame Kontrolle fehlt. Klaus-Peter Löhr hielt einen technischen Vortrag mit dem Anspruch, dass er auch für Laien verständlich sein sollte. Er propagierte im Wesentlichen S/MIME-Zertifikate für die vertrauliche E-Mail-Kommunikation und forderte die Bundesregierung auf, eine komfortable und eine kostenfreie Zertifizierungsstelle zu schaffen. Auf die Problematik mit zentralen Stellen, denen man dabei „blind" vertrauen muss, ging er nicht weiter ein und empfiehlt auch nicht PGP/GnuPG. Ansonsten erwähnte er, wie problematisch Werbeanzeigen und Cookies auf Webseiten z. B. im Gesundheitssektor sein können. Am Ende kam er zu dem Schluss, dass der Staat seinen Schutzpflichten nicht nachkomme und daher der Selbstdatenschutz (noch) notwendig sei.

Mitveranstalter waren das TZI (Technologie-Zentrum Informatik und Informationstechnik) der Universität Bremen und die FIfF-Regionalgruppe Bremen. Von beiden Vorträgen sind Videoaufzeichnungen verfügbar [4].

Ab Mai gibt es weitere Treffen, um die inhaltliche Auseinandersetzung mit dem Cyberpeace-Komplex voranzubringen, die erste öffentliche Veranstaltung auszuwerten und in die Planung von Folgeveranstaltungen einzutreten. Nach unserem Eindruck besteht ein großer Diskussionsbedarf, so dass wir unsere Bremer Initiative zur Nachahmung empfehlen, wobei natürlich immer die regionalen Gegebenheiten einbezogen werden müssen.

Referenzen

[1] http://mlecture.uni-bremen.de/ml/index.php?option=com_content&view=article&id=249

[2] http://www.galexia.com/public/research/articles/research_articles-pa08.html

[3] http://heise.de/-933700

[4] http://mlecture.uni-bremen.de/ml/index.php?option=com_content&view=article&id=263

FIfF-Konferenz 2015
Kommerzialisierung des Sozialen –
Markt und Macht im Zeitalter digitaler Kompletterfassung

Commercialisation of the Soci(et)al – Markets and Power in the Age of Total Datafication

Freitag – Sonntag, 6. bis 8. November 2015

Digitale Sensorik durchdringt zunehmend unser Leben und generiert und speichert unaufhörlich Daten, von deren Existenz wir oft gar nichts wissen. Die Daten entstehen in Computern und Smartphones, aber auch in Navigationsgeräten, Fitnesstrainern und digitalen Implantaten. Jeder Mensch, jede menschliche Interaktion hinterlässt dadurch digitale Spuren, ein Umstand, den nicht nur Suchmaschinen und soziale Netzwerke zu einem Geschäftsmodell gemacht haben. Nachdem der Mensch als Arbeitskraft und Konsument umfassend überwacht, analysiert und kommerzialisiert worden ist, folgt mit dem Internet der Dinge nun die Kommerzialisierung des privaten und sozialen Lebens? Welchen Wert haben unsere privaten und sozialen Daten und wer verdient an ihnen? Welche Konsequenzen haben Likes, LifeStyle Apps und das Internet der Dinge auf das Machtgefüge der Gesellschaft? Dieser Themenbereich steht im Zentrum der diesjährigen FIfF-Konferenz 2015 in Erlangen.

Ort: Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Medical Valley Center, Henkestraße 91, 91052 Erlangen

Organisation:
Prof. Dr. Felix Freiling
Kristin Sutara-Kleinemeier
Lehrstuhl für Informatik 1
Martensstr. 3
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
91058 Erlangen
https://www1.cs.fau.de

Webseite:
https://2015.fiff.de
https://www.fiffkon.de
https://www1.cs.fau.de/fiff

Einladung zur Mitgliederversammlung 2015

des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e.V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2015 ein.

Sie findet am Sonntag, den 8. November 2015, voraussichtlich von 11:00 bis 14:00 Uhr an der Universität Erlangen-Nürnberg, Henkestraße 91, 91052 Erlangen, statt.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl des Vorstands
8. Neuwahl der Kassenprüfer
9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
10. Anträge an die Mitgliederversammlung
    - Themenbezogene FIfF-SprecherInnen
    Weitere Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
11. Verschiedenes

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

Grundgesetz für die Bundesrepublik Deutschland, Art. 1 Abs. 1 und Art. 2 Abs. 1

Stefan Hügel, Eberhard Zehendner

Perspektiven des Datenschutzes – Editorial zum Schwerpunkt

Datenschutz – ein Thema, das angesichts des wachsenden Umfangs der IT immer wichtiger, gleichzeitig immer umstrittener wird. „*Noch vor einigen Jahren war es eine gefühlte Seltenheit, dass von uns persönliche Informationen festgehalten wurden. Heute geschieht es praktisch sekündlich, und zwar millionenfach*", so leitet Jan Philipp Albrecht, der im Europäischen Parlament für die EU-Datenschutz-Grundverordnung zuständig ist, seinen in diesem Heft rezensierten Band *Finger weg von unseren Daten* ein. Datenschutz ist der Schutz unserer Persönlichkeit, und in Form der *informationellen Selbstbestimmung* durch das Grundgesetz garantiert – so urteilte 1983 das Bundesverfassungsgericht. In der Zeit von geheimdienstlicher Ausspähung, Google, Facebook und Big Data kommt dem Datenschutz eine wesentliche Rolle zu.

Gleichzeitig ist er umstritten. Unternehmen, die mit den Daten ihrer Nutzer sehr viel Geld verdienen, sehen ihr Geschäftsmodell bedroht. Sicherheitsbehörden und Geheimdienste sammeln unsere Daten für die Strafverfolgung, für den *Krieg gegen den Terror* und, in manchen Ländern, um die Bevölkerung unter Kontrolle zu halten. „*Datenschutz ist Täterschutz*" und „*Wer nichts zu verbergen hat, hat auch nichts zu befürchten*", sagen sie, und fordern vom Gesetzgeber immer weitergehende Rechte, Daten zu sammeln und auszuwerten. Die Debatte um die *Datenschutz-Grundverordnung* in der Europäischen Union, bei der zentrale Bausteine des Datenschutzes wie die Zweckbindung und die Datensparsamkeit in Frage gestellt werden, zeigen die Widerstände, die dem Datenschutz entgegengebracht werden.

Obwohl auch vorher schon Daten und Informationen über Menschen gesammelt wurden, gibt es den Datenschutz im heutigen Sinn erst seit den 1970er-Jahren. Das erste Datenschutzgesetz in Deutschland war das *Hessische Landesdatenschutzgesetz* von 1970, das einen stark auf Datensicherung bezogenen Datenschutzbegriff zugrunde legte. Den Begriff des Datenschutzes als Regelung der Verarbeitung *personenbezogener Daten* insgesamt und damit Schutz unseres Persönlichkeitsrechts prägte Ulrich Seidel ebenfalls 1970.

Etliche Menschen hierzulande werden wohl zumindest eine ungefähre Vorstellung vom Bundesdatenschutzgesetz und vielleicht auch einem der Landesdatenschutzgesetze haben. Doch nur wenige dürften mit der konkreten Arbeit eines Landesdatenschutzbeauftragten und den Rahmenbedingungen dieser Arbeit vertraut sein. Folgen wir also zunächst dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, Dr. *Lutz Hasse*, auf seinem bissig-humorvollen Rundgang durchs Land, der uns – neben den gesetzlichen Grundlagen seiner Tätigkeit als Datenschützer und der Struktur seiner Behörde – vor allem mit einigen seiner bemerkenswerteren Fälle bekannt macht. Lauschen wir dann seinen Warnungen vor allzu freudigen Erwartungen an die neuesten Segnungen der bunten IT-Welt, tragen diese doch meistens schon den Keim späteren Datenmissbrauchs in sich. Im darauf folgenden Interview berichtet Dr. Hasse freimütig aus etwas abstrakterer und in die Zukunft gewandter Sicht, welche Instrumente einem (Thüringer) Landesdatenschützer derzeit schon zur Verfügung stehen und in welcher Hinsicht ein weiterer Ausbau erstrebenswert und auch realistisch erscheint. Er erzählt von den vielen kleinen Schritten auf dem Weg zu einer über Datenschutz gut aufgeklärten Bevölkerung; solchen, die er schon getan hat, und anderen, die er noch tun möchte. Und auch über den eher schwierigen Umgang mit dem neuen Grundrecht der Informationsfreiheit.

Die Datenschutzstandards in Europa und in den USA sind sehr unterschiedlich. Während in Europa das *Vorsorge-Prinzip* gilt, regeln die USA nach dem *Nachsorge-Prinzip* nur das, was wissenschaftlich als riskant bewiesen ist. Durch „Freihandelsabkommen" wie TTIP wird das auch für uns zum Problem, stellt *Dagmar Boedicker* in ihrem Beitrag *Die EU-Datenschutz-Grundverordnung und die ‚regulatorische Kooperation'* fest. Normen sollen im Rahmen gegenseitiger Konsultationen so angeglichen werden, dass für den internationalen Handel möglichst wenig Hindernisse entstehen. Das Ergebnis ist vorhersehbar: die Angleichung von Datenschutz-Standards nach unten.

Ein spezielles Spannungsfeld ergibt sich aus dem Datenschutz in der Politik gegen den Menschenhandel, verdeutlicht *Bärbel Heide Uhl* in ihrem Beitrag. Einerseits ist eine verbesserte Datenlage für die Entwicklung wirkungsvollerer Strategien gegen den Menschenhandel notwendig. Andererseits muss der Missbrauch der Daten verhindert und die informationelle Selbstbestimmung der Betroffenen gewahrt bleiben. Große Datenmengen und ihre intensive Nutzung machen Entscheidungen über Menschen möglich, ohne dass diesen eine Kontrolle über Zweck und Zeitraum der Datenerhebung und -verarbeitung möglich ist.

Die algorithmische Revolution und die sich ergebende Notwendigkeit eines angemessenen Datenschutzes ist Thema des litera-

rischen Beitrags von *Stefan Ullrich*. „*Wenn wir das Individuum vor datenhungrigen Organisationen schützen wollen, müssen wir ihm das Sich-Organisieren-Können zugestehen. Wir, verehrte Anwesende, brauchen eine Datenwehr*“ ist das Fazit seines *Datenschutz-Konzils*, in dem Vertreter „*verschiedene[r] Stände, Ämter, Geschlechter und nicht zuletzt: Zeitalter*“ über das Thema verhandeln.

Das Spannungsfeld zwischen einem Datenschutzbegriff, der als umfassender Schutz des Persönlichkeitsrechts verstanden wird, und einem Datenschutzbegriff, der die (technische) Datensicherheit in den Mittelpunkt stellt, behandelt *Jörg Pohle*. Er sieht in *Datenschutz by Design* die Umdefinition des Datenschutzes in Datensicherheit, und damit den Versuch, gesellschaftliche Probleme technisch zu lösen. „*Die Folgen dieser Umdefinition*“, so schreibt er, „*lassen sich bis heute in den wissenschaftlichen Arbeiten zur Technikgestaltung – und ähnlich auch in der Datenschutzpraxis – beobachten: Gerade die Technikwissenschaften sind geprägt von Arbeiten, die* IT security *als* privacy *und Daten*sicherheit *als Daten*schutz *verkaufen. Anstatt die modernen Organisationen und ihre Informationsverarbeitung unter Kontrolle zu bringen, geht es in erster Linie um Konzepte wie die Verschlüsselung von Kommunikation, die Anonymisierung erhobener und gespeicherter Informationen oder Selbstschutzmaßnahmen von Betroffenen, ohne zu reflektieren, ob diese Ansätze im konkreten Fall überhaupt geeignet sind, einen Schutz der Betroffenen sicherzustellen.*“

Einen Überblick über *Umfang, Risiken und Schutzmaßnahmen am Beispiel von Google* gibt *Angela Meindl* in ihrem Beitrag *Internet-Profiling*. „*Die Art und Weise, wie vom Nutzer unbemerkt Daten über ihn erhoben und gespeichert werden, ist nicht akzeptabel. Mit welcher Begründung auch immer sie gerechtfertigt wird. Ohne Notwendigkeit muss jeder, der an dieser Gesellschaft teilhaben will, auf seine Privatsphäre verzichten, und trägt ein nicht zu unterschätzendes Gefährdungsrisiko, während diejenigen, die für diesen Zustand verantwortlich sind, Unmengen Geld mit unserer Privatsphäre verdienen*“, so ihr Resümee. Sie fordert ein internationales Datenschutzrecht und dessen konsequente Kontrolle und Durchsetzung.

Wer bisher meinte, mit dem Berechtigungskonzept von Android datenhungrige Apps erkennen und aussperren zu können, erlebt nach der letzten Umgestaltung zu Berechtigungsgruppen eine böse Überraschung. Dies und anderes thematisiert *Carsten Seeger* in seinem Beitrag *Android? Aber sicher!?*, der auch wiedergibt, mit welch einfachen Mitteln sich eine scheinbar berechtigungslose App weitgehende Kontrolle über das eigene Smartphone erschleichen kann.

Weitere Beiträge zum Thema gibt es in der Rubrik *Retrospektive* mit dem Artikel *Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten*, in dem *Ulrich Seidel* 1970 den modernen Begriff des Datenschutzes prägte, und in der Rubrik *Lesen & Sehen*, in der *Marie-Theres Tinnefeld* den Band *Finger weg von unseren Daten* von *Jan Philipp Albrecht* rezensiert.

Wir hoffen, mit unserem Schwerpunkt interessante Perspektiven auf das komplexe Thema Datenschutz zu geben, und wünschen eine erkenntnisreiche Lektüre.

Die Schwerpunktredaktion
Stefan Hügel, Eberhard Zehendner

Lutz Hasse

Datenschutz in Thüringen – es bleibt spannend!

A. Am Anfang war – das Bundesverfassungsgericht

„Datenschutz“ wird zumeist als Synonym gebraucht für das Grundrecht der informationellen Selbstbestimmung. Dieses Grundrecht wurde bereits 1983 vom Bundesverfassungsgericht in seinem berühmten Volkszählungsurteil aus der Taufe gehoben (BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83) und mit der Entscheidung des Bundesverfassungsgerichts vom 27.02.2008 (BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07) zu dem weiteren Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme fortentwickelt und optimiert. Die Weitsicht des Volkszählungsurteils wird unter anderem in folgenden Passagen deutlich (BVerfGE a.a.O., Rz. 148, 149, 152 zitiert nach juris):

> *„Mit dem Recht auf informationelle Selbstbestimmung wäre eine Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst.“*

> *„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“*

> *„Unter den Bedingungen der automatischen Datenverarbeitung gibt es kein belangloses Datum mehr.“*

B. Verfassungsrechtliche Grundlagen

Die Vorgaben des Volkszählungsurteils haben ihren Niederschlag in Art. 6 Abs. 2 der Verfassung des Freistaats Thüringen gefunden:

> *„Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Er ist berechtigt, über die Preisgabe und Verwendung solcher Daten selbst zu bestimmen."*

Was aber sind personenbezogene Daten? Hier hilft der Gesetzgeber weiter. Nach § 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) – das insbesondere für Thüringer Behörden gilt – sowie nach § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) – das insbesondere für Unternehmen gilt – sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener). Aufmerksamkeit verdient die „bestimmbare" Person. Denn anders als bei Einzelangaben, die unmittelbar auf eine bestimmte Person schließen lassen (Name, Telefonnummer, Anschrift, E-Mail-Adresse), genügen hinsichtlich einer bestimmbaren Person solche Einzelangaben, die erst unter Hinzuziehung weiterer Angaben die hinter diesen Angaben stehende natürliche Person erkennen lassen. Also bereits Informationsmosaiksteinchen, die nur in Verbindung mit weiteren Mosaiksteinchen ein Bild von einer erst dann bestimmbaren Person ergeben können (zum Beispiel IP-Adresse in Verbindung mit weiteren Informationen), sind personenbeziehbar und damit personenbezogen und vom Grundrecht der informationellen Selbstbestimmung geschützt.

Indes ist dieser Schutz nicht absolut. Denn wie auch schon im Volkszählungsurteil angelegt, sieht Art. 6 Abs. 3 der Verfassung des Freistaates Thüringen vor, dass das Grundrecht der informationellen Selbstbestimmung auf Grund eines Gesetzes eingeschränkt werden darf.

C. Das Verbot mit Erlaubnisvorbehalt

Diese Möglichkeit, das Grundrecht der informationellen Selbstbestimmung aufgrund eines Gesetzes einzuschränken, ist in § 4 Abs. 1 ThürDSG/BDSG konkretisiert. Danach ist eine Datenverarbeitung und Datennutzung von personenbezogenen Daten nur zulässig, soweit das ThürDSG/BDSG oder eine andere Rechtsvorschrift es erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Juristen nennen das *Verbot mit Erlaubnisvorbehalt*: Das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist grundsätzlich verboten. Eine Ausnahme besteht nur dann, wenn es eine *ausdrückliche gesetzliche Regelung* dafür gibt oder die Betroffenen in die Verarbeitung ihrer Daten *eingewilligt* haben.

Unter Datenverarbeitung ist dabei das Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten zu verstehen (§ 3 Abs. 3 ThürDSG). Wichtig: Für jede der zuvor erwähnten Aktionen ist eine Einwilligung oder Rechtsgrundlage erforderlich! Unter einer *Einwilligung* wird die auf *freiwilliger* Entscheidung beruhende Willenserklärung des Betroffenen verstanden, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen (§ 4 Abs. 2 ThürDSG, § 4a Abs. 1 BDSG). In der Regel bedarf die Einwilligung der Schriftform (vgl. § 4 Abs. 3 S. 2 ThürDSG, § 4a Abs. 1 S. 2 BDSG).

Mithin ergibt sich bei Datenschützern im Falle einer Verarbeitung personenbezogener Daten folgender Gedankengang:

1. Liegt eine Einwilligung vor?

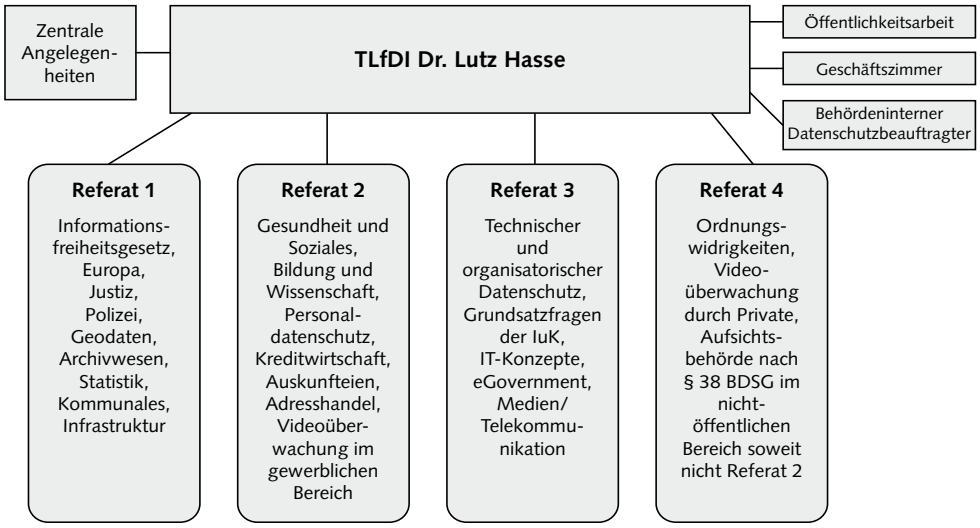
Falls nein:

2. Erlaubt eine Rechtsvorschrift die Datenverarbeitung?
   a. Spezielles Gesetz (z. B. Polizeigesetz, Schulgesetz, Sozialgesetzbuch)?
      Falls nein:
   b. Allgemeines Gesetz (ThürDSG, BDSG)?
      Falls nein:
      Datenverarbeitung ist rechtswidrig!

      Falls ja (a oder b):
      Datenverarbeitung ist rechtmäßig, wenn das Gesetz verfassungskonform ist und die vom Gesetz aufgestellten Voraussetzungen erfüllt sind.

D. Wir über uns

Die Abkürzung TLfDI steht für den *Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit*. Der TLfDI wird für sechs Jahre vom Landtag gewählt. Seit dem 29. Dezember 2012 ist er auch Beauftragter für die Informationsfreiheit im Freistaat Thüringen. Er übt diese Funktionen in völliger Unabhängigkeit aus und wird von einem engagierten Team unterstützt. Das nachfolgende Organigramm gibt Informationen zu den Aufgaben und dem Aufbau der Behörde. Weitere Infos dazu finden sich auf der Internetseite des TLfDI *(www.tlfdi.de)* unter dem Link: *http://www.tlfdi.de/tlfdi/wir/dienststelle/*.



Organigramm des TLfDI

E. Einblicke in die Tätigkeiten des TLfDI im öffentlichen Bereich (Behörden)

Der Bereich der Polizei beschäftigte den TLfDI in den vergangenen Jahren in besonders starkem Maße. Zu nennen ist die datenschutzrechtliche Begleitung des Papstbesuches, da mit diesem Ereignis zahlreiche Datenerhebungen im Vorfeld und während der Veranstaltung verbunden waren. Im sogenannten „Toilettenpapierfall" musste der TLfDI eingreifen, weil die Beschäftigten des Thüringer Landeskriminalamtes aufgrund des Verdachts des Abhandenkommens von Toilettenpapier videoüberwacht wurden. Auch gab es Fälle, in denen Polizeibeamte durch ihre Kollegen „ausspioniert" wurden. Da den TLfDI in der Vergangenheit die vielfach komplexen und mitunter recht unebenen „Regelungslandschaften" der Aufbewahrungs- und Prüffristen bei den öffentlichen Stellen beschäftigten, erarbeitete er den umfangreichen Leitfaden „Aufbewahrungsfristen für personenbezogene Daten und dienstliches Schriftgut beim Thüringer Landesamt für Verfassungsschutz, in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei sowie in den Thüringer Staatsanwaltschaften". Hierbei wurden alle einschlägigen Regelungsmaterien im Zusammenhang dargestellt und erläutert. Ein weiterer Schwerpunkt war die Fortführung der Kommunalkontrollen. Es bestand zudem der Verdacht, dass die in der Thüringer Landesverwaltung verwendeten Telefonanlagen über eine sogenannte „Babyphone-Funktion" verfügten, die es technisch ermöglichten, einen Raum zu überwachen.

Beleuchten wir nun einige der oben erwähnten Fälle aus dem öffentlichen Bereich näher:

1. Klopapier – Thüringer Landeskriminalamt von der Datenschutz-Rolle

Aufgrund von Medienberichten wurde dem TLfDI bekannt, dass das Thüringer Landeskriminalamt (TLKA) verdeckte Videoaufnahmen angefertigt hatte. Auslöser für die Ermittlungen war das unerklärliche Verschwinden von Toilettenpapierrollen – der Verdacht eines Diebstahls lag in der Luft. Um den Dieb zu finden, installierten Überwachungsspezialisten des TLKA eine Videokamera in einem Flur unweit der Toiletten, wo die Toilettenpapierrollen in Liefersäcken gelagert wurden. Ziel war es, einen möglichen Täter bei der Entwendung des angeblich so begehrten Toilettenpapiers zu überführen. Selbst nach wochenlanger Überwachung konnte kein Täter ermittelt werden. Auch die inzwischen eingeschaltete Staatsanwaltschaft stellte das Verfahren ergebnislos wieder ein.

Die datenschutzrechtliche Prüfung dieses Falles durch den TLfDI erwies sich zeitweise als schwierig, da die angeforderten Unterlagen vom TLKA nicht an den TLfDI übermittelt wurden. Die mangelnde Unterstützung seitens des TLKA wurde vom TLfDI gemäß § 39 ThürDSG beanstandet.

Die heimlichen längerfristigen Videoaufzeichnungen stellten zudem eine Verletzung des informationellen Selbstbestimmungsrechts dar, soweit sich Personen tatsächlich durch den Aufnahmebereich der Videokamera bewegt hatten. Denn eine Rechtsgrundlage, die hier die Fertigung der heimlichen Videoaufzeichnungen legitimieren konnte, war nicht vorhanden. Aus Sicht des TLfDI handelte es sich hier um eine Observation, die grundsätzlich nur durch ein Gericht angeordnet werden darf (§ 163f Abs. 3 StPO – Längerfristige Observation). Eine solche Anordnung lag hier jedoch nicht vor. Darüber hinaus waren die Videoaufzeichnungen auch nicht verhältnismäßig. Die konkrete Videoüberwachung konnte an sich schon nicht zur eindeutigen Überführung des Täters beitragen und war daher ungeeignet. Denn eine Entnahme der Toilettenpapierrollen aus dem Plastiksack im Flur hätte zunächst nicht geheißen, dass dieses auch gestohlen werden sollte. Selbst wenn eine Toilettenpapierrolle in Zueignungsabsicht entwendet worden wäre, hätte das keine Rückschlüsse auf den Dieb hinsichtlich der in den Toilettenräumen befindlichen Papierrollen zugelassen. Als milderes Mittel hätte man z. B. weniger Toilettenpapierrollen in die Toilettenräume legen bzw. zeitweise kontingentieren oder abschließbare Toilettenpapierrollenhalter anschaffen können. Zudem stand die Maßnahme außer Verhältnis zur Bedeutung der Sache und zur Stärke des bestehenden Tatverdachts. Festgestellt wurde hier lediglich ein hoher Verbrauch von Toilettenpapier im TLKA. Was diesen mysteriösen Verbrauch jedoch verursachte, konnte nicht ermittelt werden. Die datenschutzrechtlichen Verletzungen hat der TLfDI nach § 39 Abs. 1 ThürDSG beanstandet.

2. Babyphone im Dienstzimmer: Wozu?

Wer kennt das nicht: Plötzlich knackt es komisch im Telefon oder die Verbindung wird gefühlt irgendwie schlechter. Auch erscheint es manchen komisch, dass der Chef von Dingen weiß, die man anderen, aber nicht ihm erzählt hat. Hört der Chef etwa heimlich mit? Die Aufschaltfunktion bei einer Telekommunikationsanlage kann dazu missbraucht werden, dass zum einen bei geführten Telefonaten Dritte unbefugt mithören können und zum anderen bei der ebenso vorhandenen sogenannten Babyphone-Funktion – obwohl gar nicht telefoniert wird in dem Raum, in dem sich der Telefonapparat befindet – alles mitgehört werden kann. Aus datenschutzrechtlicher Sicht stellt das Ab- oder Mithören von Telefongesprächen oder Gesprächen im Raum eine Erhebung personenbezogener Daten dar. Die Verarbeitung einschließlich Erhebung und Nutzung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt). Aufgrund der Bedeutsamkeit des Themas wandte sich der TLfDI an alle Behörden der Thüringer Landesverwaltung, an die Kommunen und die kreisfreien Städte sowie auch an die Thüringer Handwerkskammern und die Industrie- und Handelskammern Thüringens und informierte die Stellen über diese datenschutzrechtliche Gefahr. Nicht nur die Dienstherren müssten die Leistungsmerkmale ihrer Telekommunikationsanlagen regelmäßig auf Rechtmäßigkeit prüfen. Auch Personalräte und Betriebsräte sollten die möglichen und tatsächlich eingestellten Leistungsmerkmale der Telekommunikationsanlagen regelmäßig hinterfragen. Der TLfDI konnte konkrete Verstöße nicht feststellen, immerhin aber, dass derartige Funktionen bestehen, die jedoch auch aufgrund der Aktivitäten des TLfDI deaktiviert wurden. Wir bleiben dran!

3. Abgeordnete des Thüringer Landtags zu Unrecht im Fokus der Polizei

In einer polizeilichen Ermittlungsakte stellte der TLfDI fest, dass sich dort personenbezogene Daten von Abgeordneten des Thü-

ringer Landtags befanden. Diese gelangten in die Ermittlungsakten, da im Rahmen einer Durchsuchung bei einem Beschuldigten auch sein privates Smartphone sowie Datenträger sichergestellt und ausgewertet wurden. Auf diesen befanden sich unter anderem auch die Daten der Abgeordneten. Eine Einwilligung zur Datenverarbeitung seitens der Abgeordneten lag nicht vor. Als Alternative zur Einwilligung käme die Existenz einer speziellen Rechtsgrundlage in Betracht, die aber auch hier nicht vorgelegen hatte. Abgeordnete des Thüringer Landtags sind nach § 53 Abs. 1 Satz 1 Nr. 4 Strafprozessordnung (StPO) berechtigt, das Zeugnis zu verweigern. Daher war hier auch der § 160a StPO zu beachten. § 160a Abs. 1 StPO bestimmt zunächst, dass eine Ermittlungsmaßnahme, die sich gegen eine zeugnisverweigerungsberechtigte Person (hier: die Abgeordneten des Thüringer Landtags) richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, unzulässig ist. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Nach § 160a Abs. 1 Satz 5 StPO gilt dies darüber hinaus entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine zeugnisverweigerungsberechtigte Person (Abgeordnete) – also einen Dritten – richtet, über diese Person (Abgeordnete) Erkenntnisse erlangt werden, über die sie (Abgeordnete) das Zeugnis verweigern dürfte. Im vorliegenden Sachverhalt erfolgte nach Aufnahme der Daten der Abgeordneten in die Ermittlungsakte eine – wie vom Gesetz vorgeschrieben – unverzügliche Löschung der Daten jedoch nicht. Der TLfDI hat dies gemäß § 39 ThürDSG beanstandet, da hier ein ungerechtfertigter Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Abgeordneten zu sehen war.

4. Polizei auf Abwegen

Die Staatsanwaltschaft Mühlhausen ermittelte gegen Polizeibeamte wegen des Verdachts des Betrugs und der Untreue. Hintergrund war eine anonyme Anzeige gegen vier namentlich benannte Tatverdächtige. Ihnen wurde vorgeworfen, dienstliche Kraftfahrzeuge und Telekommunikationsmittel während der Dienstzeit privat genutzt zu haben. Das zuständige Amtsgericht erließ auf Antrag der Staatsanwaltschaft einen Beschluss für eine längerfristige Observation gemäß § 163f Strafprozessordnung (StPO) gegen die vier Beschuldigten. Da für die längerfristige Observation der vier Beschuldigten nach § 163f StPO eine richterliche Anordnung vorlag, war eine rechtliche Grundlage für den Eingriff in das Recht auf informationelle Selbstbestimmung gegeben und datenschutzrechtlich nicht zu beanstanden. Darüber hinaus wurden jedoch im Zuge der Observationsmaßnahmen drei weitere Polizeibeamte gezielt „mit-observiert“, von denen man vage annahm, dass auch diese die Dienstwagen privat genutzt hätten. Dazu wurde die ursprüngliche richterliche Anordnung einfach „geschwärzt“. Eine solche „geschwärzte“ Anordnung, die quasi als richterliche Blankoanordnung für sämtliche Observationsmaßnahmen verwendet wurde, stellt jedoch keine rechtliche Grundlage dar, auf die eine längerfristige Observation gestützt werden kann.

Im Übrigen waren auch die Voraussetzungen für eine kurzfristige Observation einschließlich Fotodokumentationen gemäß §§ 161 Abs. 1, 163 Abs. 1 i. V. m. § 100 h StPO nicht erfüllt. Zwar ist für kurzfristige Observationsmaßnahmen und in diesem Zusammenhang auch für die Herstellung von Lichtbildern keine richterliche Anordnung vorgesehen, dennoch muss auch hier der Anfangsverdacht begründet sein; eine bloße Vermutung genügt – wie hier – nicht.

Durch den Einsatz heimlicher Observationsmaßnahmen ohne rechtliche Grundlage wurde intensiv in das Recht auf informationelle Selbstbestimmung der drei weiteren betroffenen Personen eingegriffen. Diese erhebliche datenschutzrechtliche Verletzung hat der TLfDI förmlich nach § 39 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) beanstandet.

F. Einblicke in die Tätigkeit des TLfDI im nichtöffentlichen Bereich (insbesondere Unternehmen)

Zur Einstimmung:

Dashcam – Trashcam

Auto, Fahrrad, LKW;
die Dashcam ist dabei – oje.
davor, dahinter, nebendran,
Personen, Unfall, Autobahn,
Dashcam zeichnet's auf – ein Wahn.

Tatsächlich, und da herrscht Einigkeit,
verfehlt sie die Datenschutz-Zulässigkeit.
Zwar sind schon von Gesetzes wegen
Ausnahmetatbestände vorgegeben,
die Filmen in Familienkreisen
sowie auch von privaten Reisen,
dem Bundesdatenschutz entreißen.

Dashcams muss man,
das sollte man wissen,
nach dem BDSG besser doch missen.
Das Filmen von Unfällen, eigenen – fremden,
um das dann vor Gericht zu verwenden,
ist keine persönliche Tätigkeit,
die vom Anwendungsbereich befreit.

Vom Filmen von öffentlichen Räumen,
darf der Einzelne nur träumen,
es sei denn, man hat das Hausrecht inne
und dieses dabei auch im Sinne.
Ebenfalls, so die Gesetze,
kann aus berechtigtem Interesse
dann aber nur zu bestimmtem Zwecke
die Kamera an des Hauses Ecke.

Darüber hinaus, man glaubt es kaum,
sind schutzwürdige Interessen im Raum.
Erst wenn keine Punkte vorliegen,
dass diese Interessen überwiegen,
wird es mit der Filmerei
mehr als nur `ne Träumerei.

Beim Autofahren, so sei bedacht,
ist Kamera nicht angedacht,
so liegt es nach Natur der Dinge,

auf der Straße wird's mit dem Hausrecht dünne.
Zwar sind fürs Filmen die eig'nen Interessen
des Autofahrers nicht sogleich vermessen,
doch beim Aufnehmen anderer im Verkehr,
ist für jeden erkennbar gar nicht schwer,
dass Anhaltspunkte sind vorhanden
für's Überwiegen der Interessen der and'ren,
nämlich gerade auch der Passanten.

Wegen des hier Erreimten sei dem Bürger gesacht,
dass der Datenschützer über den Datenschutz wacht.
Der Verstoß, wie grade berichtet,
wird gern mit Bußgeldern gerichtet.
Daher hier noch ein letzter Satz:
Lieber Besitzer einer Dashcam,
diese gehört ganz schnell in die „Trashcan"!

Es sind bereits Urteile zur Dashcam ergangen. So das Urteil der 4. Kammer des Verwaltungsgerichts Ansbach vom 12. August 2014 (AN 4 K 13.01634). Der Kläger wandte sich im vorliegenden Verfahren gegen einen Bescheid, mit welchem ihm untersagt worden war, mit der im Fahrzeug des Klägers eingebauten On-Board-Kamera während der Autofahrt permanente Aufnahmen des vom Kläger befahrenen öffentlichen Bereichs zu machen. Zugleich wurde dem Kläger aufgegeben, Aufnahmen, die mit der Kamera gemacht wurden, zu löschen. Maßgebend hierfür ist, dass das Bundesdatenschutzgesetz heimliche Aufnahmen unbeteiligter Dritter grundsätzlich nicht zulässt und diese einen erheblichen Eingriff in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung darstellen. Das Interesse betroffener Personen überwiegt deshalb das geltend gemachte Interesse des Klägers an der Fertigung von Aufnahmen mit einer Dashcam. Videoaufnahmen dürfen nicht ohne Zustimmung der Gefilmten angefertigt werden, wenn sie den Zweck haben, an Dritte weitergegeben zu werden. Dazu zählt neben der Veröffentlichung im Internet auch die Weitergabe an die Polizei. Der gesetzlich festgelegte Bußgeldrahmen für derartige Verstöße beläuft sich auf bis zu 300.000 EUR. Im jüngsten Urteil vom 23. April 2015 hat das Amtsgerichts Nienburg (4 Ds 155/14) erstmals eine Dashcam-Aufnahme für einen Strafprozess als Beweismittel zugelassen. Jedoch mit der Einschränkung, dass die Aufnahme aus aktuellem und konkretem Anlass erfolgen muss: In diesem speziellen Fall hat der Zeuge die Dashcam nur zur Dokumentation einer Nötigung im Straßenverkehr aufgenommen. Anders verhält es sich, wenn man die Dashcam dauerhaft aktiviert. Hier trifft wieder das o. g. Urteil des Verwaltungsgerichts in Ansbach zu, dass der Einsatz von Dashcams unter bestimmten Umständen gegen den Datenschutz verstößt. Diese Meinung vertritt auch der TLfDI.

1. Feuermelder mit Augen

Über einen anonymen Hinweisgeber wurde dem TLfDI der Tipp gegeben, dass ein Arbeitgeber in der Umkleidekabine seines Unternehmens mit angeschlossenem Duschraum eine verdeckte Videoüberwachung mit Audiofunktion – getarnt als Rauchmelder – durchführen würde. Am Folgetag hat der TLfDI vor Ort kontrolliert. Nachdem man den TLfDI widerwillig auf das Betriebsgelände ließ, musste festgestellt werden, dass der entsprechende Umkleideraum über Nacht umfassend renoviert worden war. Es roch sogar noch nach frischer Farbe. Im darauf folgenden Verwaltungsverfahren konnte festgestellt werden, dass der Arbeitgeber mit der Videokamera Einbrüche in die Spinde seiner Arbeitnehmer aufklären wollte. Die Kamera war direkt nach einem Einbruch installiert worden. Insgesamt wurde die Kamera etwa zwei Wochen betrieben. In diesem Zeitraum kam es erneut zu einem Einbruch. Die Auswertung der Überwachung ermittelte den Täter, ihm wurde gekündigt. Was vorbildlich klingen mag, ist es leider manchmal nicht, so auch in diesem Fall. Auch wenn aus Sicht des Arbeitgebers alles wunderbar geklappt hat, sind im Bereich des Arbeitsverhältnisses datenschutzrechtliche Vorschriften zu beachten. Nicht alles, was zweckmäßig erscheint, ist auch zulässig. Zwar sieht § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) explizit die Datenerhebung zu Zwecken der Aufklärung von Straftaten im Beschäftigungsverhältnis vor, jedoch sind diese nur unter besonderen Voraussetzungen zulässig. Dabei fließt mit ein, dass eine Videoüberwachung in einem Umkleideraum anders zu bewerten ist als eine Videoüberwachung in einem Kassenbereich. So darf eine heimliche Videoüberwachung nur dann durchgeführt werden, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die verdeckte Videoüberwachung praktisch das einzig verbleibende Mittel darstellt und insgesamt nicht unverhältnismäßig ist. Bereits der letzte Punkt war in dieser Konstellation nicht gegeben. Eine verdeckte Videoüberwachung in einem Umkleideraum, der für eine Komplettentkleidung vorgesehen ist, ist fast immer unverhältnismäßig, da hier in einem Maße in die Intim- und damit Persönlichkeitssphäre der Betroffenen eingegriffen wird, die eine Abwägung zu Gunsten der Interessen des Überwachenden fast unmöglich macht. Darüber hinaus wurden in diesem Fall jedenfalls nicht alle anderen Mittel zur Aufklärung ausgeschöpft. Ein Ordnungswidrigkeitenverfahren wurde eingeleitet.

2. Nackt bis auf die Haut – saunieren und (unfreiwillig) posieren

Eine Gemeinde installierte in dem Saunabereich ihres Hallenbads Videokameras, mit denen sowohl eine Videobeobachtung als auch eine Videoaufzeichnung erfolgten. Als Grund für die Bildaufzeichnungen führte die Gemeinde an, dass zum einen Diebstähle damit vermieden werden sollten und zum anderen, dass die Bademeister hätten erkennen können, ob jemand einen Herzinfarkt im Saunabereich erleidet und so ein schnelles Eingreifen ermöglicht würde. Eine Einwilligung seitens der Saunabesucher lag jedoch nicht vor. Eine verdachtsunabhängige Videoüberwachung, insbesondere, wenn die Aufnahmen gespeichert werden sollen, stellt einen nicht unerheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar und bedarf daher einer Rechtsgrundlage, die diesen Eingriff erlaubt. Es stellte sich die Frage, ob die Videoüberwachung zur Wahrnehmung des Hausrechts nach § 6 b Abs. 1 Nr. 2 BDSG zulässig war. § 6 b Abs. 1 Nr. 2 BDSG besagt, dass die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig ist, soweit sie zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen

der Betroffenen überwiegen. Dies musste hier jedoch verneint werden. Das Hausrecht berechtigt zwar, Personen von Rechtsverstößen abzuhalten, dafür müssen aber konkrete Anhaltspunkte vorliegen, dass Rechtsverstöße in der Vergangenheit bereits begangen worden sind. Das war hier jedoch nicht der Fall. Als weitere Möglichkeit stellte sich die Frage, ob die Videoüberwachung zur Wahrnehmung berechtigter Interessen gemäß § 6 b Abs. 1 Nr. 3 BDSG gerechtfertigt werden konnte. § 6 b Abs. 1 Nr. 3 BDSG besagt, dass die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur zulässig ist, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In diesem Sachverhalt lagen jedoch keine objektiven Anhaltspunkte vor, dass der bestimmte Saunabereich, der videoüberwacht wurde, besonders gefährlich war. Zum anderen überwogen die schutzwürdigen Interessen der Saunabesucher an einer unbeobachteten Nacktheit die Interessen der Saunabetreiber. Ein regelmäßiger Rundgang des Bademeisters hätte in diesem Fall als milderes Mittel im Gegensatz zu einer Videoüberwachung ausgereicht. Wäre eine Person tatsächlich bewusstlos geworden oder hätte einen Herzinfarkt erlitten, könne davon ausgegangen werden, dass andere Saunabesucher sofort Hilfe geholt hätten. Die Videoüberwachung war somit rechtswidrig.

3. Finger von der Wurst!

Ein Landwirt hatte sich mehrere Hofläden zugelegt. Allerdings nahm er es mit der Sicherung seiner Produkte etwas zu ernst. Um sein Eigentum zu schützen, in diesem Falle ging es um die Wurst, schreckte er vor moderner Überwachungstechnik nicht zurück. So installierte er nahezu flächendeckend in allen Räumen Videokameras. In einer seiner Filialen war gar der einzige unbeobachtete Ort die Arbeitnehmertoilette. Er wollte damit verhindern, dass die hungrigen Verkäuferinnen sich ungehemmt hinter seiner Verkaufstheke bedienen können. Mit dem Bundesdatenschutzgesetz (BDSG) ist eine solche Videoüberwachung von Arbeitnehmern und Kunden selbstverständlich nicht zu vereinbaren. Zwar sieht das BDSG die Möglichkeit der Datenerhebung zu Aufklärung von Straftaten im Arbeitsverhältnis vor, jedoch nur in sehr engen Grenzen und vor allem in verhältnismäßigem Rahmen. Jedenfalls muss eine solche Videoüberwachung das allerletzte Mittel sein. Vorher muss z. B. bei einem Diebstahlverdacht eine Taschenkontrolle unter Heranziehung der örtlichen Polizei erfolgen. Die Kameras waren jedenfalls zu entfernen. In diesem Fall musste der TLfDI die Einhaltung des BDSG nicht mit Hilfe einer Anordnung durchsetzen. Der Bauer hatte kurz zuvor die Kameras nebst Kabel aus Zorn über den TLfDI aus den Wänden gerissen. Zielführend …

4. Übermittlung von Patientendaten an „Herrn Dr. *med.* Hasse“

Der TLfDI, Herr Dr. *jur.* Hasse, erhält zu Hause Post: Ein Krankenhaus in Thüringen übersendet verschiedene Arztberichte an „Herrn Dr. *med.* Hasse“. Die Nachfrage im Krankenhaus ergab: Die Anschrift des eigentlich gesuchten Arztes ähnlichen Namens war nicht im Krankenhausinformationssystem eingetragen. Das Krankenhauspersonal „recherchierte“ also nach der Anschrift im Internet. Das war rechtskonform. Das Krankenhaus muss jedoch nach § 9 BDSG alles tun, damit seine Mitarbeiter bei der Verarbeitung von Patientendaten die datenschutzrechtlichen Vorgaben einhalten. Hierzu gehört zum einen, alle technischen Anlagen so zu konzipieren, dass Unbefugte keinen Zugriff haben. Zum anderen muss durch organisatorische Maßnahmen, zum Beispiel durch Dienstanweisungen, sichergestellt werden, dass die sensiblen Daten nicht in falsche Hände geraten. Es muss daher eine schriftliche Anweisung geben, wie nach den Adressen gesucht wird und wie die Gesundheitsdaten übermittelt werden dürfen, die der Schweigepflicht unterliegen. Die Übermittlung der Gesundheitsdaten war somit rechtswidrig. Der Umstand, die Patientendaten ausgerechnet an den Landesdatenschutzbeauftragten gesendet zu haben, löste dann im Krankenhaus auch „heilsame“ Prozesse aus!

G. Zukunft? Ungewiss!!

Die zuvor unter E. und F. dargestellten Einzelfälle aus der Praxis des TLfDI mögen einen gewissen Spaßfaktor beinhalten, dürfen indes den Blick auf die generellen Gefahren für das Grundrecht der informationellen Selbstbestimmung nicht verstellen.

Soziale Netzwerke sollten entschleiert werden. Nutzer müssen über das Geschäftsmodell aufgeklärt werden sowie darüber, wie man dort sein Recht auf informationelle Selbstbestimmung einigermaßen schützen kann.

Lutz Hasse

Dr. **Lutz Hasse** legte die Juristischen Staatsexamina in Niedersachsen ab. Es folgten Assistenzen an der Universität Osnabrück und ab 1992 an der Friedrich-Schiller-Universität Jena. Die Promotion erfolgte während der „Jenenser Phase“ an der Universität Osnabrück. Anschließend erfolgte der Wechsel zur Thüringer Verwaltungsfachhochschule – Fachbereich Polizei; dort wurde er Leiter der Rechtsausbildung. Nach Tätigkeiten als Referatsleiter im Thüringer Innenministerium, beim Thüringer Landesbeauftragten für den Datenschutz und im Thüringer Sozialministerium wurde er 2012 vom Thüringer Landtag zum Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt.

Smart – Vorsicht! Smart suggeriert etwas Positives. Smart meters, smart grids, smart car, smart home, smart factory (Industrie 4.0), smart city, etc. Das Smarte daran ist, dass Unmengen von personenbezogenen Daten erhoben und ausgewertet werden und daraus Persönlichkeitsprofile erstellt werden können. Warum? Jeder Mosaikstein zählt, um sich von dem Nutzer ein Bild machen zu können. Warum? Wer weiß das seit den Offenbarungen vom Edward Snowden schon! Smart watches zum Beispiel übermitteln Gesundheitsdaten. Mit anderen Körperanalysegeräten ist hier ein Milliardenmarkt entstanden. Nur durch den Verkauf der Geräte? Und der Daten! Daten werden auch an anderen Einrichtungen gesammelt: Videokameras, Paycards, Clouds (Vorsicht, wenn die Serverkette nicht nachvollziehbar ist), Spielzeug (Xbox, Smartglasses, Fernseher, Puppen …). Und im Internet der Dinge könnte ein smarter Stromzähler bei einem bestimmten Lampen-Schaltrhythmus den illegalen Cannabisanbau im Keller entlarven.

Big Data: Alle diese Daten werden zu Big Data – einer umfassenden Datensammlung, die mit Hilfe moderner Software zur Erstellung eines kompletten Persönlichkeits-, Sozial-, Bewegungsprofils genutzt werden kann. Dabei können Datensammlungen öffentlicher Stellen (z. B. Behörden) mit denen nicht-öffentlicher Stellen (z. B. Unternehmen) kombiniert werden. Findet das statt? Eine Antwort beginnt damit, dass Behörden sich der Unterstützung von Unternehmen bedienen können … Übrigens: Google speichert täglich das Tausendfache an Daten, die in allen Werken der US-Kongressbibliothek enthalten sind! Warum wohl?

Und dann die Algorithmen.

Was bei Big Data nicht unmittelbar ablesbar ist, wird mit Hilfe von algorithmisch-mathematischen Formeln prognostiziert.

Beispiele: Predictive Policing: Aufgrund von Big-Data-Analysen werden Straßen, Gruppen und Individuen überwacht, weil sie für die Verbrechensbegehung zu bestimmten Zeiten als relevant erachtet werden. Oder: Terroristen sollen mit spezieller Software anhand von Herzschlag, Atemfrequenz, Körpersprache und anderer physischer Faktoren ausfindig gemacht werden. Nur in den USA? Deutsche Landeskriminalämter testen bereits entsprechende Software. Blick in die Zukunft: Freiheitsstrafe aufgrund algorithmisch ermittelter, aber tatsächlich nicht begangener Straftat (vgl. Science-Fiction-Thriller „Minority Report" mit Tom Cruise)? Wir erkennen Entwicklungen, allerdings nur solche, die offenkundig werden – etwa die angedachte Kooperation der Schufa mit einer Hochschule zur Auswertung sozialer Netzwerke mit Blick auf die Kreditwürdigkeit von Bankkunden. Aber nicht genug: Auch Schwangerschaften werden inzwischen erkannt – die Daten der Bankcards im Kaufhaus verraten es – mit Hilfe eines Algorithmus – Tag der Niederkunft inklusive!

Was kann man tun?

Staatliche Hilfe lässt seit den Enthüllungen von Edward Snowden leider zu wünschen übrig. Bürgerliche Selbsthilfe ist mithin von Nöten: Anonymes Surfen, Verschlüsselung, aktualisierte Sicherheitssoftware, Selbstfortbildung, berufliche Fortbildung, in sozialen Netzwerken die notwendigen Häkchen setzen, Widerspruchsrechte wahrnehmen, Datensparsamkeit im privaten Bereich, keine Bilder (!), Antivirensoftware für Smartphones, Sammlung der eigenen Daten – z. B. in sozialen Netzwerken – abfragen, ggf. „Löschung" bewirken.

Zudem: Fragen Sie Ihren Datenschutz-/Informationsfreiheitsbeauftragten!

Und warum überhaupt Schutz des Grundrechts?

Das Recht der informationellen Selbstbestimmung wurzelt in dem Grundrecht der Menschenwürde. Und zum Menschsein gehört das Recht, Geheimnisse zu haben. Sich nur insoweit zu offenbaren, wie wir es wünschen. Um zu entscheiden, welcher Mensch wir für andere Menschen sein wollen und welcher nicht. Um gemocht und respektiert zu werden.

Wissen wir, was wir tun?

Einer Studie zu Folge genügen bereits 10 Facebook-„Likes" einer Person, um sie besser einschätzen zu können als Arbeitskollegen es können, die immerhin 5 Tage pro Woche mit der Person zusammenarbeiten. Bei mindestens 70 „Likes" liegt der Computer mit seiner Einschätzung besser als Freunde und ab 150 „Likes" wird die Beschreibung der Persönlichkeit treffender als die von Familienangehörigen. Die höchste Hürde stellen Ehepartner dar. Um eine bessere Einschätzung der Persönlichkeit zu erreichen, werden mindestens 300 „Gefällt-mir"-Angaben benötigt. Kombiniert mit Daten von Handys, Videokameras, Einkäufen und Verbindungen zwischen den Individuen entstehen Datenkopien von der Realität. Mit der Option der sozialen Kontrolle. Durch wen? Den Staat? IT-Konzerne? Beide? Die Herren der Algorithmen gegen den Rest der Welt?

Maschinen, Roboter, PCs werden inzwischen lernfähig. Es entstehen echte kognitive Systeme, die nicht mehr nur Schach spielen. Die Fortschritte sind spektakulär. Die Maschinen beginnen, die Welt zu begreifen, sie lernen selbstständig, korrigieren ihre Fehler und interpretieren unvorstellbare Datenmengen.

Deep Learning heißt das Zauberwort. Der Einsatz von intelligenten Robotern wird – und das kann auch mit der modern klingenden Formel „Industrie 4.0" nicht beschönigt werden – nach neueren Prognosen bis nahezu 50 Prozent der Jobs gefährden. Natürlich entstehen auch Berufe im Umfeld der Entwicklung und Steuerung von Computersystemen. Rasch werden jedoch Übersetzer, Lagerarbeiter und Lastwagenfahrer ersetzt werden. Aber auch Journalisten und Rechtsanwälte. Ärzte werden in zunehmendem Maße unterstützt werden, aber ihre Domäne noch behaupten können. Berufe, die Empathie und soziale Kompetenzen verlangen, sind noch ungefährdet. Andererseits wird an Kranken- und Altenpfleger-Robotern bereits gearbeitet. Algorithmen können segensreiche Wirkungen entfalten, nicht nur in der Medizin. Aber auch die Gefahren sind unübersehbar. Wenn – was vorhersehbar ist – Roboter intelligenter sein werden als Menschen, welche Rolle werden sie einnehmen? Was passiert, wenn sich Algorithmen als fehlerhaft erweisen? Ist die Evolution selbst lernender Maschinen vom Menschen noch prognostizierbar? Kann künstliche Intelligenz mit menschlichen Werten wie Freude, Freiheit, Gerechtigkeit, Menschenwürde gefüttert

werden? Was, wenn das nicht gelingt und nur hochgezüchtete kühle künstliche Intelligenz den Ton angibt?

Der Mensch darf nicht zur Summe seiner Daten, nicht zum bloßen Produkt degradiert werden. Ohne unser Einverständnis darf ein digitales Ich weder generiert noch von Dritten mit einem Eigenleben versehen werden, das sich auf das reale Ich (negativ) auswirken kann. Die Autonomie ist die Grundlage unseres Menschseins. Dieser Autonomie hat die Transparenz der Datenverarbeitung zu dienen und nicht umgekehrt die Transparenz des Individuums der Aufblähung von Big Data. Transparenzgesetze – auch für Unternehmen – können Abhilfe schaffen. Die notwendige Stärkung der Selbstbestimmtheit gilt es zu fördern. Etwa durch gesetzliche Betonung des Einwilligungserfordernisses der Betroffenen vor einer Datenverarbeitung. Das Individuum muss in transparenter, umfassender und verständlicher Weise über die Verarbeitung seiner Daten informiert sein, bevor es eigenverantwortlich hierin einwilligt oder eben auch nicht.

Die informationelle Eigenverantwortung muss frühzeitig erlernt werden, auch in Kindertagesstätten und in der Schule. Medienkompetenz sollen Lehrkräfte vermitteln, die während ihrer Ausbildung auf das Schulfach Medienkunde vorbereitet wurden. Fortbildungsangebote müssen sich an der raschen Entwicklung im IT-Sektor ausrichten. Das schließt Informatik-Inhalte durchaus nicht aus. Evaluationen sind unabdingbar. Schließlich muss sich der Gesetzgeber anstrengen, Ballhöhe zu erlangen, damit der stets größer werdende Abstand zwischen Rechtslage und Realität nicht noch weiter auseinander klafft. Es darf nicht sein, dass die Privatsphäre torpedierende IT-Produkte aus wirtschaftlichen Gründen entwickelt werden (müssen), nur weil der Gesetzgeber nicht in der Lage zu sein scheint, derartige grundrechtswidrige Entwicklungen zu kanalisieren.

Wie geht es weiter?

Ist es mit dem Schutz des Grundrechts der informationellen Selbstbestimmung und der Privatsphäre ernst gemeint, müssen unabhängige Kontrollinstanzen die rasanten Entwicklungsprozesse begleiten – nachhaltig und effizient! Davon ist jedoch die Ausstattung der Datenschutzbehörden weit entfernt. Eines gerät leider zunehmend in Vergessenheit: Die Würde des Menschen ist unantastbar – nicht aber ein fragwürdiges Geschäftsmodell.

Eberhard Zehendner

Perspektiven des Datenschutzes

Jens Kubieziel und Eberhard Zehendner befragten am 8. April 2015 den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI), Dr. Lutz Hasse.

Kubieziel: *Herr Dr. Hasse, können Sie uns kurz schildern, was der Inhalt Ihrer Tätigkeit ist, als Datenschützer und auch als Informationsfreiheitsbeauftragter.*

Hasse: Das sind eigentlich zwei Seiten einer Medaille. Als Datenschützer habe ich natürlich die Aufgabe, und die macht mir auch viel Freude, das Grundrecht der informationellen Selbstbestimmung der Bürger zu schützen. Und das Bundesverfassungsgericht hat ein weiteres Grundrecht hinzugefügt: die Vertraulichkeit und Integrität informationstechnischer Systeme. Das ist noch nicht so bekannt, fällt aber eben auch darunter.

Diese Grundrechte der Bürger schütze ich einmal, indem ich Behörden überwache und kontrolliere, ob sie die Datenschutzgesetze einhalten – was bisweilen nicht der Fall ist. Dann beanstande ich und wirke darauf hin, dass diese Lücken geschlossen, die Verstöße abgestellt werden.

Bei Unternehmen – da haben wir viel zu tun – habe ich mehr Möglichkeiten. Wenn dort Datenschutzverstöße festgestellt werden, kann ich Anordnungen treffen, bin also nicht nur Kontroll-, sondern auch Aufsichtsbehörde. Kann sagen, bauen Sie die Videokamera ab oder entlassen Sie Ihren Datenschutzbeauftragten. Wenn das nicht passiert, kann ich Zwangsgelder verhängen. Und wenn das immer noch nicht hilft, kann ich ein Bußgeld bis 300.000 Euro erlassen. Wir passen aber die Höhe des Bußgeldes der Stärke des Verstoßes und der finanziellen Leistungskraft des Unternehmens an.

Andererseits, als Informationsfreiheitsbeauftragter, habe ich dafür zu sorgen, dass Bürger Informationen von Behörden erhalten. Es gibt einen datenschutzrechtlichen Anspruch, dass der Bürger seine personenbezogenen Daten von der Behörde erhält. Es gibt jetzt aber auch einen Anspruch nach dem Thüringer Informationsfreiheitsgesetz, dass Bürger quasi alle Daten, die Behörden so haben, grundsätzlich bekommen können. Ziel ist, dass der informierte Bürger besser an demokratischen Prozessen teilhaben und gegenüber der Verwaltung eine gewisse Kontrolle ausüben kann. Das ist auch unmittelbar einleuchtend, finde ich.

Problem ist, dass dieses Gesetz gewisse Hürden enthält, die den Anspruch des Bürgers auf Information scheitern lassen. Etwa wenn öffentliche Interessen oder Urheberrechte gefährdet sind. Es gibt drei sehr lange Paragrafen, die für den Bürger Hürden aufbauen beim Zugang zu behördlichen Informationen. Diese Hürden müssen wir reduzieren, das wird im Koalitionsvertrag[1] auch zugesichert. Sehr ärgerlich ist, ein Unikum in der Bundesrepublik, dass ich als Informationsfreiheitsbeauftragter nicht kontrollieren darf, wenn Behörden sich auf einen Informationsverhinderungstatbestand berufen. Das ist absurd, das verstehen meine Informationsfreiheitsbeauftragtenkollegen aus anderen Ländern auch nicht, diese Vorschrift muss einfach gestrichen werden. Ich werde daher mit Hilfe meiner Mitarbeiter demnächst den Regierungsfraktionen sozusagen ein moderneres Informationsfreiheitsgesetz vorlegen.

Also, als Informationsfreiheitsbeauftragter muss man dafür sorgen, dass viele Informationen an den Bürger fließen. Es gibt aber Grenzen, wo der Datenschutzbeauftragte aktiv werden muss. Dort, wo es um personenbezogene Daten von anderen Bürgern geht, kommt das Datenschutzrecht ins Spiel, da endet der Informationsanspruch des Bürgers. Was nicht bedeutet, dass er dann gar keine Information bekommt; die personenbezogenen Daten können beispielsweise geschwärzt werden. Da muss man einen Mittelweg finden, aber das ist jetzt bei mir in einer Hand. Wir haben inzwischen schon gewisse Erfahrungswerte und können ganz gut abwägen, wann geht der Datenschutz vor, wann die Informationsfreiheit.

Der Weg zum Datenschützer

Kubieziel: *Das Datenschutzrecht ist ja erst in den 70er-Jahren in Gesetzesform gegossen und dann mehrfach novelliert worden. Und wie erwähnt, haben diverse Urteile des Bundesverfassungsgerichts neue Grundrechte begründet. Wie hat sich Ihre persönliche Auffassung von Datenschutz im Laufe Ihres Lebens geändert?*

Hasse: Fast schicksalhaft lautete das erste mir angebotene Promotionsthema: Der Datenschutzbeauftragte. Das war aber damals nicht mein Thema, ich wollte etwas im Umweltrecht machen, hatte da schon etwas vorbereitet. Dass ich dann Datenschutzbeauftragter geworden bin, findet auch mein Doktorvater interessant. Jedenfalls habe ich mich als Assistent schon mit diesem Grundrecht beschäftigt. Es gab 1983 das Volkszählungsurteil vom Bundesverfassungsgericht, da musste ich sehen, wie das eigentlich funktioniert, das stand ja nicht im Grundgesetz, und nach welchen Regeln das abläuft. Aber das hat das Bundesverfassungsgericht gut vorgegeben, eine Kombination aus Art. 1 Abs. 1 und Art. 2 Abs. 1 GG, mit einem Gesetzesvorbehalt, sodass der Gesetzgeber es einschränken kann – es funktionierte eigentlich genau wie andere Grundrechte auch.

Zwischendurch habe ich es etwas aus den Augen verloren, bin beruflich nach Thüringen gekommen, habe jedoch den einen oder anderen Aufsatz zu diesem Grundrecht geschrieben, als ich im Innenministerium tätig war, habe das immer mit mir herumgeschleppt und upgedatet. Dann bewarb ich mich beim Datenschutzbeauftragten und hatte eben auch den kleinen Vorteil, dass ich mich da schon ein wenig umgetan hatte. Ich wurde Referatsleiter, und so vertiefte sich das.

Persönlich hatte ich mit Datenschutz noch keine Probleme, habe sozusagen noch keine Eingabe bei mir selber gemacht. Ja, toller Beruf, macht mir große Freude, man eckt natürlich viel an – auch das macht mir große Freude, wann hat man schon einmal die Möglichkeit, völlig unabhängig für ein Grundrecht der Bürger streiten zu dürfen. Also, das ist schon schwer zu toppen.

Datenschutzrecht im Wandel

Kubieziel: *Wir sehen momentan verschiedene Änderungsversuche im Datenschutzrecht. Das Bundesdatenschutzgesetz soll zumindest in Bezug auf die Unabhängigkeit der Bundesdatenschutzbeauftragten an ein Urteil des Europäischen Gerichtshofs angepasst werden. Und auf der EU-Ebene gibt es Versuche, eine EU-Datenschutzrichtlinie zu begründen. Wie ist Ihre derzeitige Auffassung vom Datenschutz, ist das im Datenschutzrecht gut widergespiegelt, oder soll es Änderungen geben, und wenn ja, welche?*

Hasse: Die Europäische Datenschutzgrundverordnung, die jetzt geplant ist, wandelt sich ja stetig. Ich finde positiv, dass sich durchgesetzt hat oder zu haben scheint, dass die DS-GVO sogenannte Ausstiegsklauseln enthält, also einzelne Staaten die Möglichkeit haben, ihr hohes Datenschutzniveau weiterhin zu realisieren – das haben die Datenschützer auch immer gefordert. Wir haben dann in Europa flächendeckend einen datenschutzrechtlichen Minimalstandard, das ist grundsätzlich gut, und wir haben Leuchttürme wie z. B. Deutschland, hoffe ich wenigstens, die dann ihr Datenschutzrecht, Datenschutzgrundrecht und auch die Rechtsprechung dazu nach wie vor aufrechterhalten können.

Ansonsten einzelne Vorschriften, z. B. wann Unternehmen einen Datenschutzbeauftragten haben müssen. Ich hoffe, dass da noch einige Verbesserungen eintreten. Gehört habe ich, dass es dieses Jahr schon kommen soll, habe da aber so meine Zweifel. Die Datenflüsse in außereuropäische Staaten, insbesondere USA, TTIP beispielsweise, sind ja noch in der Diskussion. Ich hoffe, dass es da zu Kompromissen kommt, die nicht allzu weit entfernt sind von dem, was wir in Europa als Standard haben.

Durchsetzbarkeit von Datenschutzrecht

Kubieziel: *Von der juristischen Theorie zur Praxis: Lässt sich aktuelles Datenschutzrecht tatsächlich durchsetzen? Gibt es Hindernisse, mit denen Sie zu kämpfen haben?*

Hasse: Im nicht öffentlichen Bereich, gegenüber Unternehmen, ist mein Arsenal reichhaltig ausgestattet. Anfangs war der Gedanke ein wenig ungewöhnlich, dass auch Unternehmen eine Rechtsgrundlage brauchen, um Daten zu verarbeiten – das kennt man sonst nur von Behörden, gilt aber auch für Unternehmen – dieser Gedanke fasst nur allmählich Fuß. Aber wir schlagen auch bei Kontrollen in Unternehmen auf und stellen fest, dass datenschutzrechtlich noch nicht der Grund gelegt ist, vor allem dieser Gedanke, dass man eine Rechtsgrundlage braucht, unbekannt ist. Aber da haben wir die Möglichkeit, auch Druck auszuüben. Besser fände ich es allerdings, mit den Unternehmen in Sachen Datenschutz enger zu kooperieren: Runde Tische, Info-Veranstaltungen, etc. Ich plane einen Blog, in dem Unternehmen anonym ihre datenschutzrechtlichen Probleme äußern können – und wir beraten dann.

Im öffentlichen Bereich, also gegenüber Behörden, würde ich mir wünschen, mehr Kompetenzen zu bekommen, das steht auch im Koalitionsvertrag. Aber wenn ich gegenüber Behörden nicht nur Kontrollbehörde, sondern auch Aufsichtsbehörde wäre, würde das schon einen Bruch mit der herkömmlichen Rechtsordnung bedeuten. Denn da sind bisher Ministerien zuständig, und ich kontrolliere nur. Wenn ich Verstöße feststelle, beanstande ich die und informiere die Aufsichtsbehörden, damit die ihrerseits auf den Datenschutzrechtsbrecher, beispielsweise eine Kommune, einwirken. Das funktioniert aber manchmal nicht: Wenn wir einen Datenschutzverstoß feststellen, und

die staatliche Aufsichtsbehörde meint, dass das gar kein Datenschutzverstoß wäre, müssen wir wiederum diese Behörde überzeugen, dass doch ein Datenschutzverstoß vorliegt. Wenn sie sich unserer Meinung nicht anschließt, können wir diese Aufsichtsbehörde dann ebenfalls beanstanden.

Das ist alles sehr zeitraubend. Ich würde mir wünschen, dass – bevor eine Aufsichtsbehörde endgültig sagt, ein Datenschutzverstoß liegt nicht vor, obwohl wir sagen, es liegt einer vor – ein Einvernehmen oder schwächer ein Benehmen hergestellt wird. Dass man sich inhaltlich bespricht, ein Forum einrichtet, in dem wir uns argumentativ auseinandersetzen, und dann vielleicht eine dritte Instanz darüber befindet, wer auch immer. Und die Behörde im Schriftverkehr nicht nur eine halbe Seite schreibt und sagt, Datenschützer, ihr liegt daneben. Wir sind ja keine Spinner, wir sind die Fachleute, und wenn wir sagen, hier liegt ein Datenschutzverstoß vor, dann ist das in aller Regel so. Also da hätte ich schon gerne mehr Möglichkeiten, das Datenschutzrecht letztlich durchzusetzen. Aber da gibt es natürlich aus dem politischen Raum Gegenwind, meine Aktivitäten werden da ohnehin kritisch beäugt, und wenn ich dann noch mehr Möglichkeiten in die Hand bekomme, das sieht der eine oder andere nicht so gern. Wir müssen abwarten, wie innovativ Thüringen sich zeigen kann…

Zehendner: *Noch einmal zurück zum nicht öffentlichen Bereich. Speziell bei Facebook ändern sich die Datenschutzgrundsätze sehr häufig. Führt das nicht alleine schon zu einer Art Hase-und-Igel-Wettlauf, bei dem der Datenschutz zwangsläufig auf der Strecke bleibt?*

Hasse: Ja, da bleiben wir schon deshalb auf der Strecke, weil wir für Facebook nicht zuständig sind. Das war umstritten, aber Entscheidungen aus Schleswig-Holstein besagen, dass deutsches Datenschutzrecht nicht anwendbar ist, weil die Server von Facebook in Irland bzw. Kalifornien stehen. Das ist natürlich bitter. Wir können, was solche sozialen Netzwerke anbelangt, nur warnen und aufklären.

Ein spezielles Problem ist, wenn beispielsweise Lehrer mit ihren Schülern via Facebook kommunizieren. Offenbar finden Lehrer, die dieses Medium beherrschen, das toll. Wenn allerdings personenbezogene Daten – also Noten, Unterrichtsorte, Änderungen im Stundenplan, welcher Lehrer wann wo unterrichtet – fließen, zu einem Schüler, oder vom Schüler zum Lehrer oder irgendeiner Gruppe, dann ist diese Kommunikation nicht datenschutzsicher. Das ist dann ein Verstoß gegen § 9 Thüringer Datenschutzgesetz, der Sicherheit fordert, und an der mangelt es hier, weil Daten in die USA fließen, und wir nicht wissen, was dort mit den Daten gemacht wird – letztlich können sie bei der NSA landen.

Deshalb habe ich mich in dieser Richtung geäußert und gesagt, das ist datenschutzrechtswidrig. Wenn wir es feststellen bei einer Kontrolle vor Ort, wird es beanstandet. Inzwischen gibt es aber sogar Bestrebungen, schuleigene Server zu installieren, was natürlich wieder die Kostenfrage aufwirft. Über diese Server kann mit deutscher Software, wenn man so will, kommuniziert werden, was vielleicht nicht ganz so schick ist wie Facebook, aber so etwas findet schon statt, sogar hier in Thüringen. Das finde ich bemerkenswert, auf der Strecke müssen wir weiter machen. Wir haben da auch schon einen Plan.

Der TLfDI Dr. Hasse (Bildmitte) im Gespräch mit Jens Kubieziel (rechts) und Eberhard Zehendner

Zehendner: *Wenn Unternehmen klar unter inländisches Recht fallen und einen regionalen Bezug zu Thüringen haben: Entstünde da trotzdem das Problem, wenn die dauernd ihre Regularien ändern, dass man rechtlich zwar immer wieder gewinnt, aber der Erfolg wirkungslos bleibt, da es schon wieder neue Vorschriften oder neue Praktiken dort gibt?*

Hasse: Ja. Aber soweit wir hier in Kontrollen bei Unternehmen eingebunden waren, habe ich noch nicht festgestellt, dass fortlaufend die Nutzungsbedingungen geändert wurden. Ich muss allerdings zugeben, dass wir, was Software-Hersteller anbelangt, sozusagen die ersten Schritte gehen. Wir bauen gerade in unserem Technikreferat eine Versuchsstrecke auf, zwei nebeneinander gestellte Bürotische, und haben Hardware und Software angeschafft, die in der Lage ist, Apps zu überprüfen. Denn wenn ich richtig informiert bin, werden in Deutschland hergestellte Applikationen nicht auf Datenschutzkonformität überprüft, das finde ich ziemlich erstaunlich. Mein bayerischer Kollege hat damit begonnen, und wir fanden die Idee gut, uns dieser Problematik anzunehmen und Applikationen zu überprüfen. Beispielsweise beim Smartphone: welche Daten lesen sie zusätzlich zu ihrer eigentlichen Funktion aus, wohin fließen diese Daten. Das kann man, sagen mir jedenfalls meine Fachleute, inzwischen feststellen. Und falls wir da etwas feststellen, würden wir auch aktiv werden.

Datenschutz international

Zehendner: *Können Sie sich aber auch in Hinsicht auf international operierende Unternehmen, die nicht klar unter deutsches Recht fallen, für die Zukunft Lösungsmöglichkeiten vorstellen?*

Hasse: Da hoffen wir auf die europäische Datenschutzgrundverordnung. Dass international agierende Player, die ihre Produkte in Europa anbieten, an europäische Datenschutzstandards gebunden sind. Aber da ist im politischen Raum noch viel in der Diskussion. Die Datenschutzbeauftragten beäugen diesen Prozess aufmerksam. Wir versuchen auch Einfluss zu nehmen auf nationalpolitischer und europapolitischer Ebene, aber wir segeln manchmal unter der Flagge der Spielverderber, weil wir immer auf Probleme aufmerksam machen. Wir gelten als Bedenkenträger, die anderen ihren Spaß verderben wollen, aber a) ist es unsere Aufgabe, auf Rechtsverstöße und Gefahren hinzuweisen, und b) muss es einer tun. Denn sonst werden wir ja früher

oder später von wirtschaftspolitischen Gedanken, die dann allein herrschend sind, überrollt, und das kann nicht sein. Privatheit und Grundrechtsschutz stehen dem aus meiner Sicht mindestens gleichrangig gegenüber.

Zehendner: *Haben wir gegenüber Wirtschaftsgiganten, wie in den USA oder zukünftig vielleicht auch China, Chancen auf Datenschutz in unserem Sinne?*

Hasse: Auch da kann allein das Europarecht helfen. Aber Recht ist ja immer erst einmal nur geschrieben, die Frage ist dann, wenn sich beispielweise China oder die USA an europäische Standards halten wollten, wer kontrolliert das, woher wissen wir das? Hier in Deutschland ist es kein Problem, da gehen die Datenschutzbeauftragten los und schauen sich das an, die haben ja jederzeitiges Zugangsrecht zu allen Daten, bei Unternehmen und Behörden, und dann kann man sich ein Bild machen. Aber wie soll das dort funktionieren? Ich glaube, die Idee des Datenschutzbeauftragten existiert in diesen Ländern gar nicht. Man könnte versuchen, die Idee vom Grundrecht, und vom Schutz dieses Grundrechts durch eine gesonderte Institution, in solche Länder zu exportieren. Rechtskonforme Software könnte ja vielleicht auch ein Exportschlager werden.

Zehendner: *Könnte das auch ein Thema für die UN werden?*

Kubieziel: *Der UN-Menschenrechtsrat hat kürzlich die Position eines Sonderberichterstatters eingerichtet, der sich um Verstöße gegen das Grundrecht auf Datenschutz und Vertraulichkeit kümmern soll.*

Hasse: Ja, gute Idee! Unbedingt erforderlich. Denn die Datenflüsse sind global, die Kontrolle ist nicht global, die ist partiell, regional sozusagen, national, und da klaffen Lücken, die supranational geschlossen werden müssen. Europarecht ist ein Ansatz, Weltrecht ist natürlich der bessere.

Zehendner: *Facebook hat ja sehr viele Nutzer, die eigentlich auch eine Marktmacht haben. Aber man hat nicht das Gefühl, dass sie sie nutzen, um für sich Datenschutz durchzusetzen. Wird da nicht genug Druck gemacht?*

Hasse: Leider, es gibt ja keine richtigen Konkurrenzprodukte. WhatsApp war ein Konkurrenzprodukt, ist jetzt aber gleichbedeutend mit Facebook, weil gekauft. Ich weiß nicht, ob sich ein konkurrenzfähiges Produkt im Markt etablieren kann. Man liest und hört zwar immer, dass Facebook möglicherweise eine Erscheinung sein könnte, wie andere soziale Netzwerke auch, die inzwischen kaum noch eine Rolle spielen, dass Facebook in 10, 20 Jahren nicht mehr existiert. Aber die tun alles dafür, dass sie weiterhin existieren, und es fehlt an einem schicken Konkurrenzprodukt, das europarechtlichen oder besser noch deutschen Datenschutzregeln unterliegt. Die tun zwar immer so, als würden sie sich datenschutzrechtlich anpassen, aber die Datenschutzbeauftragten können das nicht kontrollieren.

Datenschutz als Bildungsthema

Kubieziel: *Ein Weg ist natürlich, sozusagen von oben als Datenschutzbehörde einzuwirken. Auf der anderen Seite wäre es aus meiner Sicht auch interessant, würden Nutzer auf die Einhaltung von Datenschutzrichtlinien oder überhaupt Grundsätzen des Datenschutzes drängen. Ich beobachte in letzter Zeit, dass es viele Diskussionen seitens der Datenschutzbehörden und anderer gibt, um Jugendliche aufzuklären. Trägt diese Diskussion bei Jugendlichen Früchte, entwickeln sie jetzt ein größeres Datenschutzbewusstsein? Was kann man noch tun, um hier weiterzumachen?*

Hasse: Eine Website[2] der Datenschutzbeauftragten namens *Youngdata* geht auf viele Fragen ein, wir müssen sehen, wie die Klickzahlen sind, ob das angenommen wird. Wir müssen auch propagieren, jeder in seinem Bundesland, dass es diese Seite gibt. Also, die finde ich gut. Jeder Datenschutzbeauftragte bearbeitet dort ein spezielles Thema, wir in Thüringen beispielsweise Video und Informationsfreiheit, aber es sind viele andere Themen, Smartphone, Facebook etc., auch Schule, da können sich Schüler und Lehrer informieren.

Bei mir steigt die Nachfrage zur Betreuung von Seminarfacharbeiten an Gymnasien. Anspruchsvolle Themen sind beispielsweise Facebook bzw. Smartphone. Facebook ist beendet, bei der Präsentation konnte ich miterleben, wie die vier Bearbeiter ihre Erkenntnisse vorgetragen haben. Ich hatte im Vergleich dazu das Publikum, also Schüler, die sich nicht vertieft damit beschäftigt hatten. Fragen aus dem Publikum und die Reaktionen machten den Wissensvorsprung derjenigen Schüler, die dieses Thema bearbeitet hatten, deutlich. Das macht natürlich Spaß, bedeutet aber auch Zeiteinsatz, Ressourceneinsatz. Schüler, die zu mir kommen, werden von Juristen und Informatikern während der Dienstzeit betreut, das halte ich für gut investierte Zeit. Meistens sind es ja vier Schüler oder Schülerinnen, die sind eine Art Multiplikatoren, die dann auf ihrem Spezialgebiet über Sonderkenntnisse verfügen. Die Ergebnisse werden auf meiner Homepage veröffentlicht und mit einer kleinen Broschüre an der jeweiligen Schule verteilt.

Dann müssen wir Lehrer, Schüler und insbesondere auch Eltern darüber aufklären, welche Gefahren im Netz bestehen, bei Smartphones, dass man Kinder nicht einfach vor einen PC setzt und in einer digitalen Parallelwelt surfen lässt, sondern kuckt, was die da machen, welche Gefahren bestehen. Manchmal habe ich den Eindruck, dass Eltern nicht so genau wissen, was da passiert. Vor kurzem hatte ich an einem Erfurter Gymnasium einen Elternkreis, 60, 70 Eltern, die interessante Fragen gestellt haben, naheliegende Fragen. Da müssen wir, auch wenn meine Behörde klein ist, weitermachen, direkt an die Leute herangehen, Eltern, Schüler, und eben auch Lehrer, um sie aufzuklären, denn es herrscht eine große Unkenntnis über das, was da eigentlich gemacht wird im Netz. Wer nur so eine Oberfläche bedienen kann, beherrscht ja das Medium nicht, und weiß nicht, was eigentlich passiert. Der erste Gedanke muss sein, ich habe hier eine Applikation, ein Programm, warum ist das kostenlos? Jeder bezahlt mit seinen Daten, auch wenn er es nicht wahrhaben will. Es muss in die Köpfe rein, dass die Leute sich Fragen stellen, auch bei WhatsApp, bei anderen Kommunikationsmitteln.

Und natürlich ist ganz wichtig, dass diese Inhalte auch an der Schule unterrichtet werden, was voraussetzt, dass die Lehrer entsprechend ausgebildet sind. Es gibt Anhaltspunkte, dass dem

nicht so ist. Ich stehe im Kontakt mit dem Kultusministerium und bin ganz guter Hoffnung, dass wir in der Lehrerausbildung weitere Schritte machen werden, dass Lehrer künftig in der Lage sein werden, das Fach Medienkunde so zu unterrichten, dass es den Schülern Spaß macht, und die Lehrer keine Angst haben müssen, vorgeführt zu werden. Und sie müssen Unterrichtsmaterialien an die Hand bekommen. Wir arbeiten gerade hier in meiner Behörde an einer kleinen Mediendatenbank, die Lehrern zur Verfügung gestellt werden soll. Da können sie beispielsweise anklicken, Klasse 8, Smartphone, und bekommen dann Angebote von uns. Zusätzlich wird in einer weiteren Datenbank Material für die Fortbildung von Lehrern zur Verfügung gestellt. Das sind kleine Schritte; wichtig ist die Lehrerausbildung, ich bin ganz guter Dinge, dass wir da etwas auf den Weg bringen können. Wir arbeiten gerade an einem Ausbildungsmodul für Lehrer.

Zehendner: *Gerade Jugendlichen wird vorgeworfen, ihre Daten aus Gleichgültigkeit zum Datenschutz freizügig weiterzugeben. Kann man das so sagen?*

Hasse: Ich habe unterschiedliche Erfahrungen gemacht. *Duckfaces*, diese Schmolllippen, oder *Sextings*, Bilder in Unterwäsche, werden häufig ins Netz gestellt und herumgeschickt, ohne dass die Betroffenen wissen, vor allem mit diesen Unterwäschebildern oder manchmal noch weniger als Unterwäsche, was mit diesen Bildern passieren kann. Es gab auch schon tragische Vorfälle, die in Selbstmord endeten.

Bei jüngeren Schülern meine ich aber festzustellen, dass sie nicht so sorglos mit ihren Daten umgehen wie andere Generationen zuvor. Die wissen schon, was passieren kann. Sie wissen es nicht genau, aber es gibt ja Informationen, Hinweise, Artikel, Fernsehsendungen, Clips, mit denen man sich über Gefahren informieren kann, das machen die offenbar. Da muss man unterscheiden zwischen streng privaten Dingen, die nach meinem Eindruck oft nicht mehr kommuniziert werden. Dann mittlere und harmlose Dinge, die in der Gruppe, im sozialen Netzwerk gestreut werden. Die echt intimen Dinge, habe ich mitunter wahrgenommen, werden nicht so sorglos verbreitet, wie man vielleicht den Eindruck hat. Ist vielleicht ein kleiner Hoffnungsschimmer.

Kubieziel: *Gibt es bei den Eltern ein ausgeprägtes Datenschutzbewusstsein? Oder muss man mehr noch als bei Schülern bei den Eltern ansetzen, sie weiterbilden?*

Hasse: Ich denke, beides. Die Eltern sind für mich noch ein bisschen Dunkelfeld. Ich habe, wie gesagt, jetzt einmal so eine Veranstaltung gehabt. Im privaten Kreis tauchen auch Fragen auf, die darauf hindeuten, dass Unkenntnis besteht, welche Gefahren für die Kids überhaupt bestehen im Netz. Dass aber auch eine große Sorge da ist. Eltern machen sich Sorgen, was kann meinem Kind passieren, wenn es gemobbt wird, was kann man dagegen tun. Das wissen die dann aber nicht. Geht man zum Datenschutzbeauftragten, geht man zur Polizei, kann man selber irgendetwas machen beim Provider, wie sind die Schritte, wie ist es mit Datenflüssen in der Schule, ist das alles rechtmäßig?

Ich muss mir noch überlegen, wie wir die Gruppe der Eltern erreichen. Von Schule zu Schule zu tingeln und dort die Eltern zu informieren ist sehr zeitaufwendig und personalintensiv. Wir machen das, aber es bindet zu viele Ressourcen. Ich muss noch überlegen, ob es mit einer Broschüre getan ist, die man ins Netz einstellt. Aber wer liest das? Es müsste kurz sein, interessant, eingängig, verständlich, witzig. Damit Eltern, wenn sie geschafft nach Hause kommen, abends noch Lust haben, da reinzukucken. Daran müssen wir noch arbeiten.

Mitwirkung der Betroffenen?

Zehendner: *Wer gut informiert ist über Datenschutz und auch sensibilisiert, den überkommt vielleicht angesichts der Handhabung durch Unternehmen ein gewisses Ohnmachtsgefühl. Brechen Unternehmen das Recht, müsste man sie juristisch bekämpfen. Oder wenn man eine Leistung erwerben will, muss man Angaben machen; sieht zwar nicht ein, wofür, bekommt aber diese Leistung nicht, wenn man es nicht tut, und wenn man sie gerade braucht, hat man nicht viele Alternativen. Und auch, wenn man vertrauenswürdigen Wirtschaftsunternehmen Daten überlässt, ist ja bei weitem nicht sichergestellt, dass die vertraulich bleiben – siehe Telekom. Kann das auch ein Grund sein, warum die Leute sagen, es nützt ja nichts, ich kann es auch bleiben lassen?*

Hasse: Mir ist das deutlich geworden nach den Offenbarungen von Snowden, verglichen mit dem Volkszählungsurteil 1983. Da ging es um Daten einer Volkszählung, da gab es eine Massenempörung, die letztlich auch im Volkszählungsurteil dazu geführt hat, dass diese Volkszählung zum Teil für verfassungswidrig erklärt wurde. Jetzt sind die Enthüllungen von Snowden in der Welt, und ich habe den Eindruck, das war ein bisschen viel, die Leute sind erschlagen. „Kleinigkeiten" wie eine Volkszählung, das ist überschaubar, konkret, ich weiß genau, wie ich betroffen bin, dagegen kann ich mich wehren. Seit der NSA-Affäre, aber es ist ja nicht nur NSA, sind die Leute, denke ich, desillusioniert. Es ist ungewiss, was passiert, es gibt fast wöchentlich neue Enthüllungen, kürzlich dass irgendwelche Smartphone-Apps von Geheimdiensten geknackt sind. Software steht ja immer im Verdacht, irgendwann geknackt, gehackt zu werden.

Dass außer uns Datenschutzbeauftragten jemand sagt, jetzt ist Schluss, jetzt schützen wir das Grundrecht ernsthaft, kann ich jedenfalls nicht erkennen. Wäre dem so, könnte man bestimmt deutlicher wahrnehmen, dass es da Aktivitäten gibt. Und der NSA-Untersuchungsausschuss? Man wird sehen, was sich da ergibt, ein Prozess, der von den Amerikanern im Übrigen aufmerksam betrachtet wird. Wenn es hier in Europa so bleibt, wie es ist, warum sollten die Amerikaner ihr Verhalten ändern? Ich hatte einmal das Bild gewählt, Dammbruch, und die Datenschutzbeauftragten stehen mit ihren Sandeimerchen da und versuchen, das Leck im Damm zu füllen. Aber besser ein Kampf wie gegen Windmühlen als gar kein Kampf mehr.

Als Datenschutzbeauftragter erlebt man natürlich, dass die Leute sich im Einzelfall, wenn sie konkret betroffen sind, schon vermehrt – wir haben ja stark steigende Fallzahlen – an uns wenden und sagen, hier hat der Nachbar eine Videokamera, oder hier habe ich den Verdacht, dass mit meiner Personalakte nicht rechtmäßig umgegangen wird. Da bekommen wir verstärkt Hinweise. Was den Umgang mit Daten anbelangt, die man irgendwo abgibt und einstellt, auch bei großen Unternehmen, da habe ich

schon den Eindruck, dass die Bürger ein gewisses Ohnmachtsgefühl entwickeln. Seit der Snowden-Affäre ist kein Vertrauen in nennenswertem Umfang wiederhergestellt worden – ich wüsste jedenfalls nicht, durch wen. Aber wenn es sich in Europa, in Deutschland abspielt, müssen sie sich dieses Ohnmachtsgefühl eigentlich nicht gefallen lassen. Da gibt es ja Institutionen, wie zum Beispiel den Datenschutzbeauftragten, der ihnen hilft.

Zehendner: *Sind Sie für Ihre Arbeit auf die Mitwirkung von Betroffenen angewiesen?*

Hasse: Ja, unbedingt!

Zehendner: *Auf einen reinen Verdacht hin können Sie nicht handeln?*

Hasse: Doch, rechtlich ist das möglich, wir können Behörden und Unternehmen kontrollieren, da gibt es keine Beschränkung. Und Tipps von Bürgern, von Mitarbeitern sind hilfreich. Erhalten wir am Nachmittag einen Tipp, und ist es gravierend, stehen wir am nächsten Morgen vor der Tür des Unternehmens und kucken nach dem Rechten. Das ist schon sehr wesentlich, gerade auch, was die Video-Problematik anbelangt. Es gibt ja keine Meldepflicht für Videokameras, wir wissen also nicht, wie viele da herumhängen bei Behörden oder Unternehmen.

Kubieziel: *Wie reagieren betroffene Unternehmen oder Behörden, wenn sie eine Videoüberwachung beanstanden? Wird das sofort abgebaut? Oder stoßen Sie auf großen Widerstand?*

Hasse: Im behördlichen Bereich kommt es glücklicherweise immer seltener, aber immerhin doch noch vor, dass uns mehr oder weniger unverhohlen gesagt wird: Ja, dann beanstandet uns doch. So offenkundiges Desinteresse am Datenschutz nervt natürlich. Deshalb bin ich dazu übergegangen, solche Verstöße von Behörden öffentlich zu machen. Nicht nur im Bericht, der alle zwei Jahre angefertigt wird, sondern sofort in den Medien. Man hat versucht, mir rechtlich eins dranzuhängen, aber nicht gewusst, dass es zu meinem sächsischen Kollegen eine BGH-Entscheidung gibt, die ausdrücklich klarstellt, dass man im behördlichen Bereich als Datenschutzbeauftragter so etwas machen darf. Das mache ich dann auch, und ich habe festgestellt, die Behörden mögen nicht, wenn ihre Verstöße sofort publiziert werden. Das ist fast ein schärferes Schwert als die Beanstandung.

In aller Regel sind Behörden schon daran interessiert, Recht einzuhalten. Bisweilen sind die datenschutzrechtlichen Vorschriften aber nicht so bekannt. Dass man für Datenerhebung, Datenübermittlung, Datenspeicherung, Datenlöschung eine Rechtsgrundlage braucht. Wenn man an einem Tisch sitzt mit meinetwegen fünf Behörden und tauscht Daten aus, und Behörde 1 verkündet ein personenbezogenes Datum, dann braucht sie dafür eine Rechtsgrundlage. Und die aufnehmenden Behörden brauchen eine Rechtsgrundlage, um diese Daten erheben zu dürfen. Daran fehlt es manchmal. Runde Tische sind immer datenschutzrechtlich kritisch, aber rechtliche Lücken kann man schließen, haben wir auch schon gemacht.

Im unternehmerischen Bereich haben wir dieses reichhaltige Instrumentarium, und wenn wir die Folterwerkzeuge einmal auspacken, läuft das in aller Regel. Wir werden nett und höflich behandelt, weil inzwischen bekannt ist, dass wir auch Bußgeldbescheide verhängen, und das in zunehmendem Maße. Das Bußgeld dürfen wir leider nicht selber behalten, das geht ans Finanzministerium. Aber das wäre auch eine Idee, dass wir an unseren eigenen Bußgeldern beteiligt würden. Trotzdem: Bußgelder sollten die Ultima Ratio sein – im Vordergrund muss ein, noch deutlich zu intensivierender, Informationsaustausch zwischen TLfDI und Unternehmen stehen.

Datenschutzbewusstsein und Datenschutzwissen

Zehendner: *Wenn wir Datenschutzbewusstsein und Datenschutzwissen der Bevölkerung über die letzten 20 Jahre grafisch auftragen, welche grundsätzlichen Verläufe sehen wir da?*

Hasse: Steigend. Man muss vielleicht unterscheiden zwischen Altersgruppen. Jugendliche sind, denke ich, schon ziemlich gut sensibilisiert, machen aber nach wie vor Fehler. Die mittlere Altersgruppe denkt, sie kann alles, blickt es aber eigentlich nicht so richtig. Auf Senioren habe ich ein besonderes Auge, weil die zwar aus verschiedenen Gründen eine gewisse Furcht haben, aber das hält sie dann unter Umständen ab, überhaupt diese Parallelwelt zu betreten. Das finde ich schade, denn dem Internet sollte man sich nicht einfach entziehen, man muss es nur eben vorsichtig benutzen.

Ich bin gerade in „Verhandlung" mit dem Senioren-Computer-Club Berlin. Zusammen haben wir Kontakt aufgenommen mit Senioren in Erfurt und wollen einen Senioren-Computer-Club – oder wie er auch immer dann heißen mag – gründen. Da sind wir schon auf einem guten Weg, und wenn das dann soweit gediehen ist, können wir über den Senioren-Computer-Club Erfurt – und vielleicht gibt es auch noch einen in Nordhausen, oder wo auch immer – durch Vorträge, das müssen nicht nur Datenschützer, sondern können auch andere sein, also Sie Informatiker zum Beispiel, denen die Materie nahebringen. Die haben Zeit und Interesse, aber zu Recht eine gewisse Furcht. Und die kann man ihnen nehmen. Ich habe eine Veranstaltung hier im Erfurter Rathaus dazu gemacht und festgestellt, dass da große Lücken sind. Wenn die irgendwann geschlossen sind, können die Senioren, die Silver Surfer, eben auch sicher surfen. Ist jedenfalls ein Ziel von mir.

Zehendner: *Wenn wir die vorliegenden Steigerungen im Bereich Sensibilisierung und Wissen abgleichen mit der Zunahme der Situationen, in denen Datenschutz relevant ist – technologisch bedingt explodiert da sozusagen die Szenerie, kann da diese Entwicklung mithalten, die wir in der Bevölkerung sehen?*

Hasse: Könnte mithalten, wenn man die Bevölkerung aufklären könnte. Das setzt aber voraus, dass man überhaupt weiß, was passiert. Stichwort Algorithmen: Ich weiß nicht, was die derzeit alles anrichten. Es ist ja auch eine segensreiche Geschichte, dass man mit Hilfe solcher mathematischer Formeln Dinge vorhersagen kann, auch menschliches Verhalten, das hat natürlich aber auch eine Schattenseite. Da ist, denke ich, viel in der Produktion, da passiert sehr viel, und der Gesetzgeber hinkt gnadenlos hinterher. Das kann man nicht mehr in Jahren ausdrücken, der hinkt Jahrzehnte hinterher, die modernsten Vorschriften des BDSG er-

fassen vielleicht 1 % dieser Entwicklung, mehr nicht. Man muss überlegen, wie man diese Lücken schließen kann. Ein Weg wäre Transparenz: die Unternehmen müssten offenlegen, welche Daten sie zu welchem Zweck verarbeiten.

Das streift auch, was Sie vorhin angesprochen haben: weiß der einzelne, oder kann der einzelne noch frei entscheiden, also das Stichwort *Einwilligung in sozialen Netzwerken*. Da muss man immer zustimmen, um auf die nächste Ebene zu kommen, um im Programm weitergeführt zu werden, und wenn man das nicht tut, dann kann man diese Leistung nicht in Anspruch nehmen. Ist das wirklich noch eine freiwillige – das ist ja Voraussetzung – Einwilligung, oder werden hier schon Zwänge aufgebaut, die man nicht mehr unter freiwilliger Einwilligung fassen kann? Diese Frage habe ich erkannt, und – meine Behörde weiß das noch nicht – die nächste Veranstaltung, die ich machen werde, wird sich mit Einwilligung befassen. Gibt es die freiwillige Einwilligung in diesen Bereichen überhaupt noch? Manche verneinen das schon. Ich will mich informieren und muss sehen. Aber es gibt keine Stelle, die informiert ist über das, was es an Software gibt. Auch wir Datenschützer wissen nicht, was es gibt. Und wenn man nicht weiß, was es gibt, kann man auch nur unzureichend aufklären.

Zehendner: *Ist das der Bereich Big Data Analytics, den Sie da ganz gezielt im Auge haben?*

Hasse: Ja, der sich ja beschleunigt. Wenn man dann noch sieht, dass Behörden mit Unternehmen kooperieren, dass Unternehmen praktisch Quasi-Behörden sind, nur unter privater Flagge segeln, und dass die Daten zwischen Behörden und Unternehmen vielleicht noch ausgetauscht werden, dann gibt es natürlich – ich habe das irgendwo gelesen, Big Government könnte man das nennen – Instanzen, die über Kenntnisse verfügen und mit Hilfe von Algorithmen diese Kenntnisse auch auswerten können – was andere nicht können. Da splittet sich möglicherweise die Gesellschaft in diejenigen, die wissen, und diejenigen, die nicht wissen und glauben müssen.

Und der Datenschutzbeauftragte von Thüringen weiß zu wenig, was aber, glaube ich, nicht auf mangelnde Initiative zurückzuführen ist – ich würde gerne mehr wissen. Wir können natürlich in die Unternehmen gehen und alles kontrollieren, aber der Aufwand ist groß, also müsste es vielleicht eine Bringepflicht der Unternehmen geben, bestimmte Dinge zu offenbaren; vielleicht nicht öffentlich, aber zumindest dem Datenschutzbeauftragten, oder einer anderen Institution.

Zehendner: *Die Rechtsprechung versucht häufig, bei neuen Problemfeldern die darauf noch nicht angepasste Gesetzgebung zu interpretieren, indem sie die Intention der Gesetze, die ja auch offenliegt, auf die neue Situation überträgt, und dann entsprechend auch Recht spricht. Hat man da bei Big Data Chancen vor Gerichten?*

Hasse: Gerichte können sich letztlich auch nicht über Recht hinwegsetzen. Sie können weiche Formulierungen des Gesetzgebers auslegen, ob aber auf diese Art und Weise das Recht auf Ballhöhe zur Realität kommt, bezweifle ich. Ich denke, der Gesetzgeber ist schon gefordert. Es gibt durchaus Initiativen, in Berlin, da etwas zu machen. Vielleicht sollte man in diesem Bereich die Datenschützer einbinden, weil da doch die Fachkompetenz ist. Bei Datenschutz fällt ja auch immer die Klappe bei vielen. Datenschutz, keiner weiß genau, was das ist, und dann heißt es, jetzt kommen die Chef-Verhinderer. Man könnte es ja anstelle von Datenschutz „Schutz der Privatsphäre“ nennen. Dann wird vielleicht deutlicher, wie der Einzelne betroffen ist. Und der Schutz der Privatsphäre, wenn man sich die ganzen Entwicklungen vor Augen hält, wird immer wichtiger, aber ich habe nicht den Eindruck, dass das schon erkannt wird.

Frühestmöglich für Privatheit sensibilisieren

Zehendner: *In welchem Alter müsste man denn anfangen, den „Schutz der Privatsphäre“ zu vermitteln?*

Hasse: Elternhaus, und dann Kindertagesstätte. Dass die Kinder schon einen Blick dafür bekommen, was in dieser Parallelwelt stattfindet. Kann man die beherrschen? Wo sind die Gefahren? Und dann kontinuierlich darauf aufbauen: Schule, Universität. Aber die Kenntnis der technischen Zusammenhänge bedeutet ja noch nicht, dass man sich Gedanken macht über Privatheit. Es müsste von ethischen Unterrichtseinheiten begleitet werden und, was ich ja immer propagiere, aber da renne ich ständig gegen die Wand, auch von rechtlichen Lehrmodulen. Dass so grundlegende Rechtszusammenhänge auch Schülern vermittelt werden.

Schüler werden im Zivilrecht unterrichtet und wissen, glaube ich, was rechtlich abläuft, wenn man Brötchen kauft. Aber von Grundrechten, insbesondere vom Grundrecht der informationellen Selbstbestimmung haben die noch nicht so viel gehört. Das erfahre ich ständig, wenn ich mit Schülern und Lehrern Kontakt habe und denen das dann erkläre. Das sind ganz einfache Zusammenhänge, aber die muss man eben kennen. Und man sollte sie auch kennen, damit man weiß, wann dieses Grundrecht der informationellen Selbstbestimmung beschädigt ist und wie ich mich dagegen wehren kann. Es gibt ja nicht nur die Datenschutzbeauftragten, es gibt auch Gerichte. Dass man den späteren mündigen Bürger rechtzeitig in Kenntnis setzt, wie er seine Rechte verteidigt.

Denn wenn der Staat dieses Grundrecht nicht verteidigt, muss man das eben selber tun. Dass immer mehr auf den Selbstschutz des Bürgers gesetzt wird, ist auch so eine Entwicklung, die ich für ungut halte, gerade in diesem Schutz-der-Privatheit-Sektor. Wenn dem so ist, ok, aber dann muss man das auch umsetzen. Zum Selbstschutz gehört, dass ich mich technisch versiert bewegen und schützen kann, aber auch, dass ich mich rechtlich bewegen kann. Aber es kommt leider immer gleich Gegenwind, wenn man sagt, von den wichtigsten Grundrechten müssten Schüler schon einmal gehört haben. Das betrifft nicht nur informationelle Selbstbestimmung, auch Meinungsfreiheit, Versammlungsfreiheit, Ehe und Familie, Religionsfreiheit.

Zehendner: *Gibt es hinsichtlich der Vermittlung Unterschiede zwischen den Bundesländern? Ist ein Bundesland besonders fortschrittlich?*

Hasse: Keine wesentlichen, würde ich sagen. Rheinland-Pfalz ist, was Medienkompetenz anbelangt, Vorreiter. Die haben so-

zusagen die Seite *Youngdata* erfunden und freundlicherweise allen Ländern zur Verfügung gestellt.

Zehendner: *Liegt es auch am jeweiligen Landesdatenschutzbeauftragten, wieviel in diesem Bereich gemacht wird?*

Hasse: Ja, natürlich. Aber der ruft nur in den Wald hinein. Wie es dann herausschallt, das ist die politische Ebene. Die Politik muss begreifen, dass dieses Feld wichtig ist und immer wichtiger wird. Es sei denn, man macht an Privatsphäre einen Haken und sagt, das gibt es gar nicht mehr, und man verkündet die Post-Privacy-Ära. Finde ich aber schlimm, denn Privatheit hat eben auch etwas mit Menschenwürde zu tun – was möchte ich von mir preisgeben, wie will ich von anderen als Individuum wahr genommen werden. Und diese Selbstbestimmung zu schützen, ist Aufgabe aller staatlichen Gewalt.

Das ist aber, ich habe ein bisschen Hoffnung, im Koalitionsvertrag gebührend verankert. Also dass der Datenschutzbeauftragte mehr bekommt: dass ich mehr Stellen bekomme, dass ich mehr Kompetenzen bekomme sowohl im nicht öffentlichen als auch im öffentlichen Bereich, dass ich eingebunden werde, dass die Gesetzeslage novelliert wird. Ich denke, da hat es Klick gemacht, das ist erkannt worden. Man muss jetzt sehen, wie es umgesetzt wird. Was ich so höre, was ich so mitbekomme von Rot-Rot-Grün[3], ist das auf gutem Weg. Mal sehen, wie es sich entwickelt.

Zehendner: *Konkret in Form von Instrumenten, die sie zur Verfügung haben, um dort einen Bildungsauftrag zu erfüllen?*

Hasse: Es dreht sich ja immer – viele mögen es schon gar nicht mehr hören – um Stellen. Ich brauche Leute, die die Arbeit bewältigen können. Wenn wir rausgehen an Schulen, an Universitäten, und machen da was, dann können wir das gerne tun. Aber wir müssen ja auch unsere anderen Dinge erledigen. Und wenn da noch so eine Sache wie Immelborn[4] reingrätscht, das bindet natürlich viele Kräfte. Tja, wie könnte man es anders machen, ohne mehr Leute? Schwierig. Multiplikatoren produzieren.

Zehendner: *Das ist eigentlich genau das, was Sie jetzt machen.*

Hasse: Versuchen, in der Lehrerlandschaft, Elternlandschaft, Schülerlandschaft. Ich bemühe mich auch, private Institutionen ehrenamtlich da einzubinden. Aber es darf ja immer nichts kosten, oft scheitert es dann schon an den Fahrtkosten. So ganz zart, denke ich, habe ich es in den letzten drei Jahren hingekriegt, dass das Rad anfängt, sich zu bewegen, aber es ist noch lange nicht in voller Fahrt.

Zehendner: *Aber man kann sagen, Thüringen ist auf einem guten Weg?*

Hasse: Ja, ich hoffe.

Zehendner: *Auch durch die neue Landesregierung? Steckt da Potential drin?*

Hasse: Ja, auf jeden Fall. Man muss jetzt sehen, ob die Papierform umgesetzt wird, aber ich gehe einmal davon aus. Ich habe auch schon Gespräche geführt, ich bin da wirklich ganz guter Dinge.

Schwieriger Umgang mit der Informationsfreiheit

Kubieziel: *Ich würde gerne noch einmal zu Ihrem zweiten Arbeitsbereich kommen, zum Informationsfreiheitsrecht. Können Sie quantifizieren, in welchem Verhältnis Datenschutz zu Informationsfreiheit steht?*

Hasse: Die Inanspruchnahme der Informationsfreiheit ist quantitativ leider noch zu vernachlässigen. Wir hatten in den letzten zwei Jahren 40 Fälle, ich habe den Bericht jetzt gerade vorgestellt. Was zeichnet sich da ab? Die Behörden – das Gesetz richtet sich ja nur an diese – haben oft keine Kenntnis, dass es dieses Gesetz gibt, oder wissen nicht damit umzugehen. Wenn jemand eine Information herausgibt, könnte das ja Geheimnisverrat sein! In diesem Spannungsfeld bewegt sich der Mitarbeiter, da ist das Gesetz verbesserungswürdig, muss mehr Klarheit geschaffen werden. Auch die Büsche, in die sich Behörden schlagen können, um Information zu verhindern, müssen ausgerupft und die Kontrollrechte des TLfDI unbedingt erhöht werden.

Die Bürger fragen dieses ihnen zustehende Recht nach unserem Dafürhalten nicht in genügendem Umfange nach. Journalisten haben noch das Auskunft- und Presserecht, das etwas anderes ist als das Informationsfreiheitsrecht und eigentlich etwas besser für Journalisten. Aber auch die berufen sich auf die Informationsfreiheit. Ich stehe gerade im Kontakt mit einem Journalisten, der Information auf diesem Wege zu bekommen versucht, aber an den Hürden scheitert, die das Gesetz selber aufbaut. Und ich kann nicht kontrollieren, ob die Behörde sich zu Recht auf diesen Nichtauskunftsgrund beruft oder nicht. Daran müssen wir etwas ändern. Ich hoffe, wenn die Behörden klarer wissen, was sie preisgeben dürfen und was nicht, wird dieses Informationsrecht weniger eingeschränkt.

Wir wollen das Gesetz in diese Richtung novellieren, zu einem – steht auch im Koalitionsvertrag – Transparenzgesetz. Das wird dann das Amts- oder Dienstgeheimnis zur Ausnahme machen. Im Grundsatz werden alle Informationen, über die Behörden verfügen, proaktiv ins Netz gestellt, nicht erst auf Antrag. Vorbild Hamburg, die scheinen zufrieden zu sein mit ihrem Gesetz. Rheinland-Pfalz ist auf dem Weg. Wir kucken jetzt, was die für Erfahrungswerte haben.

Scheint aber ein Kraftakt zu sein: einheitliche Soft- und Hardware, Beschulung der Beamten, viele zu klärende Rechtsfragen, insbesondere, was ist noch ein Geheimnis, und was ist kein Geheimnis. Es geht ja nicht nur um behördliche Geheimnisse, Behörden verfügen auch über Informationen von Unternehmen. Da müssen wir viel nachdenken, das wird auch Zeit in Anspruch nehmen. Aber wenn wir dann einmal so weit sind, ist das ein Paradigmenwechsel, komplett weg vom Dienstgeheimnis, hin zur Information, die Behörde als Dienstleister und nicht als Geheimnisverwalter.

Kubieziel: *Wenn es schon für Beamte, die diese Fälle bearbeiten, fragwürdig ist, ob das Geheimnisverrat oder Informationsfreiheit ist, wäre es dann nicht sinnvoll, in der Behörde einen Informationsfreiheitsbeauftragten zu installieren?*

Hasse: Das könnte der Datenschutzbeauftragte mitmachen, jede Behörde muss ja einen haben. Das ist natürlich eine Dop-

pelbelastung, die sich auch in Stunden niederschlagen müsste, die diese Person zur Verfügung hat. Aber gerade weil diese, speziell die informationsrechtliche Materie im Fluss ist und komplizierte Rechtsfragen anschneidet, finde ich es gut, wenn das *eine* Person ist; die natürlich fortgebildet werden müsste, und die sich auch selber fortbildet und dann über gewisse Kenntnisse in diesem Bereich verfügt und Ansprechpartner ist für die eigene Behörde. Ja, das wird möglicherweise auch in der Novellierung stehen.

Kubieziel: *Natürlich müssen die Bürger erst einmal überhaupt von ihrem Recht auf Informationsfreiheit wissen. Aber gibt es auch Formvorschriften, die ein Bürger einhalten muss, wenn er solche Informationsfreiheitsrechte beantragen will? Gibt es da vielleicht auch Hilfestellungen für die Bürger?*

Hasse: Das ist alles noch im Fluss, zu einem Zeitpunkt X nach bisheriger Rechtslage werden gewisse Informationen in einem Register abrufbar sein. Darüber hinaus muss der Bürger einen Antrag stellen. Wird dieser abgelehnt, kann der Bürger zu mir kommen, muss aber wissen, dass dies nicht die Rechtsmittelfristen unterbricht. Wenn er auf Nummer Sicher gehen will, nach derzeitiger Rechtslage, und da sind meine Flügel ja gestutzt, sollte er auch den Weg zum Verwaltungsgericht einschlagen und dort letztlich klagen.

Wir versuchen, gemeinsam mit der Behörde an die Information heranzukommen, die der Bürger haben will. Da haben wir bisher meistens Erfolg gehabt, in den wenigen Fällen, die wir hatten, weil die Behörde oft gar nicht wusste, wie geht sie mit dem Informationsfreiheitsgesetz um, und wenn wir ihr erklärt und am besten auch schriftlich mitgeteilt haben, ihr könnt das jetzt so sagen, dann ist der Beamte ja auch geschützt vor dem Vorwurf, ein Dienstgeheimnis zu verraten.

Quo vadis?

Zehendner: *Gibt es dringende Probleme im Datenschutz, die wir noch nicht angesprochen haben?*

Hasse: Da ich gerne wissen will, wo was läuft, wäre mir daran gelegen, dass Videokameras gemeldet werden müssten. So eine Vorschrift gibt es noch nicht. Videokamera, das ist ja jetzt nicht so der Brüller, aber gemessen an der Anzahl der Videokameras, die wir höchstwahrscheinlich hier in Thüringen haben, einschließlich der Videokameras im Wald, ist das schon ein Einschnitt in die Privatsphäre. Und gewisse Meldepflichten im nicht öffentlichen Bereich, das siedelt dann natürlich im Bundesdatenschutzgesetz, daran wäre mir natürlich auch sehr gelegen. Und dann gibt es ja noch spezielles Datenschutzrecht, z. B. bei der Polizei, da könnte ich mir vorstellen, dass hier und da noch ein Richtervorbehalt eingebaut wird, damit ein neutraler Jurist darüber befindet, ob ein bestimmter Eingriff in dieses Grundrecht zulässig ist oder nicht. Wir haben bestimmte Punkte, die verbesserungswürdig sind, und wollen da auch einen Vorstoß machen, das Thüringer Datenschutzgesetz nach unserer Auffassung zu novellieren. Im Großen und Ganzen geht es, aber wir haben gewissen Änderungsbedarf.

Und natürlich die Thematik *Industrie 4.0* – bei allem dargestellten Euphemismus zu dieser Entwicklung des Internets der Dinge sehe ich die Schattenseiten, zumal sich auch auf dem Gebiet der Entwicklung künstlicher Intelligenz (*Deep Learning*) Prozesse auftun, deren soziale Implikationen wir nicht erahnen können. Hier bedarf es konzentrierter Aufmerksamkeit, damit aus *Big Data* nicht ein „Monster Data" wird.

Zehendner: *Vielleicht noch einen Blick in die Zukunft. Wie könnte sich denn in zehn Jahren die Situation Datenschutzproblematik und Datenschutzrecht darstellen, die Möglichkeiten der Behörde, dann dort einzugreifen?*

Hasse: Tja, das hängt von vielen Faktoren ab. Wird die Gefährdung der Privatheit nicht erkannt, wird es sich verschlechtern. Wird sie erkannt, denke ich, kommen wir nicht umhin, mehr Schutzmechanismen einzuziehen. Denn sich darauf zu verlassen, dass das, was im Gesetz steht, auch umgesetzt wird, da hat uns ja Edward Snowden eines besseren belehrt. Und wenn das politisch als wichtig erachtet wird, was ich mir wünschen würde, müssen die Kontrollinstanzen verstärkt werden. Ich hoffe, dass dieser Gedanke in 10 bis 20 Jahren gegriffen hat.

Anmerkungen

1 *Gemeint ist der Koalitionsvertrag der aktuellen Thüringer Landesregierung.*
2 *http://www.youngdata.de/*
3 *Gemeint ist die aktuelle Thüringer Landesregierung.*
4 *Der TLfDI stellte 2013 in Immelborn ein umfangreiches Lager völlig ungesicherter, sensibler Akten sicher.*

Lutz Hasse, Jens Kubieziel, Eberhard Zehendner

Dr. **Lutz Hasse** ist Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (Biografie auf S. 21 dieser Ausgabe).

Jens Kubieziel berät Thüringer Unternehmen in Fragen der IT-Sicherheit und des Datenschutzes. Daneben ist er ehrenamtlich bei *TorServers.net* tätig und stellt Anwendern Techniken zur Anonymisierung und Zensurumgehung bereit.

Eberhard Zehendner ist Professor für Technische Informatik an der Friedrich-Schiller-Universität Jena, wo er u. a. im Bereich *Informatik & Gesellschaft* lehrt. Seit 2013 gehört er dem FIfF-Vorstand an.

Dagmar Boedicker

Die EU-Datenschutz-Grundverordnung und die „regulatorische Kooperation“

Was die Freihandelsabkommen noch bringen

Neben dem höchst umstrittenen Investorenschutz ISDS[1], der Angleichung von Standards und der Beseitigung nicht-tarifärer Handelshemmnisse sehen TTIP und TiSA die regulatorische Zusammenarbeit *zwischen der EU und den USA vor. Sie soll rechtliche Vorgaben angleichen sowie verhindern, dass bei neuen Gesetzesvorhaben Handelshemmnisse entstehen. Für die Bürgerinnen und Bürger kann sie unerwünschte Nebeneffekte haben. Am Beispiel der EU-Datenschutz-Grundverordnung erleben wir sie schon.*

Was ist regulatorische Zusammenarbeit?

In einem bi- oder multilateralen internationalen Abkommen vereinbaren die Partner, sich bei zukünftigen Regulierungsvorhaben (Gesetzen oder Standards) zu konsultieren und ihre Normen so anzugleichen, dass keine oder möglichst wenige Hemmnisse für den internationalen Handel entstehen. Dabei verpflichten sie sich auf wechselseitige Konsultationen und vereinbaren einen institutionellen Rahmen, beispielsweise einen Regulierungsrat und Arbeitsgruppen. Das Abkommen kann sich auf Gestaltung, Kontrolle, Durchsetzung oder nachträgliche Änderung von Regulierungsvorhaben beziehen, aber auch auf den gesamten Prozess.

Die OECD beschreibt regulatorische Zusammenarbeit so:

> *„There is no internationally agreed definition of international regulatory cooperation. For the purpose of this work, international regulatory cooperation is defined as any agreement or organisational arrangement, formal or informal, between countries (at the bilateral, regional or multilateral level) to promote some form of cooperation in the design, monitoring, enforcement, or ex-post management of regulation, with a view to support the converging and consistency of rules across borders.“* [2]

Im Februar 2015 haben 169 zivilgesellschaftliche Organisationen eine Stellungnahme gegen die regulatorische Kooperation durch TTIP unterzeichnet,[3] deren Botschaft auch für andere Freihandelsabkommen gilt: *„‚Regulatorische Zusammenarbeit' schwächt massiv den Einfluss von Bürgern.“* Das tut sie, weil im Prozess der Konsultation und Angleichung vor allem Konzerne mit transnationalen Interessen mitmischen. Mit ihnen stimmt sich die Exekutive ab, bevor die Abgeordneten überhaupt einen Gesetzesvorschlag zu sehen bekommen. Wenn ein unregulierter Zustand den Konzernen mehr nützt, kann ein *chilling effect* entstehen; die Regulierung unterbleibt, weil mögliche wirtschaftliche Folgen die Politik verschrecken. Auch nachträglich können so Gesetze *entschärft* werden!

Regulierer mit Stockholm-Syndrom[4]

Bei meiner Recherche zur *regulatory cooperation* bin ich über einen Begriff gestolpert, der im Zusammenhang mit der Pharma-Industrie auftauchte, die *regulatory capture[5]. Linguee[6]* bietet als Übersetzung an: „Vereinnahmung des Regulierungsakteurs durch die zu regulierende Branche“. Diese regulatorische Vereinnahmung beobachten wir in den Wirren unseres Rechtsstaats an vielen Stellen, von Umweltauflagen wie der Zulassung von genveränderten Organismen, dem Fracking oder der Regelung des Fluglärms am Frankfurter Flughafen bis zur Einführung der privaten Altersvorsorge auf Wunsch der Versicherungswirtschaft, vom Gesundheitswesen bis zur Datenschutz-Grundverordnung.

Frédéric Boehm[7] zitiert Douglas C. North (1994):

> *„Institutions are not necessarily or even usually created to be socially efficient; rather they, or at least the formal rules, are created to serve the interests of those with the bargaining power to create new rules.“*

Es wäre zu einfach, den Regulierungsakteuren bloße Korruption zu unterstellen, auch wenn es sicher verlockend ist, sich auf Augenhöhe mit den wirklich Mächtigen zu fühlen. Das ist aber noch keine Vorteilsannahme oder Bestechlichkeit. Oft bewegt den Gesetzgeber die Angst vor Sanktionen nach dem Investorenschutz, die Sorge um die Wettbewerbsfähigkeit auf einem globalen Markt oder um Arbeitsplätze. Oder die Notwendigkeit, mit Experten zusammenzuarbeiten, die von der jeweiligen Branche finanziert werden, weil dem parlamentarischen Gremium oder der Behörde die Fachleute fehlen. Das kommt auch in der EU-Kommission vor.[8] Regulierung in unserer komplexen globalisierten Welt wird von denen beeinflusst, die über die Macht verfügen. Die Zivilgesellschaft bemüht sich um Einsicht in die Folgen, ihr fehlen aber meist die Ressourcen schon für die Einschätzung angesichts von komplexen und intransparenten Entscheidungen, erst recht aber für wirksamen Druck nach einer Abwägung der Folgen.

Welche Interessen verfolgen die USA?

Die US-Handelskammer verfolgt in ihrem *Global Regulatory Cooperation (GRC) Project[9]* eine Angleichung der Handels-, Regulierungs- und Wettbewerbspolitik mit dem Ziel offener Wettbewerbsmärkte. Ob global geöffneter Wettbewerb allerdings im Interesse der Menschen ist, darüber lässt sich trefflich streiten. Die 16-seitige GRC-Broschüre aus dem Jahr 2010 offenbart interessante Einblicke in die wirtschaftspolitischen Überlegungen:

> *„Where private sector companies are obliged to compete with national champions, the market is often skewed against free enterprise.*[10] *Where government is vested in* state capitalism, *its preference is often manifested in an array of regulatory actions from oversight to licensing and procurement.“*[11]

Im Fokus ist wohl gar nicht so sehr die EU, vielmehr geht es um große *staatskapitalistische* Räume. Sorgen bereitet die Volksrepublik China, Europa kommt lediglich als ein Partner mit möglicherweise gleichen Interessen ins Bild. Die *Trans-Pacific Partnership (TPP)* beschäftigt die USA mehr als TTIP oder TiSA, denn sie können ihre Ziele mit oder ohne die EU verfolgen – Kompromisse erscheinen ihnen möglich, aber nicht unbedingt notwendig. Wenn diese Einschätzung zutrifft, könnte das auch ein Ansatzpunkt für europäische zivilgesellschaftliche Arbeit sein: Wir können auf Freihandelsabkommen verzichten, wenn sie keine Vorteile für Menschen oder Umwelt bringen. Investitionen in der EU müssen weiterhin politische Ziele verfolgen dürfen, wenn unsere Werte andere sind als Wachstum und freie, entweder ungeregelte oder nach einem Wettlauf um die niedrigsten Standards geregelte Märkte.

> *„U.S. regulators should be empowered to advocate for better regulation in cooperation with their international counterparts in order to help foster U.S. export growth."* [12]

und

> *„Smooth movement of goods and services across borders requires transparent, effective, enforceable and mutually coherent regulatory systems that are* risk and science based, *adhere to international best practices, and feature close collaboration among governments and their stakeholders."* [13]

Hier wird deutlich, wie sich die angelsächsische und die kontinentaleuropäische Rechtskultur unterscheiden: *risk and science based* bedeutet in US-amerikanischem Rechtsverständnis, dass zu regeln ist, was wissenschaftlich als riskant bewiesen ist. Diese Auffassung lässt sich auf das *Nachsorge*-Prinzip zurückführen, nach dem es keinen Anlass gibt, nützlich erscheinende Produkte nicht einzuführen. Sollten sie sich allerdings als schädlich erweisen, tragen die Anbieter das Risiko, dass Geschädigte hohe Summen einklagen können. Die europäische Auffassung folgt dagegen dem *Vorsorge*-Prinzip: Wer ein Produkt einführen möchte, muss sich an einem gesetzgeberischen Rahmen orientieren, der Risiken vorsorglich ausschließen soll.

Es wäre schwierig nachzuweisen, ob die eine oder andere Grundüberlegung einer Gesellschaft mehr nützt. Für Geschädigte im europäischen Rechtsraum liegen die Hürden für Schadenersatz hoch, sie haben es nicht leicht, ihre Rechte durchzusetzen. Es dürfte aber offensichtlich sein, dass sich die beiden grundsätzlich verschiedenen Konzepte nicht einfach verschmelzen lassen. Zwar spricht nichts gegen eine fachliche Kooperation von Regulierungsexperten und Wissenschaft, wenn sie in der Öffentlichkeit stattfindet und vernünftige Empfehlungen zu Gunsten von Mensch und Natur macht, das ist aber im Zusammenhang mit den Freihandelsabkommen nicht zu erkennen.

Europäische Werte …

Die europäischen Werte sind in den europäischen Verträgen verankert, vor allem in der Grundrechte-Charta. Wenn es so etwas wie ein *Super-Grundrecht* gibt, so ist es die Menschenwürde als ihr Grundkonzept. Von der Menschenwürde leiten sich die europäischen Freiheitsrechte ab. Auch darin unterscheidet sich das kontinentaleuropäische Rechtsverständnis von dem der USA und Großbritanniens, wo sie sich von der Freiheit von staatlichen Eingriffen ableiten, dem *right to be left alone.*

… und die Datenschutz-Grundverordnung (GVO)

Die Sicherheits-technische Lage in der EU ist ein Flickenteppich, für fast alle Bereiche sind wir auf Technik aus den USA oder China angewiesen. Das beunruhigt angesichts eines Rechtsverständnisses in China, das sich in einer großen chinesischen Firewall und zwei Millionen Zensoren für 649 Millionen Nutzerinnen und Nutzer ausdrückt[14]. Und eines Rechtsverständnisses der US-Konzerne, mit dem sie seit vielen Jahren die Erschließung globaler Märkte vorantreiben und sich erst auf ausdrückliche Aufforderung der örtlichen Justiz dazu bequemen, deren Regulierung teilweise einzuhalten. Das Motto im Silicon Valley lautet *Disruption*[15], und dieses Vorgehen belohnt diejenigen, die sich am ungeniertesten über geltendes Recht hinwegsetzen. So gesehen ist es geradezu Notwehr, die europäischen Standards gegen regulatorische Zusammenarbeit zu verteidigen. Und umso wichtiger ist eine EU-Datenschutz-Grundverordnung.

2013 haben wir als FIfF e.V. dem Europaparlament (EP) eine Stellungnahme geschickt, in der wir die GVO grundsätzlich unterstützt und einige Verbesserungsvorschläge gemacht haben. Seit mehr als einem Jahr verschleppt der EU-Rat die Verabschiedung. Für TTIP ist im EP der INTA-Ausschuss[16] federführend, der wirtschaftlich ausgerichtet ist. Für die GVO ist der LIBE-Ausschuss[17] zuständig. Er wird eine Stellungnahme dagegensetzen, die bürgerrechtliche Positionen verteidigt und fordert, den Datenschutz aus TTIP und TiSA herauszuhalten.[18] Angesichts der Verhandlungen über die Freihandelsabkommen ist es dringlich, der Liberalisierung und Deregulierung einen Datenschutz mit Biss entgegenzusetzen.

Anscheinend steht die *EU-Datenschutzreform* aber *kurz vor dem Aus.*[19] Zweckbindung und Datensparsamkeit, zwei Kernprinzipien, stehen zur Disposition. Im Entwurf des EP hätten Betroffene bei einer Zweckänderung ihre Einwilligung geben müssen, nach den durch *Statewatch* geleakten Positionen des EU-Rats sieht das jetzt anders aus, demnach:

> *„… dürfen Unternehmen, Behörden oder ‚Drittparteien' Daten für weitere Zwecke verarbeiten, wenn deren*

Dagmar Boedicker

Dagmar Boedicker ist Journalistin und technische Redakteurin und hat Politikwissenschaft studiert. Sie ist seit langem Mitglied des FIfF, war Vorstandsmitglied und stellvertretende Vorsitzende, und ist Redakteurin der *FIfF-Kommunikation*.

‚berechtigte' Interessen ‚schwerer wiegen' als die des Betroffenen. Bislang durften sie das nach deutschem Recht auch. Problematisch wird die Regel […] in Kombination mit Artikel 6.3.a (a), wonach Unternehmen und Behörden für einen bestimmten Zweck erhobene Daten ohne Weiteres auch für andere Zwecke nutzen können, ‚solange diese Zwecke mit [dem] ursprünglichen Zweck vereinbar sind.'"[20]

Und zur Datensparsamkeit schreibt Christiane Schulzki-Haddouti:

„So müssen Datenerfassungen nicht mehr ‚auf das nötige Minimum beschränkt', sondern lediglich ‚nicht exzessiv' hinsichtlich des verfolgten Verarbeitungszwecks sein."[21]

Lobbyplag[22] hat die 11.000 Seiten analysiert, belegt sie mit Quellen und stellt fest, dass allein der Spitzenreiter Thomas de Maizière 51 Änderungsforderungen angemeldet hat, die den Datenschutz abschwächen. Weitere Schwächungen haben UK, Irland, die Tschechische Republik, Schweden, Belgien, Niederlande und Frankreich eingebracht. 26 Prozent der Änderungen zu den wichtigsten GVO-Kapiteln 1 bis 3 würden den jetzigen Datenschutz-Standard verschlechtern. Angesichts der gleichzeitig laufenden Verhandlungen zu den Freihandelsabkommen wäre es bemerkenswert, wenn diese Verschlechterungen den Innenministern und Abgeordneten von allein eingefallen wären. Pläne, dass Gesetze, Verordnungen oder Standards zum Datenschutz in Europa künftig nicht mehr ohne Einmischung der USA verabschiedet werden sollen, sind angesichts der technologischen Übermacht von US-Unternehmen im IT-Bereich und den Praktiken der Geheimdienste (nicht nur der US-amerikanischen) indiskutabel.

Wenn Freihandelsabkommen, …

… dann solche, die höhere Standards für den Schutz von Menschen und Natur vereinbaren. Andere braucht die Welt nicht! Stattdessen umtanzen Politik und Wirtschaft heute gleich zwei goldene Kälber: das des Wachstums und das des Profits. *Wachsen oder Weichen* führt zu immer größeren Unternehmen und Machtkonzentration. Der meiste Profit lässt sich auf den verlängerten Werkbänken des Westens machen, dort wo niedrige Standards für komparative Kostenvorteile sorgen. Und die Marktmacht großer Konzerne verhindert, dass der globale Handel seine wahren Kosten im Transport, der Rohstoffbeschaffung oder den Arbeitsverhältnissen tragen muss. Diese Kosten tragen stattdessen Menschen und Umwelt. Ägypten baut einen zweiten Suez-Kanal, Nicaragua einen Kanal als Konkurrenz zum Panama-Kanal, die Türkei plant einen weiteren Durchstich zwischen Marmara- und Schwarzem Meer. All diese Kanäle greifen massiv in die Ökologie an Land und zwischen den Meeren ein, die Folgen sind realistisch kaum abzuschätzen. Zumindest im Fall der Türkei und Ägyptens lassen sich auch politische Konflikte nicht ausschließen.

Der Wirtschaftsraum der 28 EU-Staaten umfasst etwa 508 Mio. Menschen. Man sollte meinen, dass ein so großer Markt aus sich heraus genügend attraktiv ist. In der EU ließe sich so gut wie alles produzieren, wenn wir auf Autarkie statt auf globale Produktionsketten, auf erneuerbare Energien und Recycling statt fossiler und anderer nicht nachhaltiger Rohstoffe setzen würden. Die Abhängigkeit von Ressourcen[23,24] und die Angst, von großen Märkten abgeschnitten zu werden, waren Auslöser mehrerer Kolonialkriege und haben noch im 20. Jahrhundert zu Kriegen beigetragen, zwei besonders verheerende davon in Europa. Regionale Bescheidenheit in Europa könnte friedenstiftend sein.

Was tun?

Digitalcourage hat eine Twitter-Aktion, *#TTIPTuesday*, gestartet. Sie fragen jeden Dienstag auf Twitter die Abgeordneten des europäischen Parlaments nach ihrer Haltung zu TTIP, Datenschutz und Schiedsgerichten. (Federführend ist der INTA-Ausschuss.)

EDRi hat eine Kampagne gestartet und acht „rote Linien" für TTIP entworfen: *https://edri.org/ttip-resolution-docpool/*

Der Europaabgeordnete der Grünen und Vize des LIBE-Ausschusses, Jan Philipp Albrecht, kämpft weiterhin für die EU-Datenschutz-Grundverordnung. Über TTIP wird im Europäischen Parlament entschieden. Bis Juni sollen Parlament und EU-Rat eine gemeinsame Position erarbeitet haben. Wir sollten Jan Philipp Albrecht unterstützen.

Freihandelsabkommen umfassen viele Hunderte von Seiten. Eine Aufbereitung in der Art, wie Lobbyplag sie bietet, macht sie transparenter: *http://lobbyplag.eu*

Anmerkungen

1 *Investor-to-State Dispute Settlement*
2 *www.oecd.org/gov/regulatory-policy/irc.htm (abgerufen 12.2.15)*
3 *de-statement_regulatory_cooperation_feb_2015_3.pdf, www.corporateeurope.org/international-trade/2015/02/statement-169-civil-society-organisations-regulatory-cooperation-eu-us (abgerufen 5.3.15)*
4 *Als Stockholm-Syndrom wird die Empathie bis zur Solidarität von Geiseln mit ihren Geiselnehmern bezeichnet.*
5 *Geht zurück auf den Ökonomen und Nobelpreis-Träger George Stigler.*
6 *Ziemlich gutes Online-Wörterbuch.*
7 *Regulatory Capture Revisited – Lessons from Economics of Corruption. www.icgg.org/downloads/Boehm%20-%20Regulatory%20Capture%20Revisited.pdf (abgerufen 7.4.15)*
8 *So hat Cecilia Malmström in einer Schlüsselposition für die EU-US Handelspolitik Jan Eric Frydman engagiert, dessen Lebenslauf „reads like the dream biography of an international corporate player". www.corporateeurope.org/international-trade/2015/03/corporate-lawyer-appointed-special-adviser-eu-trade-chief (abgerufen 7.4.15)*
9 *https://www.uschamber.com/international/global-regulatory-cooperation/center-global-regulatory-cooperation (abgerufen 11.4.15)*
10 *Eine entlarvende Formulierung, weil sie sich nur auf den Rest der Welt zu beziehen scheint, obwohl auch die USA ihre nationalen Konzerne als Weltmarktführer subventionieren.*
11 *Broschüre zum GRC-Projekt, S. 10, Hervorhebung von mir.*
12 *Broschüre zum GRC-Projekt, S. 5*
13 *Broschüre zum GRC-Projekt, S. 6, Hervorhebung von mir.*

14 *El País vom 19.1.15, S. 7*
15 *Laut Jaron Lanier in Who Owns the Future, S. 60, hat disruption den Modebegriff transformation im Silicon Valley der 1970er ersetzt. In diesem Zusammenhang bedeutet Disruption das Unterbrechen der Kontinuität in Wirtschaftsbereichen oder Märkten.*
16 *Committee on International Trade*
17 *Committee on Civil Liberties, Justice and Home Affairs*
18 *http://www.europarl.europa.eu/news/en/news-room/content/20150330IPR39308/html/TTIP-Trade-agreements-must-not-undermine-EU-data-protection-laws-say-MEPs*
19 *Christiane Schulzki-Haddouti, c't Nr. 8/2015, S. 40ff*
20 *a.a.O.*
21 *a.a.O.*
22 *http://lobbyplag.eu/governments (abgerufen 7.4.15)*
23 *Beispielsweise der Briten und Franzosen vom Erdöl im Vorderen Orient, die 1916 zum Sykes-Picot-Abkommen führte, einer Ursache für Unruhen bis heute.*
24 *Vgl. beispielsweise Eduardo Galeano: Las venas abiertas de América Latina.*

Bärbel Heide Uhl

Menschenhandel und Datenschutz

Einführung

Wenn man sich die aktuellen Debatten zur staatlichen Legitimierung der Vorratsdatenspeicherung verfolgt, dient die Bekämpfung von Menschenhandel gleich nach dem ‚Krieg gegen den Terror' als Legitimation für die massenhafte Überwachung und Sammlung von Daten. Vor einigen Monaten äußerte sich zum Beispiel der niedersächsische SPD Innenminister Boris Pistorius in Unterstützung für die Einführung der Voratsdatenspeicherung mit folgender Argumentation:

> *„Die Sicherheitsbehörden haben deshalb derzeit in Deutschland leider kaum Möglichkeiten, diese Spuren [der Verbrecher] nachzuverfolgen", sagte Pistorius. Es sei zum Beispiel beim Menschenhandel und Terrorismus nicht hinnehmbar, dass es keine Möglichkeit gebe, mit Hilfe der Verbindungsdaten und verwendeter IP-Adressen die Täter zu ermitteln.*[1]

Ähnlich argumentiert der ranghohe NSA-Vertreter Richard Ledgett in einem Interview mit einer amerikanischen Denkfabrik. Die Veröffentlichungen der Überwachungsintrumente durch Edward Snowdon, so seine Argumentation, hätte nicht nur weitreichende Folgen in der Verhinderung von Terroranschlägen, sondern würde auch die effektive Bekämpfung von Menschenhandel gefährden:

> *„So, the things that he's disclosed, the capabilities, and NSA is a capabilities based organization, so when we have foreign intelligence targets, legitimate things of interest, like terrorists is the iconic example, but it includes things like human traffickers, drug traffickers, people who are trying to build, you know, advanced weaponry, nuclear weapons and build delivery systems for those, and nation states who might be executing aggression against their immediate neighbors, which you may have some visibility in some of that that's going on right now, the capabilities are applied in a very discreet and measured and controlled way. So, the unconstrained disclosure of those capabilities means that as adversaries see them and recognize, hey, I might be vulnerable to this, they move away from that."*[1]

Datenschutz und Menschenhandel

Die Argumentation, dass Menschenhandel nur durch massenhafte Datensammlung und Überwachungstechnologien bekämpft werden kann, ignoriert den Menschenrechtsschutz der Betroffenen. Gerade Opfer von Menschenhandel haben ein besonderes Bedürfnis nach Schutz der Privatheit, die der Vorratsdatenspeicherung konträr entgegen läuft. Das Verbrechen Menschenhandel ist mit einem gesellschaftlichen Stigma belegt, da es sich um sexualisierte Zwangsarbeit, irreguläre Migration oder erzwungene Straftaten handeln kann. Auch schwerwiegende Arbeitsausbeutung, die sich als Straftatbestand des Menschenhandels qualifiziert, kann mit Demütigungen und Erniedrigungen für die Opfer einher gehen, die es in der Folge den Betroffenen erschwert, über ihr erlebtes Leiden zu sprechen. Auch durch Menschenhandel erfolgter Organhandel kann weitreichende gesundheitliche und soziale Konsequenzen für die Opfer mit sich führen. Anonymität und der Schutz der Privatsphäre für Betroffene ist daher eine zentrale Forderung der zivilgesellschaftlichen Fachberatungsstellen in Deutschland und anderen europäischen Ländern.[2]

Rückkehrprogramme und globale Opferdatenbanken

Es gilt gemeinhin die Annahme, dass Menschenhandel in einem Kontext von organisierter Kriminalität und irregulärer Migration stattfindet. Daher werden die staatlichen Maßnahmen in dem Bereich sehr restriktiv gehandhabt und sind eingebettet in die Maßnahmen zur Migrationskontrolle. In der Praxis bedeutet dies, dass ein niederschwelliger und anonymer Zugang zu Beratung für Betroffene ersetzt wird durch ein bürokratisiertes System der behördlichen Anerkennung von Opfern, die die Bedingungen für den Zugang zu Schutzstrukturen festlegen.

Der Fokus in der staatlichen und zwischenstaatlichen Datensammlung als Strategie gegen Menschenhandel liegt paradoxerweise auf dem (möglichen) Opfer und nicht, wie in der Terrorismusbekämpfung, auf den mutmaßlichen Tätern. Die EU-Kommission hat in den letzten Jahren fast 3 Millionen Euro für die Entwicklung von Indikatoren ausgegeben, die zu be-

hördlichen Erkennungsverfahren von Menschenhandelsopfern führen.[3]

Die staatliche und zwischenstaatliche Erfassung von mutmaßlichen Opfern wird auch als Regierungspraxis in der 2012 veröffentlichten EU-Strategie gegen Menschenhandel im Rahmen von Rückführungsprogrammen empfohlen. Die EU spricht sich darin für die Umsetzung von ‚Transnational Referral Mechanisms', sogenannter ‚grenzüberschreitender Weiterleitungsmechanismen' aus, die auf der Weitergabe personenbezogener Daten, einschließlich Gesundheitsdaten von Betroffenen zwischen den Behörden des Ziellandes und dem Herkunftsland beruhen.[4]

Ein weiteres aus datenschutzrechtlichen Erwägungen höchst problematisches Instrument der globalen Überwachung von Betroffenen ist die globale Datenbank mit personenbezogenen Daten von gehandelten Menschen, die durch die Internationale Organisation für Migration (IOM) betrieben wird.[5]

Datenschutz als Menschenrechtsschutz

Datenschutz ist ein missverständlicher Begriff. Es geht dabei nicht um den Schutz von Daten, sondern um den Schutz von Menschen. Obwohl wir ihn meistens als einen rein technischen Begriff wahrnehmen (z. B. durch das Anklicken der Datenschutzerklärung bei Online-Einkäufen), handelt es sich bei Datenschutz um ein primäres Menschenrecht vor dem Übergriff staatlicher Kontrolle in das Persönlichkeitsrecht.

Durch die totalitären Regime in Europa im 20. Jahrhundert, vor allem in der Nazizeit, hat der Datenschutz in Europa und in Deutschland einen anderen, gewichtigeren Stellenwert als z. B. in den USA. Art. 8 der europäischen Datenschutzrichtlinie regelt ein Verbot von staatlicher Speicherung von sogenannten sensiblen Daten. Danach ist den Mitgliedstaaten die Verarbeitung personenbezogener Daten untersagt, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder politische Überzeugen oder die Gewerkschaftszugehörigkeit hervorgehen. Auch die Daten zur individuellen Gesundheit oder zum Sexualleben fallen in das Konzept der besonders schützenswerten sensiblen Daten.[6]

Es sollte dabei verhindert werden, dass staatliche Behörden wieder in die Lage kommen, Menschen als ‚Juden', ‚Homosexuelle', ‚Roma' oder in sonstige Kategorien einzuordnen und speziell zu verwalten. Datenschutz und das Recht auf Privatsphäre ist daher ein weitreichendes Rechtsgut, da in der Vergangenheit Menschen Identitäten zugeschrieben wurden, die eine staatlich-legitimierte Verfolgung mit sich führten.

Schlussfolgerung

Wir kennen den globalen Datenfluss nicht und auch nicht die Interpretationen der massenhaften Überwachungspraktiken durch Regierungen. Aus Datenbanken können neue Grenzregime entstehen, die genau definieren, welches Individuum sich in welchem geographischen Raum aufhalten darf. EUROSUR ist konzeptionell ein Beispiel für künftige Grenzkontrollen aufgrund elektronischer Überwachung.[7] Wir können nicht ausschließen, dass die heutigen Datenbanken von Menschenhandelsopfern morgen operativ für Grenzkontrollen und andere Überwachungssysteme eingesetzt werden.

Die Umsetzung eines aktiven Datenschutzes in der Anti-Menschenhandelspolitik bedeutet, ein Leben in Freiheit und ohne Stigmatisierung für die Betroffenen zu ermöglichen.

Anmerkungen

1 *Siehe http://www.noz.de/deutschland-welt/politik/artikel/558663/pistorius-fur-vorratsdatenspeicherung-gegen-terror*
2 *Siehe https://www.nsa.gov/public_info/_files/speeches_testimonies/TED_Transcript_With_R._Ledgett_March_20_2014.pdf*
3 *Siehe datact-project.org*
4 *Siehe http://ec.europa.eu/dgs/home-affairs/e-library/docs/thb-victims-identification/thb_identification_en.pdf*
5 *Siehe https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/eu_strategy_towards_the_eradication_of_trafficking_in_human_beings_2012-2016_1.pdf S. 6*
6 *Counter-Trafficking Module (CTM) unter https://www.iom.int/jahia/webdav/site/myjahiasite/shared/shared/mainsite/policy_and_research/research/Data_and_Research_on_Human_Trafficking.pdf*
7 *Art. 8, EU-Richtlinie 95/46/EG*
8 *Siehe http://www.datact-project.org/fileadmin/user_upload/pdf/Maria_Giovanna_Manieri_PICUM.pdf*

Bärbel Heide Uhl

Dr. **Bärbel Heide Uhl** ist Politikwissenschaftlerin und arbeitet seit 1994 gegen Menschenhandel in verschiedenen europäischen Ländern. Sie ist Mitbegründerin des mittel- und osteuropäischen NGO-Netzwerkes »La Strada«, arbeitete u. a. für die OSZE in der ehemaligen Bundesrepublik Jugoslawien und für das OSZE Büro für demokratische Institutionen und Menschenrechte (OSCE/ODIHR), als Sachverständige in EU-Beitrittsprogrammen in der Türkei, Kroatien und Rumänien sowie für den Europarat und die UNODC. Bis 2011 war sie Vorsitzende der EU-ExpertInnengruppe zur Bekämpfung von Menschenhandel in Brüssel.

Stefan Ullrich

Das Datenschutz-Konzil

Wir befinden uns in einer fensterlosen Privatbibliothek, die einzige Tür ist hinter einem schweren Vorhang verborgen. Sieben Personen teilen sich die vier vorhandenen Ohrensessel, wobei sie immer wieder zum Servierwagen schreiten, um sich noch einen gehörigen Schluck einzugießen. Offensichtlich kennen sich die hier Versammelten recht gut, wie sonst ist die Abwesenheit jedes Protokolls zu erklären! Verschiedene Stände, Ämter, Geschlechter und nicht zuletzt: Zeitalter sind hier vertreten.

A Club of Gentlemen by Joseph Highmore c. 1730

Monachos: „Dixit algorizmi: laudes deo rectori nostro atque defensori dignas …"

Augusta: „Na, ob er das wirklich so gesagt hat, sei dahingestellt. Das Spannende an al-Chwarizmis Schrift ist doch wohl eine andere Sache."

Monachos (sichtlich über die Unterbrechung verärgert)**:** „Und welche, bitte, wäre das, verehrte Countess?"

Augusta: „Er befreite uns von dem Joch der römischen Ziffern. Seine indischen, die wir inzwischen ja arabische nennen, sind für die Arithmetik viel besser geeignet."

Samos: „Dafür sind wir nun unter ein neues Joch geworfen. Alles ist Zahl – unabhängig davon, welche Darstellung Ihr bevorzugen mögt."

Frieda: „Und was ist so schlimm daran? Wenn alles Zahl ist, so auch dieser Disput. Dann lasst uns doch einfach ausrechnen, wer Recht hat. Calculemus!"

Jakob: „Für die Buchhaltung jedenfalls sind indische Ziffern ungleich besser geeignet. Frieda, arbeitet Ihr eigentlich noch an der Rechenmaschine?"

Frieda (tonlos)**:** „Ich entwerfe eine universelles System zur Berechnung der Antwort auf das Leben, das Universum und den ganzen Rest – und Ihr bezieht euch auf dieses Spielzeug von mir?"

Augusta: „Ein Spielzeug, fürwahr! Eure Rechenmaschine ist doch noch in den Grenzen der Arithmetik gefangen. Seht Ihr denn nicht, dass wir dem algorithmischen Weg einschlagen sollten? Lasst uns nicht einfach Zahlen addieren, multiplizieren oder dergleichen mehr. Lasst uns Symbole nach frei programmierbaren Regeln transformieren!"

Mathison (einen Apfel kauend)**:** „Hört, hört, das kommt mir doch sehr bekannt vor. Ihr schmückt euch gern mit fremden Federn, nicht wahr?"

Augusta (streng)**:** „Nur weil Euch der Ruhm versagt wurde, nehmt Ihr mir meinen übel!"

Samos: „Bitte, bitte. Beruhigt Euch. Ihr auch. Wir dürfen nicht vergessen, weshalb wir uns hier versammelt haben. Bitte tretet näher und werft einen Blick auf diese Karte. Was seht ihr?"

Die Personen versammeln sich um den Servierwagen, auf dem nun eine aufgefaltete Karte liegt; die noch ein wenig gefüllten Karaffen halten das Pergament einigermaßen glatt. Als Andrea

spricht, merken die anderen erst, dass sie bereits die ganze Zeit als stille Zuhörerin im Raum war.

Andrea: „Das, liebe Freunde, ist die Ausdehnung des Menschen."

Monachos: „Es zeigt die Ausgabe technischer Erfindungen und anderer Menschenwerke. Die ungeheure Technik! So sehr expandiert der Mensch in die ihm verantwortete Welt!"

Andrea: „So meine ich das nicht. Dies *ist* der Mensch. Wie sagtest Du einst so schön: Ecce Homo!"

Monachos: „Absurd! Wie kann etwas, das vom Menschen geschaffen wurde, der Mensch selbst sein?"

Samos: „Lasst uns doch nicht, zumindest nicht an dieser Stelle, darüber streiten, wer der Schöpfer dieses.. dieser.. Ja, was ist das eigentlich?"

Mathison: „Das Gegebene. Datum. Wir sehen hier ein kodiertes Datum."

Monachos: „Von wem kodiert? Von wem gegeben?"

Frieda (betrachtet die Nullen und Einsen verzückt)**:** „Dyadisch! Die Kodierung erfolgte mithilfe eines dyadischen Systems. Das muss göttlichen Ursprungs sein, denn nur Einer hat Alles aus Nichts gemacht!"

Augusta: „Oder maschinellen."

Mathison: „Als ob der menschliche Geist nicht dazu in der Lage wäre!"

Jakob: „Wenn das der Mensch ist … Dann kann man ihn ja plötzlich mit einem anderen vergleichen, wie wundervoll."

Andrea: „Sei mir nicht böse, aber immer, wenn du dich freust, wird mir ganz anders. Was soll denn das heißen, zwei Menschen zu vergleichen?"

Samos: „Nicht jeder Vergleich ist doch moralisch verwerflich. Hier wird doch nur erleichtert, was ohnehin schon geschieht."

Monachos: „Diese Daten dürfen nicht in falsche Hände geraten!"

Andrea: „Endlich sprechen wir über Ethik. Dürfte ich vielleicht etwas länger ausführen, warum ich uns hier zu Samos eingeladen habe? Danke. Dank der wunderbaren Vorarbeiten von euch und euresgleichen gibt es in unserer modernen Welt eine unfassbar große Menge an Daten. Sie werden erzeugt, verarbeitet und gespeichert von weltweit vernetzten …"

Frieda (unvermittelt)**:** „Computern?"

Augusta: „Stellt Euch nicht naiver als Ihr seid. Es geht nicht nur um arithmetische Rechenmaschinen, sondern um algorithmische Wirkungsmaschinen."

Mathison: „Die zudem miteinander verschaltet sind; wir sollten eher von Symbolkodetransformationsmaschinenkopplungen sprechen."

Andrea: „… informationstechnischen Systemen. Dürfte ich fortfahren? Anhand der technischen Gegebenheit und mit einigem Nachdenken sehen wir sofort, dass Freiheit und Unbeobachtbarkeit des Denkens – etwa beim Erwägen von Äußerungen oder Handlungen – künftig untrennbar mit dem Schutz eben dieser persönlichen informationstechnischen Systeme und der Daten auf ihnen verknüpft sein wird. Wir beobachten schon jetzt eine geradezu symbiotische Verbindung von Mensch, Geist, Maschine und Algorithmus, nehmt nur Monachos hier als Beispiel. Er zitiert die Klassiker doch längst nicht mehr frei, sondern mit Hilfe seines Tablets. Jakob hier nutzt für seine Buchhaltung Xerox-Maschinen, die Zahlen verdrehen …"

Jakob (verschluckt sich)**:** „Wie meinen?"

Mathison: „Das kommt davon, wenn man Probleme mit schierer Rechenkraft lösen will anstatt durch scharfes Nachdenken. Was ist an kariertem Papier mit Bleistift auszusetzen?"

Augusta: „Darf ich Euch daran erinnern, dass Ihr seit über drei Monaten mit einem simplen Schlüsseltausch beschäftigt seid, damit wir endlich verschlüsselt kommunizieren können?"

Samos: „Als Gastgeber muss ich darauf bestehen, dass keine Rede mehr unterbrochen wird. Das Thema ist ernst genug. Andrea, bitte, fahrt fort."

Andrea: „Angesichts der gegenwärtig zu beobachtenden Symbiose zwischen Mensch und Maschine, wie wird es erst werden, wenn wir die Informations- und Kommunikationstechnik in unsere Körper implantieren? Dies meine ich als Sinnbild, obwohl eine tatsächliche Verbindung so abwegig nicht mehr erscheint. Wir werden zunehmend verloren gegangene Fähigkeiten in vernetzte Universalcomputer auslagern, um sie so wiederzugewinnen. Wir werden an sie persönlichste Denk- und Merkfunktionen delegieren, um uns zu entlasten. Ihr habt Friedas Calculemus noch im Ohr; doch was, wenn nicht nur eine Berechnung stattfindet, sondern eine Simulation von gedachten Welten zur Exploration der Auswirkungen von Änderungen in den Annahmen durchgeführt wird? Wer denkt in diesem Fall eigentlich noch, wenn doch der Denkvorgang, also das Springen von einem mentalen Zustand zum nächsten, in der Virtualität stattfindet? Wenn ich nun also im Folgenden von Datenschutz spreche, so bedeutet dies nichts weniger als den Schutz des autonomen und unbeobachteten Denkens, der elementarsten und grundlegendsten Freiheit der Person."

Samos steht auf, schließt den Schrank unter dem Servierwagen auf und tauscht die leeren Karaffen gegen volle. Auf seinen fragenden Blick hin strecken sich ihm mehrere Gläser entgegen, in die er bereitwillig und großzügig eingießt. Alle nippen etwas schweigsam an ihren Getränken, Monachos und Frieda stöbern ein wenig in Samos' Bibliothek, Mathison und Augusta kritzeln gemeinsam auf einem unendlich groß wirkenden Papier herum; schließlich ergreift Jakob das Wort.

Jakob: „Einverstanden, ich stimme zu, dass es auch und gerade um Autonomie und Unbeobachtbarkeit des Denkens geht.

Aber wie steht es mit seiner Zuverlässigkeit? Mir scheint, dass der Schaden durch falsche Berechnungen vielleicht sogar erheblicher ausfällt als derjenige durch Beobachtung der berechneten Denkvorgänge. Nehmen wir einmal an, dass ich meinem geschätzten Freund Samos hier einen Brief mit einem außergewöhnlich schönen mathematischen Beweis schicken möchte, eben, weil ich weiß, wie sehr er Zahlen schätzt. Nehmen wir nun einmal an, dass ich diesen Brief in mein informationstechnisches System hineinspreche …"

Mathison: „Bequemlichkeit, wie hoch dein Preis doch ist!"

Jakob (etwas lauter, lässt sich nicht unterbrechen)**:** „… damit er als transkribiertes Werk direkt den postalischen Weg zum rechtmäßigen Empfänger findet. Stellt euch nun die Bestürzung des Samos' vor, im geöffneten Brief eine Quadratur des Kreises vorzufinden oder eine Trisektion des Winkels oder ähnlichen Unfug. Was muss er dann von mir denken?"

Frieda: „Nun, wenn er konsequent seinem Zahlen-Fetisch folgte, würde er sein Urteil über dich ausrechnen."

Mathison: „Zumal Samos mit zwei Nachkommastellen von Pi doch ganz gut auskommt. So klappt auch die Quadratur!"

Samos: „Warum diese Spitze, Mathison? Gerade du bist doch maßgeblich dafür verantwortlich, dass wir in einer Ganzzahlwelt leben."

Jakob: „Eigentlich war das eine rhetorische Frage, worauf ich hinauswollte: Die Integrität der informationstechnischen Systeme ist ebenso wichtig wie seine Vertraulichkeit. Dieses Konzil muss dafür Sorge tragen."

Monachos: „Wer muss wofür Sorge tragen? Was haben wir mit diesem Gegebenen, mit diesen Daten zu schaffen? Wir haben sie doch nicht erschaffen, sie sind, der Name sagt es, doch einfach da!"

Augusta: „Das beste wäre doch, wir würden allen Menschen zeigen, wie diese Daten entstehen, wie sie zu interpretieren und nicht zuletzt: wie sie zu vermeiden sind. Lernt programmieren, sonst werdet ihr programmiert!"

Mathison: „Hört, hört. Auch wenn ich die Forderung durchaus unterstütze, ich begreife einfach nicht, wie so ein im Wortsinne idiotisches System eine solche Macht über ein vernunftbegabtes Wesen ausüben kann."

Andrea: „Der moderne Mensch ist inzwischen abhängig von der Technik."

Frieda: „Der Mensch war schon immer abhängig von Technik, sonst hätte er niemals so lange überlebt."

Andrea: „Ich spreche von Abhängigkeit im Sinne einer Drogenabhängigkeit. Der Mensch ist süchtig nach der Belohnung, die ihm das Lösen von Problemen gibt. Allein: Ohne Computer hätten wir viele der heutigen Probleme nicht."

Samos: „Eine Verfallsgeschichte der Gesellschaft zu zeichnen nutzt uns hier auch nichts. Zumal jedes neue Medium in erster Linie kritisiert wurde. Das fing ja schon mit der Erfindung der Buchstaben an, die angeblich dem Menschen das Vergessen beibringen würden, weil sie im Vertrauen auf die Schrift vermittels fremder Zeichen die Fähigkeit zur Erinnerung vernachlässigten. Nun soll also der Computer mit seinen allmächtigen Algorithmen und bedrohlichen Daten die Jugend verderben – wie originell!"

Monachos: „Der vernetzte Universalcomputer ist mehr als nur Medium, er ist Religion und zugehörige Exegese zugleich."

Jakob: „Was soll das denn heißen? Was soll Religion damit zu tun haben? Ich finde, der Gedanke, Computer nicht nur als Rechner, sondern als Medium zu sehen, ist noch nicht zu Ende gedacht. Oder ist das inzwischen die Meinung der Allgemeinheit?"

Frieda: „Dein Bankhaus wirbt doch selbst mit einer multi*medialen* App, die einem spielerisch Geldanlagen empfiehlt. Der Computer ist Medium, das bestreitet niemand. Allerdings weist der Gedanke von Monachos in eine spannende Richtung …"

Augusta: „… die wir hier verfolgen sollten? Ich frage mal in die Runde, ob es dafür nicht schon etwas spät geworden ist."

Samos: „Ja doch, ich habe verstanden. Hier, nehmt, für die besonders späten Diskussionen. (Er gießt allen aus einer verstaubten Flasche ein.) Darf ich einen Vorschlag machen? Wir fassen noch mal die aufgeworfenen Probleme auf und entscheiden dann, wie wir weiter verfahren. Einverstanden?"

Die anderen stimmen schweigend zu, Samos' berühmter Tropfen hat noch jedes Konzil erfolgreich beendet. Ab und an kamen sogar scharf formulierte Forderungen heraus. Die Teilnehmer wunderten sich in solchen Fällen stets über ihre eigene Courage.

Stefan Ullrich

Stefan Ullrich ist einer der Herausgeber des Sammelbands *Per Anhalter durch die Turing-Galaxis*, Verlag Monsenstein und Vannerdat (2012). Wer mehr über weitere „Insassen" erfahren möchte, greife zu diesem Buch. Andrea zitiert aus Andreas Pfitzmanns Gutachten zur Online-Durchsuchung und Frieda nannte sich früher Gottfried. Aber das ist eine andere Geschichte, die ein anderes Mal erzählt wird.

Frieda: „Wir sprachen die ganze Zeit über Daten, ohne genau zu sagen, welche das sind. Dieses Konzil ist ja nicht zuletzt auch ein politisches; aufbereitete Informationen, entsprechend visualisiert oder zumindest strukturiert, sind unentbehrlich für die Politik. Jeder politisch handelnde Mensch benötigt ja eine Datengrundlage, um sinnvoll von seinem Verstand Gebrauch machen zu können. Auf dieser Karte hier stehen ja nun gerade Informationen, die doch niemanden etwas angehen."

Mathison: „Und wer entscheidet, was politische, öffentliche Daten und was persönlichste Geheimnisse sind?"

Frieda: „Wir sind schließlich ein Konzil, also entscheiden wir das."

Monachos: „Wir sind nicht gewählt, bedenkt das bitte."

Frieda: „Die Menschenrechte sind auch nicht in demokratischer Abstimmung entstanden."

Andrea: „In die gleiche Richtung würde ich argumentieren. So etwas Universelles kann man nicht zurücknehmen, wenn es einmal gedacht wurde."

Jakob: „Na, das mag wohl in der Theorie stimmen, aber ganz praktisch kann man sehr wohl auch universell gültige Menschenrechte einschränken. Das nennt man die normative Kraft des Faktischen."

Augusta: „Sehr richtig, in einer programmierten Welt gelten nun einmal die Spielregeln der Programmiererin."

Monachos: „Umso wichtiger ist es, dass die Spielregeln nicht nur akzeptiert werden, weil man eben Teil des Spiels ist, sondern sie auch akzeptiert werden wollen. Lasst uns doch einfache Regeln aufstellen und sie anschließend auf ihre Tauglichkeit abklopfen."

Natürlich hatten alle schon längst Forderungen auf den Lippen; aber es sollte ja zumindest der Anschein des tieferen Nachdenkens gewahrt werden.

Frieda: „Daten, die die Öffentlichkeit betreffen, müssen zur Verfügung gestellt werden; persönliche Daten hingegen dürfen auf gesellschaftlichen Wunsch geheim bleiben."

Mathison: „Gesellschaftlicher Wunsch? Wenn die Gesellschaft also findet, dass meine persönlichen Daten in irgendwelchen sozialen Netzwerken auftauchen dürfen, ist alles in Ordnung?"

Frieda: „Die korrekte Übersetzung von *social network* wäre übrigens *geselliger Verbund* – und ja, das wäre in Ordnung, wenn keine ökonomischen Interessen berührt wären. Und wenn man die Möglichkeit zur Geheimhaltung schafft."

Mathison: „Was ist mit dem Schutz der Andersdenkenden? Eine feine Demokratie schwebt dir da vor."

Frieda: „Das mit der Demokratie hast du als Prämisse hinzugenommen. Ich sprach nur von einer Informationsgesellschaft, von Demokratie war da nie die Rede. Wenn wir alles voneinander wüssten, wären wir sicher toleranter eingestellt."

Andrea: „Ich finde, wir sollten nicht über Namen oder Staatsformen streiten. Die Möglichkeit des Widerspruchs muss einfach gegeben sein."

Samos: „Widerspruch – wogegen?"

Andrea: „Gegen alles Mögliche. Eine Demokratie ist nur im prekären Zustand eine. Ich muss den Daten widersprechen können."

Samos: „Du meinst, du sollst gegen die Verwendung deiner Daten widersprechen können?"

Andrea: „Nein, ich muss den Daten selbst widersprechen können. Wenn mein digitaler Schatten …"

Augusta: „… algorithmischer Schatten …"

Andrea: „… größer und mächtiger wird als ich, also plötzlich zu meiner Repräsentanz und Wirkung wird, dann besitze ich keine Möglichkeit des Widerspruchs mehr. Das Wort vom Datenschutz ist eigentlich unbrauchbar, wir sprechen hier vom Schutz des echten menschlichen Lebens."

Samos: „Du variierst deine Meinung von vorhin; sag, wie findest du die Forderung öffentliche Daten nützen, private Daten schützen?"

Frieda: „So habe ich das nie gesagt!"

Jakob: „So klingt es aber griffiger; lässt sich besser verkaufen, auch angesichts der knappen Währung Aufmerksamkeit."

Andrea: „Ich unterstütze die Forderung, leite daraus aber eine weitere, viel grundlegendere ab."

Monachos (nach einigen Sekunden)**:** „Niemand unterbrach dich; oh, ich verstehe. So, du hast deine Kunstpause, nun fahre fort."

Andrea: „Wir müssen die Öffentlichkeit und die Gesellschaft schützen. Das sollte das vorrangige Ziel dieses Konzils sein. Wenn wir das Individuum vor datenhungrigen Organisationen schützen wollen, müssen wir ihm das Sich-Organisieren-Können zugestehen. Wir, verehrte Anwesende, brauchen eine Datenwehr."

Die Getränke von Samos verfehlen ihre Wirkung nicht, das Konzil nimmt die Idee einer Datenwehr begeistert auf und formuliert Zuständigkeiten, Vorgehensweisen, Evaluationskriterien, Finanzierungsmodelle, Machbarkeitsprognosen – also eine zwar spannende, doch äußerst zeitraubende Angelegenheit. Wir schleichen uns besser hinaus in das Hauptanstaltsgebäude, bevor uns die Pflegekräfte entdecken. Der Besucherausweis gilt ja nicht für den geschlossenen Teil der Klinik.

Jörg Pohle

Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens

1 Einleitung

Gleich den sagenhaften „Sieben Städten aus Gold" und „El Dorado" haben sich in den letzten Jahren „Privacy by Design" und „Datenschutz by Design" als Zielpunkte einer Debatte etabliert, die nur allzu oft versucht, gesellschaftliche Probleme als technische zu verstehen und technisch zu lösen. Während der Begriff „Privacy by Design" selbst aus der Feder Ann Cavoukians, der ehemaligen *Information and Privacy Commissioner* der kanadischen Provinz Ontario, stammt,[1] war die Idee keineswegs neu. Schon seit den 1970er Jahren haben es Forscherinnen und Forscher wiederholt unternommen, aus der Privacy- oder der Datenschutztheorie oder deren Umsetzungen im Recht stammende oder daraus abgeleitete Anforderungen für die Technikgestaltung nutzbar zu machen.[2] Die Forderung nach einer Umsetzung dieser Anforderungen in der Technik selbst ist sogar noch älter: Schon zu Beginn der modernen Debatte um *information privacy* und Datenschutz wurden die Erkenntnisse aus der IT-Sicherheit, dass Schutzmaßnahmen möglichst frühzeitig in den Systementwicklungsprozess eingebunden und nicht erst nachträglich auf das fertige System aufgesetzt werden dürften, auch auf die privacy- und datenschutzfreundliche Gestaltung von Technik übertragen.[3]

Während die Aufnahme der Forderung nach „Datenschutz by Design" in die derzeit verhandelte EU-Datenschutzgrundverordnung als großer Schritt zur Modernisierung des Rechts gefeiert wird,[4] ist es im Schatten solcher Vordenker wohl nicht überraschend, dass auch dieser Verrechtlichungsschritt keineswegs ohne Vorbild ist. Im Folgenden wird die Geschichte des ersten Versuchs im Bereich des Datenschutzes, Technikgestaltung mit Hilfe des Rechts zu steuern, dargestellt und analysiert, vor welchem Hintergrund dieser Versuch unternommen wurde, wie und von wem er zum Scheitern gebracht wurde und warum anscheinend kein Interesse daran besteht, aus diesem Versagen zu lernen.

2 Eine kurze Vorgeschichte

Die Datenschutzdebatte in der Bundesrepublik begann nicht im luftleeren Raum. Zwar wurde sie auch durch die schon laufende gesellschaftliche Debatte um *information privacy* in den USA angeheizt, die etwa von Ruprecht Kamlah über den Atlantik getragen wurde,[5] viel stärker jedoch wirkten die Diskussionen aus den 1960er Jahren nach, die sich etwa um Kybernetik und Recht,[6] Verwaltungsautomatisierung[7] und automationsgerechte Gesetze[8] drehten.

Das lag sicher auch daran, dass nicht wenige der „leidenschaftlichen"[9] Automatisierungsbefürworter der 1960er ein paar Jahre später den Nukleus der entstehenden Datenschutz-Community bildeten. In den Diskussionen wurde ein breites Spektrum an Themen diskutiert: von für eine Automation notwendigen oder zumindest wünschenswerten Eigenschaften von Prozessen oder Entscheidungen – ein Jahresbetrag, der in monatlichen Raten eingezahlt oder ausgezahlt werden soll, solle ohne Rest durch 12 teilbar sein – bis zur Frage, ob das Umschalten von automatisch betriebenen Ampeln Verwaltungsakte darstellten, von der Gestaltung automatisiert erstellter Bescheide bis zu phantastisch klingenden Forderungen wie der nach „Richterautomaten". Wesentliche Untersuchungsgegenstände waren, wie Informationsverarbeitungsprozesse rational so gestaltet werden könnten, dass sie sinnvoll formalisiert, rationalisiert und automatisiert werden könnten, welche Grenzen es dabei gebe, und vor allem auch, welche Grenzen es dabei geben sollte, etwa weil die im Grundgesetz enthaltenen Wertentscheidungen eine Automation ausschließen würden – unabhängig davon, ob es ein allgemeiner Ausschluss wäre oder einer, der nur auf dem damaligen Stand der Technik wirke.

3 Datenschutz by Design im BDSG 1977

Nicht nur auf Verlangen der Datenschutzkommission des Deutschen Juristentages[10] gab es bereits in den ersten Entwürfen zum späteren Bundesdatenschutzgesetz – Bundestagsdrucksache VI/2885 (§ 5 Abs. 3 und § 13 Abs. 4), Bundestagsdrucksache 7/1027 (§ 4) – Regelungen zur technischen Umsetzung von Daten*sicherheits*maßnahmen. Schon das Hessische Landesdatenschutzgesetz von 1970,[11] das im wesentlichen ein Daten*sicherheits*gesetz war, enthielt eine derartige Rechtsregel in § 2.

Auch in der Literatur wurde gefordert, das Recht „[n]ach den Einsichten der Lehre von der ‚automationsgerechten Rechtssetzung'" so zu formulieren, dass „Durchführung und Kontrolle von Datenschutzregelungen weitgehend durch DV zu unterstützen" seien.[12] Schließlich ging es auch in den öffentlichen Anhörungen im Innenausschuss des Bundestages zum Gesetzentwurf eines Bundesdatenschutzgesetzes im Mai 1974 und im März 1976 sowie im zweitägigen „Projektseminar Datenschutz" der Bundesakademie für öffentliche Verwaltung, an dem im November 1974 die Mitglieder aller beteiligten Ausschüsse teilnahmen, darum, wie durch rechtliche Regelungen eine am Datenschutzrecht ausgerichtete Gestaltung der Technik gesteuert werden könnte.[13]

Diese Forderung konnte damals schon auf eine gewisse Tradition zurückblicken: Der erste, der die Forderung nach einer technischen Umsetzung von Privacy-Regelungen aufstellte, war wohl Ende der 1960er Jahre Arthur R. Miller.[14] Eine mögliche Technik dafür beschrieb James P. Anderson 1972: den sogenannten „reference monitor", eine Art Middleware zur Kontrolle der Einhaltung von Rechten und Pflichten beim Zugriff auf Systemobjekte.[15] Im selben Jahr verlangte Ulrich Seidel, originäre Datenschutzrechtsanforderungen wie Herkunftsnachweise für Informationen und die Festlegung von Löschfristen technisch umzusetzen.[16] Adalbert Podlech war es dann, der als erster in der deutschen Debatte gefordert hat, die rechtlichen Vorgaben

im Allgemeinen – also auch die Zweckbindung – in „Schutzprogramme" im technischen Sinne zu übersetzen, die zu veröffentlichen seien, damit sie öffentlich kontrolliert werden könnten, getestet und – zumindest für den öffentlichen Bereich – genehmigt werden müssten.[17]

In der Folge nahmen die Abgeordneten eine einschneidende Veränderung am Gesetzentwurf vor. Bis dahin regelte der Entwurf in § 4 „[t]echnische und organisatorische Maßnahmen des Datenschutzes", allerdings in sehr enger, im Grunde nur auf die Datensicherheit zielenden Formulierung:

> *„Wer im Rahmen des § 2 Abs. 1 personenbezogene Daten verarbeitet, hat die erforderlichen und zumutbaren technischen und organisatorischen Maßnahmen gegen Mißbräuche bei der Datenverarbeitung, insbesondere gegen unzulässiges Abrufen, Weitergeben, Verändern und Löschen zu treffen. Zumutbar sind nur Maßnahmen, deren Schutzwirkung in einem angemessenen Verhältnis zu dem Aufwand steht, den sie verursachen."*

Mit dem beschränkten Ziel eines Schutzes gegen „Mißbräuche bei der Datenverarbeitung" kann die Datenverarbeitung nicht selbst als Problem begriffen werden. Der Titel ist insofern falsch, entspricht andererseits aber dem damals bei nicht wenigen Beteiligten, vor allem bei den Verantwortlichen im BMI, vorhandenen Verständnis. Die Ausrichtung des Datenschutzrechts auf das Ziel eines Schutzes auch beim (bestimmungsgemäßen) Gebrauch erfolgte jedoch erst mit der Novellierung des BDSG 1990.

Der vom Ausschuss neu gefasste § 4 ließ zwar im Titel das „des Datenschutzes" fallen, bezieht aber nun alle „Vorschriften dieses Gesetzes" in den Geltungsbereich der zu treffenden organisatorischen und technischen Maßnahmen mit ein:

> *„Wer im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen personenbezogene Daten verarbeitet, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."*

In diesem Wortlaut fand die Regelung dann auch Eingang in das 1978 in Kraft getretene Bundesdatenschutzgesetz, allerdings in § 6.

Schon im Bericht des Innenausschusses wird klargestellt, dass den Abgeordneten der grundlegende Bedeutungswandel, den sie der Regelung haben angedeihen lassen, bewusst ist. Nicht nur verweisen die Berichterstatter auf die „gewonnenen neuen Erkenntnisse", die der Änderung zugrunde liegen, sie trennen auch deutlich den Teil der Regelung, der sich auf die Umsetzung von Datenschutzanforderungen bezieht, von dem Teil, der den Daten*sicherungs*bereich abdecken soll. Letztere seien „die in der Anlage aufgeführten, den Datensicherungsbereich im wesentlichen abdeckenden zehn Zielvorgaben".[18] Hingegen beziehe sich der Hauptsatz im Gesetzestext auf „alle zum Vollzug dieses Gesetzes erforderlichen technischen und organisatorischen Maßnahmen".[19] Diesen Hauptsatz und seinen mit „insbesondere" eingeleiteten Nebensatz enthält das Bundesdatenschutzgesetz, wenn auch inzwischen in § 9, in einer im wesentlichen unveränderten Form noch heute.[20]

Parallel zum stattfindenden Gesetzgebungsverfahren unternahmen Wilhelm Steinmüller, Leonhard Ermer und Wolfgang Schimmel den ersten Versuch, die datenschutzrechtlichen Anforderungen – zu diesem Zeitpunkt waren es natürlich nur die Anforderungen des Gesetzesentwurfs – sowohl in die Gestaltung der Informationsverarbeitungsprozesse, der Organisation als auch der Technik einfließen zu lassen.[21] Mag die konkrete Umsetzung inzwischen noch so veraltet sein, konzeptionell stellt sie immer noch vieles in den Schatten, was heute als Stand der Wissenschaft verkauft wird. Vor allem beschränkt sie sich nicht, wie viele der neueren Arbeiten, auf die überkommene Vorstellung einer zu schützenden Privatsphäre.[22]

Vor diesem Hintergrund stellt sich die Frage, wie und warum eine so deutlich als Datenschutzregelung konstruierte Anforderung mittlerweile als eine reine „Datensicherheitsvorschrift" vermarktet wird; sogar in einem als „übermäßig datenschutzfreundlich" verschrienen Kommentar wie dem von Spiros Simitis herausgegebenen.[23]

4 Die Datenschutzbeauftragten ziehen dem Datenschutzrecht die Zähne der Technik

Nach einer umfassenden Auswertung der Literatur entsteht der Eindruck, dass sich noch Ende der 1970er Jahre – genauer: noch bevor § 6 BDSG mit der Anlage zu § 6 Abs. 1 Satz 1 verspätet am 1. Januar 1979 in Kraft trat – der Bundesdatenschutzbeauftragte, ein Teil der Landesdatenschutzbeauftragten sowie Vertreterinnen und Vertreter von Aufsichtsbehörden der Länder mit „interessierte[n] Kreise[n] der Wirtschaft"[24] zusammengefunden haben, um mit Hilfe von „Vorläufigen Verwaltungsvorschriften zu § 6" den Anwendungsbereich des § 6 entgegen der expliziten Absicht des Gesetzgebers nachträglich wieder einzuschränken.[25]

Während das Gesetz selbst von der „Ausführung der Vorschriften dieses Gesetzes" und mithin vom Datenschutz spricht, wird in den Verwaltungsvorschriften direkt zu Beginn behauptet, dass es in § 6 – und seiner Anlage – nur um „die Maßnahmen der Datensicherung" ginge (I.1.). Damit seien Maßnahmen gemeint, „die eine störungsfreie und gegen Mißbrauch gesicherte Datenverarbeitung zum Ziel haben" (I.1.1). Obwohl die Verwaltungsvorschriften nachfolgend dann wieder auf den Gesetzestext mit seiner umfassenderen Formulierung der Gewährleistung der „Ausführungen der Vorschriften des BDSG" verweisen (I.1.2), zielen alle weiteren Ausführungen ausschließlich auf klassische Datensicherheitsmaßnahmen ab. Selbst dort, wo etwa in Bezug auf die „Organisationskontrolle" aus dem Text der Anlage zitiert wird, dass die Organisation so zu gestalten sei, „daß sie den besonderen Anforderungen des Datenschutzes gerecht wird" (II.10.1), werden die Verfahrensschritte und Beispiele für Maßnahmen nur in ihrem Charakter als Datensicherheitsmaßnahmen beschrieben: So ist etwa die „Festlegung der Funktionen, der Zuständigkeiten und Verantwortung bei der Datenverarbeitung" (II.10.3) gerade noch keine datenschutzfreundliche Or-

ganisationsgestaltung, und die Verfahrensgestaltung – als Organisation der Informationsverarbeitungsprozesse – wird gar nicht erst angesprochen, genauso wenig wie eine mögliche technische Umsetzung von Betroffenenrechten.

Hier wurde demnach sowohl für die nachfolgende öffentliche Debatte wie die weitere Entwicklung des Datenschutzrechts, vor allem aber auch für die Datenschutzpraxis die Forderung fallen gelassen, dass das Recht nicht nur die Gestaltung der Technik, sondern vor allem auch schon die der Technikgestaltung zugrunde liegende Gestaltung von Organisation und Informationsverarbeitungsprozessen steuern können soll.[26] Während in Teilen der Wissenschaft inzwischen Verfahrensgestaltung wieder in einem umfassenden, vom Datenschutzrecht insgesamt geprägten Sinne verstanden wird,[27] vertreten die Datenschutzaufsichtsbehörden mehrheitlich die – im übrigen unbewiesene – Behauptung, dass bis zur Novellierung des BDSG 2001, mit der erst der Grundsatz der Datenvermeidung und Datensparsamkeit eingefügt wurde, die Verfahrensgestaltung selbst nicht Gegenstand datenschutzrechtlicher Anforderungen war. So wird dem Erforderlichkeitsprinzip unterstellt, es beziehe sich auf „einen gegebenen Zweck, ein gegebenes technisches System und einen gegebenen Datenverarbeitungsprozess."[28]

Die Folgen dieser Umdefinition lassen sich bis heute in den wissenschaftlichen Arbeiten zur Technikgestaltung – und ähnlich auch in der Datenschutzpraxis – beobachten: Gerade die Technikwissenschaften sind geprägt von Arbeiten, die *IT security* als *privacy* und Daten*sicherheit* als *Datenschutz* verkaufen. Anstatt die modernen Organisationen und ihre Informationsverarbeitung unter Kontrolle zu bringen,[29] geht es in erster Linie um Konzepte wie die Verschlüsselung von Kommunikation, die Anonymisierung erhobener und gespeicherter Informationen oder Selbstschutzmaßnahmen von Betroffenen, ohne zu reflektieren, ob diese Ansätze im konkreten Fall überhaupt geeignet sind, einen Schutz der Betroffenen sicherzustellen.[30]

5 Offene Fragen

Die Frage, wann und durch wen die Umdefinition einer originär auf das Datenschutzrecht insgesamt zielenden Rechtsregel in eine Datensicherheitsnorm vollzogen wurde und welche Folgen damit für die Organisations-, Verfahrens- und Technikgestaltung einhergingen, kann damit zwar beantwortet werden. Die Frage nach dem Warum jedoch nicht. Zwar ließe sich vor dem Hintergrund der Entwicklung und der beteiligten Akteure durchaus die These vertreten, eine Schwächung der Durchsetzungskraft des Datenschutzrechts sei explizit das Ziel der Beteiligten gewesen, allerdings kann auch nicht ausgeschlossen werden, dass die vorwiegend einseitig juristisch bewanderten Beteiligten die Folgen ihres Tuns für die weitere Entwicklung des Datenschutzrechts im Allgemeinen und die Organisations-, Verfahrens- und Technikgestaltung im Besonderen nicht kompetent abschätzen konnten. Da jedoch ein großer Teil der damals an den Diskussionen und den Entscheidungen Beteiligten noch gefragt werden kann, bietet sich hier ein Anknüpfungspunkt für weitere Forschungen.

Vor dem Hintergrund der inzwischen unfassbar großen Menge an Literatur zum deutschen Datenschutzrecht lässt sich auch nur bedingt nachvollziehen, warum diese Regelung, ihre Genese und ihre Umdefinition bislang überhaupt keinen Niederschlag in der wissenschaftlichen Debatte gefunden hat. Einer der Gründe dafür könnte sein, dass selbst zentrale und als datenschutzfreundlich geltende Übersichtswerke und Kommentare diese Tatsache aussparen und die Norm stattdessen zur Daten*sicherheits*regelung erklären.[31]

Problematisch an dieser Geschichte ist aber vor allem eines: Wenn eine ursprünglich so deutlich auf eine *datenschutz*freundliche Verfahrens-, Organisations- und Technikgestaltung gerichtete Rechtsnorm im Grunde so einfach und unbemerkt in eine Daten*sicherheits*norm umgewandelt werden kann, ohne dass es dafür eines – zumindest grundsätzlich – von einer demokratischen Öffentlichkeit diskutierbaren Aktes des Gesetzgebers bedarf, welche Garantie bietet dann eine Regelung, wie sie etwa in der konsolidierten Fassung des aktuellen Entwurfs für eine EU-Datenschutzgrundverordnung enthalten ist, nicht als Tiger zu starten und als Bettvorleger zu landen?

Anmerkungen

1 *Siehe Ann Cavoukian (2000). Privacy Design Principles for an Integrated Justice System – Working Paper. Toronto, Ontario: Information and Privacy Commissioner of Ontario, umfassend dann Ann Cavoukian (2010). Privacy by Design: The 7 Foundational Principles. Revised: Oktober 2010.*

2 *Für frühe Arbeiten siehe etwa Wilhelm Steinmüller, Leonhard Ermer und Wolfgang Schimmel (1978). Datenschutz bei riskanten Systemen. Berlin, Heidelberg, New York: Springer; Lothar Bräutigam, Heinzpeter Höller und Renate Scholz (1990). Datenschutz als Anforderung an die Systemgestaltung. Opladen: Westdeutscher Verlag sowie Volker Hammer, Ulrich Pordesch und Alexander Roßnagel (1992). KORA. Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungs-*

Jörg Pohle

Jörg Pohle studierte Rechtswissenschaft, Politikwissenschaft und Informatik. Derzeit promoviert er an der Humboldt-Universität zu Berlin zur Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung und koordiniert am Alexander von Humboldt Institut für Internet und Gesellschaft ein interdisziplinäres Forschungsprojekt zu Fragen der globalen Aushandlung im Privacy- und Datenschutzbereich *(http://www.hiig.de/project/privacy-governance/)*.

vorschlägen für IuK-Systeme. Techn. Ber. 100. Darmstadt: provet – Projektgruppe verfassungsverträgliche Technikgestaltung.

3 Siehe etwa Arthur Raphael Miller (1969). "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society". In: Michigan Law Review 67.6, S. 1089-1246. S. 1211 mit Verweis auf Paul Barans Aussage bei den Hearings on the Computer and Invasion of Privacy im US-Repräsentantenhaus. Siehe auch Arthur Raphael Miller (1971). The Assault on Privacy. Ann Arbour: The University of Michigan Press, S. 144, der damit die später so genannten – und patentierten – „sticky policies" erfunden hat.

4 So etwa die Gesellschaft für Datenschutz und Datensicherheit GDD in ihrer „Stellungnahme zu den Grundsätzen des Vorschlages der Europäischen Kommission einer Datenschutz-Grundverordnung" (o. J.), https://www.gdd.de/aktuelles/news/gdd-stellungnahme-zu-den-grundsatzen-des-vorschlages-der-europaischen-kommission-einer-datenschutz-grundverordnung, abgerufen am 25.04.2015.

5 Ruprecht B. Kamlah (1969). Right of Privacy. Das allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen. Köln: Carl Heymanns Verlag KG.

6 Siehe beispielhaft Ulrich Klug (1966). „Juristische Logik". In: Elektronische Datenverarbeitungsmaschinen im Recht, S. 157-172. Berlin, Heidelberg, New York: Springer-Verlag; Adalbert Podlech (1967). „Anforderungen der Kybernetik an die Rechtswissenschaft". In: Recht und Politik 3, S. 84-87; Adalbert Podlech (1968). „Anforderungen der Kybernetik an die Juristen". In: Recht und Politik 1, S. 21-23 und die fünfteilige Serie, die mit Herbert Fiedler (1970). „Automatisierung im Recht und juristische Informatik – 1. Teil". In: Juristische Schulung 10.9, S. 432-436 startete.

7 Siehe etwa Hans Peter Bull (1964). Verwaltung durch Maschinen – Rechtsprobleme der Technisierung der Verwaltung. 2. Aufl. Köln, Berlin: G. Grote'sche Verlagsbuchhandlung KG; Niklas Luhmann (1966). Recht und Automation in der öffentlichen Verwaltung. Berlin: Duncker & Humblot und Spiros Simitis (1967). Automation in der Rechtsordnung – Möglichkeiten und Grenzen. Karlsruhe: Verlag C. F. Müller.

8 Siehe etwa Malte von Berg (1968). Automationsgerechte Rechts- und Verwaltungsvorschriften. Köln, Berlin: G. Grote'sche Verlagsbuchhandlung KG und Hans Joachim von Oertzen (1969). „Automationsgerechte Gesetze als Voraussetzung der Automation". In: Deutsches Verwaltungsblatt 84.2, S. 61-67.

9 Siehe etwa Webers Beschreibung von Simitis in Hermann Weber (1970). „48. Deutscher Juristentag in Mainz". In: Juristische Schulung 10.12, S. 644-649, S. 649.

10 Siehe Datenschutzkommission des Deutschen Juristentages (1974). Grundsätze für eine Regelung des Datenschutzes. Bericht der Datenschutzkommission des Deutschen Juristentages. München: C. H. Beck'sche Verlagsbuchhandlung, vor allem S. 50 f.

11 Datenschutzgesetz in der Fassung vom 7. Oktober 1970, GVBl. I, S. 625-627.

12 Herbert Fiedler (1975). „Datenschutz und Gesellschaft". In: GI – 4. Jahrestagung. Hrsg. von D. Siefkes. Lecture Notes in Computer Science, Bd. 26. GI, Gesellschaft für Informatik. Berlin, Heidelberg, New York: Springer, S. 68-84, S. 77 f.

13 Siehe zur Übersicht Bundestagsdrucksache 7/5277, umfassend Werner Liedtke (1980). Das Bundesdatenschutzgesetz. Eine Fallstudie zum Gesetzgebungsprozeß. Dissertation München: Ludwig-Maximilians-Universität zu München.

14 Arthur Raphael Miller (1969). „Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society". In: Michigan Law Review 67.6, S. 1089-1246. S. 1211.

15 James P. Anderson (1972). Computer Security Technology Planning Study. ESD-TR-73-51. U.S. Air Force Electronic Systems Division.

16 Ulrich Seidel (1972). Datenbanken und Persönlichkeitsrecht unter besonderer Berücksichtigung der amerikanischen Computer Privacy. Köln: Verlag Dr. Otto Schmidt KG, S. 167 f.

17 Adalbert Podlech (1973). Datenschutz im Bereich der öffentlichen Verwaltung. Datenverarbeitung im Recht (DVR) Beiheft 1. Berlin: J. Schweitzer Verlag, S. 60 f.

18 Bundestagsdrucksache 7/5277, S. 6.

19 Ebd.

20 Der Bundesrat versuchte demgegenüber damals, die gesetzliche Regelung noch stärker in Richtung einer nur beschränkt als Datensicherheitsvorschrift zu verstehenden Formulierung zu verändern, siehe Bundestagsdrucksache 7/5494, S. 1 f.

21 Die Untersuchung entstand 1974, der Bericht wurde jedoch erst 1978 veröffentlicht, siehe Wilhelm Steinmüller, Leonhard Ermer und Wolfgang Schimmel (1978). Datenschutz bei riskanten Systemen. Informatik-Fachberichte, Bd. 13. Berlin, Heidelberg, New York: Springer.

22 Siehe dazu Jörg Pohle (i.E.). „Die kategoriale Trennung zwischen „öffentlich" und „privat" ist durch die Digitalisierung aller Lebensbereiche überholt – Über einen bislang ignorierten Paradigmenwechsel in der Datenschutzdebatte". In: „Worüber reden wir eigentlich?" Festgabe für Rosemarie Will. Hrsg. von Michael Plöse u. a. Humanistische Union. Berlin.

23 Siehe Ernestus in: Spiros Simitis, Hrsg. (2011). Bundesdatenschutzgesetz. 7. Aufl. Baden-Baden: Nomos Verlagsgesellschaft, § 9, Rn. 1 ff.

24 Siehe die Ausführungen im 1. TB des Bundesbeauftragten für den Datenschutz, abgedruckt in: Bundestagsdrucksache 8/2460, S. 52.

25 Der nachfolgende Teil stützt sich auf die Fassung der Vorschriften im Staatsanzeiger für das Land Hessen, Nr. 50, 11.12.1978, S. 2451-2457.

26 Siehe dazu Jörg Pohle (2014). „Kausalitäten, Korrelationen und Datenschutzrecht". In: Fundationes I: Geschichte und Theorie des Datenschutzes. Hrsg. von Jörg Pohle und Andrea Knaut. Münster: Monsenstein und Vannerdat, S. 85–105, S. 91 ff.

27 Siehe etwa Martin Rost (2012). „Faire, beherrschbare und sichere Verfahren". In: Innovativer Datenschutz. Hrsg. von Heinrich Kersten, Falk Peters und Klaus-Dieter Wolfenstetter. Berlin: Duncker & Humblot, S. 17-37.

28 Siehe Scholz in: Spiros Simitis, Hrsg. (2011). Bundesdatenschutzgesetz. 7. Aufl. Baden-Baden: Nomos Verlagsgesellschaft, § 3a, Rn. 33. Philip Scholz ist Regierungsdirektor im Amt des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Es erscheint eher unwahrscheinlich, dass er hier der Mehrheitsmeinung der Datenschutzaufsichtsbehörden widersprechen würde.

29 Siehe dazu Martin Rost (2014). „Was meint eigentlich Datenschutz?" In: Der Landkreis 3, S. 72-74.

30 Für frühe Arbeiten zu den konzeptionellen Grenzen des Betroffenenschutzes durch Anonymisierung siehe schon Klaus Lenk (1973). „Datenschutz in der öffentlichen Verwaltung". In: Datenschutz. Hrsg. von Wolfgang Kilian, Klaus Lenk und Wilhelm Steinmüller. Frankfurt am Main: Athenäum-Verlag, S. 15-50, S. 21 f. oder Wilhelm Steinmüller (1974). „Datenschutzrechtliche Anforderungen an die Organisation von Informationszentren". In: Internationale Fachtagung: Informationszentren in Wirtschaft und Verwaltung. Hrsg. von P. Schmitz. Lecture Notes in Computer Science, Bd. 9. Gesellschaft für Informatik, Fachausschuß 8 „Methoden der Informatik für spezielle Anwendungen". Berlin, Heidelberg, New York: Springer, S. 187-205, S. 193.

31 Siehe beispielhaft Marie-Theres Tinnefeld, Benedikt Buchner und Thomas B. Petri (2012). Einführung in das Datenschutzrecht. 5. Aufl. München: Oldenbourg Verlag und Spiros Simitis, Hrsg. (2011). Bundesdatenschutzgesetz. 7. Aufl. Baden-Baden: Nomos Verlagsgesellschaft.

Angela Meindl

Internet-Profiling

Umfang, Risiken und Schutzmaßnahmen am Beispiel von Google

Internet-Profiling nennt man den Vorgang, über Menschen, die sich im Internet bewegen, möglichst differenzierte Informationen zu sammeln und diese in einem möglichst genauen Persönlichkeitsprofil zusammenzuführen. Für diesen Zweck werden nicht nur die Daten gesammelt und gespeichert, die jemand, z. B. beim Ausfüllen von Formularen, selbst preisgibt. Es kann mithilfe diverser Techniken, die beim Besuch einer Webseite nicht zu bemerken sind, das Nutzungsverhalten während des Surfens in Erfahrung gebracht werden. Überspitzt könnte man sagen, alles, was man im Internet tut, wird mitgelesen.

Begründet wird dieses Verfahren in der Regel zum einen damit, besseren personenbezogenen Inhalt bieten zu können und die Usability zu verbessern. Zum anderen geht es darum, die Effektivität von Webseiten zu erhöhen und Werbekampagnen analysieren zu können.

In diesem Papier soll auf das in puncto Profiling technisch Machbare und das datenschutzrechtlich Erlaubte eingegangen werden. Es werden die gängige Praxis, die damit verbundenen Interessen und die Frage nach der Notwendigkeit thematisiert. Stellvertretend für viele andere wird dies am Beispiel von Google geschehen.

Wie werden Daten gesammelt?

Die wichtigsten Techniken, die zum Datensammeln eingesetzt werden, sind Zählpixel, Cookies und Logdateien.

Beim Zählpixel wird die Technik genutzt, mit der HTML-Bilder in eine Webseite eingebunden werden. Da das Bild nicht direkt in der HTML-Datei liegt, sondern dort nur ein Hinweis für den Browser steht, der ihm sagt, wo das Bild liegt, muss der Browser eine Verbindung zum Bilder-Server aufbauen, um das Bild zu laden. Da das Bild auf jedem Internetserver liegen kann, wird diese Vorgehensweise genutzt, um mit dem Zählpixel Daten zu sammeln. Dabei wird dem Browser mitgeteilt, dass er ein Bild laden soll. Es wird aber keine Verbindung zum Bilder-Server hergestellt, sondern zu einem Tracking-Server. Diesem Verbindungsaufbau können diverse Parameter mitgegeben werden, die dem Tracking-Server mitteilen, ob z. B. Skripte übertragen oder Cookies gesetzt werden sollen. Ein so gesetztes Cookie ist zwar ein Drittanbieter-Cookie, wird vom Browser aber nicht als solches betrachtet. So gesetzte Cookies enthalten in der Regel eindeutige Nutzer-IDs, die es ermöglichen, jemanden immer wiederzuerkennen und alle gesammelten Daten eindeutig zuordnen zu können.

Mit den Skripten können diverse Informationen über die Webseitennutzer und ihr Verhalten auf der Webseite eingesammelt und an den Tracking-Server gesendet werden, um sie dort im entsprechenden Profil zu speichern.

Die dritte Technik im Bunde ist die Auswertung der Logdateien. Ursprünglich zum Debuggen gedacht, werden in ihnen alle Aktivitäten von Server, Router oder Firewall gespeichert. Aber sie enthalten nicht nur Aktivitäten wie die aufzurufende Webseite, den Referrer oder die benutzte Suchmaschine inkl. Suchbegriff, sondern können auch diverse Informationen über das benutzte Computersystem enthalten. Dazu gehören die IP-Adresse, der Browsertyp und die Version, die eingestellte Sprache, die Bookmarks, installierte Plug-ins, die eingestellte Zeitzone, das Betriebssystem, die Bildschirmauflösung oder installierte Schriftarten.

Aus diesen Informationen lässt sich ein Browser-Fingerprint erstellen, der besonders dann dazu beitragen kann, jemanden wiederzuerkennen, wenn die Cookies und mit ihnen die Nutzer-ID gelöscht wurden. Nach einer Studie von Henning Tillmann [1] sind Browser-Fingerprints mit bis zu 92,57 % eindeutig.

Maus-, Geo- und Behavioural-Targeting

Beim Targeting geht es darum, möglichst viele Einzelheiten über das Nutzerverhalten im Internet in Erfahrung zu bringen und auswerten zu können. Dafür kommt die Möglichkeit, per Zählpixel Skripte einsetzen zu können, zum Einsatz.

Man unterscheidet hauptsächlich zwischen Maus-, Geo- und Behavioural-Targeting. Maus-Targeting wird eingesetzt, um das Leseverhalten auf der Webseite in Erfahrung zu bringen. Dabei wird die Position der Maus ausgewertet, weil man davon ausgeht, dass bei sehr vielen Menschen die Maus genau dort ist, wo gelesen wird. Aber auch wenn dies nicht bei allen Menschen der Fall ist, kann immer noch das Navigationsverhalten ermittelt werden.

Angela Meindl

Angela Meindl, B. Sc., ist Medien-Informatikerin aus Bremen, *a.meindl@artinfakt.de*

Das Geo-Targeting kommt zum Einsatz, um den Standort des Nutzers definieren zu können. Dabei werden die IP-Adresse und die Browser-Einstellungen wie Sprache und Zeitzone ausgewertet. Bemerken kann man das Ergebnis von Geo-Targeting, wenn man Google-Maps oder ähnliche Seiten aufruft. Es wird die Region angezeigt, in der der Rechner des Nutzers steht.

Die größte Rolle spielt jedoch das *Behavioral-Targeting*. Zum Einsatz kommt es in zwei verschiedenen Varianten. Entweder ausschließlich innerhalb einer Webseite oder webseitenübergreifend. Technisch wird Behavioral-Targeting, genauso wie Maus-Targeting, mit einer Kombination aus Zählpixel und Cookie umgesetzt.

Daten, die in Cookies gespeichert werden, können gelöscht werden. Daten, die mit Skripten über das Zählpixel erhoben werden, landen, ohne dass der Nutzer überhaupt etwas von deren Erhebung ahnt, direkt in der Datenbank des Tracking-Servers.

Wie und wo sammelt Google unsere Daten?

Google sammelt mit seinen Diensten wie der Suchfunktion, Google+, Google Analytics, Picasa, YouTube usw. Unmengen von Daten, weltweit und in 156 Sprachen, die beim Nutzen der Dienste entweder freiwillig eingegeben werden oder einfach anfallen. Dabei nutzt Google alle drei zuvor beschriebenen Techniken. Es werden Cookies mit eindeutiger ID auf dem Clientrechner gesetzt, die Logfiles ausgewertet und Scripting z. B. mit Zählpixeln betrieben [2]. Auch wenn sich das lange niemand klar gemacht hat, macht Google kein Geheimnis daraus. Wenn man vor allem die Google-Hilfe-Seiten und die Datenschutzrichtlinien der einzelnen Dienste aufmerksam liest und erkennen kann, wo Google seine Sammelwut schönredet, kann man dort sehr wohl ziemlich viel darüber erfahren, wann, wie und wo Daten gespeichert werden.

Wenn man vom Anfallen von Daten spricht, sind die Daten gemeint, die durch Protokolle entstehen und in den Logfiles gespeichert werden. Aus den Logfiles kann Google folgende Informationen über jede Nutzerin entnehmen:

IP-Adresse, Referrer, benutzte Suchmaschine, Suchbegriffe (d. h. alle Interessen oder Probleme, nach denen man über die Google-Suche recherchiert hat), Zeitstempel, benutzter Browser, Betriebssystem, Bildschirmauflösung, installierte Browser-Plug-ins, Lesezeichen, eingestellte Sprache, installierte Schriftarten, eingestellte Zeitzone.

Es ist wohl nur wenigen Menschen bewusst, wie viel sie über sich preisgeben, wenn sie einfach ihre Suchbegriffe bei Google eingeben und anschließend die Suchergebnisse durchstöbern und dass diese Informationen alle und für lange Zeit gespeichert und einem Profil zugeordnet werden.

Googles Wissen über uns

Wie umfassend schon die Informationen sind, die Google und andere Suchmaschinenbetreiber nur durch die Suchbegriffe über uns erhalten, zeigt das Beispiel von Thelma Arnolds. Der Fall hat 2006 in den USA für Schlagzeilen gesorgt. Damals hatte AOL eine Datei mit ihren Logfiles der AOL-Suche ins Internet gestellt. Sie wollten Informatikern diese Datei zur Verfügung stellen, damit sie verfeinerte Suchalgorithmen damit entwickeln könnten. Es wurde schnell klar, wie brisant die Daten sind, und AOL hat die Datei schnell wieder zurückgezogen. Aber es war schon zu spät. Viele Informatiker hatten die Datei schon heruntergeladen und mit der Analyse begonnen.

Auch die *New York Times* hatte einen Informatiker damit beauftragt, die Daten zu analysieren. Sie wollten sehen, ob sie eine Person nur über ihre Suchbegriffe identifizieren könnten. Sie werteten alle Suchanfragen der Nutzerin mit der Benutzerinnennummer 4417749 aus. Sie suchte unter anderem nach „taube Finger, alleinstehende Männer ab 60, Hund uriniert auf alles, Landschaftsgärtner in Lilburn GA (GA = Georgia – *Anmerkung der Autorin*), den Namen Arnolds in Kombination mit verschiedenen Vornamen".

Allein durch diese Informationen ist es der New York Times gelungen, die betreffende Person zu finden. Es handelte sich um besagte Thelma Arnolds. Eines schönen Nachmittags standen die Reporter der New York Times bei Thelma Arnolds in der Tür und lasen ihr ihre Suchbegriffe vor. Man kann sich vorstellen, wie überrascht Ms. Arnolds war.

Es werden aber nicht nur mit der Suche Daten über uns gesammelt. Auch mit allen anderen Diensten sammelt Google Daten über uns. Wobei man für alle Dienste, mit wenigen Ausnahmen, ein Google-Konto braucht, für das man persönliche Daten wie Name, Adresse, Geburtsdatum usw. angeben muss. Mit diesen Angaben können dann alle von Google gesammelten Daten eindeutig einer Person zugeordnet werden. Was Google von jemandem weiß, hängt natürlich davon ab, welche Dienste man nutzt oder auf wie vielen Webseiten man war, die von Google Analytics etc. getrackt werden. Aber zu dem, was Google über uns wissen kann, gehören die folgenden Informationen: IP-Adresse, Referrer, benutzte Suchmaschine, Suchbegriffe (d. h. alle Interessen oder Probleme, nach denen man über die Google-Suche recherchiert hat), Zeitstempel, benutzter Browser, Betriebssystem, Bildschirmauflösung, installierte Browser-Plug-ins, Lesezeichen, eingestellte Sprache, installierte Schriftarten, eingestellte Zeitzone, Name, E-Mail-Adresse, Geburtsdatum, Geschlecht, Mobiltelefon-Nr., Standort, welche Digitalkamera man benutzt, wo die Bilder aufgenommen wurden, wie wir aussehen, über welche Themen man sich mit wem in seinen Mails austauscht, mit wem man befreundet ist, mit wem man welche Interessen teilt, Vorlieben, Hobbys, Bankkonto-Daten etc.

Man kann sicher sein, dass, egal wie man mit Google in Berührung gekommen ist, ein ziemlich umfassendes Persönlichkeitsbild dabei herauskommt.

Sind wir durch Datensammlungen über uns gefährdet?

Das Beispiel von Thelma Arnolds mag für den einen oder anderen vielleicht noch nicht wirklich nach Gefahr aussehen, weil ja weder Unglück noch Schaden daraus entstanden sind. Aber es weckt schon ein wenig eine Vorstellung davon, dass so viel Wissen über eine Person Begehrlichkeiten wecken kann, die nicht zwangsläufig freundlicher Natur sein müssen.

Wenig erfreulich fanden es sicher auch WhatsApp-Nutzer, als Facebook WhatsApp gekauft hat und damit auch alle Daten, die WhatsApp über ihre Nutzerinnen gesammelt hatte, in den Besitz von Facebook übergingen. Das zeigt, dass alle Daten, die über uns gesammelt werden, in das Eigentum der sammelnden Firma übergehen und Teil ihres Wertes sind. Sie können verkauft werden und gehen bei Insolvenz in die Konkursmasse ein.

Beide Beispiele zeigen, dass wir keinerlei Kontrolle mehr darüber haben, wer was über uns erfährt oder zu welchem Zweck unsere Daten verwendet werden. Noch viel weniger können wir wissen, welche Konsequenzen der Umgang mit unseren Daten für uns oder andere haben kann.

Gefährdungen können daraus sowohl auf politischer und wirtschaftlicher als auch auf privater Ebene entstehen. Betrachtet man die politische Ebene, denken die meisten Leute vermutlich an Vorratsdatenspeicherung. Nach deutschem Recht darf nur durch richterlichen Beschluss gezielt auf einzelne Datensätze zugegriffen werden. Jetzt könnte man denken, dass man sich sicher fühlen kann, wenn man nichts zu verbergen hat. Aber abgesehen davon, dass man nie sicher sein kann, dass man nichts zu verbergen hat, gilt deutsches Recht nur für einen kleinen Bruchteil des Internets. Nämlich nur für Webseiten, die auf deutschen Servern liegen. Der Großteil der Webseiten, die auch in Deutschland viel genutzt werden, liegt aber nicht auf deutschen, sondern auf amerikanischen Servern. Dazu gehören Google, Facebook, eBay und Skype, um nur die Spitze des Eisberges zu nennen. Liegen die Seiten auf amerikanischen Servern, gilt amerikanisches Recht. Die amerikanische Regierung hat schon mehr als einmal große Internetunternehmen dazu verpflichtet, große Mengen an Daten zum Zweck der Verbrechensbekämpfung den Behörden zu überlassen.

Aber ganz unabhängig davon, wie die Gesetze formuliert sind, gibt es keine Garantie, dass sich Regierungen an ihre eigenen Gesetze halten, wie der aktuelle NSA-Skandal zeigt. Und Gesetze sind nicht in Stein gemeißelt. Sie können jederzeit geändert werden.

Wenn wir nur die möglichen Folgen für Privatpersonen betrachten, finden wir schon ein breites Spektrum an Gefährdungen. Denn überall, wo wir digitale Spuren hinterlassen, können andere diese nutzen.

Da wäre zunächst das Image-Problem. Denn alles, was die Google-Suche oder soziale Netzwerke über eine Person finden, kann jeder lesen. Was liegt also näher, als sich vor einer Begegnung mit einer Person, die man noch nicht kennt, im Internet zu informieren. Das heißt aber, dass die Informationen, die über uns im Internet zu finden sind, das Bild, das andere von uns haben, prägen. Im privaten Bereich mag das noch nicht so schwerwiegend sein. Schwieriger wird es da schon, wenn zukünftige Arbeitgeber sich im Internet über Bewerberinnen informieren. Zu den möglichen K.o.-Kriterien gehören nicht nur Partybilder. Auch das Betreiben von Leistungssport mit regelmäßigen Wettkämpfen am Wochenende, politisches oder soziales Engagement usw. können Negativpunkte bringen, weil das ein Hinweis auf mangelnde Bereitschaft sein kann, am Wochenende Überstunden zu machen.

Auch Banken und Versicherungen bedienen sich der Möglichkeiten des Internets, wenn es um den Leumund von jemandem geht, der einen Kredit haben möchte oder eine Versicherung abschließen möchte. Die Benachteiligungen, die entstehen können, sind also nicht unerheblich.

Ein weiteres Problem besteht darin, dass diese Informationen auch für Mobber, Stalker und Kriminelle viele Anhaltspunkte bieten, wenn es darum geht, jemandem zu schaden. Es können ganze Identitäten gestohlen werden.

Ist Profiling wirklich nötig?

Diese Frage muss man unter verschiedenen Aspekten beleuchten. So ist es natürlich ein Unterschied, ob jemand seine Daten selbst zur Verfügung stellt oder ob sie ohne sein Wissen erhoben und gespeichert werden.

Selbst stellt man seine Daten beispielsweise bei einem Einkauf in einem Online-Shop zu Verfügung. Ohne Informationen wie Name, Adresse, E-Mail-Adresse, Geburtsdatum, Inhalt des Warenkorbes und gewünschte Zahlungsweise ließe sich eine Online-Bestellung gar nicht abwickeln. In der Regel speichern Online-Shops zwar auch die IP-Adresse des Kunden, das ist aber unbedenklich, solange kein weiteres Tracking betrieben wird.

Ganz anders sieht es mit den Daten aus, die ohne unser Wissen erhoben und gespeichert werden. Oft wird dieses Vorgehen mit der Verbesserung der angebotenen Dienste begründet. Des Weiteren geht es um Werbeeinblendungen, die auf die einzelne Person zugeschnitten sind. Natürlich sind Informationen darüber, mit welcher technischen Ausstattung jemand auf die Webseite geht, für die Seitenbetreiber interessant. Genauso wie Informationen über die Aufenthaltsdauer auf einzelnen Seiten und die Uhrzeit des Besuches.

Wird eine Seite schnell wieder verlassen, ist das ein Hinweis auf schlechten Inhalt oder technische Probleme. Zu diesem Zweck werden oft Analysetools wie Google Analytics eingesetzt. Google Analytics legt aber eben auch sehr differenzierte Profile von jedem einzelnen Nutzer an, bei dem die Nutzer nicht selten über viele verschiedene Webseiten geradezu verfolgt werden, um wirklich jede digitale Lebensäußerung abspeichern zu können. Bei Datensammlungen in diesem Umfang geht es nicht mehr darum, Dienste zu verbessern.

Der zweite Grund für das Sammeln von Daten sind Werbeeinblendungen. Auch hier werden über Partnerprogramme sehr viele Daten erhoben, um die Werbekampagnen auszuwerten. Das wohl bekannteste Programm ist Google AdWords, dessen Werbeeinblendungen in den Suchergebnisseiten von Google eingeblendet werden.

Um eine Werbekampagne abrechnen zu können, braucht man aber lediglich Informationen darüber, wie oft die Werbebanner angeklickt wurden und wie oft es tatsächlich zum Verkauf gekommen ist. Sowohl bei Google Analytics als auch bei AdWords sind die erhobenen Daten nicht im Besitz der Seitenbetreiber, sondern sie sind im Besitz von Google. Die Seitenbetreiber erhalten lediglich eine Auswertung zur Verfügung gestellt.

Dass Seitenbetreiber ihre Webseite für ihre Nutzer optimieren möchten, ist legitim. Dafür sind aber nur Informationen darüber notwendig, mit welcher technischen Ausstattung wie viele Nutzer wie lange auf den einzelnen Seiten gewesen sind. Man muss nicht wissen, wer diese Personen sind oder was sie sonst noch so im Internet machen. Und man muss schon gar nicht die Daten an Dritte weitergeben, wie es bei den Google-Tools der Fall ist.

In einem Test habe ich geprüft, ob es möglich ist, diese grundlegenden Daten personenunabhängig zu bekommen, ohne sie an Dritte weitergeben zu müssen. Zu diesem Zweck habe ich nach Open-Source-Tools gesucht, die man im eigenen Webspace installieren kann. Fündig geworden bin ich bei Piwik [3] als Alternative zu Google Analytics und den AdServer Revive [4] als Alternative zu Google AdWords. Beide Programme habe ich auf einem lokalen Webserver ohne Internetzugang installiert, um zu testen, ob sie auch nicht heimlich die Daten an den Softwarehersteller übertragen.

Das Ergebnis war überzeugend. Beide Programme haben in Anzahl und Menge zusammengefasste Ergebnisse geliefert, ohne auf einzelne Besucher einzugehen. Beide Programme haben gut funktioniert, ohne eine Verbindung zum Hersteller aufbauen zu können. Daraus kann man den Schluss ziehen, dass Webseitenbetreiber gut auf die differenzierten Datensammlungen verzichten können und trotzdem in der Lage sind, ihre Webseiten zu optimieren und Werbekampagnen korrekt abzurechnen.

Wenn man bedenkt, welche Risiken, von denen hier ja nur eine kleine Spitze des Eisberges beschrieben wurde, Nutzer durch das Profiling tragen müssen, ist Profiling nicht akzeptabel.

Profiling und Datenschutz?

Profiling aus der Sicht des Datenschutzes ist ein durchaus komplexes Thema. Da das Internet international ist, gilt es als erstes festzustellen, welches Recht eigentlich gilt. Obwohl im Internet grundsätzlich das Recht des Landes gilt, in dem die Server stehen, auf denen die Webseiten liegen, möchte ich einen Blick auf deutsches (bzw. EU-)Recht, amerikanisches Recht und die Datenschutzrichtlinien von Google werfen.

Das deutsche Datenschutzrecht gilt als das strengste der Welt. Genau genommen besteht es aber aus einer Vielzahl von Gesetzen und Regelungen. Die wichtigsten sind wohl das Telemediengesetz, das Grundrecht auf informationelle Selbstbestimmung und das Gesetz zur Vorratsdatenspeicherung.

Das Telemediengesetz besagt, dass personenbezogene Daten nur genutzt werden dürfen, wenn die betroffene Person vor dem Nutzungsvorgang über Art, Umfang und Zweck der Erhebung und Verwendung in verständlicher Form unterrichtet wurde, auch wenn die Daten außerhalb der EU verarbeitet werden. Die Nutzerin muss ihre Einwilligung bewusst und eindeutig erteilt haben.

Das Grundrecht auf informationelle Selbstbestimmung erweitert das Ganze noch, indem es besagt, dass jede Bundesbürgerin das Recht hat, selbst zu bestimmen, wem sie Informationen über sich preisgibt und wem nicht. Eingeschränkt werden diese beiden Rechte allerdings durch die Vorratsdatenspeicherung, die alle Medienanbieter dazu verpflichtet, alle Daten, die über ihre Infrastruktur laufen, für einen vorgegebenen Zeitraum zu speichern.

Das europäische Datenschutzrecht hat eher die Funktion, für alle Mitgliedstaaten einen gemeinsamen Mindeststandard zu schaffen.

Ganz anders sieht es da im amerikanischen Datenschutz aus. In Amerika setzt man auf Selbstverpflichtung. Das heißt im ersten Schritt, dass man machen kann, was man will. Es muss nur korrekt und zugänglich beschrieben werden, wie mit den erhobenen Daten umgegangen wird. Sollten sich falsche Angaben herausstellen, gibt es eine Verwarnung und die Auflage, ein Pflichtenheft zum Umgang mit den Daten zu entwickeln, an das man dann auch gebunden ist. Erst nach einem Verstoß gegen das selbst entwickelte Pflichtenheft kann die Justiz tätig werden. Sollte eine Firma bei einem solchen Verstoß ertappt werden, kommt es meistens nur zu einer Geldstrafe.

Sieht man sich nun die Datenschutzerklärung von Google an, so weist Google eindeutig darauf hin, dass sie alle Daten sammeln, die sie bei der Nutzung ihrer Dienste von ihren Nutzerinnen bekommen können. Sie verharmlosen zwar, indem sie immer davon reden, dass die Daten möglicherweise erhoben werden. Es wird darauf hingewiesen, dass Browser-Fingerprint-Daten erhoben werden und, wenn vorhanden, mit dem Google-Konto verknüpft werden. Es wird gesagt, dass Cookies und Zählpixel zum Einsatz kommen. Es wird darauf hingewiesen, dass die Server, auf denen die Daten gespeichert werden, überall auf der Welt stehen können.

Google gesteht seinen Nutzerinnen zwar das Recht auf Änderung fehlerhafter personenbezogener Daten zu, schränkt die Umsetzung aber ein. Es darf nicht zu aufwändig werden und nicht zu offensiv eingefordert werden. Und Daten in den Google-Sicherungssystemen werden nie gelöscht. Google verschweigt auch nicht, dass personenbezogene Daten an für Google vertrauenswürdige Dritte zwecks Verarbeitung weitergegeben werden.

Vergleichen lassen sich der deutsche und der amerikanische Datenschutz kaum. Dafür sind die Herangehensweisen zu unterschiedlich. Google hält sich an das amerikanische Recht, auch wenn sie schon einmal zur bisher höchsten verhängten Geldstrafe von 22,5 Millionen Dollar verurteilt wurden [5], weil sie falsche Angaben zu Tracking-Cookies im Safari-Browser gemacht hatten.

Die Art und Weise, wie Google Daten sammelt, ist mit dem deutschen Datenschutz schon schlechter zu vereinbaren. Das Problem mit der geforderten Zustimmung der Nutzer löst Google in einem Spagat. Wie viele andere große Internetfirmen sagt Google in seiner Datenschutzerklärung, dass eine Nutzung der Dienste gleichbedeutend mit einer Zustimmung ist.

Resümee

Die Art und Weise, wie vom Nutzer unbemerkt Daten über ihn erhoben und gespeichert werden, ist nicht akzeptabel, mit welcher Begründung auch immer sie gerechtfertigt wird. Ohne Notwendigkeit muss jeder, der an den Optionen der Informations-

technik teilhaben will, auf seine Privatsphäre verzichten, und er trägt ein nicht zu unterschätzendes Gefährdungsrisiko, während diejenigen, die für diesen Zustand verantwortlich sind, Unmengen Geld mit unserer Privatsphäre verdienen.

Um dem Gedanken der Selbstbestimmung und der geforderten Zustimmung Rechnung zu tragen, sollte es für das Tracking und Profiling eine Double-Opt-in-Lösung geben. Ähnlich wie es bei Newslettern ja schon Gesetz ist. Webseiten, die getrackt werden, sollten ein vorgeschaltetes Pop-up öffnen, in dem über Art und Zweck der Datenerhebung informiert wird. Dieses natürlich noch nicht getrackte Pop-up sollte zwei Buttons enthalten. Einer, mit dem man zustimmt, und einer, mit dem man das Tracking ablehnen kann. Lehnt man das Tracking ab, müsste eine ungetrackte Version der Website geöffnet werden. Zusätzlich sollte in dem Pop-up gleich ein Link vorhanden sein, der auf eine Seite führt, auf der sich jeder anzeigen lassen kann, was über ihn gespeichert ist. Wo er die Möglichkeit hat, Korrekturen bei fehlerhaften Angaben vorzunehmen, und wo er auch das Löschen aller gespeicherter Daten inklusive derer, die an Dritte weitergegeben wurden, beauftragen kann.

Auch sollte über ein internationales Datenschutzrecht für das Internet nachgedacht werden, an das sich alle Internetseitenanbieter verbindlich halten müssten. Um dieses Recht durchsetzen zu können, wäre natürlich eine entsprechend umfangreiche Kontrollinstanz und ein wirkungsvoller Maßnahmenkatalog für Verstöße notwendig.

Referenzen

[1] Tillman, Henning: http://bfp.henning-tillmann.de

[2] Google: Google-Nutzungsbedingungen. https://www.google.com/intl/de/policies/terms/index.html

[3] Piwik: Liberating Analytics. http://piwik.org/ – Version 16.6.2014

[4] Revive Software and Services: Introducing Revive Adserver. http://www.revive-adserver.com/

[5] SPIEGEL ONLINE: Datenschutz-Verstoß: Google zahlt Rekordbußgeld. 9.8.2012. http://www.spiegel.de/netzwelt/netzpolitik/ftc-google-muss-wegen-safari-verstoss-22-5-millionen-dollar-zahlen-a-849210.html

Carsten Seeger

Android? Aber sicher!?

Die Pleiten-, Pech- und Pannenserien unserer mobilen Welt

Unser Handy ist mittlerweile ein Standard-Accessoire, so wie Schlüssel und Portemonnaie. Es ist nutzbringend, einfach zu bedienen, und man ist immer erreichbar. Früher im Wesentlichen zum Telefonieren und SMS-Schreiben gebraucht, ist es heute ein multimediales Erfolgskonzept. Facebook, Twitter, YouTube, und das alles auch noch drahtlos mit Breitband-Internet. Doch welchen Preis zahlen Nutzerinnen und Nutzer für diesen Komfort?

Google gilt als einer der Monopolisten der modernen Internetgesellschaft, unter anderem durch sein mobiles Betriebssystem Android. Mit durchschnittlich mehr als 70 % aller verwendeten mobilen Systeme ist es das weitverbreitetste Betriebssystem für Handys und Tablets.[1]

Wie sicher ist aber unser geliebtes Android-Handy wirklich? Google hat sich ja schließlich schon einige Pleiten geleistet. Während anfangs lediglich einzelne Sicherheitslücken zu verkraften waren[2], wird es heute selbst für geübte Benutzer immer schwieriger zu überprüfen, ob ihre Apps auch wirklich das tun, was sie sollen.

Überprüfen der Berechtigungen von Apps

Was eine App darf und was nicht, wird über deren Berechtigungen abgebildet. Dass man vor der Installation schauen sollte, welche Berechtigungen verwendet werden, ist keine Neuheit und wurde schon öfter diskutiert[3]. Denn es kommt häufiger vor, als man denkt, dass Apps gerne von Datenkraken verwendet werden.

Mit Einführung der neuen Berechtigungsgruppen im letzten Jahr wurde der Aufschrei wieder einmal größer und das zu Recht[4]. Denn Googles neues Gruppenkonzept ist zwar einfacher geworden, dafür aber auch unübersichtlicher. Es wurden 13 neue Gruppen eingeführt[5]. Die zunächst wichtigste Änderung beschreibt Google aber wie folgt: „*These days, apps typically access the Internet, so network communication permissions including the full Internet access permission have been moved out of the primary permissions screen.*" Internet-Zugriff wird also künftig jeder App gewährt, denn es ist ja jetzt Standard und der Benutzer muss sich nicht darum kümmern.

Was heißt das nun für uns Android-User? Jede App, egal ob nun Taschenlampe oder Facebook, erhält Zugang zum Internet und das, ohne dass es bei der Installation einen Hinweis dafür gibt. Für Social-Media-Apps wie Facebook, Twitter etc. oder Chat-Apps wie das weitverbreitete WhatsApp kommt der Nutzer ja durchaus noch selbst dahinter, dass Internet-Zugang ein notwendiges Übel ist. Was ist aber mit unserer Taschenlampen-, Batterie- oder Wecker-App? Dem Nutzer wird die Information für diese Apps nur noch über Umwege angezeigt: Dies geht nur noch über die Berechtigungsansicht der App unter den Einstellungen des Systems.

Die nächste Pleite des neuen Konzeptes folgt auf dem Fuße, denn bereits installierte Apps bekommen über die automatische Updatefunktion auch neue Berechtigungen ohne die Erlaubnis des Nutzers. Sofern also die automatische Updatefunktion aktiviert ist, darf jede App, die bereits auf dem System läuft, mit dem Update ihre Berechtigungen innerhalb der vorhandenen Berechtigungsgruppen beliebig erweitern. Das erschwert dem Benutzer ein feingranulares Steuern der Berechtigungen. Besser

ist es da, die Updates manuell durchzuführen, denn dann wird für jede App explizit gefragt, wenn neue Berechtigungen benötigt werden[6].

Hier hat man zwar dem Nutzer keine Informationen vorenthalten, aber zu Gunsten der Einfachheit einige durchaus sicherheitsrelevante Informationen an den wichtigen Stellen weggelassen. Zwar lassen sich Apps im Nachhinein auf ihre einzelnen Berechtigungen prüfen, aber dafür muss diese eben auch erst einmal installiert werden. Ein durchaus fragwürdiges Konzept.

Unterlaufen des Berechtigungskonzeptes

Berechtigungen zu *überprüfen* heißt außerdem noch nicht, dass eine App nicht auch andere Wege findet, um Dinge zu tun, die sie eigentlich nicht dürfte. Ein chinesisches Forscherteam hat uns dazu einen Einblick gewährt. In dessen Android App *VoicEmployer* wird die Sprachsteuerung benutzt, um diverse Befehle auf dem Handy auszuführen.

Diese App kann z. B. gefälschte SMS oder E-Mail schreiben, Daten auslesen und übertragen, die GPS-Position ermitteln oder teure Premium-Rufnummern anwählen[7]. Dabei werden einfach mittels vorkonfigurierter Sprachdateien Sprachbefehle auf dem geräte-eigenen Lautsprecher ausgegeben, auf die das Handy mit der Sprachsteuerung Google Voice Search (GVS) reagiert und die Befehle ausführt. Und das alles auch noch ohne eine einzige Berechtigung, denn der Lautsprecher wird einer App standardmäßig zur Verfügung gestellt.

Schließlich demonstriert uns Tod Beardsley noch einige Lücken im Android Browser[8], über die es möglich ist, Befehle auf dem Handy auszuführen oder Apps ohne Erlaubnis des Benutzers zu installieren[9], vom Session Hijacking mittels der zahlreichen gespeicherten Cookies ganz zu schweigen. Dabei surft der Nutzer doch nur auf seinen Lieblingsseiten im Netz …

„Vertrau mir", sagte Google, „bei mir sind deine Daten sicher"[10]

Dass Google selbst kein unbescholtener Mitspieler ist und unverhohlen als Datenkrake agiert, ist sogar in den unternehmenseigenen AGB nachzulesen. Das Stichwort hier ist unsere geliebte Cloud. Mittlerweile lässt sich alles mit der Cloud verknüpfen, Kontaktadressen, Email-Adressen, Backups und natürlich auch alle Apps, die man so installiert hat. Zitat aus den Google-Nutzungsbedingungen: „*Wenn Sie Inhalte in unsere Dienste hochladen oder auf andere Art und Weise in diese einstellen, räumen Sie Google (und denen, mit denen wir zusammenarbeiten) das Recht ein, diese Inhalte weltweit zu verwenden, zu hosten, zu speichern, zu vervielfältigen, zu verändern, […] zu kommunizieren, zu veröffentlichen, öffentlich aufzuführen, öffentlich anzuzeigen und zu verteilen.*"[11] Oder kurz gesagt, was einmal in der Cloud ist, mit dem dürfen Google (und Sie wissen schon wer) alles anstellen, was ihnen in den Sinn kommt. Aber unsere Daten sind ja dort angeblich sicher eingelagert, mit direkten Sicherheitskopien in den diversen Nachrichtendiensteinrichtungen gleich nebenan.

Sicher ist hier wohl nur, dass nichts sicher ist!

Anmerkungen

1 International Data Corporation (IDC): Smartphone OS Market Share, Q4 2014, https://www.idc.com/prodserv/smartphone-os-market-share.jsp

2 Denise Bergert: Schwere Sicherheitslücke betrifft 99 % aller Android-Geräte, 18.5.2011, http://www.pcwelt.de/news/Sicherheit-Schwere-Sicherheitsluecke-betrifft-99-aller-Android-Geraete-1911546.html

3 Florian Schmidt: Aufgedeckt: AGB von App-Anbietern durchleuchtet, 17.6.2011, http://www.computerbild.de/artikel/cb-News-Sicherheit-Allgemeine-Geschaeftsbedingungen-AGB-App-Abzocke-Sicherheit-Datenschutz-6271809.html

4 Reddit: What latest changes to Play Store app means for privacy, 8.6.2014, https://www.reddit.com/r/Android/comments/27n7yr/what_latest_changes_to_play_store_app_means_for/

5 Google: Vereinfachte Berechtigungen bei Google Play, 2014, https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1

6 XDA Developers: Play Store Permissions Change Opens Door to Rogue Apps, 10.6.2014, http://www.xda-developers.com/play-store-permissions-change-opens-door-to-rogue-apps/

7 Wenrui Diao, Xiangyu Liu, Zhe Zhou, Kehuan Zhang: Your Voice Assistant is Mine: How to Abuse Speakers to Steal Information and Control Your Phone. In Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM '14), Scottsdale, AZ, 3.-7.11.2014, S. 63-74. Vorabversion http://arxiv.org/pdf/1407.4923v1.pdf

8 Tod Beardsley: R7-2015-02: Google Play Store X-Frame-Options (XFO) Gaps Enable Android RCE, 10.2.2015, https://community.rapid7.com/community/metasploit/blog/2015/02/10/r7-2015-02-google-play-store-x-frame-options-xfo-gaps-enable-android-remote-code-execution-rce#comments

9 Heise: Android-Exploit schleust beliebige Apps ein, 15.2.2015, http://www.heise.de/security/meldung/Android-Exploit-schleust-beliebige-Apps-ein-2549172.html

10 Frei nach: Google: Häufig gestellte Fragen. Abgerufen am 2.5.2015, https://www.google.com/intl/de_de/policies/faq/

11 Google: Nutzungsbedingungen, Stand 11. November 2013, https://www.google.com/intl/de/policies/terms/

Carsten Seeger

Carsten Seeger erwarb an der Friedrich-Schiller-Universität Jena einen B.Sc. in Information and Management Science und einen M.Sc. in Informatik. Beide Abschlussarbeiten schrieb er im Bereich IT-Sicherheit. Beruflich ist er mit Datenbanken, Software-Entwicklung und -Test, Web-Design sowie Server-Administration befasst.

Stefan Hügel

BigBrotherAwards 2015

Nachdem die Debatte um die Ausspähung von Gesellschaft, Politik und Wirtschaft seit einiger Zeit – scheinbar ohne ernsthafte politische Konsequenzen – abzuflauen drohte, hat sie durch die jüngsten Erkenntnisse zur Rolle des Bundesnachrichtendiensts wieder an Brisanz gewonnen – dies schlägt sich auch in der Auswahl der diesjährigen Preisträger.innen des BigBrotherAwards nieder. Doch auch aus anderen Bereichen gibt es viel zu berichten – die Ausspähung von Kindern ist genauso ein Thema wie die totalüberwachten neuen, „flexiblen" Arbeitsformen, die durch Plattformen des Crowdsourcing *möglich werden.*

Bei den diesjährigen BigBrotherAwards[1], die am 17. April 2015 in Bielefeld verliehen wurden, gibt es wie immer eine breite Palette von Bereichen, in denen personenbezogene Daten verarbeitet werden und wo der Datenschutz nicht immer all zu genau genommen wird. Wie jedes Jahr wurden besonders prägnante Beispiele in mehreren Kategorien prämiert.

Wir fassen zunächst die Laudationes für die Preisträger.innen kurz zusammen. Danach drucken wir vier Laudationes im Wortlaut ab.

Kategorie *Technik*

Der BigBrotherAward in der Kategorie *Technik* ging an die Puppe **Hello Barbie**, die von den Unternehmen **Mattel** – Hersteller der Puppe – und **ToyTalk** – Anbieter der Spracherkennung – vertrieben wird, bisher allerdings noch nicht in Deutschland. Linus Neumann vom *Chaos Computer Club* hielt die Laudatio.

Hello Barbie ist eine *Barbie-Puppe*, die mit Mikrofon, Lautsprecher und WLAN ausgestattet ist. Sie ist dadurch in der Lage, mit spielenden Kindern zu sprechen – durch Spracherkennung „versteht" sie das Gesagte und kann darauf – mehr oder weniger – sinnvolle Antworten geben. Man kann wohl davon ausgehen, dass Kinder dabei auch sehr persönliche Informationen preisgeben. „*Unser Verhalten wird minutiös protokolliert, durch Analysen erklärt, und durch gezielte Maßnahmen manipuliert. Meist mit der Absicht, uns danach etwas dazu passendes zu verkaufen. Kurzum: Unser Verhalten wird monetarisiert*", so heißt es dazu in der Laudatio.

Die Spracherkennung findet dabei nicht lokal, sondern in der Cloud statt. Das Gesprochene wird in eine Server-Cloud übertragen, dort aufgezeichnet, analysiert und eine passende Antwort generiert. Um die Antwortqualität immer weiter zu verbessern, werden die Daten gespeichert. Damit entsteht ein immer genaueres Bild der Persönlichkeit des Kindes. Dies liegt „irgendwo" in der Cloud, seine Weiterverbreitung ist damit praktisch nicht mehr kontrollierbar.

Die Eltern müssen der Datenübertragung freilich vorher zustimmen. Dafür erhalten sie auch ein Protokoll dessen, was ihr Kind der Puppe anvertraut hat. Neben den Risiken durch die Verarbeitung in der Cloud können die Kinder nun also auch von ihren Eltern totalüberwacht werden. In Europa soll *Hello Barbie* allerdings wegen der Datenschutzbedenken vorerst nicht verkauft werden.

Impression der Preisverleihung mit Moderator Andreas Liebold
Foto: Matthias Hornung, CC by 4.0

„*Mit WLAN, Mikrophon und Lautsprecher ermöglicht die neue* Hello Barbie *schon unseren Kindern, sich mit einer Serverfarm irgendwo da draußen in den Weiten des Internets zu unterhalten. Sie bringt eine datenschutzrechtlich äußerst fragwürdige Technik ohne erkennbaren sinnvollen Anwendungszweck direkt in unsere Kinderzimmer*", so das Fazit des Laudators.

Kategorie *Behörden und Verwaltung*

In der Kategorie *Behörden und Verwaltung* wurde der diesjährige BigBrotherAward an den **Bundesnachrichtendienst (BND)** verliehen, „*für eine ganze Palette von Skandalen sowie Datenschutz- und Bürgerrechtsverstößen*", wie Laudator Rolf Gössner einleitend betonte. Der BND erhalte den Preis,

„1. weil er aufs Engste in den menschenrechtswidrigen NSA-Überwachungsverbund verflochten ist und damit in den globalen Massenüberwachungsskandal;

2. *weil er mit der sog. strategischen Überwachung der grenzüberschreitenden Telekommunikation und insbesondere*

mit seiner gesamten Auslandsaufklärung via Funk, Satellit oder Kabel weitgehend im rechtsfreien Raum operiert – nach Auffassung renommierter Verfassungsrechtler sogar schlicht verfassungswidrig;

3. *weil der BND täglich über 220 Millionen Telekommunikationsdatensätze sammelt, speichert, auswertet und davon Millionen an ausländische Partnerdienste übermittelt. Darunter sind auch grundrechtlich geschützte Daten von Bundesbürgern, deren Weitergabe gesetzlich untersagt ist; außerdem, so Ex-NSA-Mitarbeiter Thomas Drake, soll der BND sensible Informationen für den menschenrechtswidrigen Drohnenkrieg der USA geliefert haben, und damit für das gezielte Töten von Terrorverdächtigen.*

4. *Nicht zuletzt erhält der BND den BigBrotherAward für seine Informationsblockade und dreisten Vertuschungen geheimdienstlicher Praktiken gegenüber dem NSA-Untersuchungsausschuss des Bundestags, der sich mit aufklärungsunwilligen BND-Zeugen und überwiegend geschwärzten, lückenhaften oder anderweitig manipulierten Akten des BND herumschlagen muss – frei nach der Zeugenaussage des Nachrichtendienste-Beauftragten im Bundeskanzleramt, Klaus-Dieter Fritsche (CSU), das ‚Staatswohl' sei nun mal weit wichtiger als parlamentarische Aufklärung und Kontrolle."*

Im Rahmen der Operation Eikonal zapfte der BND den Internetknoten DE-CIX in Frankfurt am Main an und belieferte auch die NSA jahrelang mit Daten. Bei der strategischen Fernmeldekontrolle am Frankfurter Knoten, mit dem Ziel, Terrorismus, Waffenhandel und Schleusung aufzudecken, fielen auch Daten aus der geschützten Alltagskommunikation ab, die der BND weder speichern noch ins Ausland übermitteln darf. Ein Filter soll das verhindern, funktionierte aber nicht richtig, so dass auch geschützte Daten illegal an die NSA übermittelt wurden.

Dennoch soll der BND weiter aufgerüstet werden – geplant sind 300 Mio. Euro –, zur Überwachung von sozialen Netzwerken, Blogs und Web-Foren und für den Einbruch in fremde Computersysteme.

Gleichzeitig unterlässt es die Bundesregierung, die Bevölkerung und die Wirtschaft vor dieser Massenüberwachung zu schützen, was ihre verfassungsrechtliche Pflicht wäre. Auch die Bundesanwaltschaft hat sich bisher[2] darauf beschränkt, ein Strafverfahren wegen der Ausspähung des Kanzlerinnenhandys einzuleiten. Bei der Massenüberwachung der Bevölkerung verzichten sie, mangels „zureichender Tatsachen".

„Das ist angesichts der Fülle an Belastungsbeweisen und -zeugen Realitätsverleugnung oder Willfährigkeit – jedenfalls hart an der Grenze zur Strafvereitelung im Amt. Diese Rechtsschutzverweigerung ist eine Kapitulation des Rechtsstaats vor staatlichem Unrecht", so Laudator Rolf Gössner. *„Deshalb sehen wir uns in der Pflicht, mit diesem überfälligen BigBrotherAward den Blick der Öffentlichkeit erneut auf die Machenschaften des BND zu lenken und auf das Problem geheimer Institutionen in einer Demokratie."*

Kategorie *Wirtschaft*

„Für die Einführung des digitalen Taglöhnertums" – so Laudatorin Rena Tangens – geht der BigBrotherAward in der Kategorie *Wirtschaft* an **Amazon Mechanical Turk** und **Upwork** (vormals **Elance-oDesk**).

Beides sind *Crowdworking*-Plattformen: Sie vermitteln online Arbeitspakete, die von „Crowdworker.innen" bearbeitet werden – vom Mikrojob für Cent-Beträge bis zu anspruchsvollen Aufgaben wie Webdesign zum Pauschalpreis. Arbeitgeber können so Aufgaben an die Crowd vergeben, ohne dazu Mitarbeiter.innen einstellen zu müssen. Die Arbeit erfolgt auf Zuruf, ohne Risiko (für Arbeitgeber.innen), ohne Absicherung (für Crowdworker.innen). Die Verleihung an die beiden Preisträger erfolgt stellvertretend für eine ganze Branche.

Bei Amazons *Mechanical Turk* – benannt nach einem Apparat des 18. Jahrhunderts, der vorgeblich Schach spielen konnte, in dem aber ein Mensch versteckt war, der dies erledigte – ist das Prinzip: Man gibt Aufgaben an eine Web-Plattform und Menschen erledigen sie im Hintergrund. Dafür werden sie je nach Aufgabe bezahlt; häufig mit Cent-Beträgen. Gleichzeitig werden die Crowdworker.innen bewertet; von dieser Bewertung hängen dann die nächsten Aufträge ab.

Upwork (Elance-oDesk) vermittelt die „höherwertigen" Aufgaben: Web-Design, Marketingkonzepte, Businesspläne. Will man solche Aufgaben erledigen, muss man Lebenslauf, Qualifikation und Referenzkunden angeben. Gleichzeitig muss man eine Applikation auf seinem Rechner installieren, die Tastenanschläge und Mausbewegungen registriert und regelmäßig Screenshots an den Auftraggeber schickt. Upwork spricht von „Vertrauensaufbau".

„Gerne würden wir sie glauben, die Verheißungen von Freiheit, Unabhängigkeit, Vertrauen, Selbstverwirklichung und so weiter. Doch damit sie wahr werden und nicht weiterhin Euphemismen für Lohndumping, Unsicherheit, fehlende Solidarität, Dauerüberwachung und Selbstausbeutung bleiben, muss eine Menge passieren", so Rena Tangens in ihrer Laudatio. *„Wir möchten heute klarstellen, dass wir es hier auch mit einer Überwachungs- und Digitalisierungskultur von menschlichem Verhalten zu tun haben, die nichts mehr mit Freiheit und Selbstbestimmung zu tun hat, auch wenn es von den Verantwortlichen so genannt wird."*

Kategorie *Arbeitswelt*

Den BigBrotherAward in der Kategorie *Arbeitswelt* erhalten die Unternehmen **Amazon Logistik GmbH in Bad Hersfeld** und die **Amazon Koblenz GmbH**. Peter Wedde begründete die Vergabe in seiner Laudatio: *„Die beiden Unternehmen erhalten den BigBrotherAward 2015, weil sie von ihren Beschäftigten verlangen, den gesetzlich verbrieften Schutz privatester Daten – insbesondere im sensiblen Gesundheitsbereich – am Werkstor abzugeben."*

Mit dem Arbeitsvertrag wird den Arbeitnehmer.innen eine Erklärung zur Unterschrift vorgelegt, mit der man einwilligt, dass

personenbezogene Daten verarbeitet und genutzt werden können, auch soweit sie die Gesundheit betreffen. Zusätzlich willigt man damit ein, dass die Daten an eine zentrale Datenbank in den USA übermittelt, dort verarbeitet und genutzt werden. Der zitierte § 28 Abs. 1 Satz 1 Nr. 1 des Bundesdatenschutzgesetzes darf dabei seit über fünf Jahren nicht mehr auf Arbeitsverhältnisse angewendet werden. Auch die notwendige konkrete Festlegung des Verarbeitungszwecks fehlt. Auch die Übermittlung der Daten in die USA ist so ohne weiteres nicht zulässig.

Besonders problematisch sind in diesem Zusammenhang die Gesundheitsdaten. Deren Verarbeitung ist nur in gesetzlich vorgesehenen Fällen erlaubt, z. B. bei der Lohnfortzahlung im Krankheitsfall. Es gibt ebenfalls keine arbeitsrechtliche Grundlage dafür, dass Amazon das Recht einfordert, *„auf eigene Kosten eine ärztliche Untersuchung des Mitarbeiters durch einen von der Gesellschaft zu bestimmenden Arzt zu verlangen“*, wenn *„begründete Zweifel“* an der Arbeitsunfähigkeit bestehen.

> *„Den deutschen Amazon-Töchtern – und wir gehen davon aus, dass weitere Unternehmensteile mit diesen Regelungen arbeiten, weil es sich bei den uns vorliegenden Verträgen und Erklärungen um Standard-Formulare handelt – können wir nur dringend raten“,* so Peter Wedde abschließend, *„die bisher verwendeten Einwilligungserklärungen zu vergessen und die Verarbeitung und Nutzung von Beschäftigtendaten in den USA zu stoppen.“*

Kategorie *Neusprech*

Der Preisträger in der Kategorie *Neusprech*, der Begriff **Digitale Spurensicherung**, ist die neueste Wortkreation für die Vorratsdatenspeicherung, die schon oft totgeglaubt war, aber immer wieder zurückkommt. Das geschieht in immer neuem Gewand: „Mindestspeicherfrist“, „Mindestdatenspeicherung“, „Mindestspeicherdauer“, „Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“, zuletzt gar „private Vorsorgespeicherung“. Und nun also *digitale Spurensicherung*.

> *„Das klingt harmlos, weil nichts mehr an die monatelange Datenhortung erinnert und weil die Sicherung von Spuren etwas ist, auf das sicher niemand verzichten will, wenn es darum geht, ein Verbrechen aufzuklären“,* so Laudator Kai Biermann. *„Doch es ist nur der erneute Versuch, Wähler zu belügen, um ihnen etwas unterzujubeln, das sie ablehnen. Denn eine Lüge ist die digitale Spurensicherung. Es geht hier nicht um die Spuren, die Verbrecher bei einer konkreten Tat hinterlassen haben. Es geht nicht darum, Fingerabdrücke zu sichern, nachdem ein Verbrechen begangen wurde.“*

Kategorie *Verbraucherschutz*

Der BigBrotherAward 2015 in der Kategorie *Verbraucherschutz* geht an das **Bundesministerium für Gesundheit**, vertreten durch den derzeitig amtierenden Bundesminister für Gesundheit, Hermann Gröhe, für das Leuchtturmprojekt **Elektronische Gesundheitskarte**, das kommende **eHealth-Gesetz** und das Umverteilen der Milliardenetats des Gesundheitssystems in die Taschen von börsennotierten Konzernen.

Der Laudator padeluun kritisierte, dass hier eine Technologie flächendeckend eingeführt und dafür das Sozialgesetzbuch um Paragraphen erweitert wird, die nicht der Gesundheit dienen, sondern durch die eine technische Infrastruktur eingeführt wird, die vor allem teuer ist und die keine Verbesserung von Diagnostik und Heilbehandlung, der Ausbildung der Ärzt.innen oder der Personalausstattung in Kliniken bringt. padeluun: *„Das Gesetz zwingt die Krankenkassen, die teure Infrastruktur zu finanzieren – und dies aus den Taschen der Beitragszahlenden. Also auf unser aller Kosten.“*

> *„Wer ist auf die Idee gekommen“,* so padeluun weiter, *„dass wir eine neue, besonders gesicherte Infrastruktur entwickeln müssen, damit sich Ärzte gegenseitig eine sichere Mail (im eBriefumschlag mit eStempel, eUnterschrift und eBriefmarke) schicken können? Das geht doch schon längst – mit Ende-zu-Ende-Verschlüsselung mittels PGP. Über die üblichen Mailversandstrukturen. Mit gegenseitig signierten Public Keys, so dass auch der Anscheinsbeweis einer Unterschrift gewährleistet ist.“*

> *„Wir müssen darüber sprechen, dass über Jahre hinweg das Vertrauen in Ärzte massiv untergraben wurde. … Tatsächlich wird den Ärzten die Kompetenz entrissen, über den Heilungsprozess ihrer Patientinnen und Patienten zu entscheiden.“*

Kategorie *Politik*

Die Europäische Datenschutz-Grundverordnung war auch in der *FIfF-Kommunikation* wiederholt Thema – in dieser Ausgabe drucken wir beispielsweise einen Appell von 66 Bürgerrechtsorganisationen weltweit an EU-Kommissionspräsident Jean-Claude Juncker, dafür zu sorgen, dass die Versprechen der Kommission für einen starken Datenschutz eingelöst werden.

Gerade Deutschland gilt heute als das Land, in dem der Datenschutz besonders betont wird – ob zu Recht, lässt sich diskutieren. Eine Datenschutz-Grundverordnung auf europäischer Ebene soll demnach nicht hinter den Standards des Bundesdatenschutzgesetzes zurückbleiben. Doch offenbar wird aktuell gerade von deutscher Seite – entgegen anderslautender Beteuerungen – versucht, Datenschutzstandards in Europa zu senken.

Für die systematische und grundlegende Sabotage der geplanten Europäischen Datenschutz-Grundverordnung erhalten **Bundesinnenminister Thomas de Maizière** und sein Vorgänger **Hans-Peter Friedrich** den BigBrotherAward in der Kategorie *Politik*.

Beide Innenminister, der aktuelle und sein Vorgänger, so Laudator Max Schrems, ließen ihre Beamten den Datenschutz ins Gegenteil verkehren. Datensparsamkeit und Zweckbindung sollten quasi abgeschafft werden.

> *„In der Öffentlichkeit wird währenddessen vom angeblich ‚hohen deutschen Datenschutzniveau‘ gesprochen“,* erläutert Max Schrems in seiner Laudatio. *„Dabei ist das deutsche BDSG zwar der unangefochtene Europameister der Komplexität, aber in vielen Punkten auch schwächer als die Gesetze in vielen anderen europäischen Staaten – und in einigen Punkten möglicherweise sogar europarechtswidrig.“*

„Statt einem ‚hohen Datenschutzniveau'", so Max Schrems weiter, „wurden die im deutschen Recht massenhaft angelegten Ausnahmen und Privilegierungen nach Brüssel getragen und regelmäßig noch stark erweitert. Wenn die Innenminister also versprachen, das deutsche Datenschutzniveau europaweit zu verankern, dann muss man das wohl als Drohung aufnehmen – nicht als Versprechen."

Anmerkungen

1 *BigBrotherAwards, http://www.bigbrotherawards.de*

2 *Stand 17. April 2015 – bekanntlich überschlagen sich beim BND gerade die Ereignisse; dies konnte bei der Gala naturgemäß noch nicht berücksichtigt werden.*

Linus Neumann

Kategorie *Technik* – Laudatio

Der BigBrotherAward 2015 in der Kategorie *Technik* geht an die „Hello Barbie", vertreten durch die Herstellerfirmen Mattel und Toytalk.

Was soll schon so schlimm sein an einer Puppe, die mit Mikrofon, Lautsprecher und WLAN ausgestattet ist? Sie müssen nur kurz die AGB akzeptieren!

Haben Sie etwa Angst, dass Ihre Kinder belauscht werden? Keine Sorge! „Hello Barbie" zeichnet nur auf, wenn ein Knopf gedrückt wurde. Und schickt die Aufnahme dann in die Cloud. Zu Toytalk.

Toytalk ist ein amerikanisches Unternehmen, das sich auf Spracherkennung bei Kindern spezialisiert hat. Lustige kleine Smartphone-Apps haben Toytalk erst viele Millionen Dollar Investment, und dann eine Partnerschaft mit dem Spielzeughersteller Mattel eingebracht.

Spracherkennung an sich ist nichts Schlechtes. Sie erleichtert uns das Erledigen unliebsamer Aufgaben und sie ermöglicht vielen von uns ein barrierefreies Leben.

- Wir können Texte diktieren, ohne uns einen Tennis-Arm zu holen.
- Wir können beim Autofahren SMS schreiben, ohne kleine Kinder zu überfahren.
- Wir können bei unserer Bank anrufen, ohne mit dem schlecht gelaunten Betreuer streiten zu müssen.

Daten an sich sind auch nichts Schlechtes. Mit ihrer Hilfe können Krankheiten geheilt, Unfälle verhindert und politische Missstände aufgedeckt werden.

Viele Dienstleistungen der Informationsgesellschaft werden durch Datensammlung besser:

- Wir können mit Googles Hilfe schnell das Suchergebnis finden, das schon viele vor uns gesucht haben.
- Wir können Staus und zäh fließenden Verkehr umfahren, in dem andere Google-Nutzer gerade stehen.
- Wir finden immer zielsicher das beste Restaurant in der Gegend, egal wo wir gerade sind, Dank der Bewertungen anderer Gäste.

Laudator Linus Neumann, Foto: Fabian Kurz, CC by 4.0

Für das Nutzen dieser Daten bezahlen wir inzwischen häufig mit unserer eigenen Datenspende in den großen Pool. Manchmal kann das sogar ein richtig guter Tausch sein. Oft aber auch nicht.

Wenn alle unsere E-Mails mitgelesen werden, um uns daneben die passende Werbung zum Tod unserer Großmutter zu präsentieren, wenn Amazon noch vor uns selbst von unserer ungewollten Schwangerschaft weiß, wenn Facebook uns auf Fotos erkennt, ob wir wollen, oder nicht – dann ist das immer nur eine kleine Vorschau auf die Macht, die sich in den angehäuften Daten verbirgt.

Unser Verhalten wird minutiös protokolliert, durch Analysen erklärt, und durch gezielte Maßnahmen manipuliert. Meist mit der Absicht, uns danach etwas dazu Passendes zu verkaufen. Kurzum: Unser Verhalten wird monetarisiert.

Als informierte und mündige Bürger brauchen wir eine Sensibilität dafür, welche Daten wir in wessen Hände geben, und was damit angestellt wird. Wir müssen den schmalen Grat finden zwischen einer goldenen Zukunft des Fortschritts – und der Unterwerfung unseres Zusammenlebens unter die gewinnorientierten Interessen einiger weniger großer Konzerne.

Der mündige Bürger muss Kosten und Nutzen abwägen:

Ich soll verraten, wohin ich fahre, um einfacher und schneller zum Ziel zu kommen?

Okay, Deal!

Ich soll meinen Kalender online in den USA hosten lassen, damit er sich einfacher zwischen Smartphone und Laptop synchronisiert?

Na gut …

Ich soll mein Wohnzimmer abhören lassen, damit ich mit meinem Fernseher sprechen kann?

Moment mal!

Ja, George Orwell hat vieles vorhergesehen … Aber nicht, dass wir uns die panoptischen Teleschirme auch noch freiwillig kaufen würden!

… und erst recht nicht, dass sie die Form von Barbie-Puppen haben würden.

Wie so viele andere Dienste ist auch die Spracherkennung in die Cloud gewandert. Der Algorithmus verbessert sich täglich, so dass die Geräte uns immer besser verstehen. Neue Funktionen können ohne Updates eingebaut werden, und auf dem Gerät selbst werden Speicherplatz und kostbare Akkulaufzeit gespart. Gleichzeitig lernen die Großrechner in der Cloud immer mehr von und über uns, damit wir eine möglichst persönliche Behandlung erfahren.

Wenn die Spracherkennung aber in der Cloud liegt, dann geben wir die hinter einem Service stehenden Abläufe aus der Hand.

Wenn wir zum Beispiel eine Internet-Suche mit den Worten „OK Google“ einleiten, oder per Sprachbefehl den Sender an unserem Fernseher wechseln, oder über den Amazon Echo-Lautsprecher eine Bestellung tätigen, dann sprechen wir nicht mit unserem Gerät, sondern mit einer Serverfarm irgendwo da draußen in den Weiten des Internets.

Und wenn unser Smartphone dann die SMS an Mutti schreibt, einen Termin in unseren Kalender einträgt oder unsere Frage beantwortet, dann ist es genau diese Serverfarm, die unser Gerät fernsteuert.

Eine Serverfarm in den Händen eines Konzerns, der die Mikrophon-Mitschnitte der Welt sammelt, analysiert und speichert.

Machen Sie sich da regelmäßig Gedanken drüber? Haben Sie sich überhaupt schon einmal Gedanken darüber gemacht?

Ganz wichtig ist für diese Konzerne: Damit sich die Investitionen in den Elektronik-Wachstumsmarkt auch lohnen, müssen unsere lieben Kunden und Kundinnen möglichst früh mit der Technik vertraut gemacht werden. Denn was schon im Kinderzimmer normal war, ist später umso selbstverständlicher.

Mit der Barbie fängt es an, „Bob der Baumeister“ und Playmobil-Figuren werden folgen, wenn die Kunden mitspielen. Dabei weiß Mattel sehr genau, woher der Wind weht – in Europa wird die „Hello Barbie“ wegen der befürchteten Datenschutzbedenken vorerst gar nicht auf den Markt kommen.

Mit WLAN, Mikrophon und Lautsprecher ermöglicht die neue „Hello Barbie“ schon unseren Kindern, sich mit einer Serverfarm irgendwo da draußen in den Weiten des Internets zu unterhalten. Sie bringt eine datenschutzrechtlich äußerst fragwürdige Technik ohne erkennbaren sinnvollen Anwendungszweck direkt in unsere Kinderzimmer.

Damit Gespräche überhaupt möglich werden, merkt „Hello Barbie“ sich, was unsere Kinder ihr erzählen. Später kann sie im Gespräch darauf zurückgreifen, und dadurch eine echte Freundin imitieren. Die lieben Eltern sorgen sich, was ihre Kinder der Puppe, pardon, Serverfarm so alles über sich erzählen? Kein Problem! Selbstverständlich lässt Mattel Sie an den gesammelten Daten teilhaben: In einer täglichen oder wöchentlichen E-Mail erhalten Sie das Protokoll der Sorgen, Träume und Geheimnisse, die Ihr Kind seiner besten Freundin, der Serverfarm von Mattel und Toytalk, anvertraut.

Und deshalb: Herzlichen Glückwunsch zum BigBrotherAward in der Kategorie *Technik*, „Hello Barbie“, Mattel und Toytalk.

Rolf Gössner

Kategorie *Behörden und Verwaltung* – Laudatio

Der BigBrotherAward 2015 in der Kategorie *Behörden und Verwaltung* geht an den Bundesnachrichtendienst (BND), vertreten durch seinen Präsidenten Gerhard Schindler (FDP).

Der deutsche Auslandsgeheimdienst erhält den Negativpreis für eine ganze Palette von Skandalen sowie Datenschutz- und Bürgerrechtsverstößen, die wir im Rahmen dieser Preisverleihung allerdings nur ausschnittsweise behandeln können. Unter anderem wird dem BND der Preis zuerkannt,

1. weil er aufs Engste in den menschenrechtswidrigen NSA-Überwachungsverbund verflochten ist und damit in den globalen Massenüberwachungsskandal;
2. weil er mit der sog. strategischen Überwachung der grenzüberschreitenden Telekommunikation und insbesondere mit seiner gesamten Auslandsaufklärung via Funk, Satellit oder Kabel weitgehend im rechtsfreien Raum operiert – nach Auffassung renommierter Verfassungsrechtler sogar schlicht verfassungswidrig;
3. weil der BND täglich über 220 Millionen Telekommunikationsdatensätze sammelt, speichert, auswertet und davon

Millionen an ausländische Partnerdienste übermittelt. Darunter sind auch grundrechtlich geschützte Daten von Bundesbürgern, deren Weitergabe gesetzlich untersagt ist; außerdem, so Ex-NSA-Mitarbeiter Thomas Drake, soll der BND sensible Informationen für den menschenrechtswidrigen Drohnenkrieg der USA geliefert haben, und damit für das gezielte Töten von Terrorverdächtigen.

4. Nicht zuletzt erhält der BND den BigBrotherAward für seine Informationsblockade und dreisten Vertuschungen geheimdienstlicher Praktiken gegenüber dem NSA-Untersuchungsausschuss des Bundestags, der sich mit aufklärungsunwilligen BND-Zeugen und überwiegend geschwärzten, lückenhaften oder anderweitig manipulierten Akten des BND herumschlagen muss – frei nach der Zeugenaussage des Nachrichtendienste-Beauftragten im Bundeskanzleramt, Klaus-Dieter Fritsche (CSU), das „Staatswohl" sei nun mal weit wichtiger als parlamentarische Aufklärung und Kontrolle.

Dr. Rolf Gössner, Foto: Bernd Sieker, CC by 4.0

I. Ausufernde Praktiken: Illegaler Datentransfer BND – NSA – BND

Nur eine der preiswürdigen Verfahrenspraktiken möchte ich ein wenig ausführen, um die damit verbundene Problematik deutlich zu machen: Seit 2004 zapfte der BND – mit Hilfe der Telekom und an allen Kontrollgremien vorbei – einen wichtigen Internetknoten (DE-CIX) in Frankfurt an und belieferte aus dieser sprudelnden Quelle die NSA jahrelang mit gewaltigen Datenmengen (Operation „Eikonal").

Der Frankfurter Netzknoten ist der größte Glasfaser-Knotenpunkt und Datenumschlagort der Welt – ein gefundenes Fressen für den BND, um etwa Daten zur grenzüberschreitenden anlasslosen „strategischen Fernmeldekontrolle" abzusaugen, auf der Suche nach Hinweisen auf Terrorismus, Waffenhandel und Ausländerschleusung. Auch die grundrechtlich besonders geschützte Alltagskommunikation von Bundesbürgern fiel dabei gewissermaßen als „Beifang" ab, deren Metadaten der Auslandsgeheimdienst eigentlich weder speichern noch an Auslandsdienste übermitteln darf. Deshalb hätte er sie herausfiltern müssen. Doch der eigens konstruierte Filter (DAFIS) funktionierte nur unzulänglich, so dass auch viele geschützte Daten illegal an die NSA übermittelt wurden.

Unter Auslandsgeheimdiensten ist der Datentransfer ohnehin keine Einbahnstraße, sondern ein Geschäft auf Gegenseitigkeit, das mit Vorliebe im Datenringtausch abgewickelt wird. Und der funktioniert so: Weil ein Auslandsdienst die eigene Bevölkerung nicht überwachen darf (deshalb heißt er ja AUSLANDS-Geheimdienst), bespitzelt er eben die Bevölkerung anderer Länder und tauscht dann die gewonnenen Daten mit den jeweiligen Partnerbehörden. Diese gängige Praxis beschert dann auch dem BND illegal Erkenntnisse über die bundesdeutsche Bevölkerung. Ingesamt gesehen müssen wir also von schwerwiegenden Grundrechtseingriffen in das Telekommunikationsgeheimnis, die Privatsphäre und die Informationelle Selbstbestimmung von Millionen ahnungsloser Menschen ausgehen.

II. Geheimdienstliches Aufrüstungsprogramm

Doch trotz dieser ausufernden, illegalen und unkontrollierbaren Praxis wird der BND nicht etwa rechtsstaatlich gezügelt, sondern künftig noch weiter digital aufgerüstet und für das Massenüberwachungsgeschäft tauglich gemacht – für insgesamt 300 Mio. Euro, von denen bereits fast 35 Mio. bewilligt sind. Auch für dieses geheime Aufrüstungsprogramm mit dem Tarnnamen „Strategische Initiative Technik" (SIT) und für weitere Nachrüstungsprojekte wird der BND mit dem BigBrotherAward 2015 ausgezeichnet – vor allem dafür:

- dass er künftig soziale Netzwerke, Blogs und Web-Foren systematisch, flächendeckend und anlasslos ausforschen soll – und zwar sowohl die Metadaten als auch die Inhalte;

- und dass der BND mit Hilfe von Sicherheitslecks und „Nachschlüsseln" in fremde Computersysteme einbrechen und Verschlüsselungen knacken soll, um speziell solche Bürger, Firmen und Netzwerke gezielt auszuforschen, die sich besonders gegen Cyberattacken schützen wollen – wobei wohl viele treuherzig dem guten Rat des Bundesinnenministers gefolgt sein dürften, sich angesichts des NSA-Überwachungsskandals doch bitteschön per Verschlüsselung selbst zu schützen. Ein Tipp, der sich angesichts solcher BND-Pläne rasch als ziemlich perfide herausstellen könnte.

Beispiel: BND-Ausforschung sozialer Netzwerke

Demnächst soll der BND einen höchst fragwürdigen Freibrief erhalten, nämlich die Lizenz oder Ermächtigung zur anlasslosen Ausforschung sozialer Netzwerke wie Facebook, Flickr, YouTube oder Twitter, aber auch von Blogs und Internet-Foren. Die aufgefangenen Netzwerkdaten und Inhalte sowie das gespeicherte Kommunikationsverhalten der Nutzer können damit jederzeit automatisiert durchrastert, zu Persönlichkeits- und Bewegungsprofilen verdichtet oder biometrisch ausgewertet werden; auch Rückschlüsse auf soziale und politische Kontakte werden möglich. Deshalb greift diese Internet-Durchleuchtung besonders stark in Grundrechte der Betroffenen ein.

Die Behauptung der Bundesregierung, dies betreffe doch nur das Ausland, ist entweder naiv oder ganz bewusst irreführend und unzutreffend: Zum einen gelten Grund- und Menschen-

rechte auch im Ausland; zum anderen sind Server von sozialen Netzwerken quer über die Welt verteilt, so dass der innerdeutsche Datenverkehr auch über andere Länder fließt und danach als ausländisch gilt; so geraten auch bundesdeutsche Nutzer leicht ins BND-Visier.

Die globale Ausforschung sozialer Kommunikationsräume, in denen Infos, Meinungen, Bilder und andere sensible Daten ausgetauscht werden, soll dazu dienen, Stimmungen, Auffälligkeiten, Wirtschaftstrends, politische Proteste und Beziehungsgeflechte in bestimmten Ländern und Krisenregionen präventiv herauszufiltern und zu analysieren. Soziale Netzwerke wecken geheimdienstliche Gelüste auch deshalb, weil sie sich weltweit zu Mobilisierungsforen für Protestbewegungen entwickelt haben – wie etwa während des „Arabischen Frühlings". Deshalb sollen sie nun – ab 2015 – nach NSA-Vorbild auch unter die Echtzeit-Kontrolle des BND gestellt werden; ihre Auswertung ist für die Bundesregierung, den so genannten Verfassungsschutz oder die Bundeswehr von Interesse, um etwa Krisen, geopolitische und militärstrategische Probleme und politische Akteure frühzeitig zu erkennen.

Verfechter solcher modernen Massenüberwachungsmethoden behaupten, nur so könne man Terroranschläge verhindern oder Organisierte Kriminalität bekämpfen, was auch schon passiert sein soll – eine Behauptung, die schon aus Geheimhaltungsgründen nie wirklich überprüfbar war.

III. Wettrüsten im Infokrieg: Präventive Vormacht- und Herrschaftssicherung

Auf diese Weise will der BND offenbar sein Image als „Wurmfortsatz" der NSA, wie ihn Ex-NSA-Mitarbeiter Thomas Drake despektierlich nannte, loswerden und sich vom Großen Bruder emanzipieren. Wir werden also Zeugen eines fatalen Wettrüstens im Informationskrieg der Geheimdienste – einem Informationskrieg, in dem es nicht zuletzt um geostrategisch-wirtschaftliche Interessen sowie um präventive Vormacht- und Herrschaftssicherung geht, bis hin zur Absicherung militärischer Operationen. Schließlich gilt es, Staat oder Staatengemeinschaften nicht allein vor Terror und Gewalt zu schützen, sondern auch gegen mögliche soziale Unruhen, militante Aufstände oder unkontrollierte Wanderungsbewegungen und drohende Rohstoffknappheit vorsorglich zu wappnen – Aufstandsbekämpfung und militärische Interventionen inbegriffen.

Solche hochgerüsteten, letztlich unkontrollierbaren Präventionsdienste wuchern im Schatten des demokratischen Rechtsstaats, bedrohen Menschen, politisch-soziale Bewegungen und deren Freiheitsrechte. Sie wittern in jedem Menschen, jedem kritischen Gedanken und abweichenden Verhalten eine potenzielle Bedrohung, die es zu überwachen gilt. Doch Menschen, die unter ständiger Überwachung stehen, sind niemals frei. Schon wer sich nur beobachtet fühlt, verändert sein Verhalten, wird unsicher, entwickelt Ängste, passt sich an – Wirkungen, die eine offene, freie demokratische Gesellschaft schädigen, wie das Bundesverfassungsgericht bereits vor über dreißig Jahren in seinem berühmten Volkszählungsurteil festgestellt hat.

IV. Kapitulation des Rechtsstaats vor staatlichem Unrecht

Trotz massiver Bedrohungen und Bürgerrechtsverstöße durch die Massenüberwachung von NSA, BND & Co. hat es die Bundesregierung sträflich unterlassen, Bürger und von Wirtschaftsspionage betroffene Betriebe vor deren Attacken zu schützen – obwohl es zu ihren verfassungsrechtlichen Aufgaben gehört, diesen Schutz zu gewährleisten. Angesichts der regierungsamtlichen Lethargie erstatteten Anfang 2014 die Internationale Liga für Menschenrechte, der ChaosComputerClub und Digitalcourage beim Generalbundesanwalt Strafanzeige gegen Bundesregierung und Geheimdienst-Verantwortliche: wegen massiver Verstrickung des BND in das globale Massenüberwachungssystem, wegen millionenfacher Verletzung des Menschenrechts auf Privatsphäre und wegen sträflich unterlassener Abwehrmaßnahmen. Tausende unterstützten diese Anzeige.

Bekanntlich hat der Generalbundesanwalt Mitte 2014 ein Strafermittlungsverfahren eingeleitet – aber nur wegen des unfreundlichen Spionage-Angriffs auf das Handy der Kanzlerin. Eine Entscheidung, die an der Gleichheit aller Menschen vor dem Gesetz zweifeln lässt: Denn auf ein Ermittlungsverfahren wegen der ungleich schwerer wiegenden massenhaften Ausspähung der ganzen Bevölkerung verzichtet er – kurioserweise mangels „zureichender Tatsachen".

Das ist angesichts der Fülle an Belastungsbeweisen und -zeugen Realitätsverleugnung oder Willfährigkeit – jedenfalls hart an der Grenze zur Strafvereitelung im Amt. Diese Rechtsschutzverweigerung ist eine Kapitulation des Rechtsstaats vor staatlichem Unrecht.

Deshalb sehen wir uns in der Pflicht, mit diesem überfälligen BigBrotherAward den Blick der Öffentlichkeit erneut auf die Machenschaften des BND zu lenken und auf das Problem geheimer Institutionen in einer Demokratie. Das ist das Mindeste, was wir tun können, auch wenn es auf den ersten Blick effektiver scheint, die milliardenteure BND-Zentrale in Berlin einfach unter Wasser zu setzen, wie Anfang März dieses Jahres geschehen: Eine originelle Geheimoperation auf der bestgesicherten Baustelle der Nation. Wenn auch keine Dauerlösung, so lässt uns dieses „Watergate" doch auf weitere undichte Stellen hoffen – auf der dringenden Suche nach einem Snowden im BND! Und vielleicht lässt uns die Flutung des BND erahnen, wie der Auslandsgeheimdienst dereinst in seinen eigenen Datenfluten zu ertrinken droht. In diesem Sinne: „Kopf hoch", „Petri heil" und herzlichen Glückwunsch zum BigBrotherAward 2015, Herr BND-Präsident Gerhard Schindler!

Foto: Matthias Hornung, CC by 4.0

Max Schrems

Kategorie *Politik* – Laudatio

Der BigBrotherAward 2015 in der Kategorie *Politik* geht an Bundesinnenminister Thomas de Maizière und Ex-Bundesinnenminister Hans-Peter Friedrich

für die systematische und grundlegende Sabotage der geplanten Europäischen Datenschutzgrundverordnung.

Ich hatte vor einiger Zeit die zweifelhafte Freude, mit Herrn Ex-Minister Friedrich für die ZEIT ONLINE ein Doppelinterview zu haben – eine unterhaltsame Erfahrung. Da sitzt ein Bundesminister in einem Büro hoch über der Spree, und die Beamten suchen sich als „Gegner" in einer Diskussion zum Datenschutz einen ausländischen, damals 25-jährigen Jura-Studenten aus – also die möglichst geringste Gefahr. Traurig und bezeichnend.

Max Schrems, Foto: Matthias Hornung, CC by 4.0

Vor mir stand also der Bundesinnenminister der Bundesrepublik Deutschland. Eigentlich einer der mächtigsten Player im EU-Datenschutz-Poker. In der Realität ein Bayer vom Format „Provinzpolitik". „I bau eich a neiche Bruckn don kenz schnölla zum Einkaufszentrum foan" – das wäre ein Programm, das man ihm abgenommen hätte. Grundrechte, komplizierte Abwägungen und Weitblick? – Fehlanzeige.

Die Diskussion führte ich am Ende de facto mit dem zuständigen Beamten, weil Minister Friedrich von Datenschutz schlichtweg keine Ahnung hatte – die ZEIT wollte es schon als „Dreifachinterview" bringen, was das Ministerium unterband. Die Aussagen des Beamten wurden am Ende teilweise dem Minister zugeschrieben, große Teile konnte man gar nicht bringen.

Warum erzähle ich Ihnen diesen Schwank? Weil er bezeichnend ist für das Problem bei der deutschen Datenschutzpolitik: Beamte übernehmen das Ruder, weil die politische Führung versagt.

Beide Innenminister, der jetzige, Thomas de Maizière, und der ehemalige, Hans-Peter Friedrich, ließen ihre Beamten so, in enger Kooperation mit Lobbyverbänden, den europäischen Datenschutz ins Gegenteil verkehren. So sollen Errungenschaften wie die Datensparsamkeit (also dass nur jene Daten gesammelt werden dürfen, die notwendig sind), die informierte Zustimmung und die Zweckbindung (also dass z. B. Bankdaten nicht an Werbeunternehmen weitergeleitet werden dürfen) quasi abgeschafft werden.

Das deutsche Innenministerium ist, wie interne Dokumente zeigen, an dieser Grundrechts-Vernichtung federführend beteiligt. Bei unserem Projekt „LobbyPlag" führte Deutschland die Negativ-Statistik aller EU-Staaten sogar an. Kein anderes Land unterstützte in den ersten drei Kapiteln der Verordnung mehr negative Änderungen – das vermeintliche „Mutterland des Datenschutzes" verwies damit sogar Großbritannien auf Platz zwei der Datenschutzkiller. Deutschland als Europameister …

Das Justizministerium als Schattenministerium für den Datenschutz äußert zwar hinter vorgehaltener Hand Kritik – die zuständigen Minister der FDP und nun der SPD hüllten sich aber am Ende doch größtenteils in Schweigen. Und das, obwohl der aktuelle deutsche Koalitionsvertrag eigentlich das Festhalten an den Grundprinzipien des Datenschutzes festgeschrieben hat.

In der Öffentlichkeit wird währenddessen vom angeblich „hohen deutschen Datenschutzniveau" gesprochen. Dabei ist das deutsche BDSG zwar der unangefochtene Europameister der Komplexität, aber in vielen Punkten auch schwächer als die Gesetze in vielen anderen europäischen Staaten – und in einigen Punkten möglicherweise sogar europarechtswidrig.

Statt einem „hohen Datenschutzniveau" wurden die im deutschen Recht massenhaft angelegten Ausnahmen und Privilegierungen nach Brüssel getragen und regelmäßig noch stark erweitert. Wenn die Innenminister also versprachen, das deutsche Datenschutzniveau europaweit zu verankern, dann muss man das wohl als Drohung aufnehmen – nicht als Versprechen.

Die Lobbyisten sind hingegen begeistert, immerhin dachte man, Deutschland wäre eine harte Nuss in den Verhandlungen. „Liebe Mitstreiter" sind die internen E-Mails zwischen Lobbyisten und Ministeriumsmitarbeitern betitelt, und es ist wohl bezeichnend für die Situation.

„Ich bitte daher um möglichst rasche Rückmeldung, ob Sie vielleicht noch ein, zwei harte Punkte haben, die wir noch kurzfristig einbringen sollen", fragt das Ministerium bei Lobbyisten um Unterstützung an – garniert mit den neuesten (und eigentlich geheimen) Verhandlungsdokumenten aus Brüssel.

Während sich Vertreter der Zivilgesellschaft, z. B. der Verbraucherverband, nicht gehört fühlen, kommunizieren die Beamten ausführlich mit Lobbyisten oder Mitarbeitern des Internet-Instituts der Berliner Humboldt-Universität. Das von Google mitfinanzierte Institut hat „bahnbrechende" Forschungsergebnisse zur Zukunft des Datenschutzes, die de facto auf die Abschaffung der Grundprinzipien des Datenschutzes hinauslaufen – natürlich nur, um das Potential von „Big Data" für die so gern vorgeschobenen „Startups" voll auszuschöpfen. Das Ministerium tut am Ende genau das, was die Industrie wünscht.

Das deutsche Bundesinnenministerium ist unter anderem zuständig für die Polizei – und gleichzeitig für den Datenschutz. Dieser Interessenskonflikt, die Überhöhung der deutschen Datenschutzgesetze und drittens die erschreckenden Verflechtungen zwischen Beamten und Lobbyisten – all das führte dazu, dass Deutschland statt einer Bastion des Datenschutzes in Europa zu einem der größten Saboteure in den Verhandlungen wurde.

Wir leben in einer Demokratie. Wenn unsere Vertreter ihre Positionen jedoch nicht mehr an dem Willen der Menschen, sondern an Lobbyinteressen orientieren – wenn sie Grundrechte auf Zuruf der Industrie verstümmeln – und wenn der Öffentlichkeit gleichzeitig dreist zugerufen wird, dass das „hohe deutsche Datenschutzniveau" nach Brüssel getragen werden soll, dann kann ich den Ministern Hans-Peter Friedrich und Thomas de Maizière nur zum BigBrotherAward 2015 gratulieren – sie haben ihn wahrlich verdient.

Rena Tangens

Kategorie *Wirtschaft* – Laudatio

Der BigBrotherAward 2015 in der Kategorie *Wirtschaft* geht an die Crowdworking-Plattformen Amazon Mechanical Turk und Elance-oDesk

für die Einführung des digitalen Tagelöhnertums mit Arbeitsbedingungen wie in den Anfängen der Industrialisierung plus elektronische Komplettüberwachung – alles natürlich komplett „freiwillig".

Beide Plattformen vermitteln online Arbeitspäckchen – von Mikrojobs für Cent-Beträge bis Webdesign zum Pauschalpreis. Arbeit auf Zuruf, für Hungerlohn, auf eigenes Risiko, ohne jegliche soziale Absicherung. Verlockend für Arbeitgeber, die niemanden mehr einstellen müssen, weil sie sich auf dem „digitalen Arbeitsstrich" nach Lust und Laune bedienen können.

Wenn dieser Trend sich durchsetzt, wird das nicht nur unsere Arbeitswelt, sondern unsere Gesellschaft als Ganzes umkrempeln.

Es geht um Freelancing – um *freie* Arbeit. Doch das *frei* ist weder das *frei* wie in *Freibier*, noch das *frei* im Sinne von *freie Meinungsäußerung*. Es ist eher das *frei* in der zynischen Lesart von *freigesetzt*.

Kennen Sie das Wort „freisetzen"? So nennt es die Wirtschaft, wenn sie Massenentlassungen vornimmt.

Stellvertretend für die ganze Branche haben wir zwei Plattformen ausgezeichnet. Sie stehen für die zwei Enden der Skala: „Mechanical Turk" von Amazon ist fürs „Prekariat", „Elance-oDesk" eher für die „digitale Bohéme".

Rena Tangens, Foto: Bernd Sieker, CC by 4.0

Mechanical Turk

Beginnen wir mit Mechanical Turk.

Der „mechanische Türke" war eine Jahrmarktsattraktion Mitte des 18. Jahrhunderts. Es war eine Maschine, die angeblich Schach spielen konnte. Tatsächlich saß aber ein Mensch in der Apparatur versteckt und führte die Schachzüge aus. Das mit dem Schachspielen bekommen Computer inzwischen ganz akzeptabel selbst hin. Aber es gibt andere Aufgaben, für die Menschen immer noch besser geeignet, schneller oder auch einfach billiger sind. Der Name „Mechanical Turk" ist von Amazon schon sehr passend gewählt, denn die Plattform macht menschliche Arbeit unsichtbar.

Amazon nennt das Ganze „artificial artificial intelligence". Soll heißen: Die künstliche Intelligenz ist gar nicht künstlich, sondern es sieht nur so aus, als ob. Jobs werden an die elektronische Plattform übergeben, diese aber im Hintergrund von Menschen erledigt. Hier werden Fotos klassifiziert (Hund oder Katze, jugendfrei oder nicht), Übersetzungen geschrieben, Präsentationen beschriftet, Transkripte von Vorträgen oder auch von Aufnahmen von Anrufbeantwortern getippt, Umfragen und wissenschaftliche Fragebögen ausgefüllt und so weiter und so fort. Für Cent-Beträge. Amazon kassiert eine Provision von 10 %.

Arbeit wird in Häppchen aufgeteilt, sogenannte HITs – Human Intelligence Tasks.

Ja, es gibt auch kreative Aufgaben: Ein Schaf zeichnen für ein Kunstprojekt[1], Gedichte schreiben, Liebesbriefe für unbekannte Personen verfassen, bestellte Kommentare zu Blogartikeln, Einträge in Diskussionsforen, positive Produktbewertungen in Onlineshops, Schrott mit fünf Sternchen markieren … Moment mal … was?

„Turker", so nennen sich die Menschen, die bei Mechanical Turk arbeiten, selbst. Einer Umfrage unter „Turkern" zufolge würden sie über 40 % der angebotenen Arbeitsaufträge im weitesten

Sinne als „Spam“ klassifizieren. Was heißt das? Fake-Accounts einrichten für E-Mail, für Twitter, für Facebook oder bei Websites, Captchas lösen, Fake-Bewertungen für Produkte schreiben, „Likes“ für Artikel und Videos verteilen, auf Anzeigen klicken, Fake-Kommentare zu Artikeln schreiben etc. – Alles „geturkt“.

So führt Amazon mit Mechanical Turk locker das ad absurdum, was wir als Crowd-Intelligenz im Internet bezeichnen: Leser-Beteiligung an Diskussionen, Verbraucherschutz durch Feedback an Hersteller, Reputation durch Nutzerbewertungen, einfach die „Weisheit der Vielen“. Denn diese Meinungsäußerungen haben mit Beteiligung nichts mehr zu tun – sie sind gekauft.

Das ist Amazon total egal.

Ab morgen werden Sie wahrscheinlich beim Lesen einer Produktbewertung ein ähnlich mulmiges Gefühl haben wie NPD-Mitglieder in einem Thüringer Ortsverband: Wer ist hier eigentlich noch echt zwischen all den vom Verfassungsschutz bezahlten V-Leuten?!

Der locker verfasste, gekaufte Kommentar klingt wie echt, denn die Leute, die für Mechanical Turk arbeiten, sind ja nicht blöd und können gut schreiben. Aber warum geben sie sich für so etwas her? Weil die Alternative Arbeitslosigkeit ist? Weil die zweifelhaften Jobs oft etwas mehr Geld einbringen als die ehrlichen? Weil es sonst jemand anderes macht?

Und wie funktioniert das Ganze?

Auftraggeber zahlen direkt auf das Amazon-Konto der Turker. Oder auch nicht. Sie können nämlich willkürlich behaupten, der Auftrag sei nicht korrekt erledigt worden und einfach nicht bezahlen. Dadurch verschlechtert sich zugleich der systeminterne Scorewert des Auftragnehmers. Der danach möglicherweise nicht mehr berechtigt ist, besser bezahlte Aufgaben anzunehmen.

Das ist Amazon total egal.

Die Auftragnehmer werden mit jedem Mikrojob bewertet. Dagegen sind die Zahlungsmoral und sonstiges Verhalten der Auftraggeber auf der Plattform nicht sichtbar.[2]

Es gibt Leute, die Aufgaben bei Mechanical Turk aus Langeweile erledigen oder aus Spieltrieb. Und es gibt Leute, die sich dort nur nach Feierabend ein paar Dollar dazu verdienen.[3] Doch im Wesentlichen arbeitet hier das digitale Prekariat, dessen Alternative die Arbeitslosigkeit ist.

Elance-oDesk

Ganz anders bei Elance-oDesk. Hier arbeiten die coolen Freelancer, die im Café, in der Bambushütte in Thailand oder in ihrer Einraumwohnung in Klein-Bloggersdorf am Schreibtisch sitzen und programmieren, Grafiken gestalten, Websites bauen, Werbetexte, Übersetzungen, Marketingkonzepte oder Businesspläne verfassen. Anders als Mechanical Turk will diese Plattform vor der Auftragsvergabe Lebenslauf, Qualifikation und Referenzkunden wissen.

Die Vorteile für die Auftraggeber werden von Elance-oDesk offensiv angepriesen: Arbeit wird viel billiger. Als Auftraggeber bezahlen Sie immer nur die Leute, die Sie genau jetzt brauchen. (Die anderen sind nur unnütze Esser.)

Und auch die Freelancer werden umworben: Nicolas Dittberner, der Deutschland-Chef von Elance-oDesk, schwärmt in seinem Artikel in der Huffington Post über den „Aufstieg der unabhängigen Fachkräfte“: *„Die moderne Arbeitswelt ist zunehmend flexibler, mobiler und weniger hierarchisch organisiert. All das, was eine hierarchische Organisation ausmacht, steht aktuell auf dem Prüfstand: Zentrale Kontrolle und Steuerung, Beobachtung, Anwesenheitspflicht und interne Machtspielchen.“*

Und wie sieht das in der Realität aus? Wer bei Elance-oDesk nach Stunden bezahlt werden möchte, muss ein Programm auf seinem Rechner installieren mit dem freundlichen Namen „Team App“. Das registriert Tastenanschläge und Mausbewegungen – und macht in unregelmäßigen Abständen 6× pro Stunde einen Screenshot vom Bildschirm und schickt den an den Auftraggeber.

Zu diesem Kontrollwerkzeug befragt, sagt Nicolas Dittberner von Elance-oDesk: „Wir kontrollieren nicht, sondern stellen Rahmenbedingungen zum […] Vertrauensaufbau zur Verfügung.“

Kontrolle ist Vertrauen

Aha. „Kontrolle ist Vertrauen“. Klingt verdammt nach George Orwell …

Arbeitgeber werden animiert, nur für tatsächlich messbare Arbeit zu bezahlen – und messbar sind Tasten- und Mausklicks. Pausen, Nachdenken, Arbeitsvorbereitung, ein Gespräch beim Kaffee, bei dem wir neue Einfälle haben, zählen dagegen nicht dazu.

Wie soll sich Kreativität entfalten, wenn jede Regung messbar gemacht und jedes Tun oder Nicht-Tun überwacht, registriert und bewertet wird?! Im Gegenteil: Dauerüberwachung schwächt die Produktivität, denn sie verlagert die Energie auf das stetige Vortäuschen von Betriebsamkeit.

Den Freelancern wird Freiheit suggeriert. Sei dein eigener Boss! Arbeite von zu Hause! Wo du willst, für wen du willst. „Crowdworking“ – das klingt so schön nach freiwillig, gemeinsam etwas tun, die Weisheit der Vielen, irgendwie nach Demokratie – genial!

Die ganze Entwicklung ist eine hoch ideologische Angelegenheit – Logik spielt da keine Rolle. Die Fachpublikation ZDnet propagiert Crowdworking und bezeichnet die noch Festangestellten als „9-bis-5-Sklaven“. Und rät im selben Artikel zögerlichen Arbeitgebern: „Wenn Sie denken, dass die Leute im Büro die ganze Zeit arbeiten, dann hängen Sie Kameras auf – und Sie sehen, dass sie es nicht tun.“(!)

Das ist die kalifornische Ideologie: Sie vermählt die Selbstverwirklichungs-Hippie-Geschichte mühelos mit knallhartem Raubtierkapitalismus. Sie vereinzelt Menschen, um sie so zu haben, wie sie am leichtesten zu kaufen sind: verletzlich und verzweifelt – oh Verzeihung: frei und flexibel.

Das ist kein Trend, der einfach so passiert. Sondern das ist neoliberale Strategie. Sie macht Arbeit für Unternehmer, die diese Be-

zeichnung nicht verdient haben, auf Zuruf verfügbar, jederzeit kündbar, spart Sozialabgaben und Steuern und ist vor allem: billig.

Apropos Vertrauen: Dass seine Firma Elance mit Konkurrent oDesk fusioniert, erfuhr Elance-Chef für Deutschland, Österreich und Schweiz Nicolas Dittberner nicht von seiner Firma, geschweige denn wurde er in die Entscheidung mit einbezogen – nein, er erfuhr es selbst erst aus den Medien. Eine kleine Kostprobe am eigenen Leib in Sachen Vertrauen, Beteiligung und flache Hierarchie.

Gerne würden wir sie glauben, die Verheißungen von Freiheit, Unabhängigkeit, Vertrauen, Selbstverwirklichung und so weiter. Doch damit sie wahr werden und nicht weiterhin Euphemismen für Lohndumping, Unsicherheit, fehlende Solidarität, Dauerüberwachung und Selbstausbeutung bleiben, muss eine Menge passieren.

Es gibt keinen Kündigungsschutz, keinen Urlaubsanspruch, keine Weiterbildungsmöglichkeiten über das Unternehmen, keine Absicherung bei Krankheit, Unfall oder im Alter. Okay, Elance-oDesk hat im November 2014 einen Mindestlohn eingeführt. Einen Mindestlohn von 3 Dollar pro Stunde. In Worten: Drei(!) Dollar. Doch selbst die sind eher ein PR-Gag, denn Auftraggeber, denen auch das zu teuer ist, werden dann eben auf Pauschalpreise pro Auftrag ausweichen.

„Jeder-für-sich-Ökonomie“

Wir könnten hier noch vieles sagen zu volkswirtschaftlichen Folgen von entgangenen Steuereinnahmen durch diese Arbeitsformen oder zur „Jeder-für-sich-Ökonomie“, aber das tun andere auch. Wir möchten heute klarstellen, dass wir es hier auch mit einer Überwachungs- und Digitalisierungskultur von menschlichem Verhalten zu tun haben, die nichts mehr mit Freiheit und Selbstbestimmung zu tun hat, auch wenn es von den Verantwortlichen so genannt wird.

Na, bei wem würden Sie lieber arbeiten: Bei Amazons Mechanical Turk, das Menschen zum Verschwinden bringt und denen auch ansonsten ziemlich viel egal ist, oder bei Elance-oDesk mit dem sympathischen Deutschlandmanager, der Überwachung „Schaffung von Vertrauen“ nennt?

Wir konnten uns nicht entscheiden, wer unser Herzblatt ist. Deshalb:

Herzlichen Glückwunsch, Amazon Mechanical Turk und Elance-oDesk zum BigBrotherAward.

Referenzen

faz.net, 18.11.2014 Online-Arbeit – Die Zukunft der digitalen Tagelöhner von Marie Baumann, http://www.faz.net/aktuell/beruf-chance/arbeitswelt/arbeitsmodell-digitales-arbeiten-im-internet-13268407.html

zeit.de, 15.7.2014 Sharing Economy – Teile und verdiene von Tilman Baumgärtel, http://www.zeit.de/2014/27/sharing-economy-tauschen/komplettansicht

zeit.de, 7.3.2013 IT-Experten – Freiberufler sind für Firmen billiger von Tina Groll, http://www.zeit.de/karriere/beruf/2013-02/zunahme-atypische-beschaeftigung-it

Deutschlandradio Kultur, 28.10.2014 Digitale Jobvermittlung – Vom Bürosklaven zum digitalen Tagelöhner. Über die schöne neue Arbeitswelt. Von Johannes Zuber, http://www.deutschlandradiokultur.de/digitale-jobvermittlung-vom-buerosklaven-zum-digitalen.976.de.html?dram:article_id=300244

- ***Studie zu Spam als Aufgabe bei Mechanical Turk:***

Panos Ipeirotis, 16.12.2010 Mechanical Turk: Now with 40.92 % spam. http://www.behind-the-enemy-lines.com/2010/12/mechanical-turk-now-with-4092-spam.html

- ***Zu Nicolas Dittberner, Deutschland-Chef von Elance-oDesk:***

Huffington Post, 12.12.2014, aktualisiert 11.2.2015 Der Aufstieg der unabhängigen Fachkräfte von Nicolas Dittberner, Unternehmer Elance Deutschland, Arbeitswelt der Zukunft, http://www.huffingtonpost.de/nicolas-dittberner/der-aufstieg-der-unabhaengigen-fachkrafte_b_6302474.html

Gruenderszene.de, 11. Februar 2014 Online-Arbeit – „Da war ich erstmal baff“ – der Elance-Deutschland-Chef zur Fusion mit oDesk von Niklas Wirminghaus http://www.gruenderszene.de/allgemein/nicolas-dittberner-elance

- ***Überwachung am Arbeitsplatz:***

Workrights.org: Privacy under Siege – Electronic Monitoring in the Workplace (pdf), https://epic.org/privacy/workplace/e-monitoring.pdf

Electronic Monitoring: A Poor Solution to Management Problems, http://workrights.us/?products=electronic-monitoring-a-poor-solution-to-management-problem

- ***Folgen für die Gesellschaft:***

Pop Matters, Mar 18, 2011, “Every Person for Themselves” Economy, by Rob Horning http://www.popmatters.com/post/138394-/

Richard Sennett, Buch: The Corrosion of Character (Deutsch: Der flexible Mensch) New York, 1998

Die Zeit 49/1998 – Interview, Der charakterlose Kapitalismus, http://www.zeit.de/1998/49/199849.sennett-intervie.xml

Sinnsuche – Kein Leben jenseits der Arbeit, http://www.zeit.de/campus/2008/04/interview-richard-senett/komplettansicht

Barbara Ehrenreich: Nickel and Dimed – On (Not) Getting By In America (Deutscher Titel: Arbeit poor) von 2001, http://barbaraehrenreich.com/nickel-and-dimed-by-barbara-ehrenreich/

Und das Update von März 2014: Sarah Kessler: Pixel and Dimed – On (Not) Getting By in the Gig Economy http://www.fastcompany.com/3027355/pixel-and-dimed-on-not-getting-by-in-the-gig-economy

Grafiken zu Contingent Work: Dollars and Sense, The Rise of the Gig Economy By Gerald Friedman | March/April 2014 http://dollarsandsense.org/archives/2014/0314friedman.html

Buch: Crowd Work – zurück in die Zukunft von Christiane Benner (Hrsg.), http://www.igmetall.de/SID-605B7CB0-FDAEBCE5/interview-mit-christiane-benner-ueber-das-buch-crowdwork-zurueck-14548.htm

Video von ver.di: Klaus, der Cloudworker, https://www.verdi.de/themen/arbeit/++co++fd9e2f52-82fe-11e1-5004-0019b9e321e1

Anmerkungen

1 *http://www.thesheepmarket.com/*

2 *Um dieses Machtgefälle zumindest ein bisschen auszugleichen, haben zwei Wissenschaftler – Lilly Irani, Assistant Professor in Communication an der Universität San Diego und Six Silberman, Staff research associate an der Universität von Irvine – einen Webdienst und ein Plug-in für den Firefox-Browser programmiert. Das Tool trägt den schönen Namen „Turkopticon“. Damit ist es möglich, die Auftraggeber nach verschiedenen Kriterien zu bewerten und zu kommentieren. Das Plug-in macht für die Job-Interessierten sichtbar, welche Erfahrungen andere mit diesem Auftraggeber gemacht haben.*

3 *Dollar, denn Mechanical Turk nimmt keine Mitarbeiter/innen aus Europa mehr an.*

Ursprünglich wurde unter dem Begriff **Datenschutz** *der Schutz der Daten selbst im Sinne der Datensicherung, z. B. vor Verlust, Veränderung oder Diebstahl verstanden. Dieses Verständnis fand auch seinen Niederschlag im ersten Hessischen Datenschutzgesetz von 1970. Demgegenüber wurde der heute gültige Begriff des Datenschutzes erstmals 1970 in dem Aufsatz „Ulrich Seidel, Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, Neue Juristische Wochenschrift 1970, S. 1581 ff." geprägt. Dabei wurde außerdem die schutzrechtliche Aufspaltung von Daten aus der nicht geschützten Sozialsphäre und der geschützten Privat- und Intimsphäre aufgegeben und in einen einheitlichen Schutz von* **personenbezogenen Daten** *umgedeutet. In seiner Dissertation „Datenbanken und Persönlichkeitsrecht" von 1972 hat Seidel das materielle Datenschutzrecht als die Regelung personenbezogener Datenverarbeitungen insgesamt begriffen und gegenüber dem formellen Datenschutzrecht und der Datensicherung abgegrenzt. Mit seiner Arbeit hat er dem Datenschutz die seitdem allgemein und über Deutschland hinaus gebräuchliche Bedeutung gegeben (vgl. Rechtshistoriker von Lewinski, Geschichte des Datenschutzrechts von 1600 bis 1977, Freiheit-Sicherheit-Öffentlichkeit, 48. Assistententagung Öffentliches Recht, Nomos Verlag Baden-Baden 2009, S. 197 f. mit weiteren Nachweisen). Für die wissenschaftliche Begründung des Datenschutzbegriffes wurde Seidel 1986 mit dem Bundesverdienstkreuz ausgezeichnet.*

Ulrich Seidel

Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten

1. Einleitung des Problems

In den Vereinigten Staaten entfaltete sich in der zweiten Hälfte der sechziger Jahre die Diskussion über den Fragenkreis „Der Computer und der Eingriff in die Privatsphäre".[1] Anlaß hierfür war der Plan, ein statistisches Bundesdatenzentrum zu errichten, in dem die verstreuten Regierungsstellen zusammengefaßt werden sollen. Diese Pläne sind bis heute noch nicht verwirklicht, weil sich bei den *Computer Privacy* Hearings vor dem amerikanischen Kongreß[2] herausstellte, daß zur Zeit weder die rechtlichen noch die technischen Erfahrungen vorliegen, die das Individuum vor einem „computerisierten Übergriff" schützen könnten. Um dem wachsenden Bedarf an Planungsdaten Rechnung zu tragen, kann aber die bevorstehende Verwirklichung dieses Projekts wie auch die Entfaltung anderer statistischer und personenbezogener Datenbanken[3] auf internationaler Ebene nicht mehr bezweifelt werden. Inzwischen erstreckt sich das Problem des Schutzes der Privatsphäre gegenüber elektronischen Datenverarbeitungsanlagen auf alle größeren Industrieländer der westlichen Welt.[4] Für das deutsche Recht ist das Problem besonders dringlich, weil die BRD nach der Zahl der installierten datenverarbeitenden Anlagen die Spitze in Westeuropa einnimmt.[5] In der BRD entzündete sich die Diskussion dieses Problemkreises in Zusammenhang mit der geplanten Einführung eines bundeseinheitlichen Personenkennzeichens,[6] das als maschineninterner Personencode verschiedene Datenbestände aggregieren und die großen technischen Möglichkeiten der EDV für den Verwaltungsvollzug nutzbar machen soll.

2. Die Problemstellung und ansatzweise rechtliche Beurteilung

In personenbezogenen Datenbanken kann das Recht auf freie Entfaltung der Persönlichkeit bzw. das allgemeine Persönlichkeitsrecht in vielfältiger Weise verletzt werden.[7] Die Methodik der Datenermittlung hat sich der elektronischen Datenverarbeitung angepaßt und gänzlich neue Wege beschritten. Die moderne Interviewtechnik z. B. bedient sich heute der Longitudinalstudie,[8] die eine verbesserte Planung, Meinungs- und Verhaltensforschung ermöglichen soll. In den USA wurden bereits 1960 bei dem Projekt TALENT, Palo Alto, Kalifornien, die ersten Versuche eines zwanzigjährigen Befragungstests über Ausbildung und Persönlichkeitsentwicklung von high-school-Absolventen eingeleitet. Bei der Longitudinalstudie bleibt der befragte Personenkreis immer derselbe. Dieser Umstand bleibt dem Interviewten bei der ersten Befragung meist verschwiegen. Ist er aber erst einmal erfaßt, wird es für ihn schwierig, den lästigen weiteren Tests zu entgehen. Im Mikrozensus-Urteil weist das *BVerfG*[9] darauf hin, daß der Staat durch schlichtes Befragen in die nach Art. 1 und Art. 2 Abs. 1 geschützte Privatsphäre eindringen kann.[10]

Bei der Recherche sekundärer Daten, also Daten, die in irgendeinem Zusammenhang bereits ermittelt sind, kommt eine Indiskretion hinsichtlich privater Daten in Betracht. Eine Vertraulichkeit personenbezogener Informationen wird nach gefestigter Rechtsprechung nur für briefliche Aufzeichnungen,[11] heimliche Aufnahme von Bildern des privaten Lebensbereiches,[12] heimliche Tonbandaufnahmen[13] und ärztliche Aufzeichnungen[14] anerkannt. Die Weiterleitung beruflicher Werdegangsdaten wird dagegen im allgemeinen als gerechtfertigt angesehen, weil man diese Datenkategorie weniger der Privatsphäre als der sozialbezogenen Berufssphäre zurechnet. Solange man an der „Sphärentheorie"[15] festhält, die den persönlichkeitsrechtlichen Schutzbereich von der Intimsphäre bis zur Öffentlichkeitssphäre stufenartig aufteilt, ist es nicht möglich, diese wichtige Datenkategorie intensiver als bisher zu schützen.[16] In der BRD gibt es bereits mehrere betriebliche Personaldatenbanken, in denen die gesamte Personalakte einschließlich psychologischer Testergebnisse gespeichert ist.[17] Im Zuge der allgemeinen Umstellung auf EDV kann man davon ausgehen, daß in den nächsten Jahren jedes größere Unternehmen, aber auch viele Behörden, über eigene Personaldatenbanken verfügen werden.

Die meisten der heute ausgetauschten Daten sind zwar der Privatsphäre, nicht aber der privaten Geheimsphäre zuzurechnen. Ein sehr umfangreicher Datenaustausch wird durch den An- und

Verkauf von Adressenkollektionen betrieben, die in einem bestimmten privaten Zusammenhang ermittelt werden und denen in der Regel kaufvertragliche Beziehungen zugrunde liegen. Im Aufbau begriffene Datenbanken von Adressenverlagen[18] ermöglichen es, Namen und Adresse nach den verschiedensten Merkmalen zu sortieren und innerhalb kürzester Zeit tausendfach aufzulisten. Eine Verletzung durch Indiskretion scheidet hier – soweit die weitergeleiteten Daten keinen Geheimnischarakter haben – bereits begrifflich aus. Das *BVerfG* machte im Scheidungsakten-Urteil[19] deutlich, daß die durch zulässiges Eindringen ermittelten Daten nicht ohne weiteres zweckentfremdet werden dürfen. Zwar ist das *BVerfG*[20] der Auffassung, daß die Amtshilfe nur als formelle Rechtsgrundlage für die Anforderung der Personalakte im Verwaltungsverfahren in Frage komme. Doch bleibt auch nach dieser Entscheidung offen, ob die Datenweitergabe gegenüber dem Bürger auf eine materielle Rechtsgrundlage gestützt werden muß.[21]

Die Sammlung und Speicherung personenbezogener Dateien deckt ein Problem auf, dem das Individuum in der modernen Industriegesellschaft schon seit längerem ausgesetzt ist. Der räumliche Schutzbereich hat aufgehört, das alleinige Zentrum des Privatlebens zu sein, und hat mittlerweile durch den *Datenbereich* Konkurrenz erhalten. Der persönlichkeitsrechtliche Bezug dieses Schutzbereiches liegt darin, daß ein privater Lebenstatbestand aufgezeichnet und ohne Beteiligung des Individuums beliebig reproduzierbar und über große Entfernungen übertragbar ist. Damit wird die körperliche Nähe zum Einzelnen, sei es zu seiner häuslichen Umgebung oder zu seiner körperlichen Integrität selbst, verlassen. Die Umwelt des Einzelnen erstreckt sich somit auch auf die zahlreich über ihn angelegten und weit verstreuten Abbildungen seines Privatlebens.

Diese Entwicklung läßt die der „Sphärentheorie" zugrundeliegende dialektische Auffassung von „privat" und „öffentlich" fraglich erscheinen. Wenn das Persönlichkeitsrecht gegen die Aushöhlung von Kommunikationswissenschaften und Computertechnologie verteidigt werden soll, dürfen die erwähnten Begriffe nicht mehr als einander ausschließend betrachtet werden. Die Aufspaltung des Individuums in eine öffentliche und eine private Seite kann nur überwunden werden, wenn man seine sozialen Bindungen zugleich als Konkretisierung seines Anspruchs auf private Lebensführung anerkennt.[22]

Bei der Datenspeicherung gewinnt die Entstellung oder Verfälschung der ermittelten Daten an Bedeutung. Speicherökonomische Gesichtspunkte fordern nämlich eine nicht-redundante[23] Abspeicherung, d. h. es wird nur soviel „Information" ausgewählt, wie zur Erkennung einer Aussage erforderlich ist.[24] Dadurch wird ein isoliertes Verständnis hervorgerufen und mit ihm die Gefahr, daß eine Nachricht aus dem Kontext gerissen und damit verbunden einer falschen Interpretation zugänglich wird. Diese technisch bedingte, durch die schematische Verarbeitung hervorgerufene Verfälschungstendenz kann man als das „sophistische Element" im Computer ansprechen.[25] Außerdem eröffnet das Modell der Datenbank ungeahnte Manipulationsmöglichkeiten, die aber nur in einem größeren Rahmen darstellbar sind.

Schwierig ist die rechtliche Beurteilung, ob und inwieweit die Prozesse der Datenspeicherung und Datenverarbeitung als selbständige Verletzungstypen innerhalb des Persönlichkeitsrechts anzusehen sind. Immer wieder, besonders von Verwaltungsfachleuten, ist zu hören, daß alles, was ermittelt werden dürfe, selbstverständlich auch einer Speicherung zugänglich sei. Die technische Aufbewahrung sei für die Frage, ob das Persönlichkeitsrecht verletzt werde, unerheblich.

Indes begegnet diese Argumentation einigen Bedenken. Die personenbezogene Datenbank ist nicht nur eine Rationalisierung von Verwaltungsabläufen, sondern eine kommunikationsorientierte Datenbasis, in der die Information im sogenannten *Mensch-Maschine-Dialog*[26] gewonnen wird. Die Informationsgewinnung wird damit auf eine gänzlich neue Kommunikationsbasis gestellt. Die sich hier abzeichnende Problematik hat verwandte Züge mit der phonetischen Aufzeichnung eines Gespräches. Zwar ist der Gesprächspartner auf Grund der in der Gesprächsbereitschaft liegenden Einwilligung seines Gegenübers berechtigt, die mitgeteilten Informationen wahrzunehmen. Doch ist er nicht befugt, die zugrundeliegenden Daten aufzuzeichnen, weil sonst die Unbefangenheit der menschlichen Kommunikation gestört würde.[27] Löst man die an diesem Fall orientierte Rechtsprechung von diesem Fall ab und projiziert sie auf ein größeres Modell, so erstreckt sich das Selbstbestimmungsrecht, Informationen vorzuenthalten oder mitzuteilen, immer auf eine ganz bestimmte Kommunikationsform, d. h. auch eine Einwilligung in die schriftliche Fixierung eines Gespräches berechtigt nicht zu einer Tonbandaufzeichnung. Stellt man dieses Ergebnis der einleitenden Fragestellung gegenüber, so können die Daten eines schriftlich ausgefüllten Personalfragebogens nur mit Einwilligung des betroffenen Individuums gespeichert werden. Die Richtigkeit dieser Überlegung hängt ganz davon ab, ob man die Datenbank als eine selbständige Aufzeichnungsform anerkennt. Wird diese Bedingung akzeptiert, so muß bei der auskunftsverpflichteten Datenermittlung im staatlichen Bereich die Berechtigung zur Datenspeicherung gesetzlich verankert werden.

Anstatt die neue, bisher noch wenig vertraute Problematik zu vertiefen, erscheint es sinnvoller, darauf hinzuweisen, wie man sich eine Lösung dieses für die Zukunft außerordentlich wichtigen Problems schematisch vorzustellen hat und welchen Beitrag dabei die Rechtswissenschaft leisten kann.

3. Datensicherungen

Die Möglichkeit, das Persönlichkeitsrecht technisch zu sichern, ist weit gefächert und aussichtsreich, wenn auch die praktischen Erfolgschancen durch wirtschaftliche Gesichtspunkte augenblicklich noch stark eingeengt sind. Um einen allzu neugierigen Benutzer in die Schranken zu verweisen, ist es üblich geworden, programmierte Abfragesperren in Datenbanken einzurichten. Diese Sperren haben aber den Nachteil, daß sie technisch geschultem Personal gegenüber versagen. Jeder Code – mag er auch noch so gut sein – kann „geknackt" werden, wenn die Verschlüsselungsmethode begriffen wird. Fragt eine Person Daten ab, die technisch kontrollierbar sind und auf die sie zuzugreifen befugt ist, so ergibt sich die weitere Frage nach der Identitätskontrolle des vermeintlich Berechtigten. Vorschläge reichen hier vom antiquierten Losungswort bis hin zur automatischen Erkennung des Finger- und Stimmabdrucks. Neben Abfragesperren und Identitätskontrollen gibt es aber auch Schreibsperren, die verhindern sollen, daß ein fremdes Speicherbild manipuliert werden kann.[28]

4. Datenschutz

Technische Sicherungen können aber nur die Frage beantworten, wie ein vermeintlich berechtigter Benutzer mit Gewißheit erkannt und die Ausübung seiner Rechte kontrolliert werden kann. Sie lassen das Problem offen, nach welchen Kriterien der Benutzer berechtigt sein soll, auf die gespeicherten Daten zuzugreifen. Immerhin können die in der Vergangenheit vermißten Sicherheitseinrichtungen den persönlichkeitsrechtlichen Schutz wesentlich effektiver gestalten als bisher.

Die materiellrechtlichen Kriterien, an denen sich die einzelnen Datensicherungen zu orientieren haben, müssen allerdings von der Rechtswissenschaft und Rechtspraxis gemeinsam erarbeitet werden. Solche Kriterien gibt es bis jetzt noch nicht, und zwar in keinem Land.[29]

Das zentrale Problem bei der Aufstellung materiellrechtlicher Kriterien für einen Datenzugang besteht in der Ausbalancierung von personenbezogenen Planungs- und Forschungsdaten und dem Interesse des betroffenen Individuums an ihrer Zurückhaltung. Da aber das Persönlichkeitsrecht durch die Rechtswirklichkeit bereits gefährlich ausgehöhlt ist und weiter ausgehöhlt werden wird, liegt die Betonung auf dem Persönlichkeitsschutz. Die Information aus einer Datenbank könnte im kommerziellen Bereich zur Ware werden und auf staatlicher Ebene einer perfekten Überwachung dienen. Deshalb genügt es nicht mehr, nur das Lebensbild oder Teile aus ihm, sondern wie im amerikanischen Recht jedes personenbezogene Datum als schutzfähig anzusehen.[30]

Nachdem der Computer auch in der Jurisprudenz nicht mehr als bloß „überdimensionierter Rechenschieber" angesehen wird, kann man darauf hoffen, daß den mit ihm aufgetauchten persönlichkeitsrechtlichen Fragen die gebührende Aufmerksamkeit zukommt.

Der Beitrag wurde mit freundlicher Genehmigung des Autors, der Schriftleitung der Neuen Juristischen Wochenschrift und des Verlags C. H. Beck dem Heft 36 des Jahrgangs 1970 der Neuen Juristischen Wochenschrift entnommen, NJW 1970, S. 1581-1583. Wir bedanken uns herzlich für die Genehmigung zum Wiederabdruck.

Anmerkungen

Die Fußnoten am Ende der Seiten wurden aus technischen Gründen in Endnoten umgewandelt.

1 *Vgl. Chartrand, The Federal Data Center: Proposals and Reactions, Law and Computer Technology, Oktober 68, S. 12 f.; The National Data Center controversy, Data Systems, März 69, S. 20 f.*

2 *Computer Privacy, Hearings before the Subcommittee on Administrative Practice and Procedure on the Senate Committee on the Judiciary, 90th Congr. 67/68, 1st and 2nd Session.*

3 *Der Begriff der Datenbank ist wissenschaftlich nicht geklärt, hat sich aber sprachlich eingebürgert und soll darauf hinweisen, daß Daten beliebig „eingezahlt" und „abgehoben" werden können.*

4 *Deshalb befaßt sich auch der Europarat mit dem Problem, vgl. u. a. Antr. Jakobsen, Europarat-Drs. Doc. 2562.*

5 *Vgl. Ifo-Schnelldienst Nr. 44 v. 31.10.1969, S. 18.*

6 *Vgl. u. a. Badenhoop, Zentrale elektronische Datenverarbeitung: Einheitliches Personenkennzeichen, KGSt Köln, Rundschreiben Nr. 32/68; BT-Drucks. VI/598.*

7 *Gedanken über das Problem macht sich vor allem die Interparlamentarische Arbeitsgemeinschaft, Bonn.*

8 *Darunter versteht man eine Studie, bei der über einen längeren Beobachtungszeitraum ein Daten-Längsschnitt angefertigt wird.*

9 *BVerfGE 27, 1 = NJW 69, 107.*

10 *Vgl. Kamlah, Datenüberwachung und Bundesverfassungsgericht, DÖV 70, 361.*

11 *BGHZ 15, 249 = NJW 55, 260 L.*

12 *BGHZ 24, 200 = NJW 57, 1315.*

13 *BGHZ 33, 20 = NJW 60, 2043.*

14 *BGHZ 24, 72 = NJW 57, 1146.*

15 *Vgl. Hubmann, Das Persönlichkeitsrecht, Köln 1967, S. 268 f.; Wenzel, Das Recht der Wort- und Bildberichterstattung, Köln 1967, S. 65 f.*

16 *Diese Forderung wird auch von Maass, Information und Geheimnis im Zivilrecht, Stuttgart 1970, S. 26, erhoben.*

17 *Die Personaldatenbank der „Ford of Germany", Köln, speichert auch alle betriebsärztlich ermittelten Daten, beispielsweise Schwangerschaftsuntersuchungen.*

18 *Z. B. der Merkur-Verlag, Einbeck; der Bertelsmann-Verlag benutzt die moderne Adressenverarbeitung zum Ausbau seines Lesering-Systems.*

19 *BVerfG, NJW 70, 555.*

20 *aaO.*

21 *Kamlah, aaO S. 363, sieht diese Grundlage in der noch ungeschriebenen Befugnis einer Behörde, den relevanten Sachverhalt für ein Verfahren zu ermitteln. Düwel, Das Amtsgeheimnis, Berlin 1965, S. 106, kommt zu dem Schluß, daß nur eine spezialrechtliche Norm ausreichen könne.*

22 *Die Bezeichnung „private Öffentlichkeit" (Maass, aaO S. 26) zeigt die gedankliche Schizophrenie, aber auch die Möglichkeit, das Verhalten in der Öffentlichkeit als Bestandteil des Privatlebens anzusehen.*

23 *„Redundanz" (Überfluß) ist ein informationstheoretischer Begriff. Vgl. z. B. Seiffert, Information über die Information, München 1968, S. 65 f. Die natürliche Sprache ist in hohem Maße redundant. Man ist sich darüber im klaren, daß ausreichendes Verständnis und hoher Lerneffekt nur durch eine nicht-redundante Information erfolgen können.*

24 *Ob die Vergrößerung und Verbilligung der Speicherkapazität diese Verletzungsgefahr beseitigen wird, ist fraglich, da die Tendenz zu beobachten ist, immer mehr Daten dem Computer zu übergeben.*

25 *Dieses Gesichtspunkts hat sich die amerikanische Rechtswissenschaft besonders angenommen. Stellvertretend für die zahlreiche Literatur: A. Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an information-oriented Society, Michigan Law Review April 1969, S. 1089–1246.*

26 *Zur näheren Beschreibung vgl. Seidel, EDV als maschinelles Hilfsmittel einer juristischen Dokumentation, DRiZ 70, 118.*

27 *BGHZ 27, 284 (287) = NJW 58, 1344, spricht von dem Recht, das Gespräch frei, unbefangen und ohne das Gefühl des Mißtrauens und des Argwohns führen zu dürfen.*

28 *BT-Drucks. VI/648, S. 20.*

29 *Die gesetzgeberische Initiative, die in vielen Ländern zu beobachten ist, beschränkt sich meistens auf die Verankerung von Kontrollmaßnahmen.*

30 *Kamlah, aaO S. 361; ders., Right of Privacy, Köln 1969, S. 87 unter Hinweis auf die amerikanische Literatur.*

Stefan Hügel

Log 1-2/2015

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau der Bürgerrechte stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

November 2014

18. November 2014: Das Bundessozialgericht in Kassel hat entschieden, dass das Foto auf der elektronischen Gesundheitskarte nicht gegen die informationelle Selbstbestimmung verstößt und damit rechtmäßig ist (Quelle: Bundessozialgericht, Heise).

18. November 2014: Die britische Regierung will den Zugang zu Polizeidatenbanken auf dem europäischen Festland vereinfachen und zugleich eigene einschlägige Systeme Strafverfolgern aus anderen EU-Staaten öffnen. Ziel ist der weitgehende Anschluss an den Prümer Vertrag von 2007, demzufolge Sicherheitsbehörden der beteiligten Länder etwa DNA-, Fingerabdruck- und Fahrzeugregisterdaten elektronisch einfacher austauschen können (Quelle: Heise).

19. November 2014: Der Senat hat die Reform der Spionagepraktiken der NSA mehrheitlich abgelehnt. Es fehlten zwei der benötigten 60 Stimmen, um den sogenannten „Freedom Act" zur Debatte und anschließenden Abstimmung zu bringen. Das Gesetz sollte der Sammlung von Telefondaten im Rahmen des „Patriot Act" engere Grenzen setzen; unter anderem war vorgesehen, dass die NSA keinen direkten Zugriff mehr auf Verbindungs- und Standortdaten aus der Telekommunikation bei Providern haben soll. Vor allem Republikaner blockierten das Vorhaben. Sie argumentierten, die USA könnten bei einer Verabschiedung nicht mehr ausreichend vor Terroranschlägen beschützt werden (Quelle: Heise).

20. November 2014: Die Bundesregierung hat ihre Auskunft über Pläne des BND, Zero-Day-Exploits zu kaufen und einzusetzen, unter die höchste Geheimhaltungsstufe gestellt. Nach Auskunft der Bundesregierung setzen weder das Bundeskriminalamt noch die Bundespolizei, der Verfassungsschutz, der Militärische Abschirmdienst oder das Zollkriminalamt Zero-Day-Exploits ein. Dies sei auch nicht geplant. Anders sieht dies beim Bundesnachrichtendienst aus. Pläne dazu seien aber VS-Geheim. Die Bundesregierung ist der Meinung, dass die Veröffentlichung dieser Informationen die Sicherheit der Bundesrepublik Deutschland gefährden und dem Staate schweren Schaden zufügen kann (Quelle: Andrej Hunko MdB, Heise).

21. November 2014: Aus Dokumenten von Edward Snowden geht hervor, dass der britische Geheimdienst GCHQ möglicherweise über Vodafone bzw. dessen Tochterfirma Cable & Wireless deutsche Kunden abhört. Dies würde gegen deutsches Recht verstoßen. Das BSI hält das für möglich. Vodafone dagegen betonte, dass das Unternehmen „Geheimdiensten und staatlichen Behörden in keiner Form den Zugang zu Kundendaten" gestatte, es sei denn, es sei „von Gesetzes wegen dazu verpflichtet und erhalte entsprechende Aufforderungen" (Quelle: WDR, NDR, Süddeutsche Zeitung, Heise).

21. November 2014: Das Versicherungsunternehmen Generali will Versicherte für gesunde Lebensführung belohnen. Dazu werde ein Modell entwickelt, bei dem die Versicherten regelmäßig mit ihrer Versicherung kommunizieren sollen. Für eine gesunde Lebensführung sollen sie z. B. mit Rabatten und Gutscheinen belohnt werden. Laut Süddeutscher Zeitung setze die Versicherung auf Telemonitoring; Kunden müssen regelmäßig Daten zu ihrem Lebensstil, z. B. Vorsorgeterminen, sportlichen Aktivitäten etc. übermitteln (Quelle: Süddeutsche Zeitung, Heise).

24. November 2014: In Saudi-Arabien wird laut der Menschenrechtsorganisation *Human Rights Watch* das Vorgehen gegen Netzaktivisten verschärft. Dabei würden vor allem Bürger verfolgt, die über Twitter kritische Nachrichten veröffentlichten. Grundlage dafür sei ein Gesetz gegen Cyberkriminalität, das verbiete, Inhalte zu produzieren, die „die öffentliche Ordnung schädigen" (Quelle: Human Rights Watch, Heise).

24. November 2014: Mit der Spionage-Software *Regin* wurden jahrelang Unternehmen und Behörden, vor allem in Russland und Saudi-Arabien, ausgespäht. Laut der Sicherheitsfirma Symantec sei die Software dabei so komplex, dass als Auftraggeber nur Staaten in Frage kämen. Betroffen seien vor allem Betreiber von Telekommunikationsnetzen, Fluggesellschaften, Forschungseinrichtungen und das Hotelgewerbe. Weiteren Berichten zufolge wurde *Regin* auch für den Angriff auf das belgische Telekommunikationsunternehmen Belgacom eingesetzt, der nach von Edward Snowden veröffentlichten Dokumenten vom britischen Geheimdienst GCHQ ausging, der eng mit der NSA zusammenarbeitet (Quelle: The Intercept, Heise).

25. November 2014: Durch einen Angriff auf das Firmennetz von Sony Pictures wurde dessen Betrieb zum Erliegen gebracht. Unbekannte, die sich selbst als *Guardians of Peace* (GOP) bezeichnen, haben Medienberichten in den USA zufolge die gesamte IT-Infrastruktur bei Sony Pictures übernommen. Die Gruppe droht damit, interne Daten der Firma zu veröffentlichen, wenn bestimmte Forderungen nicht erfüllt werden. In einer ZIP-Datei, die die Angreifer ins Netz gestellt haben, sollen sich unter anderem Finanzberichte, private Krypto-Schlüssel, interne Präsentationen und Kopien von Pässen von Mitarbeitern befinden (Quelle: Heise).

25. November 2014: Ein britischer Gesetzentwurf soll Internet-Provider verpflichten, dafür zu sorgen, dass Internetnutzer eindeutig per IP-Adresse identifiziert werden können. Damit sollten

die im Sommer dieses Jahres in Großbritannien beschlossenen Notstandsgesetze ergänzt werden. Die Befugnisse zur Datenspeicherung sollten eng begrenzt werden und nicht dazu dienen, Zugriffe auf Server mit illegalen Inhalten nachzuvollziehen (Quelle: The Guardian, Heise).

27. November 2014: Aus Sicht des bayerischen Innenministeriums hat sich das Verfahren *Precobs* (Pre Crime Observation System), mit dem Einbrüche vorhergesagt werden sollen, bewährt. Die Machbarkeitsstudie der Software aus dem Institut für musterbasierte Prognosetechnik in München und Nürnberg seit September 2014 soll nun auf ganz Bayern ausgedehnt werden. *Precobs* ist eine Statistiksoftware auf Basis der Theorie der *near repeats*. Einbrecher, Straßenräuber und Autoknacker gehen nach bestimmten, erfolgreich „getesteten" Mustern vor; diese werden von *Precobs* gespeichert. Gemeinsam mit statistischen Korrelationen ähnlicher Gebiete werden „Treffer" erzielt, indem bestimmte Planquadrate errechnet werden, die dann stärker von der Polizei bestreift werden (Quelle: Bayerisches Innenministerium, Heise).

27. November 2014: Im NSA-Untersuchungsausschuss hat ein früherer Sachgebietsleiter des BND eingeräumt, dass der Geheimdienst seine Überwachungsbefugnisse nutze, um „Routine"-Kommunikation zu erfassen und weiterzuleiten. Es habe Bedenken gegeben, ob die „Ableitung von Routineverkehren" aus einer gesetzlich zulässigen, aber zugleich beschränkten Maßnahme rechtmäßig sei. Dies sei in einem Rechtsgutachten für das zu dieser Zeit von Frank-Walter Steinmeier geführte Bundeskanzleramt bejaht worden; dieses habe daraufhin zugestimmt (Quelle: Heise).

Dezember 2014

5. Dezember 2014: Nach Ansicht des zuständigen britischen Gerichts verstoßen die Überwachungsprogramme des Geheimdiensts GCHQ nicht gegen die Europäische Menschenrechtskonvention. Die Menschenrechtsgruppen Amnesty International, Privacy International und Liberty hatten argumentiert, die Massenüberwachungsprogramme des GCHQ verstießen gegen das Recht auf Achtung des Privat- und Familienlebens und gegen das Recht auf freie Meinungsäußerung. Die Organisationen haben Beschwerde beim Europäischen Gerichtshof für Menschenrechte angekündigt (Quelle: Heise).

6. Dezember 2014: Die Internet-Seiten des Chaos Computer Clubs (CCC) waren zeitweise in Großbritannien für einen Teil der Internetnutzer nicht zugreifbar. Dies wurde offenbar durch die Jugendschutzsysteme der britischen Internet-Provider verhindert. Der CCC teilte mit, dass seine Seiten anscheinend auf der schwarzen Liste des britischen Pornographie-Filters gelandet seien. Der Filter war für den Jugendschutz eingeführt, dann aber auf terroristische und extremistische Inhalte ausgeweitet worden. Für den CCC ist dies eine Bestätigung, dass solche Filter für Zensur missbraucht werden können bzw. durch „Overblocking" Inhalte unabsichtlich gesperrt werden. Viele britische Kunden haben den Filter nicht aktiviert, so ist unklar, wie viele Nutzer tatsächlich die Seiten des CCC nicht erreichen konnten (Quelle: CCC, Heise).

7. Dezember 2014: Das Bundesjustizministerium verweigert die Herausgabe eines Schreibens der US-Regierung vom 5. September 2014, in dem es möglicherweise um die Auslieferung von Edward Snowden geht. Der NSA-Untersuchungsausschuss hatte das Schreiben angefordert, zur Klärung, ob Snowden bei einer Einreise nach Deutschland ausgeliefert werden könnte. Das Bundesjustizministerium hält das Schreiben nach langer Prüfung für nicht erforderlich, um die Sachverhalte zu klären, für die der Untersuchungsausschuss eingesetzt wurde. Aus Sicht des Abgeordneten der Linken, André Hahn, sei diese Ablehnung „*eine erneute und nicht hinnehmbare Brüskierung des gesamten Untersuchungsausschusses durch die Bundesregierung*" (Quelle: Heise).

8. Dezember 2014: Angesichts der Veröffentlichung des Berichtes über die CIA-Folterpraktiken in den USA hat der frühere Präsident George W. Bush den Geheimdienst verteidigt. Er lobte die CIA-Mitarbeiter gegenüber CNN: „*Das sind Patrioten und was auch immer in dem Bericht steht, wenn er ihre Beiträge zu diesem Land herabwürdigt, liegt er unglaublich falsch.*" Die USA könnten sich glücklich schätzen, diese Frauen und Männer zu haben, so Bush weiter (Quelle: CNN, Heise).

8. Dezember 2014: Der Menschenrechtskommissar des Europarats, Nils Muižnieks, kommt in einem neuen Bericht über Rechtsstaatlichkeit zu dem Ergebnis, dass geheime, massive und unterschiedslose Überwachung rechtliche Grenzen überschreite. Muižnieks erkennt darin zwar die Notwendigkeit des Kampfs gegen Cybercrime und Terrorismus an. Die Überwachung könne aber die Demokratie zerstören, anstatt sie zu schützen (Quelle: The Guardian, Heise).

9. Dezember 2014: Die US-Regierung hat erneut für weitere 90 Tage angeordnet, dass Telefonanbieter die Verbindungsdaten aller Telefongespräche an die NSA weiterleiten müssen. Dies sei erforderlich, solange die von US-Präsident Obama geplante Reform noch nicht verabschiedet sei. Die Reform sieht vor, dass die Daten bei den Providern verbleiben und nur noch auf Anfrage herausgegeben werden sollen. Gleichzeitig wurde in einer Erhebung des Softwareherstellers Open-Xchange ermittelt, dass in den USA 15 %, in Großbritannien 20 % und in Deutschland 37 % der Nutzer wegen des NSA-Skandals mindestens einen Online-Dienst verlassen hätten. Meistens sei Facebook davon betroffen gewesen, in geringerem Umfang auch Google (Quelle: US-Justizministerium, Heise).

9. Dezember 2014: In der Zusammenfassung des Berichts über die „Erweiterten Verhörmethoden" erhebt der Geheimdienstausschuss des US-Senats schwere Vorwürfe gegen die CIA. Offenbar hat der Geheimdienst Regierung und Kongress über brutale Folter und deren Effektivität getäuscht. Die Methoden seien brutaler und gleichzeitig weniger effektiv gewesen, als von der CIA behauptet (Quelle: US-Senat, Heise).

11. Dezember 2014: Der Europäische Gerichtshof hat entschieden, dass auch bei privater Videoüberwachung des öffentlichen Raums die europäische Richtlinie für den Datenschutz zu beachten ist. Die betroffenen Personen müssen auch bei den Aufnahmen einer Videoüberwachungskamera der Verarbeitung ihrer Daten zugestimmt haben. Ausgenommen seien nur Videoaufnahmen, die „*zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten*" vorgenommen werden (Quelle: EuGH, Heise).

11. Dezember 2014: Gegen den Software-Hersteller Gamma werden offenbar keine Ermittlungen aufgenommen. Gegen Gamma war vom European Center for Constitutional and Human Rights Strafanzeige gestellt worden. Mit der Gamma-Software FinFisher/FinSpy waren in Bahrain Oppositionelle und eine Regierungskommission ausgespäht worden. Da aber der Hersteller in seinen Vertragsbedingungen ausdrücklich den rechtswidrigen Einsatz der Software untersage, sei die Klage gegenstandslos (Quelle: Heise).

12. Dezember 2014: Offenbar unbemerkt von vielen Kongressmitgliedern hat der US-Kongress mit der Autorisierung des Budgets der Geheimdienste einen Absatz mitbeschlossen, der das Ausspähen von US-Bürgern erlaubt. Der Paragraph 309 des *Intelligence Authorization Act* legitimiert das eigentlich „unbeabsichtigte" Aufzeichnen von Inhalts- oder Metadaten eigener Bürger beim Erfassen von Kommunikationsströmen, die primär auf „Auslandsstrecken" ausgerichtet sein sollen (Quelle: Heise).

13. Dezember 2014: Journalisten von *The Intercept* kommen zu dem Schluss, dass der Angriff auf den belgischen Internet-Provider Belgacom offenbar aggressiver und umfassender war, als bisher dargestellt. Aus Sicht von Edward Snowden handelt es sich um das erste dokumentierte Beispiel eines Cyberangriffs eines EU-Staates auf einen anderen. Zu den Kunden von Belgacom zählen auch die Europäische Kommission, das Europäische Parlament und der Europäische Rat. Genutzt wurde dabei offenbar die Cyberwaffe *Regin* (Quelle: The Intercept, Heise).

14. Dezember 2014: Nach einem Bericht des Spiegel haben BND und CIA gemeinsam Provider in Deutschland angezapft. Der BND habe im Jahr 2005 das deutsche Tochterunternehmen eines US-Netzbetreibers aufgefordert, *„Zugang zu Kommunikationsverbindungen des Unternehmens in Düsseldorf"* zu gewähren. Das Unternehmen und der BND hätten sich dann auf eine Zusammenarbeit unter Einbindung der CIA unter dem Codenamen *Globe* geeinigt. Die Daten seien in die BND-Außenstelle Rheinhausen geleitet worden (Quelle: Der Spiegel, Heise).

16. Dezember 2014: Einer Umfrage zufolge hält ca. die Hälfte der US-Bürger Folter wie Waterboarding, die die CIA angewandt hat, zumindest teilweise für gerechtfertigt. 36 % lehnten Folter ab, 57 % sind der Ansicht, Folter könne verlässliche Informationen liefern und so Terroranschläge verhindern. Dies steht im Gegensatz zum Ergebnis des CIA-Folterreports, der zu dem Ergebnis kommt, Folter sei nicht effektiv gewesen (Quelle: CBS, Heise).

19. Dezember 2014: Mit der Operation *Eikonal* wurde laut der Deutschen Telekom grundrechtssensibles Material erfasst. Laut einer Aussage im NSA-Untersuchungsausschuss warnte die Telekom den BND, dass durch die Operation bis zu 90 % Kommunikation von geschützten Grundrechtsträgern abgegriffen werden könnte. Damit bestand eine erhebliche Gefahr, dass Datenverkehr deutscher Bürger, der unter das G10-Gesetz fiel, nicht korrekt ausgefiltert und an die NSA weitergeleitet wurde (Quelle: Heise).

22. Dezember 2014: Die Überwachung und Manipulation von Rechnern, mit denen ein Ausschuss im US-Senat die Folterpraxis des Geheimdiensts untersuchen sollte, bleibt für die CIA wohl ohne Konsequenzen. Fünf Mitarbeiter der CIA, die die Maßnahmen durchgeführt hatten, haben das Vorgehen als rechtmäßig verteidigt und sich dabei auf Anordnungen des CIA-Chefs John Brennan berufen. Im Frühjahr war bekannt geworden, dass die CIA Senatoren und Mitarbeiter, die die Foltermethoden untersucht hatten, ausspioniert hatten. Betroffen waren vor allem Computer, mit denen die Dokumente der CIA analysiert wurden. Dabei seien nach Aussage der Ausschussvorsitzenden Dianne Feinstein auch Daten gelöscht worden (Quelle: Heise).

29. Dezember 2014: Einem Medienbericht zufolge wurde auf einem Rechner im Bundeskanzleramt die Spionagesoftware *Regin* entdeckt. Eine Referatsleiterin hatte nach Berichten der Bild-Zeitung eine Datei auf ihrem privaten Laptop bearbeitet; als sie diese Datei mit einem USB-Stick auf ihren Dienstrechner übertragen wollte, schlug der Virenscanner Alarm. Untersuchungen der Rechner im Bundeskanzleramt ergaben keine weiteren Funde; das IT-System des Kanzleramts sei nicht infiziert worden (Quelle: Bild, Heise).

Januar 2015

2. Januar 2015: Gegen das massenhafte Scannen von Kfz-Kennzeichen und deren Abgleich mit Fahndungsdateien wurde Verfassungsbeschwerde eingelegt. Kläger ist der IT-Experte Benjamin Erhart, der von dem Freiburger Anwalt Udo Kauß vertreten wird, der bereits bei ähnlichen Beschwerden in Hessen und Schleswig-Holstein erfolgreich war. In dem Entwurf der Beschwerdeschrift heißt es, ohne Korrektur der bisherigen Rechtsprechung drohten *„weitreichende negative Folgen für den Grundrechtsschutz"*. Weiter heißt es, dass bei konsequenter Durchführung *„der Staat ohne gesetzliche Grundlage und ohne jegliche Einschränkung Informationen über menschliches Verhalten erfassen und auswerten kann"* (Quelle: Heise).

12. Januar 2015: Zum Gedenken an die Opfer der terroristischen Anschläge in Paris sind Millionen Menschen auf die Straße gegangen. Gleichzeitig werden die Anschläge von Sicherheitspolitikern für die Ankündigung neuer Maßnahmen genutzt. Bundesinnenminister Thomas de Maizière forderte, mehr Informationen auszutauschen. Das gelte insbesondere für die Geheimdienste. Das Europaparlament soll die Blockade des europäischen Fluggastdaten-Abkommens beenden. *„Wer jetzt ein europäisches Fluggastdaten-Abkommen ablehnt, weiß nicht, was die Stunde geschlagen hat."* Justizminister Heiko Maas (SPD) kündigt ein Gesetzespaket mit Maßnahmen für einen effektiveren Anti-Terrorkampf an. Eine Wiedereinführung der Vorratsdatenspeicherung lehnt Maas zu diesem Zeitpunkt jedoch weiter ab (Quelle: Heise).

12. Januar 2015: Bilder, die in den Clouds US-amerikanischer Anbieter hochgeladen werden, werden offenbar automatisch gescannt und dabei auch auf Darstellungen des Missbrauchs von Kindern durchsucht. Meldungen über mutmaßlich illegales Material werden demnach auch an deutsche Strafverfolgungsbehörden gemeldet. Der Rechtsanwalt Udo Vetter berichtet in seinem Blog, dass bei einem seiner Mandanten ein einzelnes fragwürdiges Bild unter mehreren tausend zu einer Meldung an das Bundeskriminalamt geführt habe (Quelle: lawblog.de, Heise).

13. Januar 2015: Großbritanniens Premierminister Cameron findet, dass jede Kommunikation für Geheimdienste einsehbar sein müsse. Für den Fall seiner Wiederwahl kündigte er neue Befugnisse für die Sicherheitsbehörden seines Landes an. Einerseits soll die 12-monatige Vorratsdatenspeicherung festgeschrieben werden, die bislang nur bis 2016 gilt. Auch Kommunikationsdienste, bei denen der Inhalt der Dialoge durch Verschlüsselung vor dem Zugriff von Sicherheitsbehörden geschützt ist, dürften nach Ansicht von Cameron nicht möglich sein (Quelle: Heise).

14. Januar 2015: Nach Statistiken zur Telekommunikationsüberwachung fragen Ermittler verstärkt Verbindungs- und Standortdaten ab. Nach 9901 Anordnungen 2012, Verbindungs- und Standortdaten auszuforschen, kam dies 2013 bereits in 12.572 Fällen vor. Dies geht aus einer jetzt veröffentlichten Übersicht des Bundesjustizamts hervor (Quelle: Heise).

14. Januar 2015: Auch Bundeskanzlerin Angela Merkel reiht sich in die Phalanx der Politiker ein, die sich die terroristischen Anschläge von Paris zu Nutze machen, gebetsmühlenartig die Einführung einer Vorratsdatenspeicherung zu fordern. Justizminister Maas lehnt die Vorratsdatenspeicherung nach wie vor ab – das wird sich später noch ändern (Quelle: Heise).

15. Januar 2015: Es ist nun sicher, dass die Ausspähung der Computer des US-Senatsausschusses zur Untersuchung der Folterpraxis der CIA keine Konsequenzen haben wird. Die Abgeordneten und der Geheimdienst hätten sich nicht auf Grundregeln für die Zusammenarbeit verständigt (Quelle: Heise).

16. Januar 2015: Nach Ansicht des ehemaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, war die vertragliche Grundlage für das BND- und NSA-Projekt *Eikonal* zur Datenausspähung vermutlich rechtswidrig. Er sei auch nicht darüber unterrichtet worden, dass von einem Frankfurter Netzknoten zwischen 2004 und 2008 Daten abgegriffen und teilweise an die NSA weitergeleitet worden waren. Sei die Ausspähung lediglich auf Basis einer vertraglichen Vereinbarung, ohne Anordnung nach dem G10-Gesetz erfolgt, könne sie nicht rechtskonform sein (Quelle: Heise).

18. Januar 2015: Einem Bericht des Spiegel zufolge entwickelt der US-Geheimdienst NSA Waffen zur Führung von Cyberkriegen. In solchen Auseinandersetzungen soll wichtige Infrastruktur wie Strom- und Wasserversorgung gezielt ausgeschaltet werden. Beispiele für solche Cyberwaffen sind *Stuxnet* und *Regin*. Es sollen auch fremde Angriffe erkannt und Erkenntnisse fremder Geheimdienste genutzt werden. Wichtig sei es dabei, eigene Aktionen glaubhaft abstreiten zu können (Quelle: Der Spiegel, Heise).

21. Januar 2015: Zum Kampf gegen den Terror fordert jetzt auch Bundesinnenminister Thomas de Maizière, dass Sicherheitsbehörden in der Lage sein müssen, *„verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen"*. Dies hätten die Anschläge von Paris deutlich gemacht (Quelle: AFP, Heise).

27. Januar 2015: Aus einem geheimen Verhandlungspapier zum „Freihandelsabkommen" TTIP geht offenbar hervor, dass sich die USA und die EU künftig über Gesetzentwürfe und weitere Vorhaben abstimmen sollten. Gesetze, Verordnungen, Standards oder spezifische Regeln, beispielsweise zum Verbraucher- und Datenschutz, sollen demzufolge in Europa nicht mehr ohne Mitsprache der USA verabschiedet werden (Quelle: Heise).

29. Januar 2015: Bundesinnenminister Thomas de Maizière fordert den Austausch von Fluggastdaten auch zwischen europäischen Staaten. Dies sei die logische Konsequenz aus dem entsprechenden Abkommen zwischen der EU und den USA (Quelle: Heise).

30. Januar 2015: Im NSA-Untersuchungsausschuss räumt der technische Leiter der Operation *Eikonal* ein, dass die Netzüberwachung der Geheimdienste nicht mit der Rechtslage vereinbar sei. Dies sei im Geheimdienst selbst thematisiert worden (Quelle: Heise).

30. Januar 2015: Einem Medienbericht zufolge greift der Bundesnachrichtendienst noch mehr Daten ab, als bisher angenommen. Demnach werden täglich 220 Millionen Verbindungsdaten erfasst und an die NSA und andere Dienste weitergeleitet. Dabei würden nicht mehr einzelne Verdächtige gezielt überwacht, sondern die Daten würden massenhaft gesammelt. Dies erfolge in fünf Dienststellen des BND. Gleichzeitig werde gezielt die parlamentarische Kontrolle behindert, indem den Kontrollgremien die Arbeit so schwer wie möglich gemacht werde (Quelle: Die Zeit, Heise).

Februar 2015

1. Februar 2015: Die von Bundesjustizminister Heiko Maas initiierte Verschärfung des Sexualstrafrechts tritt in Kraft. Anlass dafür war die Affäre um den ehemaligen Bundestagsabgeordneten und Vorsitzenden des NSU-Untersuchungsausschusses Sebastian Edathy. Edathy hatte Bilder von Kindern aus dem Internet heruntergeladen, deren Besitz möglicherweise nicht strafbar war, aber nach Ansicht der Strafverfolgungbehörden auf den Besitz strafbaren Materials hingewiesen hat. Der Besitz dieser Art von Bildern soll nun auch unter Strafe gestellt werden. Kritiker befürchten, dass nun auch unbedarfte Hobbyfotografen sich durch Bilder, beispielsweise von spielenden Kindern am Strand, strafbar machen könnten (Quelle: Heise).

2. Februar 2015: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Andrea Voßhoff, ist von ihrer früheren Position, die Vorratsdatenspeicherung zu befürworten, abgerückt. *„Ich sehe nicht, dass eine Vorratsdatenspeicherung mit den strengen Auflagen des EuGH noch den Effekt erzielt, den die Sicherheitsbehörden mit diesem Instrument erreichen wollen"*, sagte sie in einem Spiegel-Interview. Angesichts des massiven Eingriffs in die Persönlichkeitsrechte könne sie die Maßnahme nicht mehr befürworten. Als Bundestagsabgeordnete hatte sich Voßhoff noch für die Vorratsdatenspeicherung ausgesprochen (Quelle: Der Spiegel, Heise).

3. Februar 2015: Jeremy Hammond, Mitglied von *Anonymous* und bekannt geworden als Stratfor-Hacker, steht auf einer Terror-Watchlist der US-amerikanischen Behörden. Dies wurde versehentlich bekannt. Beamte sollten das *Terrorist Screening Center* bei einem Kontakt informieren, aber dabei keinen Verdacht erregen. Warum Hammond, der gerade eine zehnjährige Haft-

strafe verbüßt, als Terrorist angesehen wird, ist unklar (Quelle: Daily Dots, Heise).

4. Februar 2015: Die US-Überwachung ausländischer Politiker wurde nach einem Bericht der National Intelligence Agency, der Dachorganisation der US-Geheimdienste, eingeschränkt. Verbindungsdaten von Ausländern sollen nun nach fünf Jahren gelöscht werden, vorausgesetzt, es gibt keine Sicherheitsbedenken. Wenn politische Führungspersönlichkeiten ausgespäht werden, sollten auch die diplomatischen Konsequenzen berücksichtigt werden. Diese Persönlichkeiten sollten nur ausspioniert werden, wenn dringende Sicherheitsbedenken vorlägen. Empörung hatte zuvor unter anderem die Ausspähung des Mobiltelefons von Bundeskanzlerin Angela Merkel ausgelöst (Quelle: National Intelligence Agency, Heise).

5. Februar 2015: Die zweitgrößte US-amerikanische Krankenkasse Anthem ist Opfer eines Hackerangriffs geworden. Dabei wurden die Kundendaten von Millionen Mitgliedern erbeutet, so der Präsident von Anthem, Joseph R. Swedish. Offenbar haben sich die Täter Datensätze mit Namen, Geburtsdaten, Kranken- und Sozialversicherungsnummern, Postanschriften, E-Mail-Adressen, Anstellungsverhältnissen und Gehaltsauskünften verschafft, jedoch keine Kreditkarteninformationen oder Krankenakten (Quelle: Heise).

5. Februar 2015: Der NSA-Untersuchungsausschuss wirft dem Bundesnachrichtendienst vor, ihm eine Falle gestellt zu haben, um ihn zu diskreditieren. Durch eine gezielte Indiskretion sollte dem Ausschuss Geheimnisverrat angelastet werden. In einer halböffentlichen Sitzung hätten BND-Chef Gerhard Schindler und Geheimdienstkoordinator Klaus-Dieter Fritsche detailliert über eine Operation berichtet, und gleichzeitig darauf bestanden, dass die Information nicht an die Öffentlichkeit gelangen dürfe. Es ging dabei um die Drohung des britischen GCHQ, die Kooperation mit dem BND zu beenden (Quelle: Süddeutsche Zeitung, Heise).

6. Februar 2015: Das zuständige Gericht in Großbritannien hat entschieden, dass die Überwachung britischer Bürger durch den Geheimdienst GCHQ im Rahmen der Programme Prism und Upstream gegen die Europäische Menschenrechtskonvention verstößt und damit illegal ist. Durch die Verarbeitung der Daten britischer Bürger und Bürger in Großbritannien, die von der NSA abgegriffen worden sind, sei gegen deren Recht auf Achtung des Privat- und Familienlebens verstoßen worden. Inzwischen halte sich der GCHQ aber an die Gesetze (Quelle: The Guardian, Heise).

9. Februar 2015: Der Berliner Datenschutzbeauftragte Alexander Dix zeigt sich besorgt über private Überwachungskameras, die immer billiger zu kaufen sind und immer größere Verbreitung in Geschäften, Imbissen, Kneipen, Tankstellen und Privatgrundstücken finden. Es gebe dadurch kaum noch unbeobachtete Stellen; das Recht, sich im öffentlichen Raum unbeobachtet zu bewegen, werde immer mehr eingeschränkt. Als Grund dafür sieht Dix die Technikgläubigkeit der Menschen, durch Kameras Sicherheit zu produzieren (Quelle: Heise).

9. Februar 2015: Nach den Anschlägen von Paris ist in Frankreich ein Gesetz in Kraft getreten, das den Terrorismus bekämpfen soll und dafür Provider zur Sperrung von Internet-Seiten auf Verlangen der Regierung verpflichtet. Die Seiten müssen innerhalb von 24 Stunden nach einem entsprechenden Hinweis der zuständigen Behörde gesperrt werden. Die Bürgerrechtsorganisation *La Quadrature du Net* kritisiert die Regelung als Einschränkung der Redefreiheit als wichtigster Errungenschaft der Demokratie (Quelle: The Register, Heise).

9. Februar 2015: Die im „Freihandelsabkommen" TTIP vorgesehene Schiedsgerichtsbarkeit für Investoren (ISDS) wird im EU-Parlament kritisiert. Sie sei angesichts der weit entwickelten Rechtssysteme in den USA und der EU unnötig; ein Schlichtungsverfahren und der normale Rechtsweg reichten aus (Quelle: Heise).

11. Februar 2015: Ein Studie des Bundeskriminalamts (BKA) kommt zu dem Ergebnis, Hacktivisten entstammten der Mittelschicht, seien überwiegend männlich und zwischen 16 und 30 Jahren alt. Sie gingen wie Cyberkriminelle vor, seien dabei aber nicht profitorientiert, sondern verfolgten politische oder moralische Zielsetzungen. Dabei zählt das BKA auch Kim Dotcom, Gründer des Filehosting-Dienstes Megaupload, zu den Hacktivisten. Das BKA fürchtet vor allem die nachrichtendienstliche Lenkung hacktivistischer Projekte (Quelle: Bundeskriminalamt, Heise).

13. Februar 2015: Informationen über Delikte, die die Verkehrssicherheit gefährden, sollen künftig in der gesamten EU weitergegeben werden können. Dafür hat das Europäische Parlament einen Richtlinienentwurf mit 640 Ja-Stimmen beschlossen. Der Entwurf beruft sich auf die Verbesserung der Verkehrssicherheit. Einen ersten Anlauf für den Datenaustausch gab es bereits 2011; die damalige Rechtsgrundlage, die polizeiliche Zusammenarbeit in der EU, befand der Europäische Gerichtshof (EuGH) für nicht ausreichend und den damaligen Richtlinienentwurf deswegen für nichtig (Quelle: Heise).

16. Februar 2015: Tödliche Anschläge in Kopenhagen macht sich die CSU erneut zunutze, die Einführung der Vorratsdatenspeicherung zu fordern. Die SPD solle ihren Widerstand gegen dieses Instrument aufgeben (Spoiler: Sie wird es bald tun). CDU-Innenpolitiker Wolfgang Bosbach erklärte, es gelte, das Thema Vorratsdatenspeicherung auf der Tagesordnung zu halten (Quelle: Die Welt, Nordwest-Zeitung, Heise).

17. Februar 2015: Einer Auskunft der Bundesregierung zufolge beobachtet der Generalbundesanwalt den Einsatz der Überwachungssoftware *FinFisher* gegen die Opposition in Bahrain. Es werde immer noch geprüft, ob es sich dabei um eine geheimdienstliche Tätigkeit handle. Das *European Center for Constitutional Human Rights* (ECCHR) hatte im Oktober 2014 Strafanzeige gestellt (Quelle: Kleine Anfrage der Fraktion *Die Linke*, Heise).

20. Februar 2015: Nach einem Gesetzentwurf von Bundesinnenminister Thomas de Maizière sollen die Überwachungsbefugnisse des Bundesnachrichtendienstes (BND) weiter ausgeweitet werden. Die strategische Fernmeldeaufklärung soll künftig auch zur Abwehr von „Cyber-Gefahren" Daten ausspähen dürfen. Zusätzlich zu den bisherigen Befugnissen soll nun auch im Fall eines *„internationalen kriminellen, terroristischen oder staat-*

lichen Angriffs mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland" der Abgriff der Daten erfolgen dürfen – bei „Gefahr im Verzug" durch das Innenministerium bei Zustimmung des Vorsitzenden des sonst zuständigen Parlamentarischen Kontrollgremiums (PKG). Das Gesetz, das sich auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („Computer-Grundrecht") beruft, bedeutet eine erhebliche Ausweitung der Überwachungsbefugnisse. Der Entwurf wird am 25. März 2015 ohne wesentliche Änderungen vom Bundeskabinett beschlossen (Quelle: Heise).

25. Februar 2015: *Oscar Health*, ein Startup-Unternehmen im Krankenversicherungsmarkt, will die Fitnessdaten seiner Kunden aufzeichnen und einen Bonus an Versicherte zahlen, die ein Trainingsprogramm erfolgreich absolvieren. Die Daten dafür liefern Apps für iPhones und Android-Smartphones. Beim Erreichen bestimmter Fitness-Ziele erhalten Versicherte Smartwatches und Prämien; absolvieren sie das Trainingsprogramm erfolgreich, gibt es einen Dollar pro Tag – maximal 20 Dollar pro Monat (Quelle: New York Times, Heise).

25. Februar 2015: Der Berichtsentwurf für eine geplante EU-Richtlinie sieht vor, Flugpassagierdaten auch auf innereuropäischen Strecken zu sammeln und auszuwerten. Die Daten sollen dabei für fünf Jahre gespeichert, aber nach 30 Tagen anonymisiert werden. Bei Verdacht auf schwere oder terroristische Straftaten sollen Rückschlüsse auf Personen möglich sein (Quelle: netzpolitik.org, Heise).

März 2015

2. März 2015: Die Überwachungsbefugnisse der NSA wurden erneut auf Antrag der US-Regierung durch den *Foreign Intelligence Surveillance Court* (FISC) verlängert. Die Befugnisse gelten nun bis zum 1. Juni 2015; danach laufen einige Bestimmungen des *Patriot Act* aus, unter anderem Abschnitt 215, auf dem die Überwachungsbefugnisse der NSA basieren. Es wird jedoch damit gerechnet, dass der US-Kongress bis dahin eine modifizierte Form der entsprechenden Bestimmungen beschließt (Quelle: Heise).

2. März 2015: Eine Studie des Bayerischen Landesamts für Datenschutzaufsicht in Ansbach hat ergeben, dass in Smart-TVs Datenschutzbestimmungen nicht ausreichend umgesetzt werden. Alle Vorgänge lösen bei einzelnen der 13 überprüften TV-Geräte Datenflüsse zum Hersteller aus. Die TV-Geräte müssen aber in der Grundeinstellung anonym nutzbar bleiben (Quelle: Heise).

4. März 2015: Es gibt Hinweise, dass der gesicherte Blackberry des Vorsitzenden des NSA-Untersuchungsausschusses Patrick Sensburg ausspioniert worden ist. Nach einer Funktionsstörung wurde das Gerät in einem verplombten Behälter zum Bundesamt für Sicherheit in der Informationstechnik (BSI) gesendet; offenbar wurde dieser auf dem Weg geöffnet. Das BSI soll nun prüfen, ob das Mobiltelefon ausgelesen worden ist (Quelle: Die Welt, Heise).

9. März 2015: Im Rahmen einer umfassenden Umstrukturierung soll der US-amerikanische Geheimdienst *Central Intelligence Agency* (CIA) stärker auf Cybersecurity ausgerichtet werden. Dazu soll ein Direktorat für digitale Innovationen eingerichtet werden. Es soll sich um Datenbeschaffung, digitale Spionage, Cybersecurity und Schutz der eigenen Infrastruktur kümmern. Die Bereiche der CIA sollen stärker miteinander verzahnt werden (Quelle: Washington Post, Heise).

10. März 2015: Rund 20.000 Menschen aus Medien, Politik und Diplomatie wurden offenbar in Mazedonien jahrelang gezielt ausspioniert. Die Opposition hat angebliche Mitschnitte von Telefonaten der Regierung veröffentlicht. Demnach bestehe ein Netzwerk aus Medien, Justiz, Polizei, Regierung und Geheimdiensten, das die Gesellschaft kontrolliere. Initiator der Ausspähung ist der Opposition zufolge Premierminister Nikola Gruevski. Die Regierung spricht von einem Putschversuch (Quelle: Der Standard, Economist, Heise).

10. März 2015: Einem Bericht von *The Intercept* zufolge arbeiten NSA und CIA gemeinsam daran, Sicherheitsvorkehrungen von Microsoft und Apple zu umgehen und Daten von deren Nutzern auszuspähen. Offenbar werden jährlich in einer geheimen Veranstaltung Sicherheitslücken diskutiert und Entwicklungswerkzeuge manipuliert (Quelle: The Intercept, Heise).

11. März 2015: Die Regelung zur Vorratsdatenspeicherung in den Niederlanden muss vorerst außer Kraft gesetzt werden. Nachdem der Europäische Gerichtshof (EuGH) die entsprechende EU-Richtlinie für rechtswidrig erklärt hatte, hat dies nun ein Gericht in Den Haag entschieden. Die Vorratsdatenspeicherung verletze das Recht auf Achtung des Privatlebens. Gegen die in den Niederlanden gültige Speicherfrist von einem Jahr hatten Telekommunikationsanbieter, Juristen und Journalisten geklagt (Quelle: netzpolitik.org, Heise).

12. März 2015: In Bulgarien hat das Verfassungsgericht die Regelung zur Vorratsdatenspeicherung außer Kraft gesetzt. Ombudsmann Konstantin Pentschew hatte in seiner Klage argumentiert, die Freiheit und das Geheimnis der Korrespondenz, die in der bulgarischen Verfassung garantiert sind, würden durch die Speicherung verletzt (Quelle: Heise).

14. März 2015: Die Regierungen der EU-Mitgliedstaaten weichen offenbar die Regelungen der geplanten EU-Datenschutz-Grundverordnung deutlich auf. Standards von Grundprinzipien des Datenschutzes, der Zweckbindung und der Datensparsamkeit, sollen dabei reduziert und „legitime Interessen" von Firmen und Ämtern an Personendaten über die Interessen der Betroffenen gestellt werden. Der Berichterstatter für die Datenschutzreform im Europäischen Parlament, Jan Philipp Albrecht hatte bereits zuvor erklärt, damit sei eine *„Rote Linie überschritten"*. Das Parlament könne einer solchen Position nicht zustimmen; dies würde das Ende der Datenschutzreform bedeuten. Unverständlich sei auch, dass sich offenbar die deutsche Bundesregierung für einen niedrigeren Standard als in der heute gültigen Richtlinie von 1995 einsetze (Quelle: statewatch.org, netzpolitik.org, Heise).

15. März 2015: Wirtschaftsminister Sigmar Gabriel (SPD) setzt sich für die Wiedereinführung der 2010 vom Bundesverfassungsgericht zurückgewiesenen Vorratsdatenspeicherung ein.

„Wir brauchen das … wir erleben doch gerade, dass die Welt ziemlich gefährlich geworden ist", erklärte er. Es müsse im verfassungsrechtlich vertretbaren Umfang reagiert werden können. Gabriel hatte die Datenspeicherung im Gegensatz zu Justizminister Heiko Maas bereits zuvor befürwortet (Quelle: Deutschlandfunk, netzpolitik.org, Heise).

17. März 2015: Die Spielzeugpuppe *Hello Barbie* spricht beim Spielen mit den Kindern und zeichnet dabei deren Gespräche auf. Dadurch können die Gespräche mit Spracherkennungssoftware ausgewertet und passende Antworten generiert werden. Die Puppe stelle Fragen, deren Beantwortung sensible Informationen über das Kind und seine Familie liefere, die für Marketing genutzt werden können, so die *Campaign for a Commercial-free Childhood* (CCFC). Offenbar werden die Daten auch weiterverarbeitet, um die Spracherkennungssoftware weiterzuentwickeln, und darüberhinaus an Dritte weitergegeben. Nach Aussagen des Herstellers der Spracherkennungssoftware *ToyTalk* sei für das Mitschneiden der Gespräche das Einverständnis der Eltern erforderlich; die Daten würden nicht für Marketingzwecke eingesetzt (Quelle: CCFC, Washington Post, Heise).

17. März 2015: Die französische Regierung plant eine Reform des Geheimdiensts, bei der dessen Befugnisse erweitert werden sollen. Ohne richterliche Kontrolle dürften dann Wohnungen, Büros und Autos der Zielobjekte überwacht werden; dies sei aber heute bereits Praxis. Weitere Befugnisse seien der Einsatz von IMSI-Catchern, erweiterte Möglichkeiten des Abhörens von Skype und die Verfolgung von Kommunikation über Facebook und Twitter. *Human Rights Watch* kritisiert den Entwurf, insbesondere die Kompetenz für den Premierminister, Überwachungsmaßnahmen zu autorisieren und die Pflicht für Provider, *„heimlich unspezifizierte, vom Staat vorgegebene Mittel zum Analysieren verdächtigen Verhaltens"* einzusetzen (Quelle: Le Monde, Figaro, Telepolis, netzpolitik.org, Heise).

26. März 2015: In einem Schnellverfahren hat das bulgarische Parlament die zuvor vom Verfassungsgericht gestoppte Vorratsdatenspeicherung wieder eingeführt. Dabei gelten nun kürzere Speicherfristen von einem halben anstatt einem Jahr. Die Arbeit der Sicherheitsdienste dürfte nicht erschwert werden, so die konservative Regierungspartei (Quelle: Heise).

26. März 2015: Einem Vertreter der EU-Kommission zufolge schützt des *Safe-Harbour*-Abkommen nicht ausreichend vor Datenmissbrauch. Wer fürchtet, dass seine Daten vor der NSA nicht sicher seien, *„sollte sich überlegen, ob er seinen Facebook-Account nicht besser löscht"*, erklärte er. *„So wie* Safe Harbour *derzeit in den USA rechtlich verankert ist, gibt es keine Garantie dafür, dass fundamentale EU-Datenschutzrechte beachtet werden"* (Quelle: Irish Times, Heise).

27. März 2015: Das australische Parlament hat eine sehr weitgehende Regelung zur Vorratsdatenspeicherung verabschiedet. Provider müssen Verbindungs- und Standortdaten einschließlich Geräteadressen zwei Jahre lang aufbewahren. Für den Zugriff benötigen Polizei und Geheimdienste in der Regel keine richterliche Genehmigung; diese ist nur erforderlich, wenn auf Daten von Journalisten zugegriffen werden soll. Betroffene müssen nicht über den Datenzugriff benachrichtigt werden (Quelle: Heise).

31. März 2015: Nach Vorstellung von Verteidigungsministerin Ursula von der Leyen soll Deutschland gemeinsam mit Italien und Frankreich eine Kampfdrohne entwickeln. Die Verteidigungsexpertin der Linken, Christine Buchholz, erklärte dazu, Deutschland dürfe sich *„nicht am völker- und menschenrechtswidrigen internationalen Drohnenkrieg beteiligen"* (Quelle: Der Spiegel, Heise).

April 2015

8. April 2015: Die US-Drogenpolizei hat offenbar jahrelang Verbindungsdaten auf Vorrat gespeichert und ausgewertet. Dies ist nun Gegenstand eines Gerichtsverfahrens, das *Human Rights Watch* und die *Electronic Frontier Foundation* (EFF) angestrengt haben. In der Klage wird gefordert, die Auswertung der Daten zu unterbinden und rechtswidrig gesammelte Informationen zu löschen (Quelle: EFF, netzpolitik.org, Heise).

9. April 2015: Der französische Fernsehsender *TV5Monde* ist offenbar das Ziel islamistischer Hacker geworden. Dabei fielen alle Kanäle des Senders zeitweise aus; auf den Seiten im Web und bei Facebook waren islamistische Drohungen zu lesen. Nach Aussage der IT-Chefin, Hélène Zemmour, hatten die Angreifer gleichzeitig die internen IT-Systeme und die Sendeanlagen unbrauchbar gemacht und Web-Seite, Facebook- und Twitter-Konto unter ihre Kontrolle gebracht (Quelle: FranceTVInfo, Heise).

10. April 2015: Die Menschenrechtsorganisation *Amnesty International* reicht gemeinsam mit den Organisationen *Liberty* und *Privacy International* beim Europäischen Gerichtshof für Menschenrechte Klage gegen Großbritannien wegen der Überwachungspraxis des Geheimdienstes GCHQ ein. Basis sind Dokumente, die Edward Snowden zugänglich gemacht hatte. Obwohl ein Teil der Praktiken des GCHQ in Großbritannien für illegal erklärt worden waren, kann die Überwachung von Telefon- und E-Mail-Verkehr fortgesetzt werden (Quelle: Amnesty International, netzpolitik.org, Heise).

10. April 2015: Die Anzahl der Abfragen von Bankkonten durch deutsche Behörden ist laut einer Statistik des Bundesfinanzministeriums von 142.000 im Jahr 2013 auf 230.000 im Jahr 2014 gestiegen, das entspricht einem Wachstum von mehr als 60 %. Die Bundesdatenschutzbeauftragte Andrea Voßhoff stellt dazu fest, dass die Abfragen nicht mehr nur das Austrocknen der Finanzströme von Terroristen zum Ziel hätten, wofür das Instrument ursprünglich vorgesehen gewesen sei. Inzwischen würden ohne Anlass alle Kontoinhaber in Deutschland erfasst (Quelle: Heise).

17. April 2015: Die bisherigen strengen Vorgaben für die Weitergabe von Daten aus der LKW-Maut sollen aufgeweicht werden. Die Große Koalition will die Daten auch für *„Zwecke der Verkehrslenkung und Verkehrsforschung vollständig anonymisiert und in enger Abstimmung mit den Datenschutzbeauftragten"* Dritten zugänglich machen. Die strenge Bindung an Abrechnungszwecke war bei Einführung der Maut Voraussetzung gewesen; bereits in der Vergangenheit gab es aber wiederholt Begehrlichkeiten, die Daten auch anderweitig zu nutzen (Quelle: Handelsblatt, Heise).

19. April 2015: Der Luftwaffenstützpunkt Ramstein spielt offenbar eine zentrale Rolle im Drohnenkrieg „gegen den Terror" der USA. Geheimen Dokumenten zufolge werden praktisch alle Drohnenangriffe der US-Air-Force über Ramstein abgewickelt. Ein US-Amerikaner, der mit dem Programm vertraut sei, habe die Dokumente weitergegeben: *„Von Ramstein wird das Signal übermittelt, das den Drohnen befiehlt, was sie tun sollen. Ohne Ramstein könnte keine der Drohnen gesteuert werden – jedenfalls nicht in der bisher geübten Weise."* Bereits vor einem Jahr gab es Hinweise auf diese zentrale Rolle; der ehemalige Drohnenpilot Brandon Bryant hatte damals erklärt, der Drohnenkrieg des US-Militärs sei ohne Deutschland nicht möglich (Quelle: Der Spiegel, The Intercept, NDR, WDR, Süddeutsche Zeitung, netzpolitik.org, Heise).

20. April 2015: Die Vorratsdatenspeicherung soll noch vor der Sommerpause im Schnellverfahren vom Deutschen Bundestag verabschiedet werden. Bundesjustizminister Heiko Maas, der sich zuvor immer gegen die Vorratsdatenspeicherung ausgesprochen hatte, hat nach vollzogener Kehrtwende „Leitlinien" vorgelegt, die er nun zügig zu einem Gesetzentwurf weiterentwickeln und im Bundeskabinett beschließen lassen will. Die Leitlinien sehen eine Speicherfrist von 10 Wochen vor. Unter anderem sollen offenbar Standortdaten von jedem Kommunikationsvorgang archiviert werden; dies wäre wohl auch der Fall, wenn ein Mobiltelefon automatisch prüft, ob bei sozialen Netzwerken oder Chat-Diensten Nachrichten eingegangen sind. Die liberalen Politiker Wolfgang Kubicki und Ex-Bundesinnenminister Gerhart Baum haben im Fall der Verabschiedung erneut Klage vor dem Bundesverfassungsgericht angekündigt. Aus Sicht der Bundesdatenschutzbeauftragten Andrea Voßhoff ist zweifelhaft, ob die vorgelegten Leitlinien mit der Europäischen Grundrechtecharta vereinbar sind (Quelle: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, taz, Neues Deutschland, netzpolitik.org, Heise).

22. April 2015: Der Betreiber des Internetknotens DE-CIX in Frankfurt am Main hat Klage beim Bundesverwaltungsgericht gegen die Ausleitung von Daten durch den BND angekündigt. Bei einer Niederlage würde man auch vor das Bundesverfassungsgericht gehen. Aufsichtsrat Klaus Landefeld erklärte, dass das Unternehmen die Maßnahmen für unzulässig halte. Ein Gutachten zur Unterstützung der Klage wurde unter anderem vom ehemaligen Bundesverfassungsrichter Hans-Jürgen Papier erstellt (Quelle: netzpolitik.org, Heise).

23. April 2015: Das Projekt *Eikonal*, mit dem der BND einen Frankfurter Netzknoten ausspioniert und Daten an die NSA weitergeleitet hat, war stärker gegen europäische und deutsche Interessen gerichtet, als bisher bekannt. Bis zu 40.000 Selektoren – etwa IP-Adressen, Mobiltelefonnummern oder Suchkriterien – waren gegen diese Interessen gerichtet. Scheinbar wurden auch Politiker gezielt und unrechtmäßig ausgespäht. Dieter Urmann, früherer Leiter der Abteilung Technische Aufklärung, erklärte, dass die Ausspähung der NSA beispielsweise auch auf die Begriffe „EADS", „Eurocopter" und „französische Behörden" abgezielt hätte (Quelle: Der Spiegel, netzpolitik.org, Heise).

25. April 2015: Holger Münch, Präsident des Bundeskriminalamts (BKA) kündigt an, dass eine von seiner Behörde entwickelte Software zur Ausspähung der Computer und Smartphones Tatverdächtiger im Herbst 2015 einsatzbereit sein soll. Die Software, in der Öffentlichkeit als Staatstrojaner oder Bundestrojaner bezeichnet, kann beispielsweise Internet-Telefonie, Messenger-Dienste und E-Mail-Verkehr protokollieren (Quelle: Der Spiegel, Heise).

26. April 2015: Medienberichten zufolge ist dem Bundeskanzleramt bereits seit 2008 bekannt, dass die NSA versucht hat, dem BND illegale Ausspähziele unterzuschieben (Quelle: netzpolitik.org, n-tv, Heise).

28. April 2015: Das Europäische Parlament hat mit großer Mehrheit einen Verordnungsentwurf beschlossen, nach dem ab Ende März 2018 bei neu eingeführten Automobil-Modellreihen der Einbau des Notrufsystems eCall vorgeschrieben ist. Der Notruf soll bei einem Unfall manuell oder automatisch, wenn der Airbag ausgelöst wurde, die Notrufnummer 112 anwählen und Fahrzeugklasse, Treibstoffart, Zeit und Ort des Unfalls übermitteln. Die Daten dürfen nicht ohne Genehmigung an Dritte weitergegeben werden und müssen vom Fahrer dauerhaft gelöscht werden können (Quelle: Heise).

29. April 2015: Im Zusammenhang mit dem BND-Skandal hat die Bundesregierung offenbar falsche Angaben gegenüber Parlamentariern gemacht. In der Antwort auf eine Kleine Anfrage der Linksfraktion wurde angegeben, es lägen keine Erkenntnisse zu Wirtschaftsspionage durch die NSA oder andere US-Dienste in anderen Staaten vor. Mittlerweile scheint aber klar, dass der BND das Bundeskanzleramt bereits seit Jahren auf Versuche der NSA hingewiesen hat, Wirtschaftsspionage in Europa und Deutschland zu betreiben (Quelle: Deutscher Bundestag, Heise).

30. April 2015: Das Verfassungsgericht der Slowakei hat entschieden, dass die Bestimmungen des dortigen Gesetzes zur Vorratsdatenspeicherung gegen die Verfassung der Slowakischen Republik, die Europäische Menschenrechtskonvention und die Charta der Grundrechte der Europäischen Union verstoßen. Geklagt hatte das *European Information Society Institute* (EISI) (Quelle: netzpolitik.org)

30. April 2015: Das Flugzeugunternehmen *Airbus* kündigt an, Strafanzeige gegen Unbekannt wegen Industriespionage zu erstatten. Offenbar wurde der Konzern und das Vorgängerunternehmen EADS jahrelang von englischsprachigen Geheimdiensten, den *Five Eyes*, ausgespäht. Tom Enders, der Chef von *Airbus*, soll sich über das Schweigen der Bundesregierung verärgert gezeigt haben; er forderte sie auf, endlich Stellung zu den Vorwürfen zu beziehen (Quelle: Der Spiegel).

Stefan Hügel

Stefan Hügel ist Vorsitzender des FIfF, arbeitet als IT-Berater und lebt in Frankfurt am Main

Marie-Theres Tinnefeld

Jan Philipp Albrecht: „Finger weg von unseren Daten! Wie wir entmündigt und ausgenommen werden“

Jan Philipp Albrecht ist Parlamentsabgeordneter und stellvertretender Vorsitzender im Innen- und Justizausschuss im Europäischen Parlament (EP) und dort insbesondere Berichterstatter der geplanten EU-Datenschutz-Grundverordnung (DS-GVO), die seit drei Jahren in Arbeit ist und Ende 2015 vorliegen soll. Dann würden sich die Verhandlungen im Trilog zwischen Rat, Parlament und Kommission (Art. 294 AEUV) anschließen. Die vorliegenden Ausführungen des engagierten Politikers können als Erläuterung des Datenschutzreformprozesses auf EU-Ebene betrachtet werden, auf deren Agenda ein wirkkräftiger Datenschutz im globalen 24/7-Milieu (7-Tage-Woche im 24-Stundentakt) steht. Es geht dabei um die datenschutzrechtliche Einbindung persönlicher Zeiten, Aktivitäten und Daten in die Parameter der digitalen Kommunikation, es geht um *Big Data* auf den Halden der Geheimdienste und mächtiger Suchdienste, die nach spezifischen, häufig diskriminierenden, Such-Kriterien ausgewertet werden und eine flächendeckende Kontrolle ermöglichen.

Jan Philipp Albrecht (2014): Finger weg von unseren Daten! Wie wir entmündigt und ausgenommen werden, München: Knaur Verlag, 192 Seiten, Preis €7,00 ISBN 978-3426-78687-1

Das Taschenbuch beginnt mit dem Thema „der Globalisierung als gesellschaftlicher Umbruch und der Digitalisierung als technischer Katalysator dieses Umbruchs“ (S. 11), in dem der Aufbruch in eine selbstbestimmte Zukunft bislang verpasst worden sei (S.16). An praxisnahen Beispielen fordert der Verfasser den verfassungsrechtlich gebotenen Schutzauftrag des nationalen Staates für den Datenschutz ein (S. 28). Es gelte das Grundrecht auf Datenschutz in „letzter Schlacht um unsere Freiheit“ zu verteidigen (S. 35). Das Ende der Selbstbestimmung könne insbesondere durch einen effektiven europäischen und weltweiten Datenschutz verhindert werden (S. 36-52). In weiterer Folge legt der Verfasser dar, auf welche Weise der „Ausverkauf unserer Daten“, etwa der Gesundheitsdaten gegenüber Versicherungen oder in App-Käufen eingedämmt und gleichzeitig die digitale Daten-Souveränität aufgrund von menschenrechtlichen Regelungen gegenüber repressiven Staaten wie China und Russland, aber auch gegenüber Spähaktionen ausufernder Geheimdienste gestärkt werden kann (S. 53-69). In diesem Kontext mahnt der Verfasser technischen Sachverstand an, ohne den ein effektiver Datenschutz nicht realisierbar sei (S. 70-94). Die „vernetzte Gesellschaft“ könne an freiheitlicher Demokratie durch die Informationsfreiheit wie im „arabischen Frühling“ sowie der Stärkung des informationellen Selbstbestimmungsrechts gewinnen (S. 95-106).

Albrecht tritt für eine „digitale Unabhängigkeitserklärung“ in Form einer wirkkräftigen EU-Regelung ein (S. 107-115) und setzt sich detailliert mit der europäischen Datenschutzreform, den politischen Barrieren in EU-Mitgliedstaaten etwa in Deutschland auseinander (S. 116-146). Die digitale Datenverarbeitung ist zwar in allen wirtschaftlichen und gesellschaftlichen Bereichen eine unabdingbare Voraussetzung zur Bewältigung der jeweiligen und häufig vernetzten Aufgaben. In Bezug auf die öffentliche Verwaltung und die speziellen Traditionen in den EU-Mitgliedstaaten wäre es allerdings wünschenwert, wenn sich der Verfasser kritisch mit der Frage auseinandergesetzt hätte, ob der Datenschutz für die öffentliche Verwaltung statt in der Verordnung nicht in einer Richtlinie mit Gestaltungsspielräumen für die Mitgliedstaaten geregelt werden sollte (s. u. a. S. 140). Albrecht setzt sich desweiteren mit den übersteuerten Sicherheitsbestrebungen in der Politik auseinander, die mit der Injurie arbeitet, dass diejenigen, die dagegen opponieren „etwas zu verbergen“ haben. Zu Recht kritisiert der Autor die Erfindung eines obskuren „Grundrechts auf Sicherheit“. Der Datenschutz diene nur in einem erweiterten Sinn auch der Sicherheit von Bürgern dergestalt, dass sie ihre europäischen Grundrechte ohne maßlose Überwachung, Registrierung oder diskriminierende Profilbildung wahrnehmen können (S.147-172). Albrecht vertieft diese Frage in seinen Ausführungen „Der politisch-industrielle Komplex“ im Kontext der Entwicklung und Finanzierung von neuer Sicherheitstechnik und die schwammige völkerrechtliche Einbindung etwa im Fall von video- und sensorbestückten Drohnen (S.173-181). In Anbindung an den mutigen Schritt des Whistleblowers E. Snowden verfasst der Autor ein „Plädoyer an Politik und Gesellschaft“. Er wendet sich gegen den Export von IT-Systemen für Computer- und Smartphone-Überwachung sowie gegen eine wachsende Zensurinfrastruktur, wo staatliche Kräfte und ein „kapitalistischer“ Markt Hand in Hand tätig werden (S.182-188). Bei der von Albrecht aufgezeigten veränderten Aufgabenstellung im Recht des Datenschutzes ist es unverzichtbar, die Betroffenenrechte über die EU-Grenzen hinaus auch technisch zu stärken, eine sachgerechte Ausstattung der Datenschutzbehörden zu garantieren, die Kontrolle im öffentlichen Bereich und die Aufsicht über den privaten Bereich zusammenzulegen. Das verständlich und kenntnisreich geschriebene Buch ist geeignet, die gesellschaftliche Debatte darüber anzustossen, was notwendig ist, um den europäischen Datenschutz mit Inhalt zu füllen.

Die Rezension erschien zunächst in DuD Datenschutz und Datensicherheit 4/2015. *Wir danken Autorin und Redaktion herzlich für die freundliche Genehmigung zum Nachdruck.*

FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

FIfF-Mailinglisten

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder
Beiträge an: *mitglieder@lists.fiff.de*

Mailingliste Videoüberwachung:
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

FIfF online

Das ganze FIfF
www.fiff.de
Twitter FIfF e.V. – *@FIfF_de*

Cyberpeace
cyberpeace.fiff.de
Twitter Cyberpeace – *@FIfF_AK_RUIN*

Faire Computer
blog.faire-computer.de
Twitter Faire Computer – *@FaireComputer*

Newsletter (im Mitglieder-Wiki)
https://wiki.fiff.de/wiki/NewsLetter

FIfF-Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Leonie Dreschler-Fischer** (Hamburg); Prof. Dr. **Christiane Floyd** (Hamburg); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (Konstanz); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (Marburg); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (München); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr. **Klaus-Peter Löhr** (Berlin); **Werner Mühlmann** (Oppung); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Bremen); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); Prof. Dr. **Dirk Siefkes** (Berlin); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Rainer Rehak – Berlin
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Sara Stadler – Bremen
Thomas Reinhold (Campaigning) – Lübeck

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 100 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Sara Stadler
Schwerpunktredaktion	Eberhard Zehendner, Stefan Hügel
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de.* Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	Stefan Hügel, Eberhard Zehendner
Druck	Meiners Druck, Bremen

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

31. FIfF-Konferenz 2015
6. bis 8. November, Friedrich-Alexander-Universität in Erlangen
„Kommerzialisierung des Sozialen: Markt und Macht im Zeitalter der digitalen Kompletterfassung"

FIfF-Vorstandssitzung
27. Juni, 10:30 bis 17:00 Uhr, Bremen,
Uni Bremen, OAS 3000 Linzer Str. 9a

FIfF-Kommunikation
3/2015 »Rüstung und Informatik/Cyberpeace«
Dietrich Meyer-Ebrecht, Hans-Jörg Kreowski u. a.
Redaktionsschluss: 7. August 2015

4/2015 »Cybercrime«
Eberhard Zehendner
Redaktionsschluss: 6. November 2015

1/2016 »31. FIfF-Konferenz 2015«
Stefan Hügel u.a.
Redaktionsschluss: 5. Februar 2016

W&F – Wissenschaft & Frieden
1/15 – Afrika (mit Dossier 77: Rechter Terror in Deutschland)
2/15 – Technikkonflikte (mit Dossier 78: Zivilklauseln)
3/15 – Friedensverhandlungen (mit Dossier 79: Kriegführung im Cyberspace)

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#206/207 (2-3/14) – Geheimdienstliche Kommunikationsüberwachung außer Kontrolle?
#208 (4/14) – Europäische Abschottungstendenzen
#209 (1/15) – Cybersicherheit

DANA – Datenschutz-Nachrichten
3/14 – Datenschutz im Reiseverkehr
4/14 – Big Data
1/15 – Mobilität/Telematik
2/15 – Flüchtlinge und Datenschutz

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung) und Sara Stadler
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

neue Bankverbindung
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Schluss FIfF

Eberhard Zehendner

Blindes Vertrauen in Passwort-Checker?

„Dieses Kennwort-Prüfprogramm erfasst, speichert und überträgt keine Daten." So ist es häufig zu lesen, so sollte es auch sein – ist es aber bei Weitem nicht immer. Insbesondere nach Bekanntwerden massiven Ausspähens von Log-in-Daten liegen die Nerven blank, wird schnell zu einem Passwort-Checker gegriffen, um die Stärke des eigenen Passworts zu überprüfen. Neben zumindest gut gemeinten legitimen Seiten erscheinen dann verstärkt Fälschungen im Netz, deren einziger Zweck darin besteht, Benutzerkennungen und zugehörige Passwörter zu „phishen".

Zeichnung: Conrad Arthur Zehendner

Da muss es doch das Herz wärmen, wenn einem wie Alastair Coote auf seiner Seite *http://www.is-mytwitterpasswordsecure.com/* in schmunzelnd-erzieherischer Absicht die perfekte Fälschung der Fälschung gelingt. Nachahmung unbedingt erwünscht!

Quelle: Paul Ducklin: Beware Twitter "password check" sites - there are fakes, and there are fake fakes! Naked Security, 24. April 2013, https://nakedsecurity.sophos.com/2013/04/24/beware-twitter-password-check-sites-there-are-fakes-and-there-are-fake-fakes/

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.