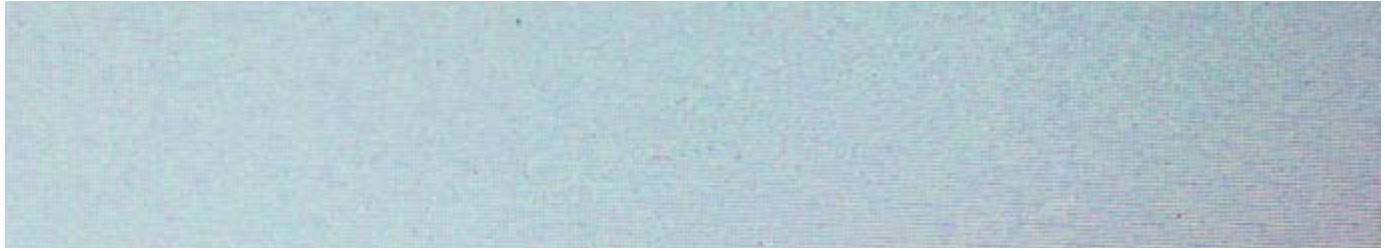
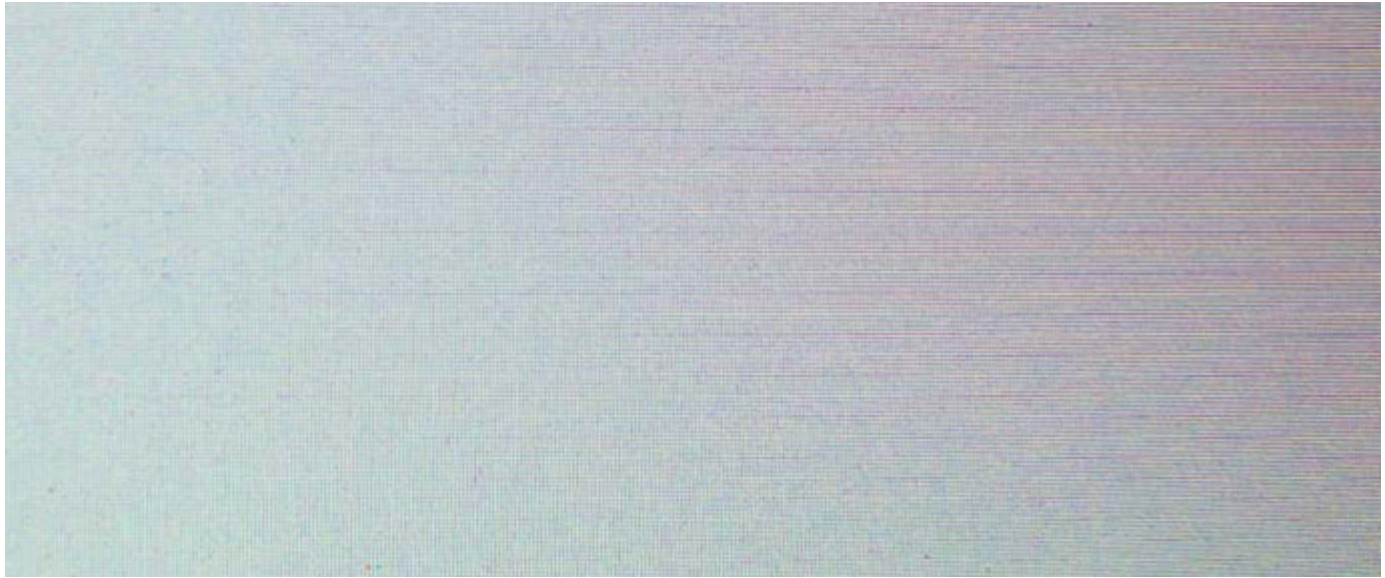


Digitale Schwellen

Privatheit und Freiheit in der digitalen Welt

Mit Beiträgen von: Ulrike Ackermann, Marion Albers, Jan Philipp Albrecht, Leonard Dobusch, Hannes Federrath, Marco Ghiglieri, Yvonne Hofstetter, Stefan Köpsell, Benjamin Lange, Johannes Lichdi, Johannes Näder, Marcel Rosenbach, Peter Schaar, Hervais Simo, Matthias Spielkamp, Holger Stark, Michael Waidner



weiterdenken
HEINRICH BÖLL STIFTUNG SACHSEN
NETZPOLITIK

DIGITALE SCHWELLEN – PRIVATHEIT UND FREIHEIT IN DER DIGITALEN WELT

Digitale Schwellen – Privatheit und Freiheit in der digitalen Welt

Herausgegeber:
Weiterdenken - Heinrich-Böll-Stiftung Sachsen
Johannes Lichdi

Diese Publikation wird unter den Bedingungen einer Creative-Commons-Lizenz veröffentlicht: http://creativecommons.org/licenses/by-nc-nd/3.0/de/ Eine elektronische Fassung kann heruntergeladen werden. Sie dürfen das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen. Es gelten folgende Bedingungen: Namensnennung: Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen (wodurch aber nicht der Eindruck entstehen darf, Sie oder die Nutzung des Werkes durch Sie würden entlohnt). Keine kommerzielle Nutzung: Dieses Werk darf nicht für kommerzielle Zwecke verwendet werden. Keine Bearbeitung: Dieses Werk darf nicht bearbeitet oder in anderer Weise verändert werden.

Weiterdenken – Heinrich-Böll-Stiftung Sachsen, Schützengasse 18, 01067 Dresden
fon 0049 351 49 43 311 | fax 0351 49 43 411 | www.weiterdenken.de

© Weiterdenken – Heinrich-Böll-Stiftung Sachsen

Redaktionsschluss: April 2015
Druck: Union-Druckerei Dresden
Satz/Layout, Grafik: Antje Meichsner
Fotoserie «Annäherung an den Bildschirm»: Antje Meichsner

Bestelladresse:
Weiterdenken - Heinrich-Böll-Stiftung Sachsen | www.weiterdenken.de

NETZPOLITIK

Digitale Schwellen

Privatheit und Freiheit in der digitalen Welt

INHALT

Vorwort 7

Einführung 11

I. Unsere alltägliche Überwachung 19

Holger Stark und Marcel Rosenbach:
Warum und wie die NSA das Internet beherrschen will 21

Matthias Spielkamp: Journalismus nach Snowden 31

Johannes Lichdi: Fallbeispiel Dresden, 19. Februar 2011:
Von der körperlichen Raumkontrolle zur elektronischen Kommunikationskontrolle 39

Hannes Federrath: «Mein Smartphone weiß mehr als ich» –
Beobachtung und Sammlung von Nutzeraktivitäten 57

Marco Ghiglieri, Benjamin Lange, Hervais Simo, Michael Waidner:
Security und Privacy bei Smart TVs – Bedrohungspotential und technische Lösungsansätze 67

II. Regulierung der Digitalen Revolution? 85

Peter Schaar: Lässt sich die globale Überwachung einhegen? 87

Jan Philipp Albrecht: EU-Datenschutzreform: Blockade made in Germany 99

Stefan Köpsell:
Dezentralität, Diversität und Redundanz – Bausteine für eine bürgerorientierte Netzwelt 105

Leonhard Dobusch:
Probleme digitaler Plattformregulierung zwischen Verboten, Geboten und Entflechtung 115

III. Die Herausforderung für Freiheit und Demokratie 121

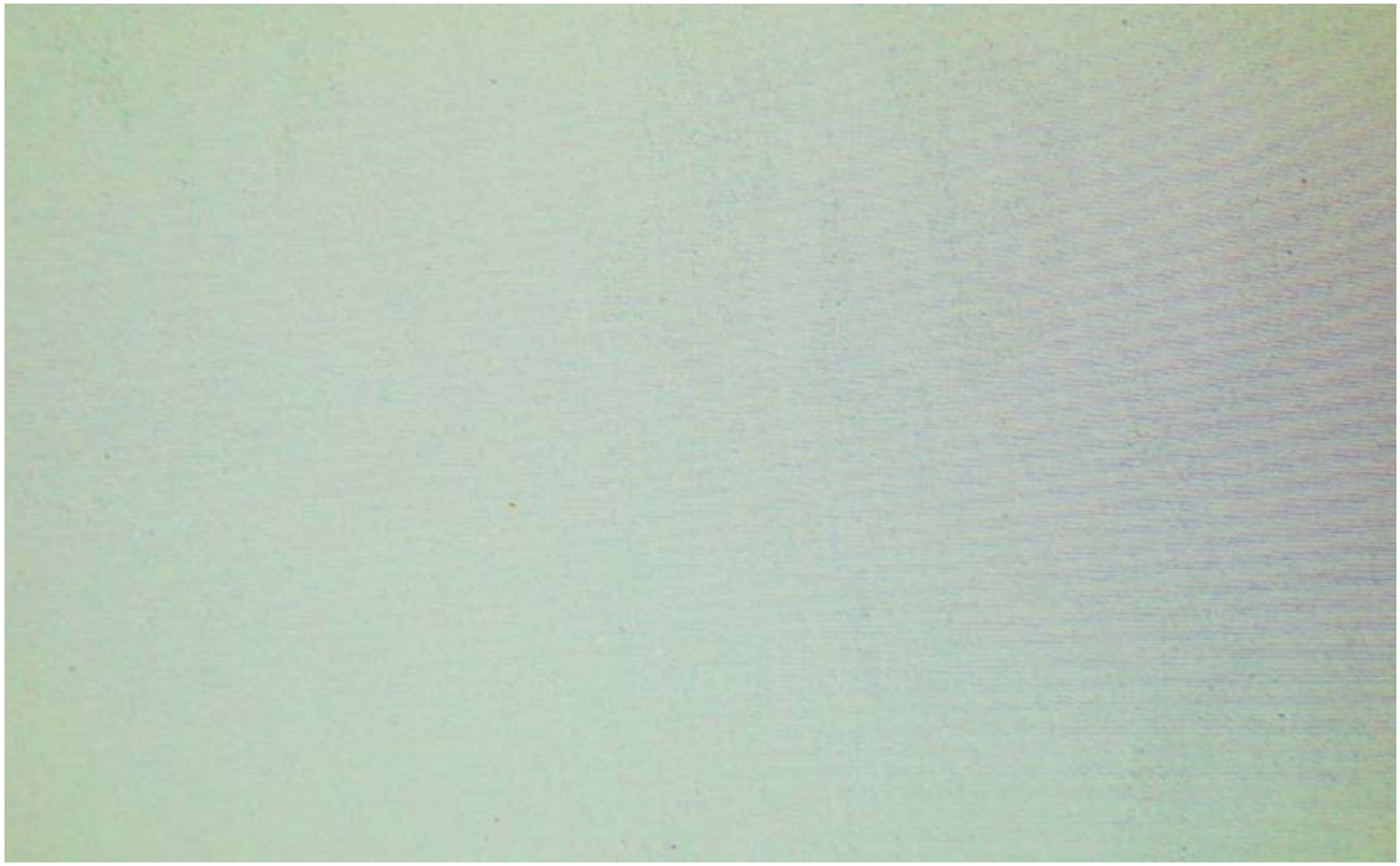
Ulrike Ackermann: Digitale Revolution – Eine Herausforderung für die Freiheit 123

Marion Albers: Zukunftsszenarien polizeilicher Überwachung 135

Johannes Näder: Weder Fluch noch Segen –
Die digitale Schwelle als Herausforderung der demokratischen Gesellschaft 149

Yvonne Hofstetter:
Big Data: Von der Analyse riesiger Datenmengen zur Steuerung des Menschen 163

Autorinnen und Autoren 175



Vorwort

Eine Welt digitaler Techniken im weitesten Sinne verändert die Kommunikationsbeziehungen, die sozialen Beziehungen der Menschen untereinander und damit auch die sozialen Verhältnisse der Menschen in der Gesellschaft in fundamentaler Weise. Wir stehen ganz offensichtlich erst an der Schwelle des Verstehens dieser komplexen und alle Lebensbereiche verändernden Revolution.

Die technischen Möglichkeiten, die unser Leben ja auch erleichtern können und schöner und klüger machen, werden in großer Geschwindigkeit erweitert, immer neue Schwellen des Mach- und Denkbaren werden permanent überschritten.

Unser alltägliches Leben kann inzwischen mühelos aufgrund der hinterlassenen Datenspuren rekonstruiert werden. Staaten scheinen durch umfassende und präventive Überwachung mehr Sicherheit für Bürger_innen bieten zu können. Spätestens seit den Enthüllungen von Edward Snowden sollte klar sein, dass das, was technisch an Überwachung möglich ist, auch tatsächlich für Überwachung genutzt wird. Auch hier sehen wir, wie sich immer neue Schwellen zwischen den Freiheiten, die das digitale Netz uns bietet, und den unsere Freiheit und Bürgerrechte einengenden digitalen Kontrollmechanismen zeigen.

Welche Bedingungen braucht und welche Chancen hat die zivilgesellschaftliche Rekonstruktion digitaler Freiheit durch die Entwicklung freier, nicht überwachungsgeeigneter Software oder die Bereitstellung nicht überwachungsgeeigneter Versorgungsstrukturen? Welches sind die Möglichkeiten, um die Strukturen der heraufziehenden digitalen Gesellschaft in freiheitsgeeigneter Weise umzuprägen oder neu zu schaffen?

Die Rückeroberung eines privaten und öffentlichen Freiheitsraums wäre auch Voraussetzung einer freiheitlichen Demokratie, die einen militärisch, sicherheitsmäßig und kommerziell geprägten digitalen Raum nicht wird überleben können. Dass hier eine Herausforderung für uns liegt, ist unbestreitbar. An Lösungen haben Techniker_innen, Politiker_innen, Jurist_innen, Künstler_innen und politisch engagierte Bürger_innen gearbeitet, oft blieben und bleiben sie aber dabei hinter den Schwellen ihrer Professionen stehen. Erst seit Kurzem bewegen sie sich aufeinander zu, um im Austausch der verschiedenen Erfahrungen und Herangehensweisen Perspektiven für ein freiheitsorientiertes Netz zu entwickeln.

Der vorliegende Band beleuchtet in wesentlichen Ausschnitten den aktuellen Stand und diskutiert Chancen digitaler Strukturen, Rahmenbedingungen, Technik und Verhaltensweisen, die an Freiheit und der Möglichkeit von Privatheit orientiert sind.

Der vorliegende Sammelband ist Ergebnis einer Veranstaltungsreihe, die wir von April bis Juli 2014 im Kleinen Haus des Staatsschauspiels Dresden durchgeführt haben. Die Reihe fand in Kooperation mit dem Staatsschauspiel Dresden und dem Lehrstuhl für Datenschutz und Datensicherheit der TU Dresden statt. Diese thematischen Reihen sind ein wichtiges und ertragreiches Format von Weiterdenken.

Die Dokumentationen zu den bisherigen gemeinsamen Reihen zwischen Theater, Stiftung und verschiedenen Lehrstühlen der TU Dresden finden sich auf der Website von *Weiterdenken* - Heinrich-Böll-Stiftung Sachsen (www.weiterdenken.de):

- «Kapitalismus heute – und morgen?» (2010/11)
- «GERECHT.» (2011)
- «Alle inklusive? Zusammenhalt in einer vielfältigen Gesellschaft» (2012)
- «Open-Up! – Politisch kommunizieren zwischen Talkshow, Tweet und Theater» (2012/13)
- «Was kostet die Welt? Die Ökonomisierung der Gesellschaft» (2013/14)
- «Digitale Schwellen» (2014)
- «Die demokratische Frage neu gestellt» (2014/15)

Ich bedanke mich herzlich für die anspornende und produktive Zusammenarbeit mit Dr. Stefan Köpsell vom Lehrstuhl für Datenschutz und Datensicherheit der TU Dresden sowie bei Kerstin Harzendorf und Johannes Lichdi. Ohne ihre Expertise und ihre Kontakte wären weder die Veranstaltungsreihe noch der Sammelband zu Stande gekommen. Johannes Lichdi danke ich für das Lektorat.

Die Reihe hat wie immer ein professionelles und anregendes Zuhause in der Glacisstraße gefunden, auch dem Staatsschauspiel Dresden und insbesondere seiner künstlerischen Produktionsleiterin Mary Aniella Petersen sei deshalb für die langjährige Zusammenarbeit gedankt. Nicht zuletzt danke ich Antje Meichsner für den künstlerischen Beitrag zum Band.

Dresden, Mai 2015

Stefan Schönfelder

Weiterdenken - Heinrich-Böll-Stiftung Sachsen

JOHANNES LICHDI

Einführung

Die Enthüllungen des NSA-Whistleblowers Edward Snowden teilen die kollektive Wahrnehmung der Digitalen Revolution in die Zeit vor und die Zeit nach Snowden. Vor Snowden konnten noch naive Träume in die unmittelbar demokratisierende Wirkung des scheinbar wildwüchsigen autonomen Internets blühen. Nach Snowden ist klar, dass zumindest die angloamerikanischen Geheimdienste der «Five Eyes» unter Führung der NSA wirklich «das Internet speichern» und die Datenspuren sämtlicher Nutzer auswerten. Der Traum vermeintlich unbegrenzter Autonomie und unkontrollierbarer Freiheit des Netzes hat sich als Alptraum eines digitalen Käfigs entpuppt. Seitdem ringen wir um das Verständnis, welche Chancen Privatheit, Freiheit und Demokratie in einer zukünftigen Welt noch haben, die immer unentrinnbarer alle unsere Lebensäußerungen in digitalen Spuren aufzeichnet und der Ausbeutung unterwirft. Die Beiträge der Vorlesungsreihe nehmen die Arbeit der Geheimdienste und Polizeien samt der zugehörigen Ideologien, des Journalismus, der Anbieter und Anwender von Apps und Smart-TVs, die Notwendigkeit der Medienbildung sowie der Regulierungsbemühungen auf internationaler und europäischer Ebene in den Blick. Dabei wird sichtbar, wie radikal die Machtinteressen der Geheimdienste und die kommerziellen Interessen der Internetkonzerne das bisher geltende Bild von der unantastbaren Würde des Menschen umwerfen und mit der Auflösung von Privatheit auch die Axt an Freiheit und Demokratie legen. Bisher ist die Radikalität dieses Angriffs bei Vielen noch unverstanden, die sich an den scheinbar unendlichen Möglichkeiten der Kommunikation und Vernetzung berauschen. Erforderlich ist nichts weniger als die Neuerfindung der vor der Digitalen Revolution erkämpften Menschen- und Grundrechte als Voraussetzung einer freiheitlichen und demokratischen Gesellschaft. Bisher steckt dieser Prozess noch in den Kinderschuhen; freilich haben 2014 die Urteile des Europäischen Gerichtshofs zum «Recht auf Vergessen» und zur Rechtswidrigkeit der Richtlinie zur Vorratsdatenspeicherung wichtige Pflöcke eingeschlagen.

1. Unsere alltägliche Ausspionierung

Die SPIEGEL-Autoren **Holger Stark** und **Marcel Rosenbach** beschreiben in ihrem Buch «Der NSA-Komplex – Edward Snowden und der Weg in die totale Überwachung», wie der Schock der Anschläge des 11. September 2001 die amerikanische Führung veranlasste, die bisherigen Schranken der Überwachung von «Metadaten» über Bord zu werfen. Die Erhebung dieser Datenspuren und ihre Auswertung, die bei einer elektronischen Kommunikation anfallen, sollte eigentlich auf Fälle eines «begründeten Verdachts» im Zusammenhang mit «internationalem Terrorismus» beschränkt werden. 2007 arbeiteten 3000 Mitarbeiter im Überwachungsprogramm «Starbust». Die NSA verfüge über etwa 40.000 Mitarbeiter und 2013 über eine Etat von 10 Mrd. Dollar. Diese Aufrüstung ist Ausdruck einer neuen Überwachungsideologie: Denn die NSA und ihre Helfer, zu denen nach dem Bekanntwerden der Operation «Eikonal» und dem «Selektorenskandal» auch der Bundesnachrichtendienst zu

rechnen ist, streben unter dem Vorwand der «Terrorbekämpfung» nichts weniger als die weltweite «information superiority», die Informationsvorherrschaft, an. Die von Snowden enthüllten Überwachungsprogramme sind also keineswegs aus dem Ruder gelaufene Grenzüberschreitungen eines unkontrollierbaren Geheimdienstes, sondern spiegeln dieses strategisch verfolgte Ziel. Dafür müssen tatsächlich alle Daten erfasst werden, denn man brauche «den Heuhaufen, um die Nadel zu finden, wie NSA-Chef Keith Alexander sagte.»

Der Journalist und Gründer von iRights.info **Matthias Spielkamp** beleuchtet die Angriffe und Vorwürfe von Berufskollegen auf den Helfer von Edward Snowden, den Journalisten Glenn Greenwald, der die Grenze zur politischen Kamapagne überschritten habe. Dagegen plädiert Spielkamp für ein politisches Verständnis von Journalismus, dass sich nicht hinter einer vordergründigen Ausgewogenheit verstecken soll. Zudem verweist er auf die Notwendigkeit ganz praktischer Aspekte journalistischer Arbeit, zu der heutzutage zwingend der digitale Quellenschutz gehört. So sind alle Möglichkeiten der Anonymisierung und Vertraulichkeit zu nutzen, um Quellen zu schützen.

Angesichts der flächendeckenden Überwachung und Auswertung unserer Kommunikationsdaten wirken die nachholenden Anwendungen nachrichtendienstlicher Überwachungsmethoden durch die deutschen Polizeien geradezu wie niedliche Sandkastenspiele aus der Postkutschenzeit. Die Fallstudie des Dresdner Rechtsanwalts **Johannes Lichdi** beleuchtet, wie sich polizeiliche Kontrolltechniken aus der analogen Welt in einer bestimmten politischen Lage zu einer Überwachung des elektronischen Kommunikationsraums radikalisierten. Am 19. Februar 2011 ist der polizeiliche Versuch einer Zonierung des öffentlichen Raums in exklusive Zonen für gegenläufige politische Demonstrationen krachend gescheitert. An diesem Tag war es tausenden Gegendemonstrierenden gelungen, in die vorgesehene exklusive Nazizone in der Dresdner Südvorstadt zu gelangen und durch Platzbesetzungen einen rechtsextremistischen Aufzug zu verhindern. Sofort danach erfasste die Polizei unter Mißbrauch der strafprozessualen Voraussetzungen einer Funkzellenabfrage alle Telekommunikationsdatenspuren aller Personen, die sich in der Südvorstadt an bestimmten Punkten aufgehalten haben. Diese Erfassung zielte auf die Auswertung von Kommunikationsbeziehungen. 2011, zwei Jahre vor Snowden, erregte diese neue Überwachungsdimension mit ihrem totalen Zugriff noch die Gemüter; inzwischen ist sie offenbar schon polizeilicher Alltag ohne jeden Aufmerksamkeitswert geworden.

Seitdem ist die alltägliche Überwachung unserer Datenspuren mit der allgemeinen Verbreitung von smartphones, die einen wesentlichen Teil unserer Kommunikation von der physischen Welt ins internet verlagern, wesentlich erleichtert und intensiviert worden. **Hannes Federrath**, Informatikprofessor in Hamburg, erklärt, warum unser «smartphone mehr weiß als ich» und wie Internetkonzerne und Geheimdienste laufend und massenhaft Daten mit Apps über uns sammeln und auswerten. Mit sogenannten «Wearables» werden auch sehr persönliche Daten wie Herzschlag, Atemfrequenz, Muskelkontraktion und Blutzucker messbar. Federrath beschreibt die Gefahren für unsere Privatsphäre durch Lösungen, die software und hardware zunehmend integrieren und so die Schutzziele der IT-Sicherheit, nämlich Vertraulichkeit, Integrität der Daten und Verfügbarkeit verletzen. Leider erlauben die Apps den Nutzern nicht, Sammlung und Weitergabe ihrer Daten wirksam zu kontrol-

lieren. Federrath weist darauf hin, dass die GUIDs (global user identification) nicht wie Cookies gelöscht werden können und so eine Langzeitverkettung der Netzaktivitäten und eine Langzeitbeobachtung möglich wird. Allerdings ist auch über andere Merkmale eine faktische Browsersignatur («browser-fingerprinting») erkennbar und verfolgbar. Federath wirbt für einen «informed consent», also eine ausreichende Information des Smartphone-Nutzers über die erhobenen Daten vor seiner Zustimmung sowie für Datenschutzstandards und Gütesiegel, die leider noch fehlen.

Aber nicht nur unere Kommunikationsinstrumente liefern laufend Datenspuren unserer Kommunikation, auch das «Internet der Dinge», die Ausstattung von Gegenständen unseres täglichen Lebens mit Sensoren, Übertragungsvorrichtungen und Vernetzungen mit anderen Gegenständen bewirkt einen weiteren Überwachungsschub. Eine Arbeitsgruppe am Fraunhofer-Institut für Sichere Informationstechnologie an der TU Darmstadt – **Michael Waidner, Marco Ghiglieri, Benjamin Lange** und **Hervais Simo** – beleuchtet die Möglichkeiten und Gefahren des «Smart-TV» als Beispiel für die wachsende Vernetzung von Haushaltsgeräten («Smart Home»). Smart TV sind Fernsehgeräte mit Internetanschluss, die mit der Funktion Hybrid Broadcast Broadband TV (HbbTV) ausgestattet sind, über die Inhalte aus einer Mediathek zur Verfügung gestellt werden können. Man kann im Internet surfen, Bilder anschauen, Musik hören oder videotelefonieren. Smart-TVs können über Smartphones oder Tablets gesteuert werden. In Deutschland soll die Anzahl HbbTV-fähiger Geräte bis 2016 auf über 13 Millionen steigen. Auch greifen Apps vielfach und intransparent auf Nutzerdaten zu, auch Schadsoftware kann über den Browser installiert werden. Eingebaute Sensoren können von außen so konfiguriert werden, dass sie als Abhör- und Späheinrichtungen funktionieren. Die Arbeitsgruppe empfiehlt die Einhaltung des Grundsatzes der Datensparsamkeit, so dass nur Daten übertragen werden, die für die Funktionalität erforderlich sind. Eine wirksame Aufklärung der Nutzer benötige eine benutzergerechte Visualisierung und Deutung der Daten. Nötig ist schließlich eine aktive Steuerungsmöglichkeit des Nutzers am Gerät selbst und regelmäßige Software-Aktualisierungen.

2. Regulierungen der Digitalen Revolution?

Angesichts der immer weitgreifenderen Überwachung bis in die letzten Winkel unseres privaten Lebens ist zu fragen, ob überhaupt und wie erfolgreich demokratische Gesellschaften versuchen, rechtliche Regeln zum Datenschutz einzuführen. Die rechtlichen Regeln sind trotz vorhandener Ansätze im internationalen und europäischem Recht bisher nicht so stark, dass sie die Grundrechte der Bürgerinnen und Bürger wirksam schützen könnten. Im privatrechtlichen Bereich erschwert die Eigenart der Technologie eine Regulierung der großen Plattformen von facebook, Google & Co.

Die Fragmentierung des Rechts in Rechtsordnungen verschiedener Staaten angesichts des Internets mit seiner globalen Struktur ist selbst zu einem Faktor geworden, der die Überwachung erleichtert. So rechtfertigen die NSA und der britische GCHQ ihre Totalüberwachung des Internets mit dem Argument, sie würden ja amerikanisches und britisches Recht einhalten – was aber nicht bedeutet, dass sie sich an deutsches, französisches oder europäisches Recht hielten. **Peter Schaar**,

Bundesdatenschutzbeauftragter 2003 bis 2013 und heute Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz Berlin (EAID) fordert die wirksame Durchsetzung eines internationalen Rechts auf Datenschutz. Ausgehend von Art. 12 der Allgemeinen Erklärung der Menschenrechte von 1948, nach der niemand «willkürlichen Eingriffen in sein Privatleben» ausgesetzt werden darf, schlägt er die Verabschiedung eines Zusatzprotokolls zu Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte von 1966 vor. Der Autor bespricht Art. 8 der Charta der Grundrechte der Europäischen Union von 2009, der ausdrücklich ein einklagbares Grundrecht auf Datenschutz vorsieht.

Die Datenschutzrichtlinie der EU von 1995 verlangt ein «hohes Datenschutniveau» – und zwar auch beim Export von Daten europäischer Bürger in die USA. Da die USA aber nicht bereit sind, ihre Firmen, dem strengeren europäischen Datenschutzrecht zu unterwerfen, hat sich die EU im Jahr 2000 im «safe-harbor»-Abkommen mit den USA mit dem bloßen Versprechen begnügt, dass sich US-Firmen an vergleichbare Datenschutzregeln halten würden. Zudem besteht eine allgemeine Ausnahme für die «nationale Sicherheit». Da damit im Ergebnis Daten europäischer Bürgerinnen und Bürger ohne jeden Schutzstandard in die USA exportiert werden, verlangt das Europäische Parlament nach den Snowden-Enthüllungen die Neuverhandlung des «Safe-Harbor»-Abkommens. Schaar begrüsst die Planungen des EU-Parlaments im Zuge der Neuerarbeitung der Datenschutzgrundverordnung das Markortprinzip einzuführen. Danach hätten sich ausländische Firmen der Datenschutzaufsicht des Landes zu unterwerfen, in dem sie Geschäfte machen. US-Firmen könnten sich nicht mehr wie bisher in dem Land niederlassen, das das geringste Datenschutzniveau hat.

Der Berichterstatter des Europäischen Parlaments zur EU-Datenschutzverordnung, der grüne Abgeordnete **Jan Philipp Albrecht**, beleuchtet aus der Innensicht die Gesetzgebungsarbeit des Europaparlaments die Blockaden der Regierungen, vor allem auch der deutschen, gegen die Verabschiedung eines wirksamen Datenschutznivaus. Fortschritte sind bisher nur aufgrund der Einigkeit aller politischen Kräfte des Parlaments wie durch die Urteile des Europäischen Gerichtshofs zum «Recht auf Vergessen» und zur Grundrechtswidrigkeit der Vorratsdatenspeicherung erreicht worden. Dagegen fehlt es an der Bereitschaft der Regierungen, ihre Bürger wirksam zu schützen. **Peter Schaar** bleibt allerdings skeptisch, ob bald wirksame Datenschutzrechte international durchgesetzt werden können, vor allem gegen die USA. Letztlich handele es sich um eine politische Auseinandersetzung, wieviel echten Datenschutz die Bürgerinnen und Bürger einfordern. Der Beitrag endet mit einem Apell, Edward Snowden politisches Asyl in Deutschland zu gewähren.

Der Informatiker Dr. **Stefan Köpsell** von der TU Dresden betont die monopolistische Prägung der Infrastrukturen der digitalen Kommunikation. So besitzen etwa die US-amerikanischen Firmen Cisco, Intel und Microsoft in ihren Märkten je einen Anteil zwischen 60 bis 80%. Die geringe Anzahl von Datenleitungen und Austauschpunkten (gateways) für den Datentransport erleichtere das Abhören und die Manipulation von Datenströmen. Stichworte wie TEMPORA oder Eikonal zeigen, dass NSA, GCHQ und BND diese Möglichkeiten tatsächlich im großen Stil nutzen. Köpsell fordert einen Umbau des Internets anhand der Kriterien der Dezentralität, Diversität und Redundanz, um Überwachung und Manipulation strukturell zu erschweren: Dezentrale statt zentrale Strukturen, diverse Lösungen durch unterschiedliche

Realisierungen für gleiche Systembestandteile und redundante Mehrfachabsicherung einer Funktion anstelle einer einzigen Lösung. Leider würden redundante Lösungen in den letzten Jahren immer weiter abgebaut. So verschmelzen «All-IP»-Lösungen die vormals getrennten Kommunikationswege von Telefon, Fernsehen und Internet. Das gängige Cloud-Computing missachte mit seiner Datenspeicherung und Programmausführung in einer Cloud diese Prinzipien. Im kommenden «Internet der Dinge» ist eine weitere Verschärfung zu erwarten. Köpsell ist aufgrund der erforderlichen riesigen Investitionen und rechtlicher Restriktionen skeptisch, ob die Technikentwicklung erfolgreich in Richtung Dezentralität, Diversität und Redundanz gelenkt werden könnte.

Macht und Machtmißbrauch der großen privaten Plattformbetreiber wie Google, Facebook, Apple, Amazon und Microsoft führen zu Forderungen, die von einem Verbot von Persönlichkeitsprofilen, der Offenlegung von Algorythmen bis zur Entflechtung der Konzerne reichen. Dabei stellt sich für den Berliner Professor für Organisationstheorie, **Leonhard Dobusch**, die Frage nach geeigneten Regulierungsformen. Denn Regulierungen sind wegen der Dynamik der technologischen Entwicklung und der Wirkungslosigkeit klassischer kartellrechtlicher Instrumente wie Preiskontrollen und Entflechtungen schwierig. Für eine wirksame Regulierung müssen die Eigenarten des Marktes und der Technologie, nämlich die Skalen-, Netzwerk- und Koordinationseffekte als Ursachen für die marktbeherrschende Stellung des Unternehmens beachtet werden. Skaleneffekt bedeutet, dass mit der Erstellung der Plattform alle Kosten aufgebracht und mit weiteren Nutzern keine weiteren Kosten entstehen. Netzwerkeffekte treten ein, wenn jeder weitere Nutzer die Marktmacht etwa von facebook durch seine Teilnahme stärkt. Koordinationseffekte entstehen, wenn die Plattform Rechtssicherheit gegenüber vielen nationalen Rechtsordnungen bietet. Staatliche Entflechtungen von Konzernen könnten daran strukturell nichts ändern. Dobusch schlägt eine weitgehend unabhängige Regulierungsbehörde mit flexiblen Instrumenten auf europäischer Ebene vor, deren Ziel es ist, die Gründe für die marktbeherrschende Stellung zu verändern. Um Skalen- und Netzwerkeffekten entgegen zu steuern, könnten Plattformbetreiber etwa gezwungen werden, ihre Datenbasis für Drittanbieter zu öffnen.

3. Die Herausforderung für Privatheit, Freiheit und Demokratie

Die Enthüllungen Edward Snowdens stellen die Gesellschaften vor die sehr grundsätzlichen Fragen, ob und wie sie Privatheit, persönliche Freiheit und gesellschaftliche Demokratie zurückerobern und bewahren wollen und können. Die Heidelberger Politikwissenschaftlerin **Ulrike Ackermann** begründet den Zweck von Privatheit als Voraussetzung individueller und gesellschaftlicher Freiheit. Dabei gerät «Privatheit als Hort der individuellen Freiheit im Zuge der digitalen Revolution unter massiven Druck». Die zahlreichen Eingriffe des Staates würden einen längerfristigen Mentalitätswandel vom Wert der Freiheit zum Wert der Sicherheit wiederspiegeln. Die Internetmonopolisten gründen ihre Geschäftsmodelle auf die Sammlung, Auswertung und Verkauf der privaten Daten ihrer Nutzer. Individualisierte Profile ermöglichen eine personalisierte Werbung. Privatheit würde zudem von den Nutzern selbst in einem «neuen Exhibitionismus» aufgegeben. Das eigene Zimmer, ehemals Rückzugsort ins Private, wird zur Bühne für die Welt. Ackermann beschreibt

Privatheit als Bereich jenseits sozialer Kontrolle, als kreativen Raum, der jenseits von Konformitätsdruck erlaubt, Kraft, Ideen und unabhängige Vorstellungen zur Gestaltung des eigenen Lebens und der Gesellschaft zu schöpfen. Privatheit erfordert aber Vertrauen in seinen Bestand, den der Staat als Voraussetzung der Autonomie und Freiheit seiner Bürger gesetzlich zu gewährleisten habe. Die Aufhebung der Trennung von Privatheit und Öffentlichkeit sei ein Zeichen von Diktaturen. «Transparenz» sei aufgrund des allgegenwärtigen Zwangs zu ihr zu einem trügerischen Versprechen geworden. Mit der Neigung zur Selbstdarstellung sei tatsächlich der «gläserne Bürger» enstanden. Die gegenseitige soziale Kontrolle wächst, wodurch neue Formen der Vergemeinschaftung und Kollektivierung entstünden. Sphären der Privatheit veränderten sich und konstituierten sich neu.

Ackermann berichtet von einer Analyse der Parteien zu den Fragen «Starker Datenschutz und staatliche Regulierung» oder «Schwacher Datenschutz und Selbstregulierung». CDU / CSU und FDP würden ein «positives Narrativ» über den digitalen Wandel und dessen großes Potential propagieren, der sich am besten ohne die Einmischung der Politik und neue Regulierungen entfalten könne. SPD, Grüne und Linkspartei betonten dagegen die Risiken eines unkontrolliert ablaufenden digitalen Wandel. Die Politikwissenschaftlerin tritt zum Schutz der Privatsphäre für Regulierungen des Staats wie ein Koppelungsverbot zwischen Service und Datenhandel, ein «Recht auf Vergessen» und auf Löschung, ein Profilbildungsverbot und wirksame «opt-in» und «opt-out»-Rechte ein.

Die Hamburger Rechtsprofessorin **Marion Albers** beschreibt den Wandel der «Sicherheitsarchitektur» seit den frühen Siebzigerjahren bis heute. Zunächst erklärt Albers die eingrenzende und damit freiheitssichernde Funktion traditioneller polizeirechtlicher Begriffe wie der «Gefahr», des «Störers» oder der «Verhältnismäßigkeit». Seitdem aber der scheinbar einleuchtende Gedanke der Vorsorge, der Prävention, zur Leitidee geworden ist, wurden polizeiliche Eingriffsrechte für die Polizeiarbeit für Sachverhalte eingeführt, bei der noch keine Gefahr erkennbar ist oder eine Straftat bevorsteht. Ziel der Polizeiarbeit soll nicht mehr allein die Gefahrenabwehr oder die Aufklärung von Straftaten sein, sondern die Erstellung von «Lagebildern» zu Szenen sein, die für gefährlich gehalten werden. Damit folgt die Polizei Methoden und Erkenntniszielen, die traditionell Geheimdiensten vorbehalten waren. Zudem werden die Bundespolizeien immer weiter ausgebaut und das Bundeskriminalamt zur informationellen Schnittstelle wie neuerdings bei der sogenannten «Antiterrordatei» aufgewertet. Diese Tendenzen scheinen sich im Leitbild «prädiktiver» («vorhersagender») Polizeiarbeit weiter zu verstärken. Das Leitbild bündelt Ansätze wie Data Mining-Strategien, Crime Mapping (Lokalisierung von Kriminalitätsschwerpunkten) oder Netzwerkanalysen. Dabei sind die von privaten Firmen entwickelten Auswertungsprogramme und Algorithmen keine neutralen Techniken, sondern enthalten als «eingefrorener Diskurs» bestimmte Hypothesen und Theorien über Kriminalität. Die Polizeiarbeit benötige deshalb «neue freiheitssichernde Muster». Es gehe um neue Formen institutionalisierter und öffentlicher Kontrolle über die Ausgestaltung polizeilicher Datenverarbeitungsprogramme, insbesondere aufgrund der zunehmenden datenmäßigen Vernetzung der «Sicherheitsbehörden».

Ausgehend von der Begeisterung für «Facebook-» oder «Twitter-Revolutionen» einerseits, andererseits aber der tiefen Enttäuschung nach den Snowden-Enthüllungen (Lobo: «Das Internet ist kaputt») betont der Dresdener Kulturwis-

senschaftler **Johannes Näder**, dass Technikoptimismus wie Technikpessimismus denselben Ausgangspunkt teilen: nämlich eine deterministische Weltsicht, nach der die Digitale Revolution wie eine unbeeinflussbare Naturgewalt über die Gesellschaften hereinbreche. Näder kritisiert den einseitigen Blick auf die Wirkungsseite von Internet und Digitaler Revolution, der vergesse, dass digitale Infrastrukturen «immer wieder gezielten Einflüssen politischer, wirtschaftlicher und ideologischer Natur ausgesetzt waren.» Näder stellt drei Haupttendenzen des digitalen Wandels fest: «eine beispiellose Durchdringung unserer Gesellschaft mit digitaler, vernetzter Technologie», «ungeahnte Möglichkeiten der Speicherung, Übertragung und Verarbeitung von Informationen» sowie die zunehmende «Komplexität digitaler Technologien», die einen Kontrollverlust des Nutzers bewirkten. Aufgrund des Auseinanderfallens von Mediennutzungskompetenz und Medienwissen gingen «technischer Fortschritt und individuelle Technikunmündigkeit Hand in Hand «. Näder möchte dem individuellen Kontrollverlust durch «Medienwissen sowie Technikgestaltung und -kontrolle» begegnen. Als Orientierungspunkte für die Medieninfrastruktur einer demokratischen Gesellschaft, die nicht schon auf «technologisch-infrastruktureller Ebene Vermachtung mit sich bringt», nennt er die ungehinderte Teilhabe aller, Zensurfreiheit, Wahrung der Privatsphäre und Offenheit der technischen Infrastrukturen. Abschließend plädiert Näder für eine «rekursive Gesellschaft», deren Voraussetzung aber ein vertieftes Medienwissen in der gesamten Gesellschaft sein muss.

Die Geschäftsführerin der Terramark Technologies GmbH und Münchener Essayistin **Yvonne Hofstetter** ruft dazu auf, die Rechte der Person in Zeiten der Überwachung und manipulativen Beeinflussung menschlichen Verhaltens zu bewahren. Big data - Analysen stammten aus der militärischen Aufklärung, bei der erstmals Datenfusionssysteme mit den Elementen «Überwachen - Analysieren - Steuern» entwickelt worden waren. So sollten militärische Entscheidungen auf der Grundlage großer analysierter Datenmengen rationaler getroffen werden können. «Data scientists» versuchen aufgrund der Analyse der Handlungen relevanter Akteure in der Vergangenheit sowie bekannter und «latenter» Variablen ein Interaktionsmodell zu erstellen, das dann in ein mathematisches Modell übersetzt wird. Wenn dieses Modell die Vergangenheit «korrekt» beschreibt, sollen daraus Trends für die Zukunft abgeleitet werden. Dabei werden lernende Maschinen eingesetzt, die in Echtzeit die neuesten Informationen eines Lebensbereichs überwachen, analysieren und Entscheidungshinweise geben. Heute ist der amerikanische Börsenhandel zu 70% ein durch Algorithmen bestimmter Hochfrequenzhandel, was schon zu «flash crashs», dem kurzzeitigen Absturz der Kurse, geführt hat. Mit der Realwirtschaft hat das nichts mehr zu tun. Seitdem die verfügbaren personenbezogenen Daten aufgrund der exzessiven Nutzung von Smartphones und Tablets seit 2010 geradezu explodiert sind, stehen jetzt auch genügend Daten für personenbezogene Kommunikations- und Bewegungsbilder zur Verfügung. Hofstetter weist darauf hin, dass die Wirtschaftskonzerne mit dem wachsenden «Internet der Dinge» immer mehr Datenspuren ohne Einwilligung der Menschen erheben, die sie hinterlassen. Big data bringt unser Bild vom Menschen als ein mit Würde augestattetes Wesen ins Wanken. Die Big data - Industrie verleugne, dass der Mensch Subjekt seiner Lebensverhältnisse ist, denn sie degradiere ihn zum Lieferanten des Daten-Rohstoffs. Ganz offen werde zudem die Demokratie als

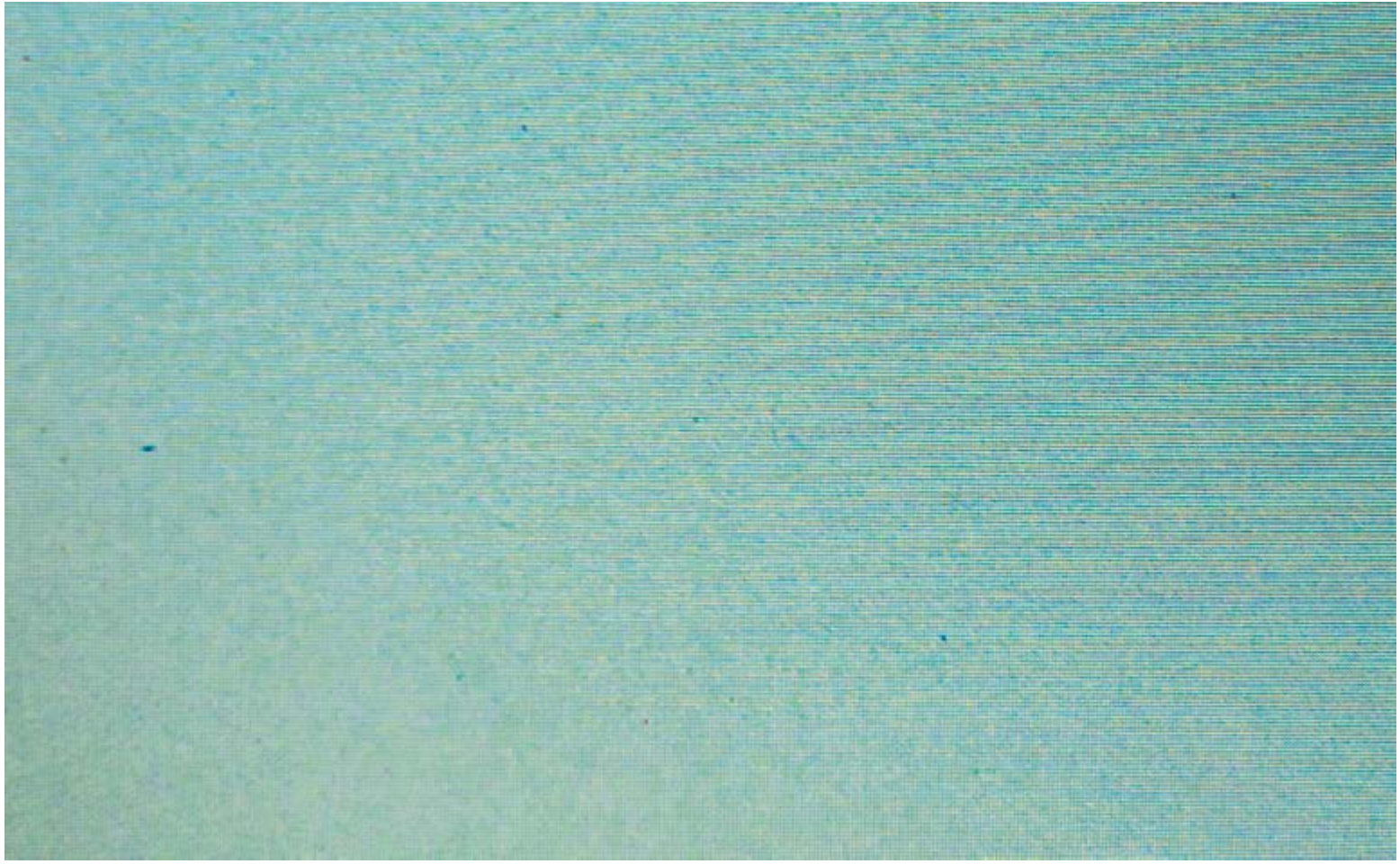
«veraltete Technologie» abgelehnt. Derzeit konzentrierten die Internetgiganten mit den Daten und den Big Data - Schlüsseltechnologien Rohstoff und Schlüsseltechnologien in einer Hand und gewönnen so demokratisch unkontrollierte Macht.

Hofstetter wirbt für einen «gesellschaftlichen Konsens, wie wir die intelligenten Maschinen der digitalen Ökonomie beherrschen», denn sonst «werden wir in Kürze bald selbst von ihnen beherrscht«. Sie setzt ihre Hoffnung darauf, dass die westlichen Gesellschaften dem «Irrtum des Kapitalismus», der die Menschen seinem Wirtschaften unterordnen wolle, wie bei der Humanisierung der Arbeit mit Schutzrechten für unsere Daten entgegen treten werden. «Nicht nur unsere menschliche Arbeit, auch unsere Daten «erben» die Subjektivität der menschlichen Person. Genau wie die menschliche Arbeit verdienen sie deshalb einen ganz besonderen Schutz.» Hofstetter plädiert dafür die Datenzufuhr zu unterbrechen, denn «keine Daten, wenige und unvollständige Daten bedeuten eine unwirksame Kontrollstrategie.» Der Staat sei verpflichtet, unsere Daten zu schützen: Wer die digitale Abstinenz wähle, dürfe nicht diskriminiert werden, wer seine Daten zur Verfügung stelle, dürfe nicht ausgebeutet werden. Das Recht des Datensubjekts Mensch müsse dem Recht auf wirtschaftliche Entfaltung vorgehen.

4. Ausblick

Unsere Mühen dauern an, die digitalen Schwellen zu verstehen, und daraus die richtigen Konsequenzen zu ziehen. Staatliche wie kommerzielle Datenkraken nutzen dies schamlos aus. Die NSA & Co. reden ihre Totalüberwachung und ihr Streben nach «information superiority» immer noch als «Kampf gegen den Terrorismus» schön. Edward Snowden und die anderen Whistleblower werden weiter als Verräter verfolgt. Der BND tut so, als ob seine beflissenen Hilfsdienste für die Amerikaner mit dem Grundgesetz und den Grundsätzen einer freiheitlichen Gesellschaft vereinbar wären. Die Bundesregierung schweigt, verschleiert und blockiert im NSA-Untersuchungsausschuss und bereitet einen neuen Anlauf zur Legalisierung der Vorratsdatenspeicherung vor. Auch die großen privaten Internetplattformen bauen ihr Geschäft im Namen von wirtschaftlicher Freiheit und Wachstum aus. Daten sind nicht harmlos, vor allem in der auswertbaren Masse. Die Datenkraken meinen, dass unsere Daten nicht uns gehören, sondern beuten sie als kostenlosen Rohstoff in grenzen- und maßloser Weise aus. Wie im Frühkapitalismus die menschliche Arbeitskraft und bis heute die natürlichen Lebensgrundlagen werden unsere Daten ausgesaugt, enteignet und verwertet. In den heutigen gesellschaftlichen Kampfzonen wie dem Berliner NSA-Untersuchungsausschuss des Bundestags kommt man kaum über Skandalisierungen hinaus. Die Auseinandersetzung um eine wirksame EU-Datenschutzgrundverordnung in Brüssel tritt auf der Stelle. Das transatlantische Freihandelsabkommen TTIP gefährdet ganz grundsätzlich Sozial- Umwelt- und auch Datenschutzstandards. Dabei sind Deutschland und die EU keineswegs die Guten, für die sie sich immer halten. Staatliche Entscheidungsträger werden sich nur bewegen, wenn jede und jeder Einzelne und die Gesellschaft insgesamt die Achtung unserer Privat- und Freiheitssphäre einfordern und wir mit Aussicht auf Erfolg einklagbare Rechte durchsetzen, um die Herrschaft über unsere Daten wieder zu erlangen.

I. Unsere alltägliche Überwachung



MARCEL ROSENBACH UND HOLGER STARK

Warum und wie die NSA das Internet beherrschen will[1]

1. Der 11. September und die Folgen

Für alle Verantwortlichen in den amerikanischen Sicherheitsbehörden waren die Anschläge vom 11. September 2001 ein Desaster. Ein Heer von mehr als einem Dutzend Geheimdiensten hatte die Attentäter nicht rechtzeitig erkannt (und auch deutsche Behörden hatten nicht gewusst, welch monströse Pläne in der Marienstraße in Hamburg-Harburg geschmiedet wurden). Für NSA-Chef Hayden war es eine besonders tiefe Demütigung, denn es stellte sich bald heraus, dass Chalid al-Midhar und Nawaf al-Hamsi sowie drei weitere Attentäter Wochen vor der Tat nahe der NSA-Zentrale gelebt hatten. Sie hatten sich im Valencia Motel in Laurel, Maryland, einquartiert, einem Ort, der nur 15 Autominuten von Fort Meade entfernt ist und als Schlafstadt für Angestellte des Geheimdienstes gilt. Die späteren Attentäter verbrachten hier mehrere Wochen, gingen einkaufen und essen und trainierten im Fitnessstudio. Wahrscheinlich liefen sie dabei mehrmals NSA-Mitarbeitern über den Weg. Ende August 2001 trafen auch Ziad Jarrah und Mohammed Atta ein, die zwei der Flugzeuge steuern sollten und zuvor in Hamburg Teile des Anschlagplans vorbereitet hatten. Die führenden Terroristen des 11. September versammelten sich direkt vor der Nase der NSA.[2] Viele der in den darauffolgenden Wochen, Monaten und Jahren getroffenen Entscheidungen lassen sich nur vor dem Hintergrund dieses kompletten Versagens der Geheimdienste verstehen. [...]

Diese Serie von kleinen und großen Pannen löste quälende Diskussionen darüber aus, ob die Attentate nicht hätten verhindert werden können, wenn beispielsweise für die NSA erkennbar gewesen wäre, dass einer der Anrufe in Sanaa aus San Diego gekommen war. Die Phase der Zermürbung dauerte allerdings nicht lange, das ließen US-Präsident George W. Bush und sein Vize Dick Cheney nicht zu. Noch unter dem frischen Eindruck des Anschlags auf Amerika begann die US-Regierung sehr schnell sehr weitgehende Entscheidungen zu treffen. So befahl Verteidigungsminister Donald Rumsfeld noch am Nachmittag des 11. September, mit den Vorbereitungen eines Vergeltungsschlages gegen den Irak zu beginnen - obwohl der Irak nichts mit den Anschlägen zu tun hatte und der NSA längst Hinweise vorlagen, dass die Attacken von al-Qaida verübt worden waren.

Neben den Kriegsvorbereitungen begann die Regierung unverzüglich, die Sicherheitsbehörden umzubauen. Vizepräsident Cheney war der Ansicht, dass die USA auf die akute Terrorgefahr mit einer massiven Aufstockung des Sicherheits-

1 Dieser Text ist ein mit Überschriften versehener Auszug aus dem Buch Der NSA-Komplex – Edward Snowden und der Weg in die totale Überwachung (2014) von Rosenbach und Stark. Die Herausgeber danken der Deutschen Verlagsanstalt für die Abdruckgenehmigung.

2 James Bamford: The Shadow Factory, S.76 f.

apparates und einer Ausweitung von dessen Kompetenzen reagieren müsse. Diese Einschätzung führte nicht nur zur Gründung neuer Behörden wie dem Ministerium für Heimatschutz, sie hatte auch weitreichende Auswirkungen für die NSA, wie aus einem 49-seitigen Bericht des für die Untersuchung interner Vorgänge zuständigen NSA-Generalinspekteurs hervorgeht – jenem Dokument, das Edward Snowden so empört hatte, dass er sich zum Handeln entschloss.[3]

Diesem als «Streng geheim» eingestuften Dokument zufolge war es der damalige CIA-Chef George Tenet, der seinem NSA-Kollegen Michael Hayden unmittelbar nach den Anschlägen eine dringende Nachricht aus dem Weißen Haus überbrachte: Die NSA müsse die vorhandenen Lücken in der technischen Aufklärung benennen und solle Vorschläge erarbeiten, wie diese künftig zu schließen seien. Dabei wurde schnell deutlich, dass juristische Bedenken keine Rolle mehr spielen würden. «Gibt es etwas, das ihr tun könnt?», soll Tenet gefragt haben. «Nicht mit der gegenwärtigen Gesetzeslage», so Haydens Antwort. «Danach habe ich nicht gefragt», erwiderte Tenet. «Gibt es etwas anderes, das ihr tun könnt?»[4] Tenet galt als Intimus des Weißen Hauses, er sollte in Cheneys Auftrag Druck auf den bis dahin politisch wenig eingebundenen Hayden ausüben.

Mindestens dreimal kam es in den ersten 20 Tagen nach dem 11. September dann auch zu persönlichen Treffen zwischen NSA-Chef Hayden und dem Vizepräsidenten Cheney. Über diese Gespräche, bei denen es darum ging, die Kompetenzen der Behörde auszuweiten, existieren angeblich keine Protokolle oder Dokumente. Gegenüber dem Generalinspekteur erinnerte sich Hayden daran, den Vizepräsidenten während der Termine darüber unterrichtet zu haben, dass das bis dahin praktizierte Fisa-Verfahren nicht flexibel und schnell genug sei, um der Terrorgefahr wirkungsvoll zu begegnen. Deshalb habe er sich dafür eingesetzt, künftig anhand von Metadaten – also den Informationen, wann wer wen wie lange angerufen hat – auch die Kontakte von US-Bürgern untersuchen zu dürfen, um auf verdächtige Beziehungen ins Ausland zu stoßen. «General Hayden betonte, dass Metadaten nicht demselben verfassungsrechtlichen Schutz unterliegen wie Inhalte», heißt es in dem Bericht. Zudem habe der NSA-Chef gegenüber dem Vizepräsidenten klargemacht, dass es die Arbeit seiner Behörde erheblich beschleunigen und verbessern würde, wenn sie künftig die Kommunikation von US-Bürgern mit dem Ausland auch ohne Gerichtsbeschluss überwachen könnte. «Mister Vizepräsident», sagte Hayden, «wir können das, aber wie Sie wissen, müssen wir vorsichtig sein»; seit dem Church-Komitee stehe die NSA unter Beobachtung. Für Cheney muss es wie eine Ironie der Geschichte gewirkt haben: Als der NSA vom Church-Komitee erstmals rechtsstaatliche Fesseln auferlegt wurden, hatte Cheney unter Präsident Gerald Ford als Stabschef des Weißen Hauses gearbeitet. Als Vizepräsident setzte er nun alles daran, diese Fesseln so weit wie möglich zu lockern.

3 Es handelt sich um einen Untersuchungsbericht für den Chefjustiziar der NSA mit Datum vom 24. März 2009. Die Zahlen und Fakten der folgenden Absätze stammen aus diesem Report.

4 Zitiert nach Peter Baker: Days of Fire. Bush and Cheney in the White House, New York 2013. So erinnert sich auch Hayden in dem internen NSA-Untersuchungsbericht.

2. Rechtliche und technische Aufrüstung der Überwachung

Cheney trug Haydens Einwand bei George W. Bush vor, der den NSA-Chef zu sich lud. «Mike, danke fürs Kommen», sagte der Präsident. «Ich verstehe Ihre Bedenken, aber wissen Sie, wenn es Dinge gibt, die getan werden können, dann sollten wir sie tun.»[5] Für die Ausarbeitung einer entsprechenden Direktive wurde Hayden an Cheneys Berater David Addington verwiesen, einen Juristen und Hardliner, der den ersten Entwurf für die massive Ausweitung der NSA-Kompetenzen verfasste.[6] Bereits am 14. September 2001 ordnete Hayden an, nach Telefonverbindungen zwischen Krisenländern und den USA zu suchen. Die Überwachung galt zunächst nur für Staaten wie Afghanistan, aber das sollte sich bald ändern. Nur drei Wochen nach den Anschlägen, am 4. Oktober 2001, unterschrieb George W. Bush die entsprechende rechtliche Anweisung, um «terroristische Akte in den Vereinigten Staaten zu verhindern». Damit durfte die NSA mit sofortiger Wirkung Internetkontakte und Telefongespräche von Zielen überwachen, die mit «internationalem Terrorismus» in Zusammenhang standen – selbst wenn sich ein Gesprächspartner in den USA befand. Das erweiterte das Spektrum der Überwachung erheblich. Zudem reichte dafür bereits ein «begründeter Verdacht» aus, das Ziel könnte Kontakte ins Terrormilieu haben, was die juristischen Hürden zusätzlich senkte. Nach dieser Direktive durfte die NSA alles, im In- wie im Ausland, ohne jede Kontrolle. Der grenzenlosen Überwachung waren Tür und Tor geöffnet. Gemeinsam mit Addington überarbeitete Hayden die Order später zumindest insoweit, dass rein inländische Kommunikation zwischen Amerikanern von ihr ausgenommen war. «Wir sind ein Auslandsgeheimdienst», begründete Hayden diese Einschränkung, dabei solle es bleiben; er wolle nicht für Inlandsüberwachung ins Gefängnis gehen. Am 2. November 2001 unterzeichnete Bush die modifizierte Anordnung, Cheney weihte die sogenannte «Gang of Eight» ein, eine Gruppe der wichtigsten acht Vertreter von Republikanern und Demokraten in Senat und Repräsentantenhaus.[7] Die Volksvertreter verzichteten auf ihr Recht, für die Sonderrechte ein Gesetz zu erlassen, und ließen die Regierung gewähren.

Der Umgang mit den neuen juristischen Möglichkeiten zur Überwachung war innerhalb der Regierung von höchster Geheimhaltung geprägt. Selbst die zuständigen Abteilungsleiter für die Terrorismusbekämpfung innerhalb der NSA, die damit arbeiten mussten, bekamen Bushs «Executive Order» vom 4. Oktober nicht zu Gesicht, sie wurde in Haydens Safe aufbewahrt und nur einer Handvoll seiner engsten Mitarbeiter gezeigt. Als der NSA-Justiziar Robert Deitz zur Absicherung um eine Kopie der Stellungnahme des für die verfassungsrechtliche Prüfung zuständigen Justizministeriums bat, wurde ihm diese ebenfalls verweigert. Dick Cheneys Rechtsberater Addington las ihm lediglich ein paar Zeilen am Telefon vor, die signalisieren sollten, dass alles mit rechten Dingen zugehe. Es sei ihm bewusst gewesen, dass dieses Programm «politisch sehr sensibel und kontrovers» war und zu einem späteren Zeitpunkt kritisch geprüft werden würde, erklärte Hayden dem NSA-Justiziar. Er sei allerdings überzeugt, dass es rechtmäßig gewesen sei; dies habe die Rechtsabteilung des Nachrichtendienstes am 5. Oktober 2001 auch bestätigt. Der

5 Interner NSA-Untersuchungsbericht von 2009.

6 Ebenda.

7 Peter Baker: Days of Fire.

leiche NSA-Chef, der «ThinThread» noch unter anderem aus rechtlichen Gründen hatte stoppen lassen, wollte nun von juristischen Bedenken nichts mehr wissen.

Das geheime Plazet des Präsidenten vom 4 Oktober 2001 löste in Fort Meade hektische Betriebsamkeit aus. Am 6. Oktober 2001, einem Samstag, wurden erfahrene Analysten aus dem Wochenende geklingelt und der neuen Aufgabe zugeordnet. Am 8. Oktober, einem Feiertag, schwor Hayden die frisch zusammengestellte Truppe auf ihre Mission ein. In wenigen Tagen hatte die NSA einen neuen, speziell gesicherten Arbeitsbereich eingerichtet, das «Metadaten Analysezentrum» («Metadata Analysis Centre»), das den Codenamen «Starbust» erhielt. 50 neue Server wurden aufgestellt, um die neu anfallenden Daten zu bewältigen. 90 erfahrene Analysten hatte der Dienst innerhalb von einer Woche zusammengezogen, die für das Programm in drei Schichten US-Bürger mit mutmaßlich verdächtigen Auslandskontakten 24 Stunden täglich, an sieben Tagen der Woche überwachten. Noch im Oktober 2001 begannen die privaten amerikanischen Telekommunikationsfirmen, massenhaft Telefondaten und Internetinhalte nach Fort Meade zu schicken. In den folgenden sechs Jahren erhielten mehr als 3000 Mitarbeiter die notwendige Geheimhaltungseinstufung, um an «Starbust» mitzuarbeiten.[8]

Doch das spektakulärste Wahrzeichen für die neue Ära der Überwachung entstand in Bluffdale, einem Vorort von Salt Lake City im Mormonenstaat Utah. In staubiger Wüstenumgebung, umrahmt von den Wasatch- und Oquirrh-Gebirgen, wuchs auf dem Armeegelände Camp Williams in den vergangenen Jahren das «Utah Datenzentrum» empor. Es ist ein Gebäude der Superlative, weniger wegen seiner Abmessungen oder Kosten von rund zwei Milliarden Dollar. Aufsehenerregend ist vor allem das Innenleben der vier Server-Hallen. Sie sind das Herz der Anlage, die jährlich so viel Energie verbrauchen soll wie eine Stadt mit 65 000 Einfamilienhäusern. Damit die Rechner voller Überwachungsdaten aus aller Welt nicht Heißlaufen, benötigen sie schätzungsweise sieben Millionen Liter Kühlwasser am Tag. Sie sollen das Tordeila-Gebäude in Fort Meade ergänzen, wo bislang in einem speziell gekühlten Komplex die meisten Server der Behörde stehen. Die Begründung für die Dimension des Projekts sagt viel über das Amerika aus, dem Sicherheit über alles geht. «Wir haben es so groß gebaut, weil wir es konnten», sagt der Technikchef der NSA, Lonny Anderson. «Es ist das schönste Datenzentrum der US-Regierung und vielleicht das schönste, das es gibt.» Auf jeden Fall dürfte es das leistungsfähigste sein, auch wenn die Angaben über das Fassungsvermögen auseinandergehen. «Es ist gebaut, um lange Bestand zu haben», sagt Anderson. Das Datencenter soll so etwas wie der Knoten des weltweiten NSA-Überwachungsnetzes werden, hier fließen die Daten der übrigen Standorte auf Hawaii, in Georgia und Texas zusammen. Vor allem aber ist das Datenzentrum in Utah ein Symbol, das steinerne Selbstbild einer Behörde, die die Depression aus den Tagen nach dem 11. September 2001 längst hinter sich gelassen hat und die im letzten Jahrzehnt immer größer und mächtiger geworden ist. Die NSA scheint auf dem Zenit ihrer Möglichkeiten. Die Zahl der Mitarbeiter ist um ein Drittel auf mittlerweile rund 40 000 gestiegen, ihr Etat hat sich verdoppelt, auf 10,6 Milliarden Dollar im Jahr 2013. Insgesamt, das geht aus dem geheimen Budgetplan des Weißen Hauses hervor, hat die US-Regierung für ihre Geheimdienste im Jahr 2013 6 Milliarden Dollar beantragt, mit insgesamt 107 035

8 Ebenda.

Planstellen. Hinzu kommt noch das Heer der privaten Vertragsfirmen, die für die NSA arbeiten - ihre Zahl hat sich nach einer Analyse der «Washington Post» seit 2001 mehr als verdreifacht.[9]

3. Die Überwachungsideologie der «Informationsvorherrschaft»

Neben all diesen Superlativen hat sich noch etwas viel Wichtigeres verändert. Die Autorisierung des US-Präsidenten vom 4. Oktober 2001 war die Geburtsstunde einer neuen Überwachungsideologie. Wie die Geschichte der NSA und ihrer Vorläufer zeigt, hat die Behörde schon öfter Grenzen übertreten, die der Gesetzgeber vorgeschrieben hatte. Im Ausland war schon immer jede Person, die der NSA interessant erschien, ein Ziel ohne rechtliche Einschränkungen. Mit dem präsidentiellen Freifahrtschein, auch US-Staatsbürger im Inland mit verdächtigen Auslandskontakten ohne richterliche Genehmigung überwachen zu dürfen, fiel eine wichtige Schranke (auch wenn die NSA mittlerweile dafür zumindest das Fisa-Gericht anrufen muss). Und mit der Interpretation aus den Tagen nach dem 11. September 2001, dass Metadaten nicht wie Kommunikationsinhalte unter den Schutz des vierten Verfassungszusatzes fallen, war der Weg in ein neues Zeitalter der Überwachung geebnet.

Offiziell rechtfertigt die NSA diesen Anspruch, alle Daten überall sammeln zu können, mit dem 11. September 2001 und der Bedrohung durch den islamistischen Terrorismus. In einem Sprechzettel für NSA-Mitarbeiter, die der Öffentlichkeit ihre Arbeit erklären sollen, findet sich die Aussage: «Ich erkläre Ihnen heute viel lieber unsere Programme, als Ihnen ein weiteres Ereignis wie 9/11 erklären zu müssen, das wir nicht verhindern konnten.» Und weiter heißt es: «Nach 9/11 haben wir festgestellt, dass die Geheimdienst-Community vorhandene Erkenntnisfäden nicht verknüpft hat - nach 9/11 haben wir verschiedene Fähigkeiten entwickelt, die uns das ermöglichen.»[10] Intern sprechen die Führungskräfte der Behörde ehrlicher über ihre Motive. Der Kampf gegen den Terror spielt auch hier eine wichtige Rolle. Aber es geht bei der Arbeit der NSA im Zeitalter der globalen digitalen Vernetzung längst um mehr. Die digitale Revolution habe der NSA eine «einzigartige Position» verschafft, argumentierte NSA-Chef Alexander in einem Strategiepapier vom Juni 2010.[11] Alexander nennt als Vision die «global cryptologic dominance», eine weltweite Dominanz im Bereich der Kryptologie und Datensicherheit Die Mission der NSA sei es, durch klandestine Operationen «unter allen Umständen einen Vorteil für Entscheidungen unserer Nation und unserer Alliierten» zu erlangen. Noch deutlicher wird ein hochrangiger Mitarbeiter der Abteilung für Rechtsfragen in einem internen Schreiben. Es gehe der NSA «um die weltweite Informationsvorherrschaft».[12]

---

9 NSA growth fueled by need to target terrorists, in: Washington Post, 21.7.2013.

10 Die Sprechzettel wurden durch eine Anfrage nach dem Informationsfreiheitsgesetz öffentlich, siehe Revealed: NSA pushed 9/11 as key sound bitt o justify surveillance, in: Al Jazeera,17.10.2013, Originaldokument abrufbar unter: http//:america.aljazeera.com/articles/2013/10/30/revealed-nsa-pushed911askeysoundbitetojustify-surveillance.html

11 Geheimes Strategiepapier der NSA/CSS, Juni 2010, hier: Vorwort von Keith Alexander.

12 NSA-Dokument, etwa 2006: National Security Agency, Central Security Service – Overview Briefing.

Früher als fast alle anderen Behörden hat die NSA erkannt, was sich durch das Internet ändern würde. Schon im Juni 1996 erhielt der Nachrichtendienst eine neue Ausrichtung, die den Weg zur Totalüberwachung des Internets bereitete und die der damalige Direktor Kenneth Minihan in einer Mitteilung an alle NSA-Mitarbeiter so zusammenfasste: «Eine Informationsrevolution fegt durch die Welt, die so radikale Veränderungen erzwingt wie einst die Entwicklung der Atombombe. So wie die Kontrolle der industriellen Technologie einst der Schlüssel zu militärischer und ökonomischer Macht während der vergangen zwei Jahrhunderte war, wird die Kontrolle der Informationstechnologie der Schlüssel zur Macht im 21. Jahrhundert. [...] Wir müssen unseren traditionellen Anspruch auf technische Aufklärung und Informationssicherheit ausrichten, wenn wir relevant bleiben und eine führende Rolle als offensive und defensive Komponente einer neuen nationalen Bemühung spielen wollen, die einem einzigen Ziel dient - der informationellen Vorherrschaft für Amerika.»[13]

Es ist ein imperialer Anspruch, aus dem die NSA ihre offensive, aggressive Strategie abgeleitet hat. Michael Hayden hat uns darauf hingewiesen, dass der Anspruch der Vorherrschaft für die amerikanische Armee auch zu Wasser, Luft und Land gelte und dies lediglich die konsequente Fortsetzung amerikanischer Politik im digitalen Raum sei. Mag sein. Aber wenn ein Land das Internet beherrschen möchte, bedeutet dies automatisch, dass das Netz kein freies Medium mehr ist. Aus einer Behörde, die einst entstanden war, um im Kalten Krieg die Sowjetunion und deren Satellitenstaaten zu überwachen, ist eine Organisation zur Kontrolle des Internets geworden, ein maßloser Moloch, der über ein einzigartiges Arsenal verfügt. Die Waffen der NSA tragen Namen wie «Quantum», «Prism» oder «Tempora», und es gibt kaum einen Ort auf dieser Welt, an dem sie nicht eingesetzt werden. Zusammengenommen ergeben sie eine einzigartige Matrix der globalen Überwachung. [...]

4. Die «Heuhaufen-Theorie»

Auf die Rückfrage, ob die bis dahin bereits bekannt gewordenen Spähprogramme nicht auf einen überbordenden Datenhunger der Behörde hindeuteten, sagte Alexander: «Sie brauchen den Heuhaufen, um die Nadel zu finden.» Die Heuhaufen-Theorie ist die am häufigsten vorgetragene Rechtfertigung, warum die NSA möglichst alles wissen will.[14] Damit erhebt der Geheimdienst unverblümt den Anspruch, die gesamte globale Kommunikation zu überwachen. Denn aus Sicht der NSA besteht «der Heuhaufen» aus sämtlichen verfügbaren Informationen aller denkbaren Kommunikationswege des digitalen Zeitalters.

Noch vor 25 Jahren war die Welt der Kommunikation vergleichsweise überschaubar. Die meisten Menschen in den Industrieländern verfügten über einen Festnetzanschluss, den sie kaum jemals wechselten, schon weil Anbieter wie die

13 Zitiert nach NSA: Cryptologic Foreign Relations Patnership. A Strategy for Partnership, 30.09. 1996.

14 «Wenn du nach einer Nadel im Heuhaufen suchst, brauchst du einen Heuhaufen», sagt zum Beispiel Jeremy Bash, der einmal Stabschef beim früheren CIA-Direktor Leon Panetta war. Alexanders langjähriger Vize John Inglis führte den Heuhaufen bei einer Anhörung vor dem Kongress am 29.10.2013 an.

Deutsche Telekom staatliche Monopolisten waren. Ab und zu schrieben sie Briefe empfingen ein Paket, versendeten ein Telegramm oder ein Fax. Ein paar Freaks und Technikbegeisterte funkten nach Feierabend. Das war's. Doch in den vergangenen zwei Jahrzehnten sind die Kommunikationsmöglichkeiten durch das Aufkommen der Mobiltelefone und vor allem durch den Siegeszug des Internets explodiert. Mit einem Smartphone können wir nicht mehr nur telefonieren, sondern unter anderem mailen, simsen, chatten, skypen, twittern, surfen und Facebook-Mitteilungen verschicken. Zugleich ist die Menge der Daten, die wir in unserem Alltag produzieren, exponentiell gewachsen. Unsere individuelle Datenspur beginnt vor unserer Geburt, mit den ersten Ultraschallbildern auf dem Rechner eines Gynäkologen, und sie hört nach dem Tod nicht auf. Die Möglichkeit, große Datenmengen zu speichern, wächst unaufhaltsam. Selbst unsere privaten Festplatten fassen inzwischen ein Terabyte (1000 Gigabyte) und mehr. 2012 wurden in jeder Minute zwei Millionen Google-Suchen gestartet und 48 Stunden neues Videomaterial bei YouTube hochgeladen. Bei Instagram wurden in der gleichen Zeit 3600 neue Fotos gepostet und in Apples AppStore 47000 Apps heruntergeladen. Jede Minute wurden mehr als 204 Millionen E-Mails verschickt.[15]

Für eine Behörde, deren Anspruch es ist, dass ihr kein relevanter Informationsschnipsel entgeht, ist diese Entwicklung auf den ersten Blick ein Alptraum - zumal viele Nutzer inzwischen in der Lage sind, ihre Kommunikation zu verschlüsseln. Am Festnetztelefon von einst musste man dafür noch in vorher vereinbarten Codes und Rätseln sprechen. Heute sind Techniken wie GSM, auf denen Mobilfunknetze basieren, automatisch grundverschlüsselt, das Gleiche gilt für Internetstandards wie SSL. Und auch Privatpersonen können sich mit geringem Aufwand Verschlüsselungssoftware für Chats oder E-Mails herunterladen. Auch deshalb finden sich in den von Edward Snowden geleakten Dokumenten der NSA viele Passagen, in denen von den enormen «Herausforderungen» die Rede ist, die die digitale Revolution für die Geheimdienste darstellt. Aus Sicht der NSA besteht diese Herausforderung vor allem in einer grundlegenden Verschiebung der zu überwachenden Infrastrukturen. Jahrzehntelang fokussierten die USA und ihre engsten Verbündeten, die «Five Eyes», ihr nachrichtendienstliches Interesse auf Satelliten. Die Antennen der am weltumspannenden Satellitenüberwachungsnetzwerk «Echelon» beteiligten Stationen waren in den Orbit gerichtet und vor allem für das Abhören internationaler Telefonverbindungen gedacht. Dieses System läuft unter dem Namen «Fornsat» noch immer, wie eine Karte der Satelliten-Abhörstationen veranschaulicht. Die britische Satelliten-Abhörstation Bude im Norden Cornwalls trägt demnach den Codenamen «Carboy», ihr Pendant in den Vereinigten Staaten heißt «Timberline» - dahinter verbirgt sich der NSA-Standort Sugar Grove im Norden Virginias.

Gleichzeitig ermöglicht die Digitalisierung für die Nachrichtendienste den Eintritt in eine neue Welt der globalen Überwachung. Die Jagd auf die Bits und Bytes ist eröffnet. Die Welt von heute mag zwar unübersichtlicher sein, als sie es vor 20 Jahren war, aber für die Geheimdienste bieten sich völlig neue Anzapfquellen. Es geht nicht mehr nur um die laufende, um die Echtzeit-Kommunikation. Sie sind

15 Inzwischen dürften die Zahlen deutlich höher liegen. Die Infografik, aus der diese Zahlen des Jahres 2012 entnommen wurden, ist abrufbar unter: http//:mashable.com/2012/06/22/data-created-every-minute.

zunehmend auch an den sogenannten «ruhenden Daten» interessiert, die nicht nur auf Privatrechnern und Smartphones gespeichert sind, sondern auf den Servern kommerzieller Anbieter oder in der Cloud, virtuellen Festplatten. Ist der Einbruch in diese reichen Datengründe erst einmal gelungen, übernehmen Supercomputer und ausgeklügelte Analyseprogramme in Fort Meade die Aufgabe, einen Großteil der abgefangenen Kommunikation zu filtern und zu analysieren. Das «goldene Zeitalter der Überwachung» sei angebrochen, heißt es in einem fünfseitigen Strategiepapier der NSA für die Jahre 2012 bis 2016. Es werde möglich, «jedermann» zu überwachen und fast in Echtzeit «jedes Endgerät» auf einer interaktiven Karte abzubilden, «jederzeit, überall».[16] Das ist der Traum der NSA, darauf richtet sie ihre Anstrengungen.

Der Großteil der Daten, die täglich durch das Internet fließen, läuft durch Glasfaserkabel. Hunderte von ihnen umspannen den Erdball, sie bilden das Rückgrat des Internets und kommen dem nahe, dass der damalige amerikanische Vizepräsident Al Gore in den neunziger Jahren als «Daten-Highway» bezeichnete. Für die NSA sind diese Kabel wichtige Ziele, sie sind «Herausforderungen», wie es in einem internen Dokument heißt. Ein modernes Kabel sei in der Lage, innerhalb von 14 Sekunden den Inhalt der amerikanischen Kongressbibliothek zu übertragen. Ein einziges dieser Glasfaserkabel übersteige damit die Kapazität aller Satelliten zusammengenommen.[17] Die Antwort der NSA auf das Internet kann niemanden überraschen, der die Geschichte der Behörde durch die vergangenen Jahrzehnte verfolgt hat. Nur Monate nach dem 11. September 2001 hatte die Regierung von George W. Bush ein Programm mit dem vielsagenden Namen «Totale Informationserfassung» («Total Information Awareness») ins Leben gerufen, das von einer Forschungseinrichtung des US-Militärs geleitet wurde. Dieses Programm hatte die massenhafte vollautomatisierte Überwachung zum Ziel und sah unter anderem die Einrichtung einer Megadatenbank mit persönlichen Profilen von US-Bürgern vor. Nach massiver Kritik an dem Programm bewilligte der US-Kongress im Jahr darauf keine neuen Mittel, doch dank der Enthüllungen von Snowden wissen wir, dass wesentliche Teile des Projekts insgeheim weitergeführt wurden - unter anderen Codenamen und in Verantwortung der NSA.

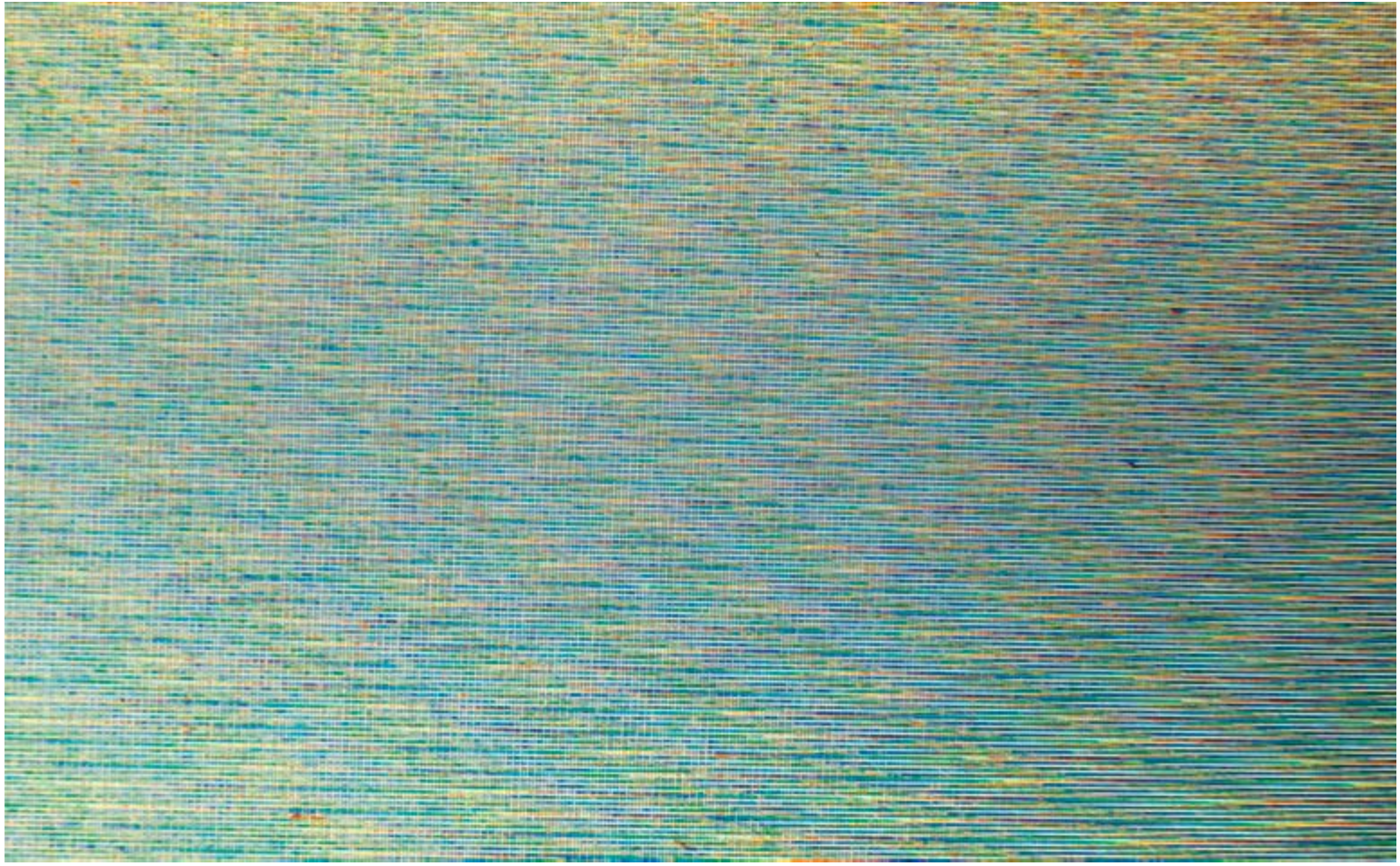
Die NSA selbst beschreibt ihr Ziel für das digitale Zeitalter in einem Dokument aus dem Februar 2012 als «Owning the Internet» - sie will das Internet besitzen oder zumindest kontrollieren.[18] Ähnlich drückt es das britische GCHQ aus. Eine Präsentation der Briten, die das großflächige Anzapfen von Glasfaserkabeln beschreibt, ist mit» Mastering the Internet» überschrieben, etwa: «Das Internet beherrschen.»[19]

16 NSA-Dokument vom Februar 2012: SigInt Strategy 2012-2016.

17 NSA-Dokument (undatiert): National Security Agency, Central Security Service – Overview Briefing.

18 NSA-Dokument vom Februar 2012: SigInt Strategy 2012-2016.

19 GCHQ-Dokument: „Mastering the Internet."



MATTHIAS SPIELKAMP

Journalismus nach Snowden – Wie das Internet die Medien verändert hat

Am 6. Juni 2013 veröffentlichte die britische Tageszeitung und Nachrichten-Website Guardian einen Artikel unter der eher unauffälligen Überschrift: NSA collecting phone records of millions of Verizon customers daily («Die NSA erfasst täglich Telefonaufzeichnungen von mehreren Millionen Verizon-Kunden»).[1] Sieht man sich allein die Zahl der Kommentare an, die auf der Website des Guardian zu dem Artikel abgegeben wurden – mehr als 2.500 – beginnt einem zu dämmern, dass dies der Anfang der bei weitem wichtigsten Geschichte des Jahres war, einer Story, die nicht wenige als Knüller des Jahrhunderts betrachten. Der Beitrag war der Beginn einer Lawine von Artikeln[2], die auf dem Material basierten, das der US-amerikanische Whistleblower Edward Snowden einigen Journalisten übergeben hatte. Diese Artikel waren auch der Auslöser für die wichtigste Geschichte dieses Jahres über die Medien, über die Rolle des Journalismus in der Gesellschaft, über die Rolle, die Journalisten in den Medien spielen. Auf diesen Aspekt möchte ich mich konzentrieren.

1. Journalismus oder Aktivismus?

Für diesen Vortrag habe ich zwar den Titel «Journalismus nach Snowden» gewählt, doch der erste Teil müsste eigentlich «Journalismus nach Greenwald» heißen. Denn es ist Glenn Greenwald, dieser brillante, streitbare und unangepasste Bestsellerautor, aus dem erst ein Blogger, dann ein Journalist wurde - und der von Kritik, persönlichen Angriffen und sogar offenem Hass seitens anderer Journalisten überflutet wurde. Ihm haben wir nicht nur für die Offenlegung der Snowden-Enthüllungen zu danken, sondern auch dafür, dass er eine Diskussion vorangebracht hat, die überfällig war. Es ist eine Diskussion über den schmalen Grat zwischen Journalismus und Aktivismus; darüber, ob es wichtiger ist, «fair und ausgewogen» zu sein, oder lieber wahrheitsgetreu. Und ob man sich einen «Journalisten» nennen darf, wenn man offen sagt, auf welcher Seite man steht. Diese Diskussion ist durchaus nicht neu und wird tatsächlich seit langem geführt. Voran getrieben hat sie in jüngster Zeit Dan Gillmor, heute Leiter des Knight Centre for Digital Media Entrepreneurship an der Arizona State University und Autor des Buches «We the Media», in dem er das Konzept des Bürgerjournalismus populär machte.[3]

Ein Jahr nach der «Lehman Brothers»-Pleite, die die Finanzkrise 2008 auslöste, veröffentlichte der Guardian einen Artikel Gillmors unter der Überschrift «The new

1 Greenwald, Glenn (2013): NSA collecting phone records of millions of Verizon customers daily. London; http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

2 Greenwald, Glenn et al. (2015): The NSA files. London; http://www.theguardian.com/us-news/the-nsa-files.

3 Gillmor, Dan (2006): We the Media. Sebastopol; http://it-ebooks.info/book/137.

rules of news» («Die neuen Regeln des Nachrichtenjournalismus»).[4] «Die Berichterstattung» zur Finanzkrise, so erklärte Gillmor recht unbescheiden, «erinnerte mich daran, dass Journalisten schon vor dem Auftreten der Krise des vergangenen Jahres dabei versagt hatten, ihren Auftrag zu erfüllen, und ihn auch weiterhin nicht erfüllen.» Daher machte er 22 Vorschläge, die er umzusetzen würde, wenn er Leiter einer Nachrichteneinrichtung wäre. Nummer 17 lautet: «Je mehr wir glauben, eine Angelegenheit sei für unsere Gemeinschaft von Bedeutung, desto hartnäckiger sollten wir an ihr dranbleiben. Wenn wir zu dem Schluss kommen, dass es gefährlich wäre, eine aktuelle politische Richtung weiter zu verfolgen, sollten wir uns aktiv dafür einsetzen, die Menschen davon zu überzeugen, die Richtung zu ändern. Das hätte zum Beispiel bedeutet, laut und beharrlich vor der Immobilien- und Finanzblase zu warnen, die sich in diesem Jahrzehnt gebildet hatte, und die ganz klar zu erkennen gewesen war.»

Schauen wir uns an, was Glenn Greenwald tut. Greenwald leistet zweifellos eine Weltklasse-Berichterstattung zu der gewaltigen Menge ungeheuer komplexer Daten und Akten, die Edward Snowden geliefert hat. Gleichzeitig erklärt er ohne ein Blatt vor den Mund zu nehmen, was das bedeutet: dass wir in einem Überwachungsstaat leben, dass unsere Regierungen gegen das Gesetz und sogar gegen das Grundgesetz verstoßen, und dass die Geheim- und Sicherheitsdienste, wie die NSA der USA, der britische GCHQ und viele andere, völlig außer Kontrolle sind.

2. Eine Schande für den Rechtsstaat, aber keine Überraschung

Die meisten von Ihnen wissen, was mit Edward Snowden geschah. Die US-Regierung zog seinen Pass ein und entzog ihm dadurch sein Reiserecht. Die Regierung der USA veranlasste die Regierungen von Portugal und Frankreich, das Flugzeug mit dem bolivianischen Präsidenten an Bord nicht über ihr Territorium fliegen zu lassen, da man annahm, dass auch Snowden mitflog. Man zwang das Flugzeug zur Landung, um es durchsuchen zu können. Diesen Vorgang halten viele Experten für einen Verstoß gegen das Völkerrecht. Verbündete der USA wie Deutschland wurden unter Druck gesetzt, kein Asyl zu gewähren. Dies alles ist skandalös, allerdings wenig überraschend. Es ist jedoch sehr aufschlußreich, sich anzusehen, was mit Glenn Greenwald geschah, dem Journalisten, der eine peinliche und schmerzende Geschichte nach der anderen darüber veröffentlichte, wie die Spionagedienste ihre Macht missbrauchen. Ich spreche nicht von der Tatsache, dass Personen, die mit ihm zusammen arbeiten, etwa die Filmemacherin Laura Poitras und Sicherheitsspezialist Jacob Appelbaum, von den US-Grenzpatrouillen stets schikaniert werden, wenn sie ihr Heimatland betreten, so dass sie sich gezwungen fühlten, sich außerhalb der USA niederzulassen. Ich spreche hier auch nicht von der Tatsache, dass die britischen Behörden mit dem Segen höchster Regierungskreise Greenwalds Lebensgefährten David Miranda neun Stunden auf dem Flughafen London-Heathrow festhielten, und dabei ganz offensichtlich das ohnehin schon sehr umstrittene britische Anti-Terror-Gesetz missbrauchten. Noch einmal: Das alles ist eine Schande für Regierungen, die sich selbst als demokratisch bezeichnen. Doch es ist zu erwarten, dass diejenigen, die den Überwachungsstaat angreifen, auf heftigste Reaktionen stoßen.

4 Gillmor, Dan (2009): The new rules of news. London; http://www.theguardian.com/commentisfree/cifamerica/2009/oct/02/dan-gillmor-22-rules-news.

3. Die Angriffe von Journalisten auf Glenn Greenwald

Weniger zu erwarten war es jedoch, dass Journalistenkollegen Greenwald in Scharen angreifen würden, noch dazu unter der Gürtellinie. Greenwald wurde vorgeworfen, er leiste Beihilfe und Anstiftung zu einem Verbrechen, weil er die vertraulichen Informationen von Snowden veröffentlichte. Ihm wird vorgeworfen, die Grenze zwischen eigener Meinung und direkter Berichterstattung zu verwischen. Ein Kolumnist der New York Times sagte in einer Talkshow, «Ich wäre fast bereit, Glenn Greenwald einzusperren – diesen Journalisten da draußen, der [Snowden] helfen will, nach Equador zu entkommen.» Bill Keller, ehemaliger Chefredakteur der New York Times, erklärte, dass unter seiner Leitung Greenwald als Reporter keinen Artikel zu den Snowden-Daten hätte veröffentlichen dürfen, denn er sei Kolumnist, kein Reporter. Und Bob Woodward, bekannt aus der Watergate-Affäre, griff Greenwald dafür an, dass er seine Quelle nicht geschützt hätte und keine zusammenhängende Geschichte über die Informationen, die er erhalten hatte, herausbrachte.

Ich bin ein großer Freund der Medienkritik. Ich denke, es ist notwendig, die sogenannte vierte Gewalt zu kontrollieren, eine gewisse Kontrolle und Rechenschaft der Institution auszuüben, die zum System der Kontrolle und Rechenschaft gehören sollte. Aber hier haben wir die Situation, dass Menschen anscheinend ein Problem damit haben, sich mit der Tatsache anzufreunden, dass der Journalismus sich verändert hat – und zwar für immer. Das hat viel mit dem Aufkommen von Blogs zu tun und damit, dass heute jeder über das Internet veröffentlichen kann. Aber es ist nicht der leidige alte Streit namens «Blogger gegen Journalisten». Der ist vorbei.[5] Es ist die Frage danach, wie Journalismus und Aktivismus zueinander stehen; die Frage, ob Journalisten Chronisten der Ereignisse sind oder für Veränderung kämpfen.

In Ländern mit einem britischen Kulturerbe, insbesondere in den USA, ist die Trennung zwischen Berichterstattung und Kommentar geradezu eine Glaubensfrage. Wer an diese Unterscheidung glaubt, ist Journalist; wer nicht daran glaubt, ist Aktivist. Und Aktivist zu sein, ist in den Augen eines Journalisten eher verachtenswert. Denn angeblich vermittelt der Journalist Fakten und der Aktivist tritt für eine Ansicht, Weltanschauung oder Ideologie ein. Das Internet hat die Dinge ein wenig ins Wanken gebracht, und die Snowden-Story hat dieses Wanken zu einem kräftigen Schaukeln verstärkt. Denn sie rückt eine Art der Berichterstattung in den Vordergrund, die bislang auf regionale Nachrichten beschränkt war, und darauf, im Internet praktiziert zu werden, statt in einer 192 Jahre alten britischen Zeitung mit einer weltweiten Leserschaft von monatlich mehreren Millionen Menschen.

Wir haben den Reportern des Guardian zu danken, dass sie diese Geschichte hartnäckig verfolgt haben, selbst als sie intensivem politischen Druck ausgesetzt waren. Sie berichteten unter rechtlichen Verhältnissen, die es einer Regierung nicht nur gestatten, die Berichterstattung massiv zu behindern und Journalisten zu zwingen, Beweismaterial zu vernichten. Sie arbeiten auch unter einer Regierung, die diese einer modernen Demokratie unwürdigen Befugnisse auch tatsächlich nutzt. Wir müssen der Redaktion aber auch danken, dass sie jemand wie Greenwald an der Geschichte weiter arbeiten ließ. Denn sie tut dies auch in einer Weise, die zu tun bereit ist, was Gillmor fordert. Ich erinnere daran: «Je mehr wir glauben, eine Angele-

5 Rosen, Jay (2005): Bloggers vs. Journalists is Over. New York; http://archive.pressthink.org/2005/01/21/berk_essy.html.

genheit sei für unsere Gemeinschaft von Bedeutung, desto hartnäckiger sollten wir selbst dranbleiben. Wenn wir den Schluss ziehen, dass ein Weiterverfolgen eines aktuellen politischen Weges gefährlich wäre, sollten wir uns aktiv dafür einsetzen, die Menschen davon zu überzeugen, die Richtung zu ändern.»

Jetzt – und das ist die jüngste verrückte Entwicklung in dieser Geschichte voller verrückter Entwicklungen – will Greenwald noch einen Schritt weiter gehen. Er hat beschlossen, den Guardian zu verlassen und eine Nachrichtenorganisation mit dem Geld des Milliardärs und Ebay-Gründers Pierre Omidyar aufzubauen. Das ist eine einmalige Gelegenheit, sagt Greenwald, und man muss ihm zustimmen. Ob es gelingt und er und seine Mitgründer etwas aufbauen können, das funktioniert und sich nicht im Laufe der Zeit zu einer normalen Nachrichtenredaktion entwickelt, bleibt abzuwarten. Ich freue mich schon sehr darauf, dieses Experiment zu verfolgen.

4. JournalistInnen und Technik: Ein angespanntes Verhältnis

Ich habe noch einen letzten Punkt auf meiner Liste. Er betrifft Technologien. Ich war fast 15 Jahre als Dozent an Universitäten und als Lehrer an Schulen für Journalismus tätig und bin es manchmal heute noch. Mein Spezialgebiet ist alles Digitale: Online-Recherche, der Umgang mit Social Media im Journalismus, wie man eine gute Website aufbaut und so weiter. Wann immer ich die Möglichkeit hatte, den Lehrplan selbst zu gestalten, habe ich ein Thema eingebaut, das ich «Kommunikationssicherheit für Journalisten» nenne. Ein besserer Titel ist wahrscheinlich «digitaler Quellenschutz». Es geht darum, Technologien zu nutzen, um Technologien abzuwehren, Verschlüsselung zu nutzen, um die Spionageprogramme der NSA von der eigenen E-Mail-Kommunikation fernzuhalten und eine Festplattenverschlüsselung zu verwenden, um die eigenen Informationen zu schützen, wenn man von einem «Schurkenstaat» wie dem britischen verhaftet und verhört wird, oder Anonymisierungstechnologien wie TOR zu verwenden, um im Internet zu surfen, ohne dass jemand erfährt, wohin man geht oder woher man kommt.

Meine Erfahrung war folgende: je weniger repressiv das Regime in dem Land war, aus dem die Teilnehmer an den Seminaren kamen, desto geringer war das Interesse an solchen Dingen. Ich bin mir recht sicher, dass ich niemals in einem meiner Workshops auch nur einen deutschen Journalisten überzeugt habe, Technologien zur E-Mail-Verschlüsselung aktiv und dauerhaft zu verwenden. Als ich jedoch vor einigen Jahren noch vor dem Krieg in Syrien war, musste ich niemanden überzeugen, Technologien zur Verschleierung der eigenen Internetkommunikation zu verwenden. Die Kolleginnen und Kollegen dort verwendeten sie ohnehin schon alle. Und nun stellen wir fest, dass wir es waren, die Journalistinnen und Journalisten in den «demokratischen Rechtsstaaten», die nicht aufgepasst haben. Wir haben auf unsere Verfassungen vertraut, die Rede- und Pressefreiheit garantieren, auf die Allgemeine Erklärung der Menschenrechte[6] und den Internationalen Pakt über bürger-

6 Vereinte Nationen (1948): Allgemeine Erklärung der Menschenrechte; http://www.un.org/depts/german/menschenrechte/aemr.pdf.

liche und politische Rechte[7], der verspricht, die freie Meinungsäußerung und Privatsphäre im Internet zu schützen.

Die Global Network Initiative erklärt: «Staaten haben sich dazu verpflichtet, diesen Schutz allen zu garantieren, die sich innerhalb ihrer effektiven Regierungsgewalt und Kontrolle befinden. In vielen Fällen müssen sie auch Einzelpersonen vor der Verletzung ihrer Rechte durch andere Personen oder Unternehmen schützen. Einschränkungen von Rechten müssen sich auf veröffentlichte, klare, spezielle Rechtsnormen gründen; einem legitimen Zweck in einer demokratischen Gesellschaft dienen, für dieses Ziel «notwendig» und «angemessen» sein, dürfen keine Diskriminierung beinhalten, dürfen den zuständigen Behörden kein übermäßiges eigenes Ermessen zugestehen und müssen wirksamen Schutzmaßnahmen und Rechtsbehelfen unterliegen.» [8]

Wir erkennen nun, dass es unsere eigenen Geheimdienste und Regierungen sind, die uns betrügen, die uns ausspionieren und die uns wie Kriminelle und Staatsfeinde behandeln. Es gab viele Warnzeichen, wie die Enthüllung des Echelon-Spionageprogramms der USA 2001[9]; die meisten von uns haben diese Hinweise ignoriert, so wie ich selbst auch. Wir dürfen diesen Fehler nicht noch einmal begehen.

5. Mathematik und Technik erhöhen die Kosten der Überwachung

Gegen Überwachung gibt es keine einfache Lösung. Ja, wir können der Mathematik vertrauen, wie der Kryptographie-Experte Bruce Schneier argumentiert, doch nur in gewissem Umfang.[10] Denn der Überwachungsstaat ist ein Zustand, ein Stand der Dinge. Wir können uns nicht mit Technik vor Leuten schützen, die die Genehmigung besitzen, in unser Haus einzubrechen, unsere Büros zu durchsuchen, unsere Mobiltelefone und Computer zu konfiszieren, die unsere Telefongespräche mithören und unsere E-Mails mitlesen dürfen, ohne ein einziges Beweisstück für ein Fehlverhalten vorlegen zu müssen. Ja, wir müssen bestimmte Technologien verwenden, um uns zu schützen, und ich rate dringend dazu, es zu tun: PGP, Tor, TLS und IPSec, OTR und Open-Source-Technologien. Wer nicht weiß, was all das bedeutet, der sollte es herausfinden. Dazu gibt es eine Reihe von Tools und Anleitungen.[11] Man kann dazu ein wenig im Internet recherchieren, sollte aber darauf achten, «disconnect»[12] zu nutzen, um Daten vor Google zu verbergen. Davon sollte

7 Vereinte Nationen (1966): Internationaler Pakt über bürgerliche und politische Rechte. New York; http://www.auswaertiges-amt.de/cae/servlet/contentblob/360794/publicationFile/3613/IntZivilpakt.pdf.

8 Brown, Ian/ Korff, Douwe (2012): Digital Freedoms in International Law. Washington, DC; https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf.

9 Europäisches Parlament (2011): Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)) - PE PE 305.391 / A5-0264/2001. Straßburg, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//DE.

10 Schneier, Bruce (2013): NSA surveillance: A guide to staying secure. London; http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance.

11 Tactical Technology Collective and Front Line Defenders (2015): Security in-a-box. Berlin; https://securityinabox.org.

12 https://disconnect.me.

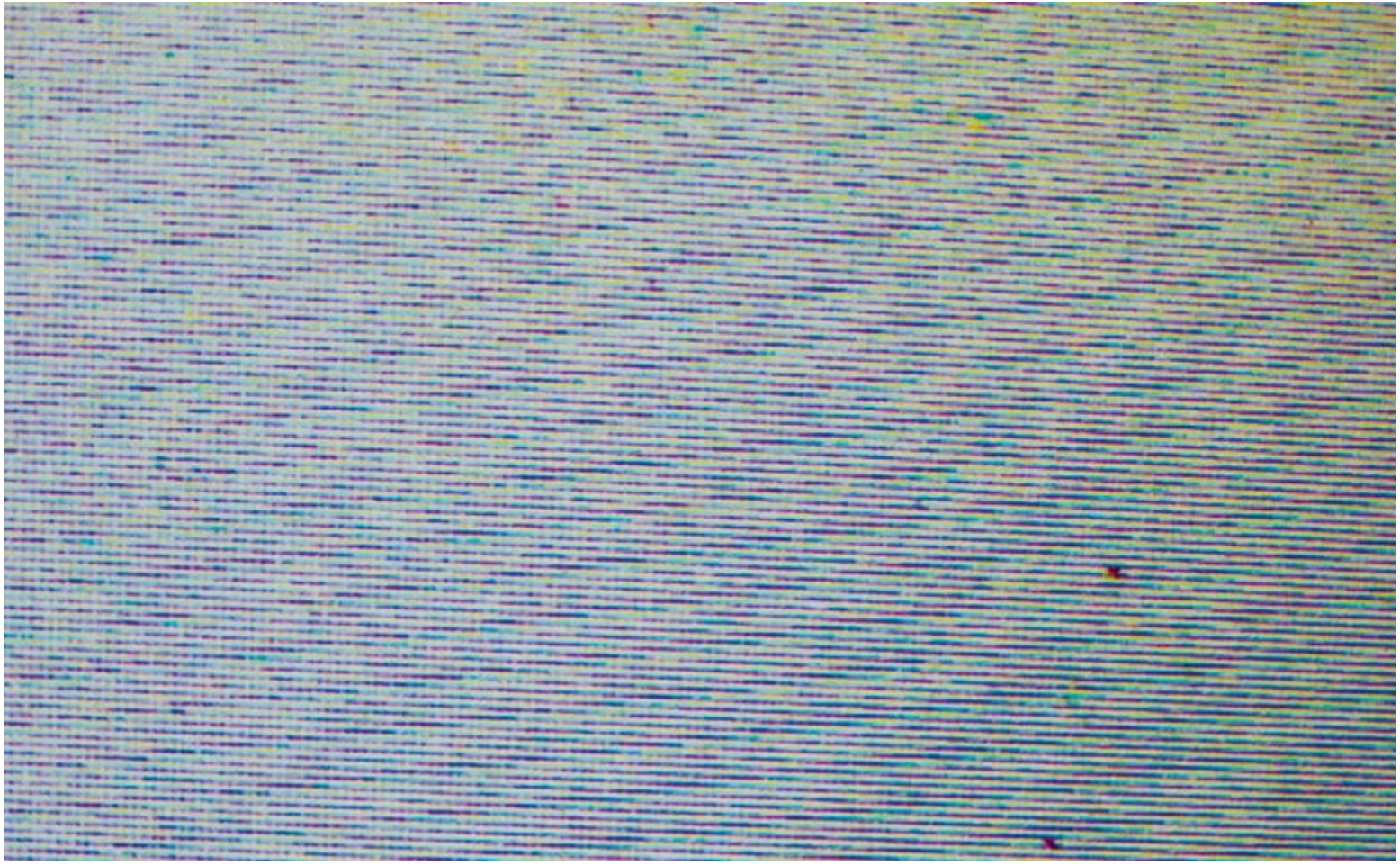
man Freunden, Verwandten und Kollegen erzählen, und darüber berichten: in der Zeitung, im Radio, im Fernsehen, in Blogs und in der Vereinspostille. Hauptsache, die Informationen verbreiten sich. Denn je mehr von uns diese Dinge nutzen, desto höher sind die Kosten der Überwachung. Das verleiht uns keine vollständige Sicherheit. In einem Überwachungsstaat gibt es keinen vollkommenen Schutz der Privatsphäre und des Redaktionsgeheimnisses. Aber es ist um Einiges besser, als sich in das vermeintliche Schicksal zu ergeben, dass unsere gesamte Kommunikation rund um die Uhr überwacht wird.

6. Falsche Ausgewogenheit und fauler Journalismus

Dies bringt mich wieder zu meinem Ausgangspunkt zurück, der Kritik an der sogenannten «falschen Ausgewogenheit». Sie gehört zu einer bestimmten Idee des Journalismus, der von einem Reporter praktiziert wird, der nicht voreingenommen ist, keine eigene Meinung hat und keinen Anteil an dem, was passiert. Das funktioniert so:[13] Eine Seite gibt eine Erklärung ab. Der Reporter schreibt sie auf und bittet die andere Seite um ihre Reaktion. Damit ist alles abgedeckt, der Fairness Genüge getan und die Wahrheit liegt irgendwo in der Mitte. Dass das nicht stimmt, wissen wir alle. Es ist nicht so, dass es einige Gründe dafür gibt, die verfassungsbrechende Massenüberwachung von Bürgern schlecht zu finden, und einige, sie in Ordnung zu finden. Und dass dann die Wahrheit irgendwo in der Mitte liegt. Das zu denken ist einfach nur fauler Journalismus. Aber die Wahrheit ist: Selbst wenn ich jetzt ausführlich von Konzepten und ihrer Bezeichnung gesprochen habe, sei es «Journalismus kontra Aktivismus», «Berichterstattung kontra Einflussnahme» – es ist mir eigentlich egal, wie Sie es nennen.[14] Es ist mir gleichgültig – so lange wir alle für eine Gesellschaft kämpfen, in der wir unser Recht auf Privatsphäre als Individuen wahrnehmen können, eine Gesellschaft, in der die Medien ihrer Aufgabe nachkommen können, ohne dass sie von einer internationalen Bande von Regierungen unter Missachtung von Rechtmäßigkeit und Legitimität ausspioniert werden.

13 Rosen, Jay (2011): «He Said, She Said» Journalism: Are We Done With That Yet?, New York; http://www.huffingtonpost.com/jay-rosen/he-said-she-said-journali_b_187682.html.

14 Rosen, Jay (2013): Politics: some / Politics: none. Two ways to excel in political journalism. Neither dominates. New York; http://pressthink.org/2013/06/politics-some-politics-none-two-ways-to-excel-in-political-journalism-neither-dominates.



JOHANNES LICHDI

Dresden, 19. Februar 2011: Von der Raumkontrolle zur elektronischen Kommunikationskontrolle

Die Abfrage der elektronischen Verkehrsdaten in der Dresdner Südvorstadt anläßlich der Demonstrationen des 18. und 19. Februars 2011 hat der deutschen Öffentlichkeit schon vor den Enthüllungen Eward Snowdens eine Ahnung vom Ausmaß anlassloser Massenüberwachung sowie der Skrupellosigkeit staatlicher Überwachungsbehörden vermittelt. Was angesichts der NSA-Überwachung geradezu als harmlose Sandkastenspiele einer überforderten Polizei erscheint, taugt doch als Lehrstück für den Einsatz polizeilicher Überwachungstechniken an der Schwelle herkömmlicher Formen der Raumkontrolle zur neuartigen Kontrolle des elektronischen Kommunikationsraums. Das Fallbeispiel zeigt, wie sich der Einsatz räumlicher und elektronischer Kontrolltechniken in einer bestimmten politischen Situation ergänzten und ablösten, in der sich der sächsische Staat bedroht sah.

I. Die Ereignisse

1. Vorgeschichte 2010

Seit Jahren spaltet die Frage nach dem angemessenen Umgang mit der Zerstörung Dresdens am 13. Februar 1945 und dem richtigen Totengedenken die Stadt. Die Ereignisse vom 19. Februar 2011 zeigen, wie das in Sachsen herrschende Leitbild vom «stillen Gedenken» amtlich durchgesetzt werden sollte. Im Vorjahr war es einem bundesweiten Bündnis «Dresden nazifrei» gelungen, durch sogenannte «Massenblockaden» den alljährlichen auf mehrere Tausend Teilnehmer angewachsenen Aufzug der Neonazis zu verhindern. Seit dem Morgen des 13. Februar 2010 war es tausenden Menschen gelungen, die Plätze und Straßen rund um den Schlesischen Platz am Neustädter Bahnhof zu besetzen, so dass die Nazis ihre Versammlung gegen 18 Uhr abbrechen mussten. Damit hatte sich das neue Konzept der Platzbesetzungen, das schnell bundesweit zum Vorbild wurde, als unerwartet erfolgreich erwiesen. Jetzt schien ein geeignetes Mittel gefunden, Widerstandsformen der Antifa mit dem Aktions- und Protestbedürfnis breiter Schichten zu verbinden. Der sächsische Staat hat diese Ereignisse als Niederlage empfunden. Daher wollte er 2011 unbedingt demonstrieren, dass nur er selbst zu entscheiden habe, was am 13. Februar geschehen darf und was nicht. Daher sollte diesmal der Naziaufmarsch unbedingt durchgesetzt werden.

2. Das Scheitern des polizeilichen Raumkontrollkonzepts

a) Präventive Raumzonierung

Die Polizeiführung entwickelte ein weiträumiges Raumkontrollkonzept, um die politisch gegenläufigen Demonstrationen möglichst weit zu trennen. Dabei ging es nicht um die berühmte «Steinwurfweite», vielmehr sollten entlang natürlicher geographischer Grenzen wie dem Bahndamm und der Elbe ganze Stadtteile einer einzigen politischen Kraft vorbehalten werden. Die gegenläufigen Versammlungsrechte der Neonazis und ihrer Gegner wurden so einem aus Sicht der Polizei optimalen Einsatzszenario unterworfen. So sollten drei Versammlungen verschiedener Anmelder aus dem Nazi-Spektrum in Dresden-Cotta zusammengelegt werden. Das Verwaltungsgericht Dresden erklärte diese Zwangszusammenlegung verfassungsrechtlich zutreffend für rechtswidrig. Darauf erlaubte die Stadtverwaltung Dresden dem Anmelder Maik Müller auf dem Nürnberger Platz in der Südvorstadt zwar eine Kundgebung, aber keinen Aufzug seiner neonazistischen «Freien Kräfte». Im Klageverfahren räumte die Polizei aber ein, dass sie auch einen Demonstrationszug über die Fritz-Löffler-Straße zum Hauptbahnhof und Zurück gewährleisten könne. Daher entschied das Verwaltungsgericht in diesem Sinne. Polizei und Stadt sorgten nun für die Schaffung einer exklusiven Nazizone in der Südvorstadt: Sie setzten den Rektor der TU Dresden, Prof. Müller-Steinhagen, erfolgreich unter Druck, seine für das benachbarte Universitätsviertel angemeldete Antinazi-Demo abzusagen. Zugleich verbot die Stadt eine Versammlung des DGB am Gewerkschaftshaus, das zwar 2 km vom Aufzugsort Müller entfernt liegt, aber eben doch südlich der Elbe. Alle Antinaziproteste wurden auf die nördliche Elbseite in die «alternative» Neustadt verbannt. Die Verantwortlichen wagten aber nicht, die zahlreichen Mahnwachen der Kirchen im Stadtgebiet auch in der exklu-

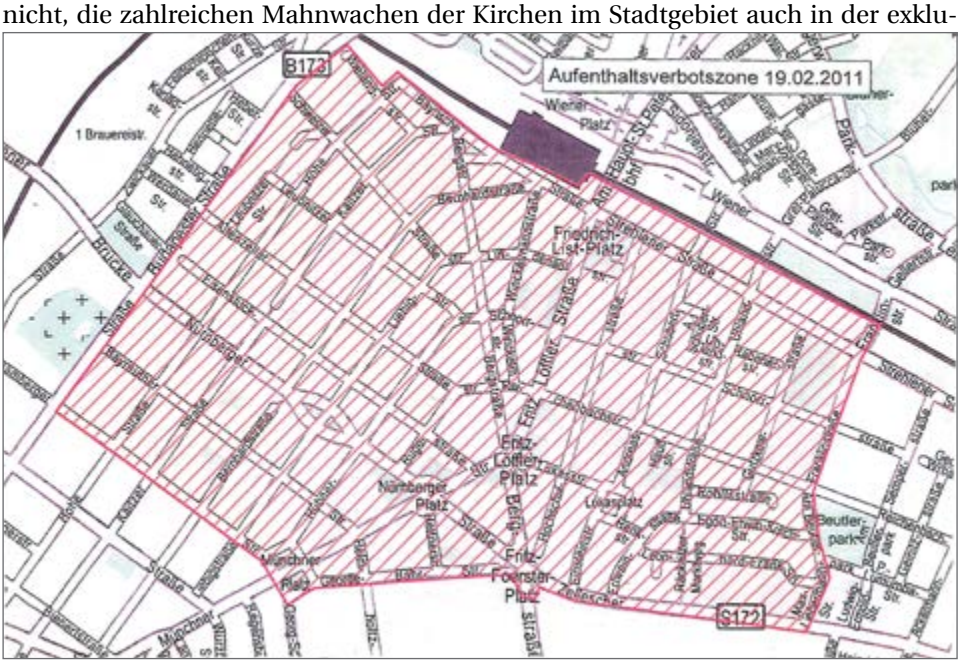


Abb. «Aufenthaltsverbotszone» am 19. Februar 2011 in Dresden

siven Nazizone zu verbieten. Die von der Polizei auf Geheiß des Innenministeriums[1] durchgesetzte räumliche Anordnung spiegelte so exakt die in der «Sächsischen Demokratie» herrschende Extremismustheorie wieder: Im Zentrum der Innenstadt, um Frauenkirche, Rathaus und Zwinger, die offiziöse Menschenkette der Oberbürgermeisterin als staatlich erwünschte Versammlung, am Rande außer Sichtweite und durch Bahndamm und Elbe säuberlich getrennt, die «extremistischen» Flügel der Gesellschaft: die Neonazis außerhalb der Innenstadt südlich des Hauptbahnhofs in der Südvorstadt und die Nazigegner, die die Staatsmacht in Sachsen seit jeher für «Linksextremisten» hält, in der «alternativen» Neustadt. Nur die evangelische und katholische Kirche durften ihre Mahnwachen wie angemeldet in allen Stadtteilen durchführen – auch in der exklusiven Nazizone. So blieb etwa die Lukaskirche in der Nähe der Aufzugsstrecke Müller ein legaler Anlaufs- und Versammlungspunkt.

b) Besetzung der «Platzverweiszone» und Nazigewalt

Die eingesetzten Polizeikräfte hatten eine Karte erhalten, in der weite Teile der Südvorstadt als «taktische Platzverweiszone» schraffiert war. Sie versuchten an diesen Grenzen als «Raumschutz rechts» durch Sperren und Polizeiketten das Eindringen vermuteter «Störer» in die exklusive Nazizone zu verhindern. Gegendemonstrierende sollten einen Platzverweis erhalten. Auch die Staatsanwaltschaft ging später bei ihren Ermittlungen gegen die friedlichen Platzbesetzer auf der Kreuzung Löfflerstraße / Reichenbachstraße wegen «grober Störung» einer Versammlung davon aus, dass es in der Südvorstadt eine «Aufenthaltsverbotszone» für Gegner des Aufzugs Müller gegeben habe.[2] Eine solche Zone hätte nach § 21 Abs. 2 des Sächsischen Polizeigesetzes für bestimmte Personen eingerichtet werden können, nicht aber für eine unbestimmte Anzahl. Da es in rechtlicher Hinsicht nie eine «Aufenthaltsverbotszone» gegeben hat, war es legal, sich am 19. Februar 2011 in der exklusiven Nazizone aufzuhalten.

Wie bei der Größe des abzusperrenden Gebiets nicht anders zu erwarten, ist das Raumkontrollkonzept der Polizei kläglich gescheitert. Obwohl nach Auskunft eines hohen Dresdner Polizeiführers 50 Hundertschaften nötig gewesen wären, waren tatsächlich «nur» 36 Hundertschaften im Einsatz. Zudem hatte die Polizei nicht damit gerechnet, dass tausende Nazigegner über die Autobahn und den Zubringer ins Gebiet laufen würden, nachdem die Polizei ihre Busse weit vor Dresden gestoppt hatte. Zwar wurde auch von Nazigegnern Gewalt gegen Polizisten und Sachen ausgeübt. Es ist aber gerichtlich festgestellt, dass der Zugang in das Gebiet friedlich und ohne Gewaltanwendung möglich war. Ein Polizeiführer sagte vor Gericht aus, dass es bereits um 11 Uhr klar gewesen sei, dass «die Rechten an diesem Tag nicht laufen würden». Seit dem Vormittag des 19. Februar kam es in- und außerhalb der exklusiven Nazizone zu zahlreichen Platzbesetzungen. Ab ca.

1 Die Spitze des Innenministeriums hat das präventive Raumkontrollkonzept veranlasst. Sie versteckt sich hinter dem damaligen Dresdner Polizeipräsidenten Hanitzsch, der Mitte 2011 gefeuert wurde. Meine Informationen stammen aus Polizeikreisen, die ich in meiner damaligen Eigenschaft als Landtagsabgeordneter vertraulich erhalten habe.

2 Zu den Einzelheiten des Sachverhalts mit Nachweisen siehe die Verfassungsbeschwerde des Verfassers vom 7. 11. 2014 abrufbar unter http://www.johannes-lichdi.de/fileadmin/user_upload/Judica/14-11-6.VB-SaechsVerfGH.pdf .

13 Uhr versammelten sich mitten im Gebiet bis zu 1700 Personen auf der Kreuzung Fritz-Löffler-Straße / Reichenbachstraße. Die Polizei verzichtete etwa um 15 Uhr auf die um 14.30 Uhr angedrohte Räumung. Um ca. 16.30 Uhr sagte die Polizei die Versammlung Müller auf dem Nürnberger Platz ab und begann sofort danach die Menschen, die sich auf der Kreuzung Fritz-Löffler-Straße / Reichenbachstraße befanden, einzukesseln und deren Identität festzustellen. In den nächsten Jahren wurden insgesamt 465 Personen wegen «grober Störung einer Versammlung» nach § 21 des Versammlungsgesetzes strafrechtlich belangt.[3] Das politisch motivierte Raumkontrollkonzept war nicht nur erfolglos, es verhinderte auch die Erfüllung des polizeilichen Kernauftrags, nämlich den Schutz der Bürgerinnen und Bürger vor Gewalt und Sachbeschädigungen. So griff eine Streifenwagenbesatzung nicht ein, als ein gewalttätiger Nazimob das linke Hausprojekt «Praxis» minutenlang mit Steinen bewarf.[4] Wie Polizeipräsident Hanitzsch später gegenüber der Presse bestätigte, standen keine Polizeikräfte zur Verfügung, weil sie zur Absperrung der exklusiven Nazizone eingesetzt waren.

3. Kontrolle der elektronischen Kommunikation

Während die Raumkontrollmaßnahmen der Polizei öffentlich zu erleiden waren, erfolgte die elektronische Kommunikationskontrolle verdeckt und geheim.

a) Einsatz eines IMSI-Catchers und Telekommunikationsüberwachung

Das Landeskriminalamt Sachsen setzte am 18. und 19. Februar 2011 in der Nähe des «Hauses der Begegnung» in Dresden – Pieschen, in dem sich Büros der Partei «Die Linke» befinden und das Bündnis «Dresden nazifrei» arbeitete, einen sogenannten «IMSI-Catcher» ein. IMSI-Catcher sind Geräte, mit denen die auf der Mobilfunk-Karte eines Mobiltelefons gespeicherte «International Mobile Subscriber Identity», die «IMSI» ausgelesen werden kann. Der IMSI-Catcher simuliert mit einem starken Signal eine Funkzelle und veranlasst alle Mobiltelefone in der Umgebung zum Einloggen. So kann der Standort eines Mobiltelefons eingegrenzt werden. Ein IMSI-Catcher taugt auch zum Mithören der Kommunikationsinhalte. Zudem hörte das Landeskrimalamt bestimmte Mobilfunknummern ab. Beide Maßnahmen wurden mit einem Strafermittlungsverfahren gegen eine sogenannte Antifa-»Sportgruppe» wegen des Verdachts der Bildung einer kriminellen Vereinigung gerechtfertigt. Die Gruppe soll seit Jahren politischen Gegnern aufgelauert und diese körperlich misshandelt haben. Nach jahrelangen Ermittlungen ist das Verfahren im Herbst 2014 ergebnislos eingestellt worden.

b) Erfassung der Verkehrsdaten

Im Juni 2011 enthüllte der Journalist Paul Wrusch in der «tageszeitung», dass die Polizei Hunderttausende elektronischer Verkehrsdaten von Personen ermittelt hatte, die sich am 18. und 19. Februar vornehmlich in der exklusiven Nazizone

3 Sächsischer Landtag, Drucksache 5 / 13410.

4 https://www.youtube.com/watch?v=ab6CesvX5pI .

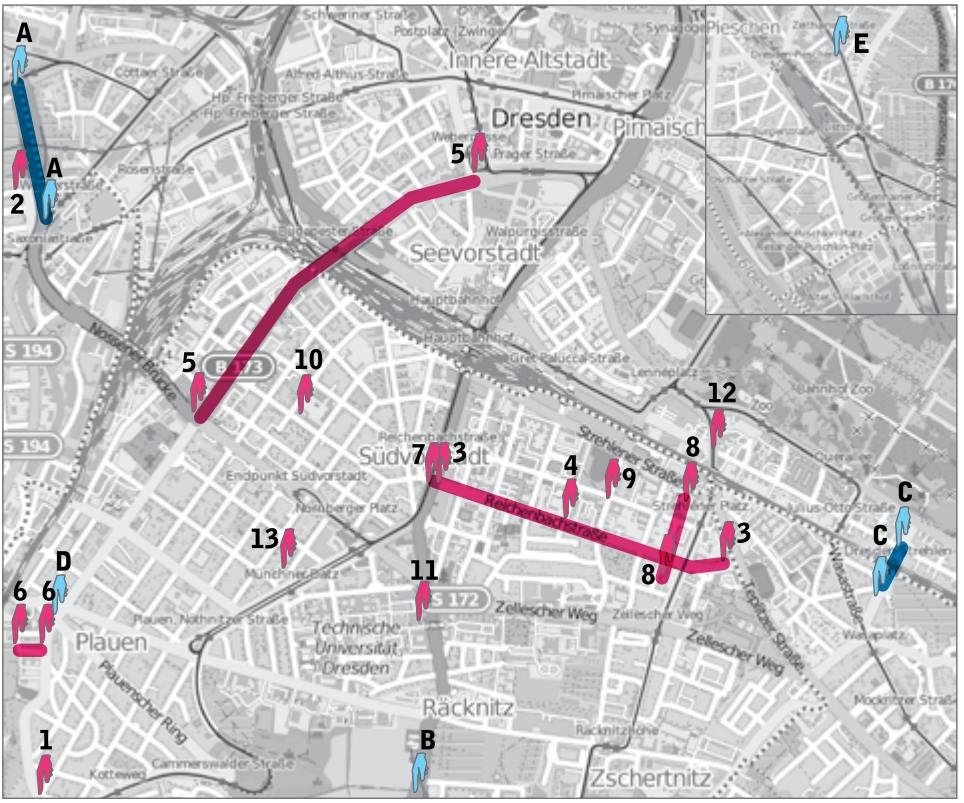


Abb. Karte mit Erhebungsorten in Dresden 2011, Legende (Nr. | Straße: Zeit | Details):

1-14 Sonderkommission 19. Februar der PD Dresden

1 Coschützerstr. / Kaitzerstr.: 13:45 -14:15
2 Wernerstr./Columbusstr.: 13:45 -14:15
3 Reichenbachstr.: 11:17-11:20/ 11:55 -12:10/ 14:00-15:30/17:10-17:35
4 Reichenbachstr./Gutzkowstr.: 14:15 -14:35/ 16:25 -16:35/ 17:25 -17:35
5 Nürnbergerstr./Budapesterstr.: 12:10 -12:40/ 15:50 -16:10
6 Kantstr.: 13:40 -14:00
7 Fritz-Löfflerstr./Reichenbachstr. 12:10 -12:25/ 16:25 -16:35
8 Reichenbachstr./AmBeutlerpark/ Zellescher Weg: 11:35-12:10/ 14:00-14:15
9 Schnorrstr./Franklinstr.: 14:45 -15:05/ 15:20 -15:35
10 Kaitzerstr. 27: 12:40 -13:00
11 Bergstr./Fußgängerbrücke Uni: 11:45 -12:20
12 Richard-Strauss-Platz: 12:20 -12:40
13 Müchner Pl./Georg-Schumann-Str.: 09:20-09:40/ 11:00-11:25

A bis E - Landeskriminalamt

A Fröbelstr. / Tharandterstr.: 07:00 - 19:00
800.600 Verkehrsd. und 229 Bestandsd.; Aufgrund des Beschlusses Az.270 Gs 711/11
B Kohlenstr. / Südhöhe
C Wiener Str. / Gustav-Adolph-Pl.
D Coschützer Str. 8 und 12 in Freital bei Dresden: 14:00 - 18:00
14.243 Verkehrsd. und 4.755 Bestandsd.; Aufgrund des Beschlusses Az.270 Gs 712/11
E Großenhainer Str. 93 18:02 - 19:02
81.299 Verkehrsd. und 35.748 Bestandsd.; «Haus der Begegnung» - Geschäftsstelle der Linken

der Südvorstadt aufgehalten hatten.[5] Das Amtsgericht Dresden hatte die Verkehrsdatenerhebungen mit zwei Anordnungen auf Antrag der «Sonderkommission 19. Februar» (Soko 19/2), die die Polizeiführung zur Verfolgung der Straftaten an diesem Tage eingerichtet hatte, sowie auf Antrag des Landeskriminalamts (LKA) zugelassen, dass die kriminelle Vereinigung aufspüren wollte. Die Telekommunikationsdienstleister übergaben der Soko 19/2 104.808 und dem LKA 1.127.975 Verkehrsdatensätze. Verkehrsdaten dokumentieren die Umstände jeder elektronischen Kommunikation: bei Mobiltelefonen die Nummern des Anrufers und des Angerufenen, die Dauer der Kommunikation sowie den Standort der Funkzelle, über die das Gespräch abgewickelt wird. Erfasst werden auch Kommunikationsversuche, SMS, Mails oder andere Internetdienste. Verkehrsdaten zeigen also Beteiligte, Zeitpunkte und Orte eines elektronischen Kommunikationsvorgangs an, nicht aber den Kommunikationsinhalt. Die Erfassung und Auslieferung aller Verkehrsdaten einer Funkzelle trifft vielleicht auch Verdächtige, ganz bestimmt aber sehr viele Unverdächtigte, auch besonders geschützte Berufsgeheimnisträger wie Ärzte, Rechtsanwälte, Abgeordnete oder Geistliche. Die Massenausspähung geschieht heimlich, da die Öffentlichkeit nichts bemerkt und nicht informiert wird.

c) Auswertung mit «eFAS» und «FARMEX»

Die Öffentlichkeit hat die massenhafte und heimliche Erfassung der Kommunikationsverkehrsdaten zu Recht als Skandal wahrgenommen. Sie ist aber nur der erste Schritt, um über die Auswertung von Kommunikationsbeziehungen soziale Gruppen herauszufiltern und deren Interaktionen aufzudecken. Die Polizei wollte so die von ihr unterstellten koordiniert operierenden Tätergruppen identifizieren. Das LKA führte die Daten des 18. und 19. Februar mit früher erhobenen Verkehrsdaten zusammen und wertete sie mit Hilfe des «ermittlungsunterstützenden Fallanalysesystem eFAS» sowie dem Programm «FARMEX» aus. Die Staatsregierung hatte das Software-Programm «eFAS» Ende 2008 für 3 Mio Euro von der Firma «rola Security solutions» erworben. Diese Firma soll jetzt auch die sogenannte Antiterror-Datei des Bundes technisch aufrüsten. Die Staatsregierung behandelt die Funktionalitäten der Analyseprogramme wie ein Staatsgeheimnis. Offenbar geht es um die Feststellung der Häufigkeiten von Telekommunikationen einzelner Adressen zu bestimmten Zeiten und Orten. Der Sächsische Datenschutzbeauftragte teilt in seinem lesenswerten Bericht zur Dresdner Funkzellenabfrage mit: «Das „ermittlungsunterstützende Fallanalysesystem“ (eFAS) ... dient zur „effektiven Bewältigung besonders hoher Informationsaufkommen ... Die Daten können importiert und mittels verschiedener Funktionalitäten bearbeitet und verwaltet werden. ... Das eFAS ist auch zur Durchführung von Rasterfahndungen geeignet. ... Auch die

5 Siehe schon Lichdi, Handygate Dresden 2011, Einblicke in Denken und Handeln sächsischer Ermittlungsbehörden, in: weiterdenken - Heinrich-Böll-Stiftung Sachsen, «Sachsens Demokratie», 2012, S.48 - 61 und die Verfassungsbeschwerde von Frau Katrin Göring-Eckardt zum Bundesverfassungsgericht, abrufbar unter http://www.johannes-lichdi.de/fileadmin/user_upload/Judica/VB-E_0609_mitck.pdf.

SoKo 19/2 hat das eFAS bei ihrer Arbeit eingesetzt."[6] Das Urteil des Amtsgerichts Dresden vom 13. Januar 2013 berichtet, dass LKA und Soko 19/2 «verdachtsbezogene Analysen» durchgeführt hätten: «Dabei wurden die Verkehrsdaten entsprechend den im Beschluss angefragten 14 Tatorten kopiert. Im Rahmen der Auswertung der Verkehrsdaten wurden im März 2011 ein Cross-Over zu den Rufnummern durchgeführt, d.h. ein Kreuzvergleich bezüglich der Anzahl der Tatorte, bei denen die Rufnummern festgestellt wurden."

Geheimdienste und Polizeien, die NSA wie der BND, und auch die Verantwortlichen in Sachsen, betonen gerne, dass ja «nur» Verkehrsdaten und keine Kommunikationsinhalte erhoben würden. Sie wollen damit der Öffentlichkeit einreden, dass die Erhebung von «Metadaten» oder Verkehrsdaten für das Grundrecht auf informationelle Selbstbestimmung irrelevant oder harmlos sei. Dem hat das Bundesverfassungsgericht schon 2010 in seiner Entscheidung zur Vorratsdatenspeicherung zu Recht widersprochen: «Die Aussagekraft dieser Daten ist weitreichend ... Adressaten ..., Daten, Uhrzeit und Ort erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden. ... Je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Bezogen auf Gruppen und Verbände erlauben die Daten ... unter Umständen die Aufdeckung von internen Einflussstrukturen und Entscheidungsabläufen».[7] Genau darum ging es am 19. Februar 2011: Um die Bereitstellung einer möglichst großen Datenmenge – in der Sprache des NSA eines «Heuhaufens», um daraus Kommunikations-, Bewegungs- und Sozialprofile abzuleiten und zu erstellen.

d) Identifizierung der Bestandsdaten

Die Erhebung der Verkehrsdaten und ihre Auswertung zielt auf die Identifizierung der Kommunikationsteilnehmer mit Hilfe einer Bestandsdatenerhebung. Bestandsdaten sind die beim Mobilfunkbetreiber gespeicherte Adresse und Klarname des Inhabers, sein Geburtsdatum, sowie eine Vielzahl weiterer Daten. Die Bestandsdatenabfrage ist seit 2012 im Bund und in Sachsen erweiternd neu geregelt worden. Das Landeskriminalamt erhob 55.499 Bestandsdaten, offenbar identifizierte das LKA standardmäßig alle Kommunikationsteilnehmer. Dagegen begnügte sich die Soko 19/2 mit der Erhebung von 649 Bestandsdaten. Gegen die so identifizierten Kommunikationsteilnehmer oder genauer, der bei den Anbietern registrierten Personen, können dann weitere Ermittlungsmaßnahmen eingeleitet werden. Trotz des riesigen Aufwands ist bisher nicht bekannt geworden, dass koordiniert handelnde gewaltätige Tätergruppen entdeckt und verurteilt werden konnten.

---

6 Der Sächsiche Datenschutzbeauftragte, Bericht zu den nichtindividualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung, Sächsischer Landtag, Drucksache 5 / 6787.

7 BVerfG vom 2.3.2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, R.211 - Vorratsdatenspeicherung.

II. Die Perspektive der Überwacher

1. Raumkontrolle

a) Behauptung des kommunikativen Schlachtfelds

Die Polizei nimmt für sich in Anspruch, nur entsprechend ihres gesetzlichen Auftrags zu handeln und die Gesellschaft vor gefährlichen Straftätern zu schützen. Guten Gewissens weist sie empört den Vorwurf zurück, vorsätzlich ungerechtfertigt in Grundrechte einzugreifen. Schließlich seien Grundrechtsbeeinträchtigungen durch Straftaten jedenfalls wesentlich intensiver als ihre Ermittlungseingriffe. Ihr Einsatzkonzept unter dem Stichwort «Trennungsgebot» rechtfertigt sie mit der Gefahr gewalttätiger Gegendemonstrierender. Dabei war es im Vorjahr zu Platzbesetzungen, aber nicht zu gewalttätigen Ausschreitungen gekommen. Die Polizei hielt an ihrer Strategie einer Trennung der Demonstrationsräume fest, obwohl sie wusste, dass ihr nicht genügend Einsatzkräfte zur Verfügung standen und sie auf unvorhergesehene Ereignisse nicht würde reagieren können. Letztlich ging es der Polizei also nicht um die Gewährleistung der öffentlichen Sicherheit, sondern um eine archaische Siegergeste: die sichtbare Behauptung ihrer Raumzonierungsfähigkeit auf dem kommunikativen «Schlachtfeld» Dresden. Die Behauptung der «taktischen Platzverweiszone», die den Einsatzkräften als Leitlinie aufgegeben wurde, rechtfertigte die Polizei als rechtsverbindliche «Aufenthaltsverbotszone», obwohl eine solche nie bestand. Dies zeigt das taktische Verhältnis der Polizei zu den Rechtsgrundlagen, die ihr Verhalten eigentlich steuern sollten: Die Polizeiführung legt ihr taktisches Einsatzkonzept fest und nennt dann beliebig Vorschriften zur Kritikabschirmung.

b) Durchwinken polizeilicher Gefahrenprognosen bei den Verwaltungsgerichten

Innenministerium und Polizei konnten ihr Raumkontrollkonzept nur planen, weil sächsische Verwaltungsgerichte seit Jahren die polizeilichen Gefahrenprognosen akzeptiert und das Trennungskonzept als scheinbar notwendige Folgerung durchgewunken hatten. Das Verwaltungsgericht Dresden und das Oberverwaltungsgericht Bautzen hatten alle Klagen von Nazigegnern gegen die Verweigerung ihres Demonstrationsrechts in Sicht- und Hörweite von Nazidemos abgewiesen. Sie haben damit Nazigegner rechtlos gestellt und so psychologisch wesentlich zur Eskalation beigetragen. Dennoch ist die öffentliche Rechtfertigung der Polizei falsch, die Gerichte hätten ihr ein Trennungskonzept vorgeschrieben. Innenministerium und Polizei wollen auf diese Weise ihre Verantwortung für das falsche und gescheiterte Einsatzkonzept nur wegschieben. Vielmehr haben die Gerichte das polizeiliche Trennungskonzept akzeptiert, aber keineswegs angeordnet.

c) Symbolische Strafverfolgungen

Die sächsischen Strafgerichte vom Amtsgericht über das Landgericht bis zum Oberlandesgericht Dresden haben die friedlichen Platzbesetzer auf der Kreuzung Löfflerstraße / Reichenbachstraße wegen «grober Störung einer Versammlung» verurteilt. In der Sache reichte schon aus, dass sich die Demonstrierenden innerhalb der von der Polizei deklarierten exklusiven Nazizone aufhielten. Auch hielten

sie es für irrelevant, dass die Polizei die Demonstration Müller bereits vor Beginn der Platzbesetzung für undurchführbar gehalten hatte. Die strafrechtlichen Verurteilungen schützen daher nicht wie behauptet die Grundrechte der Teilnehmer der Demonstration Müller, sondern mißbrauchen eine mißglückte Vorschrift des Nebenstrafrechts zur abschreckenden Bestrafung der Nichtbefolgung eines polizeilichen Einsatzkonzepts. Anstatt die Gewalttäter des 19. Februar zu verfolgen, beschäftigte die Staatsanwaltschaft die Öffentlichkeit mit demonstrativen Prozessen gegen Symbolfiguren wie den Jenaer Pfarrer Lothar König. Hier bestehen zahlreiche tatsächliche Anhaltspunkte für eine bewusste Manipulation des Belastungsmaterials zum Nachteil des Angeklagen.[8] Mittlerweile ist das Verfahren gegen Geldauflage eingestellt. Auch das Verfahren gegen den angeblichen Rädelsführer zum Landfriedensbruch, Tim H. («Kommt nach vorne»), endete in zweiter Instanz mit Freispruch.

2. Elektronische Kommunikationskontrolle

a) Ausforschung der «linksextremistischen» Szene

Die Sonderkommission 19. Februar sah sich unter erheblichem Handlungsdruck, nachdem Polizeipräsident Bernd Merbitz und führende Regierungspolitiker öffentlich die hohe Anzahl verletzter Polizeibeamter beklagt hatten. Obwohl die Funkzellenabfrage nach dem Gesetzestext nur «letztes Mittel» sein sollte, beantragte die Soko eine Funkzellenabfrage als erste Ermittlungsmaßnahme überhaupt. Dagegen war der Antrag des Landeskriminalamts auf Funkzellenabfrage nur ein Baustein in der seit 2010 laufenden Ausforschung der «linksextremistischen» Szene. Wie unbefangen, ja unverfroren die Strafverfolger mit den Daten umgingen, zeigen diese Beispiele: Obwohl die Strafprozessordnung den Einsatz der Funkzellenabfrage nur bei schweren Straftaten vorsieht, setzte die Polizei die Verkehrsdaten auch in den Ermittlungen gegen die friedlichen Platzbesetzer auf der Löfflerstraße / Reichenbachstraße ein. Dies war eindeutig rechtswidrig, wie sogar die Staatsanwaltschaft Dresden als vorgesetzte Behörde im Mai 2011 feststellte. Selbst danach beharrte die Polizei darauf, dass friedliche Platzbesetzungen «nicht unterhalb des Bereichs der mittleren Kriminalität» einzuordnen und die Verwendung der Kommunikationsdaten gegen die Platzbesetzer daher «vertretbar» gewesen sei. Zur Erinnerung: die meisten Verfahren wurden eingestellt, die wenigen Verurteilungen bewegen sich zwischen 10 bis 15 Tagessätzen. Zum zweiten nahmen die Ermittlungsbehörden keinen Anstoß daran, die für das Landeskriminalamt erhobenen Daten zur Verfolgung einer kriminellen Vereinigung auch der Soko 19/2 zu übermitteln, was die strenge Zweckbindung der erhobenen Daten unterlief. Auf die Intervention des Datenschutzbeauftragten löschte die Soko die erhaltenen LKA-Daten.

b) Kampagne gegen den Datenschutzbeauftragten

Natürlich verteidigte die Staatsanwaltschaft wie jede Behörde ihr Vorgehen. Sie hat die Massenfunkzellenabfragen aber zudem systematisch verharmlost und den Eindruck erweckt, es gebe eigentlich gar keinen Grundrechtseingriff. So erklärte

8 Johannes Eisenberg / Lea Voigt / Manuel Vogel (Hg.), Der Prozess gegen den Pfarrer Lothar König, Antifaschismus als Feindbild, 2014.

Oberstaatsanwalt Avenarius, es könne doch keinen Unterschied für die Zulässigkeit einer Funkzellenabfrage machen, ob ein Mord in einer einsamen Gegend oder einer belebten Innenstadt geschehe.[9] Dabei ging es gar nicht um Mord und die Schwere der Tat allein rechtfertigt noch keine Funkzellenabfrage. Die Staatsregierung versuchte der angekündigten Veröffentlichung des Berichts des Sächsischen Datenschutzbeauftragten Schurig vorab den Wind aus den Segeln zu nehmen und präsentierte der Öffentlichkeit ein Gutachten unter dem Namen von Prof. Ulrich Battis, dass die Rechtmäßigkeit der Funkzellenabfragen behauptete.[10] Als sich die Öffentlichkeit davon unbeeindruckt zeigte, traten die Verteidiger der Massenüberwachung eine regelrechte Schmutzkampagne gegen den sächsischen Datenschutzbeauftragten los. So erklärte der sächsische Generalstaatsanwalt Klaus Fleischmann – nicht zufällig wieder in der Sächsischen Zeitung, die sich zum Sprachrohr der regierungsoffiziellen Version gemacht hatte –, die Vorwürfe des Datenschutzbeauftragten seien «widersprüchlich» und «für Juristen nicht nachvollziehbar». Der frühere sächsische Polizeipräsident und ehemalige Innenstaatssekretär Fleischmann wirft dem Datenschutzbeauftragten aber nicht nur Inkompetenz, sondern auch Voreingenommenheit und eine Zuständigkeitsüberschreitung vor: Er vermisse «letztlich die gebotene Objektivität. Herr Schurig bewegt sich offensichtlich auf einem für ihn fremden Gebiet, für das er zudem gar nicht zuständig ist.»[11] Schließlich kritisierte auch der Sächsische Richterverein, unterstützt vom Präsidenten des OLG Dresden Ulrich Hagenloch, öffentlich eine Verletzung des Richtervorbehalts. Dabei hatte der Datenschützer ausdrücklich nur die «Anregung» der Polizei und den Antrag der Staatsanwaltschaft auf Funkzellenabfrage bewertet.

c) Gerichtsverfahren und Einstellung der Ermittlungen

Amtsgericht und Landgericht Dresden haben die Funkzellenabfrage im Grundsatz für zulässig erklärt. Auch das Landgericht hat die Funkzellenabfrage nicht in der Sache, sondern nur aus formalen Gründen verworfen. Damit ist der Dresdner Praxis der Massenausspähung gerade kein Riegel vorgeschoben. Im übrigen ist es ein eklatanter sächsischer Justizskandal, dass Amtsgericht und Landgericht die zahlreichen Beschwerden einfach liegen lassen und bis heute nicht entscheiden. Daher sind seit 2013 mehrere Verfassungsbeschwerden beim Bundesverfassungsgericht anhängig gemacht worden.[12] Die Staatsanwaltschaft hat die Ermittlungsverfahren des LKA wegen des Verdachts der Bildung einer kriminellen Vereinigung eingestellt, die die massiven Grundrechtseingriffe rechtfertigen sollten. Wieder einmal hat sich die alte Erfahrung bewahrheitet, dass Ermittlungsverfahren wegen schwerster Straftaten wie «Bildung einer kriminellen» oder gar «terroristischen Vereinigung» im Nichts enden, aber zuvor jahrelang das gesamte Arsenal strafprozessualer Ermitt-

9 Christian Avenarius, Was gehen die Polizei meine Handy-Daten an?, Sächsische Zeitung vom 7. Juli 2011.

10 Ulrich Battis, Gutachten zur Gewaltenteilung im Strafermittlungsverfahren und zur Verhältnismäßigkeit der Anordnung einer nachträglichen Funkzellenabfrage, 13. September 2011, im Auftrag des Sächsischen Staatsministeriums des Innern.

11 Interview in der Sächsischen Zeitung vom 14. September 2011.

12 https://netzpolitik.org/2013/handygate-in-dresden-dritte-verfassungsbeschwerde-gegen-funkzellenabfrage-zu-anti-nazi-proteste.

lungsinstrumente angewendet wurde. Mit der Einstellung haben sich Polizei und Staatsanwaltschaft auch einer unabhängigen gerichtlichen Überprüfung ihres Vorgehens entzogen. Auch nach vier Jahren konnte mit der Verkehrsdatenauswertung kein einziger Landfriedensbrecher ermittelt oder verurteilt werden. Dennoch ist damit zu rechnen, dass die erhobenen Daten weiter gespeichert und auch in anderen Verfahren verwendet werden.

3. Selbstermächtigung der Ermittlungsbehörden

a) Zulässigkeit nur gegen Verdächtige

Die sächsischen Gerichte rechtfertigten die Maßnahmen der Polizei und Staatsanwaltschaft mit § 100g der Strafprozessordnung. Danach dürfen Verkehrsdaten einer Person erfasst und ausgewertet werden, die aufgrund anderer Tatsachen einer schweren Straftat verdächtig ist, wenn dies die einzige Möglichkeit zur Aufklärung ist. Ein Unterfall des § 100g StPO erlaubt auch die Erfassung der Verkehrsdaten, wenn die Telekommunikation nur «örtlich und zeitlich» bezeichnet ist. Ein Anfangsverdacht aufgrund konkreter Anhaltspunkte ist die entscheidende rechtsstaatliche Schwelle, um Unverdächtige vor staatlichen Eingriffen zu schützen. Die Praxis in Dresden und anderswo hat einfach verdrängt, dass auch im Fall nicht-individualisierter Funkzellenabfragen ein Tatverdacht bereits gegen die Person vorliegen muss, deren Daten erhoben werden. Stattdessen benennen die Ermittlungsbehörden durchaus großzügig Orte und Zeiten und behandeln umstandslos alle Personen als verdächtig, die sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort aufhalten. Dies entspricht der Gedankenwelt von Polizei, LKA und politischer Führung, die alle Menschen, die sich in der sogenannnten «Aufenthaltsverbotszone» befanden, für Gewalttäter hielten. Die Abkehr vom Tatverdacht hat weitreichende Folgen: Letztlich kann so mit jeder Konstruktion einer polizeilichen Gefahrenlage – oder «Gefahrenzone» wie in Hamburg – ohne weiteres in die Grundrechte von Unverdächtigen, ja aller Menschen eingegriffen werden. Die Intensität des Eingriffs wird tendenziell maßlos, da sie nicht mehr mit der Schwere der Tat oder des Tatverdachts gegen eine bestimmte Person abgewogen werden kann. Auf diese Weise läuft das allgemeine rechtsstaatliche Verhältnismäßigkeitsprinzip leer. Die Abkehr vom Tatverdacht als Voraussetzung eines Grundrechtseingriff bewirkt letztlich eine Beweislastumkehr: Nicht mehr der Staat hat den eingriffsrechtfertigenden Verdacht nachzuweisen, sondern der Betroffene muss dulden, dass der Staat seine Daten zur Ermittlung von Verdächtigen nutzt.[13]

b) Verkehrsdatenabfrage als Standardmaßnahme

Masseneingriffe zur Verkehrsdatenauswertung sind seit einigen Jahren faktisch zur polizeilichen Standardmaßnahme geworden. Der Berliner Senat nennt für 2013 die Erfassung und Auswertung von 50 Millionen Verkehrsdaten für den Stadtstaat. Das Fachportal netzpolitik.org geht bundesweit von 50 Anordnungen für Funkzellenabfragen am Tag (!) aus. Seitdem die Polizei in Sachsen wie auch in anderen Bundesländern das Auswertetool «eFAS» angeschafft hat, gilt die Funkzellenabfrage

13 Dazu Albers in diesem Band.

als Wunderwaffe. Offenbar setzt die Polizei bei jedem Fußballspiel und bei jeder Demonstration, bei denen Straftaten geschehen, aber auch bei jedem EC-Karten-Mißbrauch an Bankautomaten die Funkzellenabfrage ein. Jede und jeder muss also damit rechnen, schon viele Male in Verkehrsdatenerfassungen und Rasterungen einbezogen worden zu sein! Somit werden Ausmaß und Reichweite der Grundrechtsbeeinträchtigungen nicht wie es im Rechtstaat sein sollte durch die Gesetze, sondern durch selbstgestrickte Gefahrenprognosen und den Fortschritt technischer Überwachungsmöglichkeiten gesteuert.

4. Fazit

Die Perspektive der Überwacher aus Polizei und Staatsanwaltschaft wird durch den politischen Handlungsdruck, die Erwartungen der Öffentlichkeit und die organisationsspezifischen Gefahrenwahrnehmungen geprägt. Verhalten und Erklärungen offenbaren auch bei schwerwiegendsten Grundrechtseingriffen ein hemmungslos gutes Gewissen und eine beängstigende Unbekümmertheit. Sollte bei einzelnen Mitarbeitern Skrupel bestehen, sind sie jedenfalls nicht nach außen gedrungen oder handlungsleitend geworden. Im richtig verstandenen Rechtsstaat ist es eigentlich nicht die Aufgabe unabhängiger Gerichte, Maßnahmen der Exekutive mit dem Heiligenschein der Rechtmäßigkeit gegen Kritik abzuschirmen, sondern die Grundrechte der Bürgerinnen und Bürger gegen Eingriffe der Staatsgewalt zu schützen. Leider haben sich die Dresdner Gerichte der Sichtweise der Polizei angeschlossen und deren Kontrollkonzepte durchgewunken. Sie fühlen sich dem reibungslosen Funktionieren des Staatsapparats mehr verpflichtet als dem Grundrechtsschutz. Nichts löst aber mehr Angst aus, als vor der Übermacht des Staates rechtlos gestellt zu werden. Dies hat wesentlich zur Verunsicherung und Einschüchterung, aber auch zur Eskalation beigetragen.

III. Die Perspektive der Überwachten

1. Grundrechtseinschränkungen

a) Verunsicherung und Einschüchterung

Die Maßnahmen der Raumkontrolle störten die Bewohner der Südvorstadt in Dresden und die Besucher der Universität erheblich in ihrem Alltag. Sie erlebten am 19. Februar 2011 eine massive Einschränkung ihrer Bewegungsfreiheit und mussten sich wie im Ausnahme- oder Belagerungszustand fühlen. Umherziehende Demonstrierende, Wasserwerfer und mit Schild, Helm und Schlagwaffen ausgerüstete Polizisten erschütterten ihr unbefangenes Gefühl persönlicher Sicherheit.[14] Noch persönlicher hat die Erfassung und Auswertung der elektronischen Kommunikation die sozialen Beziehungen der Menschen betroffen. Die Ermittlungsbehörden meinten, die flächendeckende elektronische Kommunikationskontrolle hätte die

14 Eindrücke aus der Bevölkerung sind dokumentiert in der Broschüre Fraktion Bündnis 90 / DIE GRÜNEN im Sächsischen Landtag, «Protest unerwünscht?», 2011, und dem Film von Barbara Lubich und Claudia Jerzak, Come together, 2012.

Bereitschaft, die eigenen Grundrechte auf Meinungs- und Versammlungsfreiheit auszunutzen nicht eingeschränkt, da die Betroffenen ja keine Kenntnis davon gehabt hätten. Dagegen hat der Sächsische Datenschutzbeauftragte mitgeteilt, dass «der Einschüchterungseffekt staatlichen Handelns auch im vorliegenden Fall durchaus präsent» sei, wie die «Vielzahl und der Inhalt von Anfragen und Petitionen von Bürgern» zeige.[15] In der Tat haben die Kontrollbemühungen der Polizei nicht nur das Vertrauen der Bürgerinnen und Bürger in die ungehinderte angstfreie Bewegungsfreiheit an ihrem Wohn- und Lebensort erschüttert, sondern auch ihr Vertrauen in die Vertraulichkeit ihrer Kommunikation mit Handys, Telefon oder Internet. Für viele Menschen dürfte dies die erste Erfahrung eines staatlichen Angriffs auf die eigenen Grundrechte gewesen sein und deren Vertrauen in die Redlichkeit und die Schutzfunktion staatlicher Behörden dauerhaft erschüttert haben.

b) Grundrechtlicher Schutz der Vertraulichkeit elektronischer Kommunikation

Dieses Vertrauen mag aus heutiger Sicht – nach den Enthüllungen von Edward Snowden – naiv erscheinen, gründet aber in der grundrechtlichen Garantie der Kommunikationsfreiheit nach Art. 10 des Grundgesetzes. Denn dieses Grundrecht schützt eben nicht nur die Vertraulichkeit der Inhalte, sondern auch die Umstände der Kommunikation, also auch die Verkehrsdaten. Mit den Worten des Bundesverfassungsgerichts will Art. 10 «die Bedingungen einer freien Telekommunikation aufrechterhalten. Die Nutzung des Kommunikationsmediums soll in allem vertraulich möglich sein.» Das Grundrecht soll verhindern, «dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen.»[16] Auch der Europäische Gerichtshof, das höchste Gericht der Europäischen Union, hat 2014 in seinem bahnbrechenden Urteil zur Vorratsdatenspeicherung festgestellt, dass die Speicherung und Nutzung der Daten ohne Information der Betroffenen «geeignet (sei) bei den Betroffenen ... das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung» ist.[17] Wir alle haben also einen verfassungsrechtlich gewährleistetes Grundrecht, dass der Staat unsere Verkehrsdaten weder erfasst noch auswertet - und schon gar nicht heimlich. Das Bundesverfassungsgericht bejaht bei Eingriffen gegen zahlreiche Unverdächtige eine hohe Eingriffsintensität, da der Betroffene selbst keinen Anlaß für die Erhebung seiner Daten geschaffen hat.[18] Es betont die besondere Gefährdung bei heimlicher Erhebung elektronischer Kommunikationsdaten, denn sie treffe den Bürger «in einer Situation vermeintlicher Vertraulichkeit».[19] Schließlich stellt es fest, dass die automatisierte Erhebung «praktische Erschwernisse der Datenerhebung weithin beseitigt und die Daten der Betroffenen ohne zeitliche Verzögerungen ... zur Verfügung stellt».[20]

---

15 Bericht des Sächsischen Datenschutzbeauftragten (wie Anm.6), S.30 und S.45.
16 BVerfG vom 12. März 2003, 1 BvR 330/96, 1 BvR 348/99, R.50 und R.101 - Handyüberwachung.
17 EuGH vom 8. April 2014, Rs. C 293/12, C 594 / 12, R.37 - Vorratsdatenspeicherung.
18 BVerfG vom 4. April 2006, 1 BvR 518/02, R.117 - Rasterfahndung.
19 BVerfG vom 12. März 2003, 1 BvR 330/96, 1 BvR 348/99, R.77 - Handyüberwachung.
20 BVerfG vom 24. Januar 2012, 1 BvR 1299/05, R.156 - Bestandsdatenauskunft.

2. Angriff auf die freiheitliche Willensbildung des Volkes

Die Verunsicherungs- und Einschüchterungswirkung der Überwachung hat aber auch gesamtgesellschaftliche Bedeutung und Wirkung. Grundrechtseingriffe gegen sehr viele Unverdächtige wie bei der Funkzellenabfrage haben eine einschüchternde, ja abschreckende Wirkung auf die Bereitschaft der Bürgerinnen und Bürger, ihre Grundrechte auszuüben: «Ein von der Grundrechtsausübung abschreckender Effekt muss nicht nur zum Schutze der subjektiven Rechte der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird dadurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist. Es gefährdet die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen.»[21] Daher ist festzuhalten: Eine anlasslose geheime technische Massenüberwachung der elektronischen Kommunikation auch von Unverdächtigen enttäuscht die berechtigten Vertraulichkeitserwartungen der Bürgerinnen und Bürger. Sie begründet ein Gefühl ständiger Überwachung, das einschüchternde, ja abschreckende Wirkung auf die Unbefangenheit der Kommunikation hat. Dies beschädigt die Selbstbestimmung der Menschen sowie ihre Handlungsfähigkeit. Bürgerinnen und Bürger, die selbstbewusst, selbstbestimmt und ohne Angst miteinander kommunizieren, werden aber für die in der Demokratie vorausgesetzte freiheitliche politische Willensbildung des Volkes gebraucht. Leidet also die persönliche Freiheit, beschädigt das unweigerlich auch die Freiheit politischer Willensbildung des Volkes und damit die freiheitlich-demokratische Grundordnung selbst.

IV. Kontrolle an der digitalen Schwelle

1. Ablösung analoger Raumkontrolle

Die Dresdner Ereignisse vom 19. Februar 2011 zeigen, wie die Kontrolle des analogen Bewegungsraums und des digitalen Kommunikationsraums ineinander greifen. Sie zeigen insbesondere die Ablösung und Ersetzung untauglicher Kontrollversuche im analogen Raum durch eine höchst effektive Kontrolle des elektronischen Kommunikationsraums. Was die Polizeikette leisten sollte, bewirkt die Auswertung der gespeicherten Verkehrsdaten: die totale Kontrolle der Bewegungen von Menschen. Gefordert von den politischen Instanzen und von den Gerichten durchgewunken haben die Ermittlungsbehörden das maßlose sichtbare Raumkontrollkonzept in den unsichtbaren Raum der elektronischen Kommunikation verlängert und aufgrund der weitreichenderen technischen Möglichkeiten auch radikalisiert. Beide Konzepte zeigen den staatlichen Willen zur totalen Kontrolle menschlicher Regungen. Während die öffentlichen Absperrungen der Südvorstadt für alle sicht- und spürbar waren, erfolgte die digitale Kontrolle des elektronischen Kommunikationsraums unbemerkt und heimlich. Und während die analogen Kontrollversuche an der Zahl verfügbarer

21 BVerfG vom 12. März 2003, 1 BvR 330/96, 1 BvR 348/99, R.50 und R.101 - Handyüberwachung.

Polizeibeamten und der schieren Unmöglichkeit scheiterten, ein gesamtes Stadtgebiet hermetisch abzuschließen, werden die digitalen Kommunikationsdaten einfach und vollständig mit einem Mausklick überstellt. Der entscheidende Unterschied besteht in der Wirksamkeit des Zugriffs auf den digitalen Kommunikationsraum. Er wird deutlich, wenn man sich in einem Gedankenexperiment die «analoge Parallele» vorstellt. Dann ist zu fragen, mit welchen Mitteln die Informationen der Verkehrsdatenauswertung bei analoger, nicht-elektronischer Kommunikation hätten erhoben werden müssen, um dieselbe Informationsdichte zu erhalten. Die Erfassung aller Kommunikationspartner und der Bewegungen aller Menschen in einer Funkzelle hätte bedeutet, dass die Kommunikationen aller Menschen in diesem Raum zu den angegebenen Zeitpunkten hätten beobachtet und aufgeschrieben werden müssen. Wir müssten uns etwa vorstellen, dass auf der Schulter jedes Menschen ein kleiner Überwachungskobold sitzen müsste, der jedes Gespräch seines Trägermenschen auf Papier aufzeichnen würde. Unser Überwachungskobold müsste jeden Schritt in jede Richtung notieren. Diese tausende Protokolle müssten alle sofort in eine große Halle getragen werden, in der tausende Kobolde sich blitzschnell ihre Protokolle vorlesen müssten. Das würde natürlich einige Zeit in Anspruch nehmen, vielleicht mehrere Wochen. Schließlich würden alle Beziehungen auf eine riesige Tafel gezeichnet erscheinen. Eine absurde Vorstellung, aber genau so hat man sich die Wirkung des massenhaften Zugriffs auf den digitalen Kommunikationsraum vorzustellen: Die elektronische Erfassung und Auswertung überwindet alle bisher bestehenden faktischen zeitlichen und mengenmäßigen Kapazitätsgrenzen amaloger Überwachung.

2. Ermittlung sozialer Beziehungen

Die Funkzellenauswertung ersetzt aber nicht nur die analoge Raumkontrolle durch wirksamere Kontrollmittel, sondern reicht wesentlich weiter: Es geht nicht mehr um die punktuelle Abwehr einer Gefahr, die durch den Zutritt bestimmter Personen an einen bestimmten Ort zu einer bestimmten Zeit entstehen könnte. Gefahrenabwehr und Strafverfolgung sind nicht mehr der Zweck staatlichen Handelns, sondern nur mehr ein für die Öffentlichkeit plausibel erscheinender Eingriffsanlass. Die Datenauswertung taucht von der Oberfläche des Meers der Verkehrsdaten auf den tiefen Grund sozialer Beziehungen zwischen Menschen und in Gruppen hinab. Es geht um die Durchleuchtung und Offenlegung grundlegender sozialer Beziehungen zwischen Menschen und um die Identifizierung von Gruppen. Diese Methode erlaubt die Erstellung von Bewegungs-, Persönlichkeits- und Sozialprofilen von Menschen und Gruppen, die das Bundesverfassungsgericht für unvereinbar mit dem Menschenbild des Grundgesetzes hält. Wir müssen also davon ausgehen, dass das was bei den Geheimdiensten seit langem üblich und bei der «Bekämpfung» der sogenannten «Organisierten Kriminalität» auch Polizeiauftrag ist, jetzt in die alltägliche Polizeiarbeit vordringt.

3. Zusammenfassende Schlussbemerkung

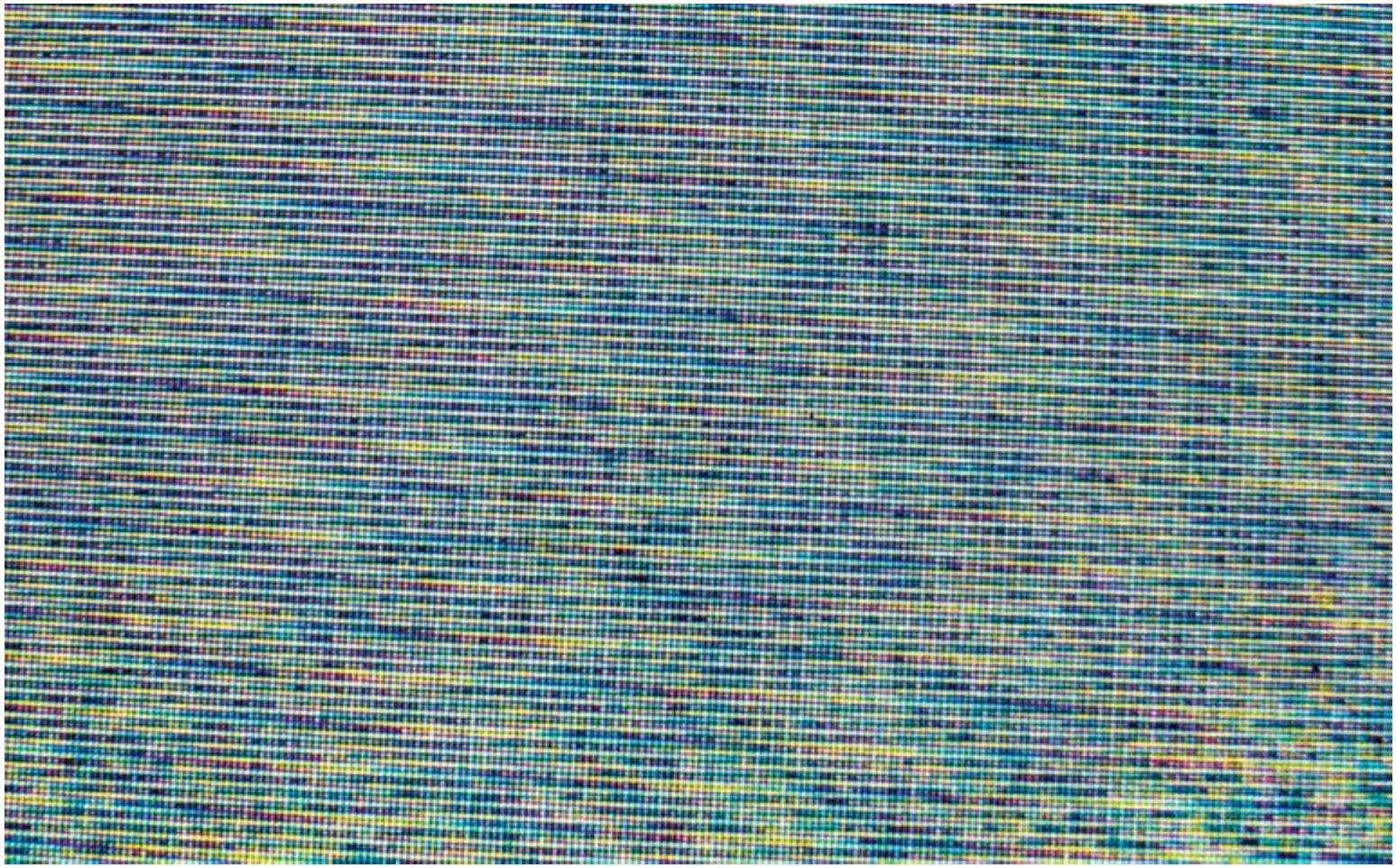
(1) Die fortschreitende elektronische Vermittlung unserer alltäglichen Lebensäußerungen, die digitale Revolution, zwingt uns immer unentrinnbarer, Datenspuren zu hinterlassen. Diese Datenspuren lassen eine immer umfassendere Rekonstruktion unseres Alltags, unserer Kommunikationsverhältnisse, Bewegungsprofile, ja potentiell unseres gesamten öffentlichen und privaten Lebens zu. Das unlöschbare digitale Abbild unserer Lebensvollzüge legt zunehmend das Bild unserer Persönlichkeit in der Öffentlichkeit fest und damit die Axt an den Kern unseres Allgemeinen Persönlichkeitsrechts, nämlich das Recht, sich jederzeit selbst neu erfinden zu können und zu dürfen. Dieses Datenabbild unserer Existenz ist bislang entlang der realen Machtstrukturen der Ausbeutung kommerzieller, militärischer und polizeilich-geheimdienstlicher Interessenten ausgeliefert. Diese Ausbeutung bietet Möglichkeiten der Überwachung und Kontrolle, von denen Diktaturen vor der digitalen Revolution nur träumen konnten!

(2) Der automatisierte Zugriff auf und die Verarbeitung der Verkehrsdaten erlaubt eine Massenerhebung und -auswertung, ja potentiell eine Totalüberwachung sämtlicher Kommunikationsregungen der gesamten Bevökerung. Das gute Gewissen der Strafverfolger bei ihrem Zugriff auf unsere elektronischen Kommunikationsdaten zeigt einen Konflikt um die Grenzziehung zwischen dem Öffentlichen und dem Privaten an. Während das Bundesverfassungsgericht auch die elektronische Kommunikation den Vertraulichkeitserwartungen privaten Lebens unterstellt, verhalten sich Strafverfolger, Geheimdienste und Internetkonzerne so, als ob die elektronischen Kommunikationsdaten allgemein für sie verfügbar wären. Über kurz oder lang tritt daher ein flächendeckender Vertrauensverlust in die Vertraulichkeit elektronisch vermittelter Kommunikation ein. Die totale Überwachung unserer Datenspuren schafft einen digitalen Käfig, der bezüglich der Intensität und Dichte der Aufzeichnung unserer Lebensregungen nur mit einem Gefängnis oder Lager zu vergleichen ist.

(3) Die Massenüberwachung unterminiert die für die Demokratie wesentliche Freiheit der politischen Willensbildung. Die kommerziellen und staatlichen Überwachungsinteressen laufen den Interessen einer demokratischen Gesellschaft auf Transparenz, Respekt vor der individuellen Selbstbestimmung des Einzelnen sowie dem Anspruch auf demokratische Steuerung und Verantwortung gesellschaftlicher Prozesse zuwider. Die ungehemmte Anwendung der technischen Überwachungsmöglichkeiten ist demokratieunverträglich.

(4) Daher gilt es den verloren gehenden Freiheitsraum zu verteidigen und zurückzuerobern. Wir brauchen wirksame Grundrechte, die unsere individuelle Freiheit vor den neuen Angriffen schützt und als Grundlage einer freien politischen Willensbildung der Bürgerinnen und Bürger bewahrt. Heute muss die digitale Freiheit wie im 19. und 20. Jahrhundert die klassischen Freiheiten auf Respekt des privaten Lebensbereichs oder der Meinungs- und Versammlungsfreiheit neu politisch erkämpft werden. Es ist eine Illusion zu glauben, unsere Freiheit wäre in

guten Händen, weil wir unsere Regierungen frei gewählt haben. Dieser Freiheitskampf erfordert einen stetigen Gebrauch unserer Grundfreiheiten und ihre Verteidigung gegen staatliche Zumutungen wie am 19. Februar 2011 in Dresden.



HANNES FEDERRATH

«Mein Smartphone weiß mehr als ich» – Beobachtung und Sammlung von Nutzeraktivitäten

Die Überwachungsmöglichkeiten im Internet sind nicht erst seit den NSA-Enthüllungen durch Edward Snowden bekannt. Mittlerweile verlagert sich ein Großteil der Kommunikation der Menschen von der physikalischen Welt ins Internet. E-Mail-Kommunikation, Kurznachrichten beispielsweise per WhatsApp oder iMessage und Facebook sind passende Beispiele. Zunehmend werden mobile Endgeräte wie Smartphones und Tablets verwendet. Solche Geräte sind neben den üblichen Ein- und Ausgabeschnittstellen mit einer Vielzahl von Sensoren ausgestattet. Dabei rückt die Sensorik auch immer näher an den Körper heran: Passende «Wearables» wie Armbänder und Uhren, die gewöhnlich direkt auf der Haut getragen werden, ermöglichen die Überwachung von Körperfunktionen und senden ihre Daten an das Smartphone. Obwohl viele Endnutzer die neue Funktionsvielfalt sehr schätzen, stellen sie sich zunehmend Fragen nach dem Schutz ihrer Privatsphäre: Wie und welche Daten werden in und mit Hilfe von Smartphones gesammelt? Welche Trends sind hier erkennbar? Welche Schutzmaßnahmen können ergriffen werden?

1. Appification und Sensoren

Für nahezu jedes Kommunikations- und Informationsbedürfnis findet man heute eine eigene Softwareanwendung (engl. Application, kurz: App). Datenschützer sehen diese «Appification» des Lebens durchaus mit großer Sorge, zumal moderne Apps die Daten nicht mehr nur lokal speichern, sondern die Möglichkeit bieten, über vernetzte Online-Dienste wie iCloud oder Dropbox die Daten auch auf anderen (eigenen) Geräten (z.B. dem heimischen PC) zugänglich zu machen und mit anderen zu teilen. Die in den Geräten verfügbare Sensorik ermöglicht auch neue Apps. Moderne Geräte stellen mindestens folgende Schnittstellen und Sensoren bereit, über die eine Vielzahl an Umgebungsdaten gesammelt werden kann: Global Positioning System (GPS), WiFi, GSM/3G/LTE, Bluetooth, Mikrofone, Kameras, Zeit, Temperatur und Luftdruck, Bewegungs- und Lagesensoren, Beschleunigungssensoren, biometrische Sensoren (Fingerabdruck) und Anschlussmöglichkeiten für weitere Sensoren.

Mit Wearables werden zusätzlich noch sehr persönliche Daten wie Herzschlag, Atemfrequenz, Muskelkontraktion und Blutzucker messbar. Längst sind für Smartphones auch Hardwareschnittstellen und teilweise auch Softwarelösungen zum Anschluss an Autos (CAN-Bus) und Häuser (Smart Meter, Heizung, Alarmanlage) verfügbar. Wenn beispielsweise Google den Rauchmelder- und Thermostathersteller Nest kauft, der über Lösungen für die intelligente Steuerung von Haustechnik verfügt, so steckt möglicherweise die Strategie dahinter, auch innerhalb des häuslichen Umfeldes der Nutzer Lösungen anzubieten, die das Leben

erleichtern. Rauchmelder, die gleichzeitig Thermostat, Wireless-LAN-Repeater und Bewegungsmelder sind und noch eine LED-Beleuchtung eingebaut haben, dazu noch formschöne Designobjekte sind, haben zweifellos einen Nutzen. Sie sind aber auch geeignet, kontinuierlich Daten über ihre Besitzer zu sammeln, auszuwerten und deren Lebensgewohnheiten zu analysieren. Die Werbeindustrie verfolgt dabei das Ziel einer möglichst präzisen Kundenansprache, die mit genauen Daten über die Lebensgewohnheiten der Kunden vermutlich am Besten gelingt.

2. Verletzlichkeit durch integrierte Lösungen

Hard- und Software bilden heute bei vielen mobilen Geräten eine Einheit: Auf einem iPhone kann man nicht sinnvoll ein anderes Betriebssystem wie iOS nutzen, auf Android-basierten Geräten gilt das analog. Dieses Zusammenwachsen von Hardware und Software zu integrierten Lösungen gelingt auf technischer Ebene einerseits durch Standardisierung und ermöglicht somit offene Lösungen von vielen verschiedenen Anbietern. Andererseits streben jedoch immer mehr Software- und Hardwarehersteller nach eigenen proprietären integrierten Lösungen, grenzen sich also ganz bewusst von der Konkurrenz ab, was aus Sicherheitssicht für alle drei Schutzziele der IT-Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) gefährlich ist:

(1) Vertraulichkeit: Zentrale Kontrolle durch einen einzigen Anbieter führt zunächst sowohl auf ökonomischer als auch auf technischer Ebene in die Abhängigkeit. Hinzu kommt, dass der Anbieter durchgehenden Zugriff auf alle innerhalb seiner zahlreichen Systeme gespeicherten Daten hat, was die Vertraulichkeit beeinträchtigen kann.
(2) Integrität: Wie bei der Vertraulichkeit kann aufgrund der zentralen Konzentration bei einem Anbieter auch eine Vielzahl von Daten ggf. unberechtigt verändert werden.
(3) Verfügbarkeit: Fehlende Diversität kann zu einer unkontrollierten Fehlerausbreitung führen: Befindet sich eine fehlerhafte Komponente (z.B. eine Softwarebibliothek) in sehr vielen vernetzten Systemen dieses Anbieters, können auch sehr viele Komponenten ausfallen und damit die Verfügbarkeit beeinträchtigen.

Potentielle Angreifer sind dabei nicht etwa nur die Anbieter der integrierten Lösungen wie Apple oder Google. Fällt das Masterpasswort eines Endnutzers in falsche Hände oder wurde von ihm zu einfach gewählt, sind die Online gespeicherten Daten auch für Fremde zugänglich.

3. Datensammlung innerhalb von Apps

Auch innerhalb von mobilen Geräten werden heute üblicherweise Nutzungsdaten gesammelt. Dabei ist zu unterscheiden zwischen Daten, die eine App autonom verarbeiten kann, und Daten, die durch das Betriebssystem kontrolliert werden.

Eine App kann alle Daten, die innerhalb der App entstehen, ohne Einschränkungen kontrollieren. Hierzu zählen das Datum und die Zeiten von Start und Stopp der App sowie Datum und Zeiten von Start und Stopp aller App-Funktionen. Zudem können alle Inhaltsdaten, die innerhalb der App verarbeitet und gespeichert werden,

gesammelt werden, also beispielsweise in Messenger-Apps empfangene und gesendete Nachrichten, in Mailprogrammen empfangene und gesendete E-Mails sowie in Passwortmanagern gespeicherte Passwörter. Teile dieser Daten (z.B. die Starts und Stopps der App) können zur Protokollierung ins Netz gesendet werden, zumindest dann, wenn der Nutzen der App von vorhandener Internet-Konnektivität abhängt. Sie werden üblicherweise vom Anbieter zur Optimierung des Angebots ausgewertet. Zudem kontrolliert das Betriebssystem (z.B. iOS, Android, aber auch Windows, MacOS, Linux u.s.w) den Zugriff auf

(1) Global User IDs (GUIDs) wie die Seriennummer des Geräts, aber auch die SSID (Service Set Identifier), also den Namen des Wireless-LANs,
(2) Ortsdaten wie die GPS-Koordinaten, die Nummer der Funkzelle (Cell Identity, CI), aus Funkwellen gewonnene Triangulationsdaten (z.B. Time-Of-Arrival, TOA), aber auch kartographierte Wireless-LAN-Namen,
(3) das Adressbuch (lesend und ggf. auch schreibend),
(4) Sensordaten sowie alle Daten, die auf dem Gerät gespeichert sind.

4. Zugriffsschutzmodelle

Möchte eine App oder das Betriebssystem Zugriff auf Daten erhalten, existieren folgende Möglichkeiten beim Schutz vor Zugriffen:

(1) Keine Information des Nutzers über den Zugriff und/oder die Übermittlung,
(2) Zugriffserlaubnis durch den Nutzer vor oder während der Installation einer App,
(3) Zugriffserlaubnis durch den Nutzer vor dem erstem Start der App oder beim ersten Zugriff auf Sensordaten,
(4) Zugriffserlaubnis durch den Nutzer bei jedem Zugriffsversuch durch das Betriebssystem und/oder die App.

Das Zugriffsschutzmodell 1 besteht heute nicht mehr, war aber in den Anfangszeiten von iOS implementiert. Heute fragt iOS beim ersten Start einer App nach den Zugriffserlaubnissen, die der Anwender später in den Einstellungen ändern kann (Zugriffsschutzmodell 3). Allerdings ist der Satz an Privilegien auf Ortsdaten, Netzzugriff und das Adressbuch begrenzt. Auf andere Daten kann nicht (direkt) zugegriffen werden. Android liefert während der Installation einer App detaillierte Informationen über deren Zugriffswünsche (Zugriffsschutzmodell 3). Mit der Installation der App hat der Nutzer seine Zugriffserlaubnisse erteilt und kann diese nicht mehr einfach rückgängig machen, es sei denn, er löscht die App. Es existieren allerdings auch Funktionen innerhalb von Android, die zumindest für «Power-User» feingranulare Einstellmöglichkeiten bieten. Wie sich die verbreiteten Zugriffsschutzmodelle in der Praxis auswirken können, soll an zwei Beispielszenarien gezeigt werden.

Im ersten Beispiel lädt sich ein Android-Nutzer eine kostenlose Taschenlampen-App. Er liest vor der Installation die sehr vielversprechende Funktionsbeschreibung. Natürlich kann die App nicht nur das Kameralicht dauerhaft leuchten lassen, sondern auch als Signalleuchte verwendet werden, und beherrscht sogar den Morse-Code. Während der Installation fragt die App nach folgenden Privilegien: Sie möchte Zugriff auf das Adressbuch und auf das Internet zugreifen. Kostenlose Apps wollen häufig auf das Internet zugreifen, um Werbung nachzuladen und einzublenden. Daran hat sich der Endnutzer bereits gewöhnt und akzeptiert dies. Warum jedoch auch auf das Adressbuch zugegriffen werden soll, erschließt sich dem Nutzer nicht.

Er wird skeptisch und verzichtet auf die Installation. Er hat davon gehört, dass einige bösartige Apps die in den Kontakten gespeicherten E-Mail-Adressen für Spamming missbrauchen. Da die Taschenlampen-App im Rahmen der ihr gewährten Privilegien Daten beliebig speichern, auswerten und übermitteln kann, könnte sie ohne Weiteres diese Daten missbrauchen. Beim Zugriffsschutzmodell 2 kann die App z.B. bei einem Update nach weiteren Rechten fragen. So könnte von einem heimtückischen Softwareentwickler zunächst ein unbedenklicher Satz an Zugriffsrechten gefordert werden, der später unauffällig erweitert wird, nachdem Vertrauen aufgebaut wurde.

Im zweiten Beispiel nutzt ein iOS-Nutzer eine ebenfalls kostenlose Bahn-App. Mit der App können Verbindungen des öffentlichen Nah- und Fernverkehrs herausgesucht und dafür Tickets gekauft werden. Die App möchte bei der Eingabe des Start- und Zielbahnhofs sowohl auf den aktuellen Ort als auch auf das Adressbuch zugreifen. Obwohl der Nutzer beide Zugriffe verweigert, funktioniert die App einwandfrei; es handelt sich um nützliche Komfortfunktionen, die eine schnelle Eingabe von Start und Ziel ermöglichen (entweder aktueller Ort oder Adresse eines vorhandenen Kontakts). Das Beispiel zeigt noch eine Optimierungsmöglichkeit heutiger Lösungen: Die aktuellen Betriebssysteme gewähren nach Erlaubnis des Nutzers den Zugriff auf das gesamte Adressbuch. Das Zugriffsschutzmodell 4 könnte nun diese Betriebssysteme so erweitern, dass die App nur Zugriff auf den vom Nutzer ausgewählten Kontakt (bzw. dessen Adresse) bekommt und diese Erlaubnis jedes Mal und für jeden Kontakt erneuert werden muss.

5. Verkettung über GUIDs

Insbesondere die Möglichkeit der Verkettung über Global User IDs (GUIDs) ist in mobilen Geräten wie Smartphones und Tablets gefährlich, da bekannte Schutzmechanismen aus dem Bereich des Websurfens hier nicht greifen. Beim Websurfen werden zur Verkettung der Zugriffe eines Nutzers sog. Cookies verwendet. Dies sind kleine Datensätze, die beim ersten Besuch eines Webservers auf dem Rechner des

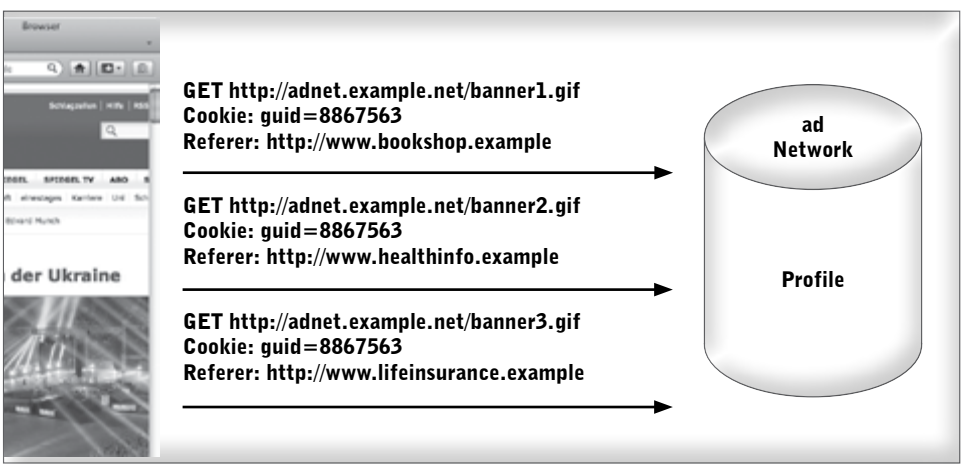


Abb. 1: Third-Party Cookies zur Langzeitverkettung über Werbenetze

Nutzers gespeichert werden. Alle weiteren Zugriffe auf diesen Webserver enthalten auch die Cookies dieses Servers. Cookies bleiben auch nach dem Beenden des Browsers gespeichert, sofern ein in ihnen enthaltenes Ablaufdatum noch nicht erreicht ist, und können daher auch zur Langzeitverkettung benutzt werden, besonders dann, wenn sie als Third-Party Cookies in Werbenetzen eingesetzt werden (siehe Abb. 1). Allerdings bieten fast alle Browser sowohl auf PCs als auch auf mobilen Geräten die Möglichkeit, Cookies zu löschen und somit die Langzeitverkettung per Cookie zu verhindern.

Bei den GUIDs (Gerätekennungen, App-interne IDs etc.), die bei der Datensammlung auf mobilen Geräten oder innerhalb von Apps verwendet werden, gelingt das Löschen oder Zurücksetzen nicht. Erstens ist dies zumindest bei den hardwarenahen GUIDs wie MAC-Adresse (Medium Access Control) oder IMEI (International Mobile Equipment Identity) ohnehin nicht ohne Weiteres möglich und zweitens haben die Geräte- und Softwarehersteller daran gar kein Interesse. Mit IPv6 wird sich dieser Zustand weiter verschärfen. Wann immer also Daten wie Start / Stopp-Zeitpunkte von Apps zur Protokollierung und späteren Nutzeranalyse in Mobile Logging Networks (als Teil von Werbenetzen) gesendet werden, sind sie global und über lange Zeiträume hinweg verkettbar, wenigstens solange, bis der Nutzer sein Endgerät wechselt. Mit Kennungen wie der Google-ID oder der Apple-ID sind zumindest für den Plattform-Anbieter (Android bzw. iOS) auch lebenslange Verkettungen möglich und haben somit das Potential zu enormen Datenschutzverletzungen, wenn die anvertrauten Daten missbraucht oder gehackt werden.

6. Online-Werbung

Mit mobiler Online-Werbung wird Geld verdient. Nach einer Bitkom-Studie wurden im Jahr 2009 mit Online-Werbung (Werbebanner, Pop-Ups, Streaming-Ads) 1,5 Milliarden Euro Umsatz gemacht. Auch der Umsatz von Produkten steigt durch Werbung deutlich, je Dollar Werbung sollen sieben Dollar Produktumsatz erzielt werden. Insbesondere Profile, die über ein breites Spektrum der Internetangebote

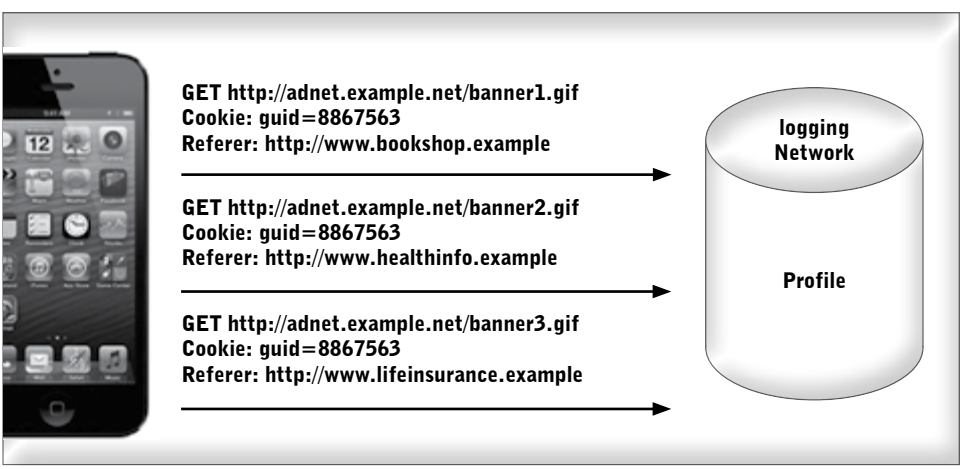


Abb. 2: Mobile Logging Networks zur Langzeitverkettung des Nutzerverhaltens

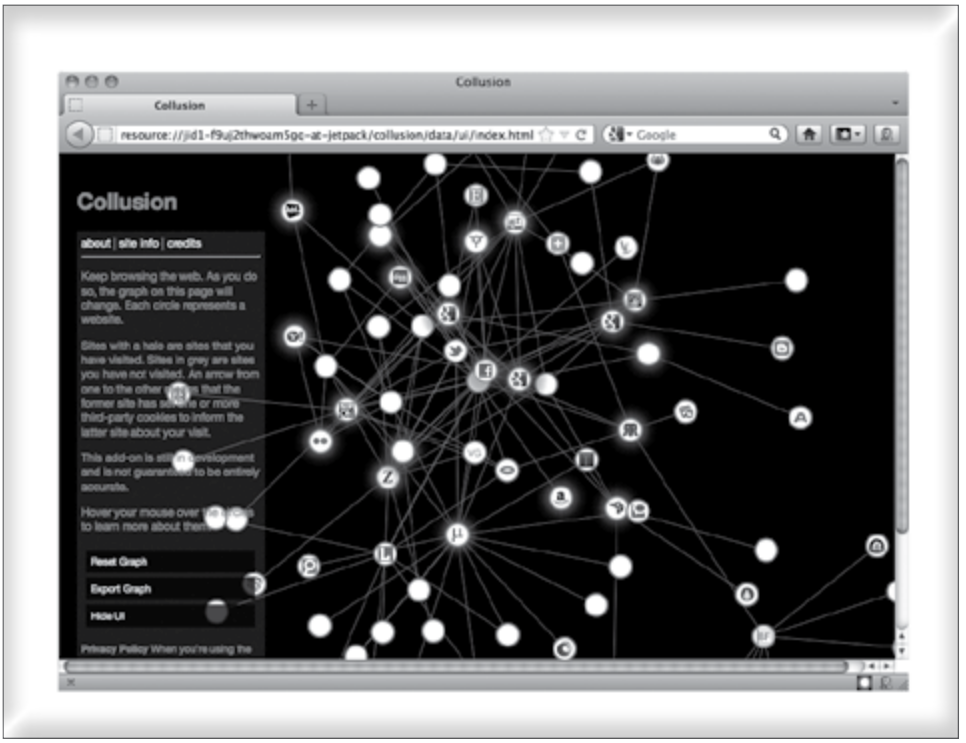


Abb. 3: Die Firefox-Erweiterung Lightbeam (vormals Collusion) visualisiert Abhängigkeiten zwischen Websites

(z.B. webserverübergreifend mittels Third-Party Cookies) über lange Zeit angelegt wurden, haben hier für die Kundenansprache großen Nutzen, weil sie eine genauere Extrapolation von Interessen in die Zukunft ermöglichen. Mit der Firefox-Erweiterung Lightbeam (vormals Collusion, siehe Abb. 3) lässt sich die in der Praxis heute bereits durchgeführte webserverübergreifende Verkettung mittels Third-Party Cookies sehr gut visualisieren.

Die Sensibilität der Nutzer hat inzwischen zugenommen: Erstens signalisieren große Anbieter die Verwendung von Cookies auf ihren Webseiten, da sie durch die Cookie-Richtlinie der Europäischen Union dazu angehalten werden. Wie bereits erwähnt, haben zweitens heute fast alle Browser die Möglichkeit zum Löschen der Cookies beim Beenden, wovon mehr und mehr Benutzer Gebrauch machen. Drittens installieren sich Nutzer Browsererweiterungen wie AdBlock und Ghostery, mit denen Werbung ausgeblendet und Third-Party Cookies blockiert werden können. Viertens existiert mit dem Do-Not-Track Header (DNT) auch die Möglichkeit, bereits mit dem ersten Webseitenbesuch zu signalisieren, dass keine Verkettung gewünscht wird. Hierzu muss der Nutzer über die Browsereinstellungen «Websites mitteilen, meine Aktivitäten nicht zu verfolgen» (Firefox). Leider respektieren bisher die wenigsten Webserver diese explizite Opt-Out-Datenschutzerklärung des Endnutzers.

Die Sensibilität der Anbieter von Inhalten für die Belange des Datenschutzes mag ebenfalls zugenommen haben, allerdings machen einige Anbieter bereits heute von sog. impliziten Verkettungsmerkmalen Gebrauch. Während Cookies explizit

Abb. 4: Canvas Fingerprinting nutzt Darstellungsunterschiede der Browser

zur Verkettung verwendet werden, eignen sich zahlreiche innerhalb eines Requests gesendete Daten ebenfalls zur Verkettung. Hierzu zählen beispielsweise:

(1) die HTTP-Header wie User-Agent und HTTP_ACCEPT-Header,
(2) im Browser installierte Schriftarten und Plug-Ins,
(3) Informationen zur Sprache, Zeitzone, Bildschirmauflösung und Farbtiefe des Browsers.

Üblicherweise ist ein Webserver berechtigt, diese Informationen zu erfahren, um eine bestmögliche Darstellung und Lokalisierung (Auswahl der Sprache) der Webseite zu erreichen. Panopticlick zeigt sehr anschaulich, wie eine Kombination dieser Merkmale auch ohne Cookies zu einer «Browsersignatur» und damit in den meisten Fällen zu einer eindeutigen Identifizierbarkeit jedes Browsers führt. Eine derartige Verkettung wird daher auch als Browser-Fingerprinting bezeichnet und verschärft die Situation für den sensiblen Endnutzer, da das Tracking (im Gegensatz zur Verkettung mittels Cookies) kaum noch verhindert werden kann.

Browser-Fingerprinting kann auch auf die Spitze getrieben werden: Das Canvas Fingerprinting nutzt winzige Darstellungsunterschiede innerhalb des Browsers (siehe Abb. 4). Das Remote Physical Device-Fingerprinting nutzt deterministische, gerätespezifische Ungenauigkeiten der internen Uhr eines Geräts und ist

somit nicht nur auf das Websurfen beschränkt, sondern lässt sich in jeder App zur Langzeitverkettung nutzen. Ein theoretischer Schutz kann nur durch Modifikation des TCP-Standards (Transmission Control Protocol) oder Hinzufügen eines künstlichen Time-Jitter erreicht werden.

Wie bereits erwähnt, existieren insbesondere auf mobilen Geräten wie Smartphones Identifier, die einer langfristigen und App-übergreifenden Verkettung dienen können. Mit der iPhone-App «Unique?» lassen sich ähnlich wie Panopticlick die Möglichkeiten des Device-Fingerprinting anzeigen.

7. Schlussbemerkungen

Die Anbieter von mobilen Apps und Smartphones werben natürlicherweise mit jeder kleinen Innovation in diesem sehr umkämpften Marktbereich. Leider werden die Risiken für die Privatheit, die mit Smart Watches, Wearables und der verbauten Sensorik einhergehen, wenig oder nicht erwähnt. Dabei ist ein «Informed consent», d.h. die präzise Information darüber, welche Daten wann, wo, wie lange und von wem gesammelt und gespeichert werden, nach der heutigen Rechtslage zwingend erforderlich. Glücklicherweise gibt es genügend Aktivismus und «App-Testing» zugunsten von Privacy, die mangelnde Information wieder wettmacht. Nützlich wären aus Sicht des Endnutzers auch Datenschutz-Gütesiegel für Apps. Bisher fehlen jedoch die konkreten Datenschutz-Standards. In anderen Bereichen (z.B. Smart Metering) werden sog. Protection Profiles von Datenschutz- und Sicherheitsbehörden bereitgestellt, nach denen sich die Anbieter richten müssen. Für den Smartphone-Bereich fehlen derartige Vorgaben zur Förderung von Transparenz und Datenvermeidung komplett. Bestenfalls wäre Datenschutz ein wettbewerbsförderndes Element; bereits vor vielen Jahren wurde dieser Ansatz propagiert. Mit einer entsprechenden internationalen Rahmengesetzgebung wäre ein solcher Ansatz sicherlich nach wie vor interessant. Allein auf Selbstverpflichtungen und den Markt sollte man nicht hoffen.

Literatur

Hannes Federrath (2013): *Computerüberwachung - Methoden und Möglichkeiten,* in: Forschung & Lehre 8 (2013) 614-616.
https://www2.informatik.uni-hamburg.de/svs/publ.php?search=forschung-und-lehre, Abruf am 18.09.2014.

Hannes Federrath (2013): *The Appification of the society – a technical viewpoint,* in: 35th International Conference of Data Protection and Privacy Commissioners (Closed Session), Warszawa, 23. September 2013. https://www2.informatik.uni-hamburg.de/svs/publ.php?search=appification, Abruf am 18.09.2014.

Forbes (2014): *Google Acquires Smart Thermostat Maker Nest For $3.2 Billion,* 13.01.2014. http://www.forbes.com/sites/aarontilley/2014/01/13/google-acquires-nest-for-3-2-billion/print, Abruf am am 28.05.2014.

Hannes Federrath, Andreas Pfitzmann (2000): *Gliederung und Systematisierung von Schutzzielen in IT-Systemen,* in: Datenschutz und Datensicherheit DuD 24/12 (2000) 704-710. https://www2.informatik.uni-hamburg.de/svs/publ.php?search=FePf2000, Abruf am 18.09.2014.

Golem.de (2014): *Promi-Bilder angeblich aus der iCloud gestohlen,* 01.09.2014. http://www.golem.de/news/security-promi-bilder-angeblich-aus-der-icloud-gestohlen-1409-108933.html, Abruf am 18.09.2014.

Herbert Braun (2013): *Android verbietet Nutzern Kontrolle über App-Rechte,* in: Heise-News 13.12.2013, http://www.heise.de/newsticker/meldung/Android-verbietet-Nutzern-Kontrolle-ueber-App-Rechte-2065505.html, Abruf am 18.09.2014.

Bitkom: *Internetjahr 2009: Rekord bei Online-Werbung,* http://www.bitkom.org/de/markt_statistik/64038_62318.aspx, Abruf am 28.05.2014.

Anne Kunz (2011): *Wie Werbung wirkt.* Zeit Online, 24. Januar 2011, http://www.zeit.de/wirtschaft/2011-01/werbung-internet, Abruf am 28.05.2014.

Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 29. November 2009

Peter Eckersley (2010): *How unique is your browser? Electronic Frontier Foundation,* 2010. http://panopticlick.eff.org, Abruf am 28.05.2014.

Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, Claudia Diaz (2014): *The Web never forgets: Persistent tracking mechanisms in the wild,* in: CCS 2014, https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf, Abruf am 18.09.2014.

Tadayoshi Kohno (2005): *Remote physical device fingerprinting,* in: IEEE Transactions on Dependable and Secure Computing, 2(2), April-June 2005, http://homes.cs.washington.edu/~yoshi/papers/PDF/KoBrCl2005PDF-Extended-lowres.pdf, Abruf am 18.09.2014.

So eindeutig lässt sich jedes iPhone zuordnen, http://www.iphone-ticker.de/oh-mein-gott-so-eindeutig-laesst-jedes-iphone-zuordnen-66244, Abruf am 28.05.2014.

Helmut Bäumler, Albert von Mutius (Hg., 2002): *Datenschutz als Wettbewerbsvorteil,* in: DuD-Fachbeiträge, Vieweg Verlag 2002.

MARCO GHIGLIERI, BENJAMIN LANGE, HERVAIS SIMO,
MICHAEL WAIDNER

Security und Privacy bei SmartTV: Bedrohungspotential und technische Lösungsansätze

1. Einführung

Die Vernetzung technischer Geräte im Haushalt nimmt von Tag zu Tag zu.[1] Eine zunehmende Anzahl kann Daten aus dem Internet empfangen und verarbeiten oder mit anderen Smart Home Geräten kommunizieren. Häufig können sie aus dem Internet oder dem lokalen Netzwerk ferngesteuert oder kontrolliert werden. Im Bereich von Entertainment-Geräten wie internetfähige Set-Top Boxen, Spielekonsolen und Blue-Ray Playern ist diese Entwicklung bei modernen Fernsehgeräten besonders auffällig. Jüngste Fortschritte in digitaler Rundfunktechnik, schnellen Internetzugängen und Web-Technologien ermöglichen den nächsten logischen evolutionären Schritt der Fernsehtechnik: die Konvergenz zwischen Internet und TV. Das Herzstück ist das SmartTV, also Fernsehgeräte, die über zusätzliche Funktionen und Schnittstellen wie Internetanschluss, USB, Speicherkarten und Netzwerkanschluss verfügen. Neben dem Empfang von Rundfunksignalen können so auch interaktive sender- oder programmbezogene Inhalte und Dienste aus dem Internet empfangen werden. Zusätzlich zum Fernsehen werden durch die Funktion Hybrid Broadcast Broadband TV (HbbTV) Medieninhalte aus dem Internet zur laufenden Sendung oder damit verbundene Inhalte aus einer Mediathek zur Verfügung gestellt. Ein SmartTV bietet neben der klassischen Nutzung als Fernsehgerät auch die Möglichkeit im Internet zu surfen, Bilder anzuschauen, Musik zu hören oder Video-Telefonie zu betreiben.[2] Aufgrund der Netzwerkanbindung können SmartTVs häufig über Smartphones oder Tablets gesteuert werden. In Deutschland wird bis 2016 die Anzahl aktiv vernetzter TV-Geräte auf voraussichtlich 20 Millionen Geräte ansteigen[3], davon über 13 Millionen HbbTV-fähige Geräte.[4] Ein ähnlich deutlicher Trend ist in den USA zu beobachten.[5]

Moderne SmartTVs gelten dementsprechend zunehmend als Multimedia-Center, die externe Kommunikations- und Fernsehdienste mit anderen intelligenten elektronischen Haushaltsgeräten verbinden können. Neben hohem Nutzerkomfort und einfacher Bedienbarkeit zielt die Verbindung zwischen TV und Internet auf wirtschaftliche Vorteile für Gerätehersteller, TV-Sender, Content-Anbieter sowie

1 Statista (2010).
2 Pricewaterhousecoopers (2013).
3 Statista (2011-a); Sattler (2011).
4 Statista (2011-b) .
5 Emarketer (2013); StrategyAnalytics (2014).

Infrastrukturbetreiber und Werbetreibende. Mit der erweiterten Funktionalität von SmartTVs entstehen jedoch auch Risiken für die Privatsphäre der Nutzer. Sie werden durch die aus Nutzersicht unübersichtliche Dienstleistungsstruktur der beteiligten Akteure und die fehlende Transparenz des Internetverkehrs verschärft. So haben sich mehr als ein Fünftel der SmartTV-Nutzer in Unkenntnis über die Internetfunktionalität und fast die Hälfte der Nutzer nur unzureichend über die Möglichkeiten von HbbTV informiert.[6]

Dieser Beitrag gibt zunächst einen Überblick über die technischen Möglichkeiten von SmartTVs. Auf dieser Grundlage werden verschiedene Angriffsvektoren aufgezeigt. Die Risiken für die Privatsphäre der Nutzer werden anhand der bei der Nutzung von SmartTVs anfallenden Daten und den daraus resultierenden Privacy-Implikationen aufgezeigt. Der Beitrag nennt schließlich neue technische Lösungsansätze zum Schutz der Privatsphäre.

2. Technische Möglichkeiten von Smart TVs

a) Technische Ausstattung

Moderne Fernsehgeräte können anders als bei konventionellen TV-Geräten direkt mit dem Internet über LAN oder WLAN verbunden werden, ohne dass ein Anschluss an einen externen Rechner oder eine Set-Top Box notwendig ist. Ähnlich wie mobile Endgeräte sind Smart TVs vernetzte Plattformen, die mit leistungsstarken Prozessoren sowie teilweise mit eingebauten Steuerungs- und Bewegungssensoren bestückt sind. Die Internetfunktionalitäten eines Smart TVs können in herstellerabhängige und -unabhängige Merkmale unterteilt werden. Der HbbTV Standard ist beispielsweise eine herstellerunabhängige Funktion. Diese stellen Rückkanäle zur Verfügung, die dem Nutzer die Interaktion und Partizipation am TV-Programm oder die Nutzung von Web-Anwendungen wie Sprach-Chat-Diensten oder sozialen Netzwerken ermöglichen. Moderne Smart TVs werden mit einer Vielzahl von Sensoren ausgestattet. Dazu gehören neben Mikrofonen und Kameras auch Bewegungs-, Temperatur- oder Luftfeuchtigkeitssensoren.

b) HbbTV-Standard

Die Verknüpfung von Rundfunk mit interaktiven Online-Diensten auf Smart TV-Geräten ist mit gängigen Web-Technologien möglich. Prominentes Beispiel ist der offene internationale Standard HbbTV.[7] HbbTV ist ursprünglich eine pan-europäische Initiative zur Harmonisierung der Rundfunk- und Breitband Bereitstellung von Multimediainhalten durch internetfähige Fernseher. Die HbbTV-Spezifikation[8] basiert auf der Erweiterung bestehender Web-Technologien und Standards wie JavaScript, HTML, CSS. Mittlerweile wird der HbbTV-Standard über Europa hinaus als ernsthafte Alternative und Ergänzung bestehender Rundfunkstan-

6 PricewaterhouseCoopers (2013).

7 Auf SmartTV-Geräten können HbbTV-Dienste von TV-Sendern per Knopfdruck aufgerufen werden; ETSI (2012).

8 ETSI (2012).

dards betrachtet.[9] Der HbbTV-Standard eröffnet die Möglichkeit, neben linearem Fernsehen (herkömmliches Programmfernsehen) den Zuschauer sowohl zusätzliche webbasierte Medienangebote (z. B. Werbung, Wetterberichte oder Teletext) zum laufenden und zukünftigen Programm, als auch On-Demand Dienste zur Verfügung zu stellen. HbbTV-Dienste werden in der Regel über die rote Taste auf der Fernbedienung aufgerufen, und werden daher oft als «Red Button»-Dienste bezeichnet. Anbieter von HbbTV-Diensten sind entweder die jeweiligen Programmveranstalter oder die Entertainment Provider. Für die Werbetreibenden und TV-Sender bestehen die Vorteile des «Red-Button» mit HbbTV in der Möglichkeit, neue interaktive TV-Geschäftsmodelle zu etablieren.[10] Zudem können die Eigenschaften von HbbTV personalisierte Empfehlungen für webbasierte Inhalte ermöglichen.[11]

c) Erweiterbare Plattform

Die Integration von Web-Technologien in Fernsehgeräte ermöglicht einen Zugriff auf Inhalte des World Wide Web, etwa durch einen zum Teil rudimentären Web-Browser als auch durch Kommunikationsdienste wie Musik-Player, E-Mail, Spiele, Social Media, VoIP-Dienste, Bezahlungsdienste oder Online-Banking. Web-Browser und Kommunikationsdienste werden dem Nutzer im «Smart Television Ökosystem» in Form von Apps, also als herunterladbare Software, die direkt auf dem Fernseher ausführbar ist, oder als Zugang zu unterschiedlichen Diensten wie z. B. Spielen, Videos, News zur Verfügung gestellt. SmartTV-Apps werden überwiegend vorinstalliert, können aber auch von Online-App-Stores heruntergeladen oder von externen Speichermedien installiert werden. Die meisten Fernsehgerätehersteller betreiben einen eigenen App-Store und bieten in der Regel Apps für iOS- oder Android- Geräte an. Diese ermöglichen etwa eine Echtzeit-Synchronisierung zwischen den SmartTVs und einer mobilen App auf dem Smartphone oder Tablet des Zuschauers. Das Konzept ist unter dem Begriff «Second-Screen Ansatz»[12] bekannt; auch mit HbbTV ist Second-Screen möglich.[13]

3. Mögliche Angreifer und Angriffsvektoren

Zur Erfassung der Gefährdungslagen im SmartTV Ökosystem ist eine Charakterisierung relevanter Angreifermodelle nützlich. Dabei ist zwischen unterschiedlichen Angreifertypen, die sich nach ihren Zielen, finanziellen und technischen Möglichkeiten sowie ihren Kenntnissen des gesamten oder eines Teils des IT-Systems zu differenzieren.

9 Deutsche TV Plattform (2014).
10 BLM (2012).
11 hbbtv-infos.de (2014).
12 Kuri (2013).
13 IRT GmbH (2014).

3.1. Mögliche Angreifer

a) Passive und aktive Angreifer

Der passive Angreifer ist in der Lage, alle Kommunikationskanäle im Haushalt abzuhören. Dazu zählen sowohl die Kanäle, die zwischen den Endkunden/Fernsehgeräten und den unterschiedlichen Back-End- bzw. Cloud-Infrastrukturen verlaufen als auch Kommunikationskanäle zwischen Gerätehersteller/ Servicetechniker, Infrastrukturbetreiber, Werbetreibenden und TV Sendern. Der aktive Angreifer kann abhören, kritische Komponenten des SmartTV-Ökosystems kompromittieren und Zugriff auf die dort gespeicherten Daten erlangen. Zudem kann ein aktiver Angreifer die über diese Kommunikationskanäle übertragenen Daten nicht nur lesen, sondern auch blockieren und manipulieren.

b) Interne und externe Angreifer

Ein Angreifer kann entweder ein Außenseiter sein, wie etwa professionelle Hacker, die im großen Stil Fernsehgeräte mit Schadsoftware infizieren, um unbemerkt Daten der Zuschauer zu entwenden, oder als Insider mit einer legitimen Systemrolle agieren, zum Beispiel Mitarbeiter eines SmartTV Herstellers. Angreifer kann entweder eine einzelne Person sein (z. B. ein Nachbar oder ein Mitglied einer koordinierten Gruppe professioneller Hacker. Während Einzelne möglicherweise durch Neugier getrieben oftmals nur über begrenzte Ressourcen und Wissen verfügen, zeigen Erfahrungen aus anderen digitalen Anwendungsszenarien wie bei mobiler Kommunikation oder bei klassischen Internet-Diensten, dass koordinierte Gruppen professioneller Angreifer in der Regel finanziell motiviert sind (organisierte Kriminalität) oder im Auftrag von Strafverfolgungsbehörden oder Geheimdiensten handeln. Das Infizieren einer sehr großen Zahl von Haushalten ermöglicht die Errichtung leistungsfähiger Botnets, die die Angreifer entweder für «Denial of Service»-Angriffe oder automatisierte Massenüberwachung einsetzen können.[14]

3.2. Angriffsvektoren

Im Folgenden betrachten wir die Angriffsvektoren, die Einfallstore für Angriffe: SmartTV-Geräte, Kommunikationsnetze und die Cloud und andere Back-End-Infrastrukturen der Dienstanbieter. In der Praxis können diese Möglichkeiten auch kombiniert auftreten und sind in der Regel mit Social Engineering Ansätzen verbunden. Damit sind Angriffsmethoden gemeint, die den Zuschauer so beeinflussen, dass er unbeabsichtigt präparierte Schadsoftware ins Ökosystem einschleust und vertrauliche Informationen preisgibt. Nicht alle diese Angriffsvektoren und Angriffsflächen sind spezifisch für das SmartTV-Ökosystem, sollten aber bei einer ganzheitlichen Gefährdungsanalyse in Betracht gezogen werden.

14 Heise (2014).

3.2.1. Angriffsvektoren im Smart TV-Gerät

Angriffsvektoren in SmartTVs umfassen potentielle Schwachstellen in auf dem Gerät vorhandener Soft- und Hardware, also Schwachstellen aus der Erweiterung der SmartTV Plattform durch Apps, Angriffsflächen im SmartTV Browser und HbbTV-Browser, Ausführungen verschiedener Multimedia-Inhalte sowie integrierte Sensoren und Hardware-Schnittstellen.[15]

a) SmartTV-Apps

Apps haben in der Regel umfassenden Zugriff auf geräte- oder nutzerspezifische Daten. Nutzer sind sich oft nur begrenzt bewusst, welche Daten bei der Nutzung einer App anfallen, auf welche Daten Apps zugreifen und für welchen Zweck sie benötigt werden. Apps greifen auf eine Vielzahl externer Multimediainhalte zu. Koreanische Forscher des GrayHash-Offensive Security Research Center zeigten 2013, wie Angreifer fehlende Transparenz über die Erhebung und Verarbeitung sensibler Daten durch Apps ausnutzen können, um Schadsoftware in Fernsehgeräte einzuschleusen.[16] Unabsichtlich installierte oder mitgelieferte datenschutzunfreundliche SmartTV-Apps können so vom Angreifer benutzt werden, um auf im SmartTV anfallende sensible Daten zuzugreifen.

b) SmartTV-Browser und HbbTV-Browser

Browser in Smart TVs und ihre Unterstützung von Cookies, Javascript oder HTML eröffnen Angreifern Wege, um unbemerkt den ungefähren Standort des SmartTVs sowie Informationen zum Gerätetyp genauer und kontinuierlich zu erfassen. Ferner erlauben sie Angreifern, den Fernseher mit Schadsoftware zu infizieren sowie den Datenaustausch zwischen Browser und Webserver abzuhören, zu manipulieren oder zu unterbinden. Diese Gefahr wird verschärft, weil die angewendeten Sicherheitsfunktionen häufig unzureichend sind und zusätzliche Sicherheitsmängel im SmartTV-Browser (z. B. durch inkorrekte Überprüfung der digitalen Zertifikate bei der Unterstützung des HTTPS-Standards)[17] ein Einfallstor für Spähsoftware und andere bösartige Inhalte wie Phishing-Websites sein können.[18] Ein HbbTV-Browser ist gewöhnlich nicht sichtbar und vom SmartTV-Browser auf dem Fernsehgerät getrennt. Es gelten allerdings die gleichen Gefahren, wie auch für einen SmartTV-Browser. Der Unterschied besteht darin, dass der Nutzer den HbbTV-Browser häufig nicht vom eigentlichen TV-Programm unterscheiden kann, da er bei eingeschalteter HbbTV-Funktionalität transparent auf dem übertragenen TV Programm liegt. Bei vielen SmartTV-Geräten ist die HbbTV-Funktionalität standardmäßig aktiviert. Nutzer wissen nicht, ob bestimmte Elemente auf dem angezeigten Bildschirm tatsächlich aus dem Internet oder über das Rundfunksignal kommen.

15 Auriemma (2012); SeungJin/Kim (2013).
16 SeungJin/Kim (2013).
17 HTTPS ist der Standard für die verschlüsselte Übertragung von Daten zwischen Browser und Webserver.
18 Ghiglieri (2014).

c) Multimedia-Inhalte

Spähsoftware und andere Schädlinge können als Multimediainhalte eingeschleust und unentdeckt bleiben.[19] Dabei machen sich die Angreifer Schwächen der auf fast allen SmartTV Modellen integrierten Media-Playern zu Nutze. Der Player und die damit verbundenen Codes ermöglichen das Öffnen und Ausführen unterschiedlicher Dateitypen einschließlich von Videos und Bildern. Diese Dateien werden typischerweise entweder von einem Datenträger (USB, Speicherkarte) oder von einem externen Server auf den SmartTV gespielt. Sie sind potentiell Träger von Trojanern, deren Ausführung dem Angreifer erlaubt, unbemerkt die Kontrolle über Hardware-Module wie Kameras und Mikrofone zu erlangen, auf persönliche Daten (z.B. Kontakte, Passwörter, Kreditkartenummern, Standort des Gerätes zuzugreifen oder das Gerät zum Absturz zu bringen.[20] Ähnlich können etwa datenhungrige Gerätehersteller, TV-Sender oder Servicetechniker Schwachstellen im Design der Fernwartungsstrategie für SmartTVs ausnutzen, um Nutzer dazu zu bewegen, präparierte Firmware-Updates mit integrierter Spähsoftware auf dem Fernseher auszuführen. Daher ist es wichtig, dass Sicherheitsaktualisierungen in allen Teilsystemen auf dem Smart TV beim Nutzer auch schnell ankommen. Veraltete Systeme erhöhen signifikant das Risiko von Sicherheitsvorfällen.

d) Integrierte Sensoren und Hardware-Schnittstellen

Moderne SmartTVs[21] werden mit einer Vielzahl von Sensoren wie z. B. Mikrofonen sowie Kameras, Bewegungs-, Temperatur- oder Luftfeuchtigkeitssensoren ausgestattet. Einerseits stellen diese Sensoren Rückkanäle zur Verfügung, die die Interaktion und Partizipation am TV-Programm oder die Nutzung von Web-Anwendungen wie Skype oder Facebook ermöglichen. Anderseits steigt mit dem Trend zur Ausstattung des TVs mit einer HD-Kamera, Mikrofon und Bewegungssensoren auch das Risiko für Schwachstellen in den verwendeten Apps und der Software für die Sensorsteuerung. Angreifer können Kenntnis über die Architektur der eingebauten Hardware oder Sensoren und über das Zusammenspiel zwischen diesen und weiterer Software auf dem SmartTV erlangen und dieses Wissen nutzen, um das System zu kompromittieren. Geräte mit höherer Ausstattung besitzen bereits Kameras oder Bewegungssensoren sowie Mikrofone; sie können durch schadhafte Firmware so manipuliert werden, dass sie als Wanze genutzt werden können.[22] Eine Untersuchung unterschiedlicher SmartTV-Modelle der Firma Samsung hat 2013 gezeigt, wie vorinstallierte Web-Anwendungen wie Skype oder Facebook von Angreifern manipuliert werden können, um Zuschauer in dessen Wohnzimmer oder Schlafzimmer über in SmartTVs eingebaute Webcams und Mikrofone auszuspionieren.[23] Dabei gibt das Fernsehgerät nicht mehr den üblichen Hinweis, etwa durch rotes oder grünes Licht, auf den Status der Kamera oder des Mikrofons, so dass der Nutzer den Betrieb nicht mehr kontrollieren kann.

19 Michéle/Karpow (2014).

20 Auriemma (2012); SeungJin/Kim (2013).

21 Häufig bieten Hersteller verschiedene Produktreihen mit verschiedenen ausgestatteten Smart TV-Geräten an.

22 Michéle/Karpow (2014).

23 Grattafiori/Yavor (2013).

3.2.2. Angriffsvektoren in Kommunikationsnetzen

Weitere Einfallstore nutzen Design und Implementierungsschwächen in Protokollen zur Übertragung von Daten zwischen dem Smart TV und externen Parteien aus, um den Datenverkehr abzuhören, manipulierte Datenpakete einzuschleusen oder den Datenverkehr zu filtern oder zu blockieren. Gelingt es einem passiven Angreifer, den Verkehr zwischen SmartTV und externem Webserver (z. B. des Geräteherstellers oder des Online Bezahldienstes) auszuspähen, kann dieser unbemerkt und unautorisiert Zugriff auf sensible Zuschauer- und Fernseherdaten erlangen. Ghiglieri et al.[24] zeigten 2013, wie Dritte Schwächen des HbbTV Protokolls ausnutzen können, um das Nutzungsverhalten der Zuschauer eines HbbTV tauglichen Fernsehers mit WLAN Nutzung ohne deren Wissen oder das der TV-Sender aufzuzeichnen. Der Angriff ist selbst dann möglich, wenn das WLAN mit Hilfe von WPA2 abgesichert und der Angreifer nicht Teil des Netzwerkes ist.[25] Denn TV-Sender verwenden unterschiedliche und jeweils charakteristische Paketgrößen für die übertragenen Daten. Durch Abgleich mit einem eigenen Smart TV kann ein Angreifer sogar bei verschlüsselten Datenpaketen leicht Übereinstimmungen in der Größe der Pakete feststellen und bei Erkennung einer bestimmten Paketreihenfolge den eingeschalteten Sender erkennen.
Zudem dokumentierten die Autoren, wie HbbTV Features den Sendeanstalten ermöglichen, sensible Daten wie das Nutzungsverhalten ihrer Zuschauer zu erfassen. Diese Schwachstelle könnte auch von aktiven Angreifern ausgenutzt werden, um bestimmte Inhalte zu blockieren, zu zensieren oder präparierte Datenpakete als Vorstufe eines großflächigen «Denial of Service» Angriffs einzuschleusen. Eine weitere Angriffsmöglichkeit erlaubt das Rundfunksignal mit der Internet-Adresse für die HbbTV Anwendung. Durch Manipulation der HbbTV-Adresse im Rundfunksignal können Inhalte großflächig auf HbbTV-fähigen Fernsehern manipuliert werden. Die Schutzmaßnahmen im Rundfunksignal sind äußerst niedrig. Oren et al. zeigten 2014 einen Angriff, der bis zu 20.000 Haushalte mit einem niedrigen Kostenaufwand manipuliert.[26]

3.2.3. Angriffsvektoren in der Cloud und Back-End-Infrastruktur

Angriffsvektoren bei Cloud-basierten Webdiensten sind zahlreich und nicht spezifisch für SmartTVs als Anwendungsszenario. Die drei typischen Angriffsvektoren werden im Folgenden zusammengefasst.

a) Böswilliger Insider beim Cloud-Betreiber

Es handelt sich dabei um Angreifer, häufig Angestellte der Cloud-Betreiber mit privilegiertem Zugang zu Kundendaten und mit Kenntnissen über die interne grundlegende Architektur der aktuellen Cloud-Computing-Angebote. Je nach Berechti-

24 Ghiglieri/Oswald/Tews (2013).
25 Ghiglieri/Oswald/Tews (2013); Ghiglieri/Tews (2014).
26 Oren/Keromytis (2014).

gungen kann der böswillige Insider Kundendaten löschen, ändern oder kopieren und im schlimmsten Falle sogar an kriminelle Organisationen verkaufen.[27]

b) Schwachstellen in der «Shared Architecture»

Schwachstellen sind Isolationsbrüche, unsichere virtuelle Maschinen und die unvollständige Löschung sensibler Daten. Die Tatsache, dass in der Cloud mehrere virtuelle Maschinen auf einem Rechner laufen und sich dementsprechend verschiedene Cloud-Anwender (Anbieter von Webdiensten) Ressourcen wie CPU, Speicher oder Netzwerk teilen müssen, kann mit Schwachstellen im Design oder der Implementierung des Hypervisors[28] ausgenutzt werden, um auf fremde Daten, Ressourcen und Anwendungen zuzugreifen.[29] Häufig veröffentlichen unachtsame Entwickler Images (Details zur Konfiguration von virtuellen Maschinen), die noch private kryptografische Schlüssel, Zertifikate und Passwörter enthalten.[30] Für einen Angreifer mit Wissen über diese sensiblen Informationen ist eine Kompromittierung der virtuellen Maschine mitsamt der Kundendaten und Anwendungen keine große Herausforderung. Im Rahmen vieler Cloud-basierter Angebote kann es aus unterschiedlichen Gründen dazu kommen, dass ein neuer Kunde eine virtuelle Maschine erhält, auf der die Datenbestände vorheriger Anwender nicht vollständig gelöscht wurden. Dies erhöht das Risiko, dass sensible Kundendaten in falsche Hände geraten könnten.

c) Unsichere Managementschnittstellen und -APIs

Cloud-Dienste werden in der Regel über Schnittstellen und Interfaces verwaltet, welche wiederum über das Internet erreichbar sind. Diese können in Kombination mit einer schwachen Authentifizierung oder gefälschten Identitäten unbefugt verwendet werden, um auf Kundendaten und Anwendungen zuzugreifen. Für einen relativ aktuellen Überblick über Angriffsvektoren und Bedrohungen in der Cloud sei auf CSA, Zeit Online[31] und Buchmann[32] verwiesen.

4. SmartTV-Daten: Welche Daten fallen bei Smart TVs an?

Bei der Verwendung eines SmartTVs offenbaren Nutzer absichtlich oder unbewusst viele personenbezogene oder personenbeziehbare Daten.

a) Konto- und Registrierungsdaten

Einige Dienste auf Smart TVs erfordern eine Registrierung des Gerätes online sowie gültige Nutzerkonten mit Anmelde- und Profildaten. Bei Verknüpfung des SmartTV-Geräts mit einem Account können die jeweiligen Dienstanbieter verschiedene persönliche Daten, wie etwa Namen, Geburtsdatum, Geschlecht, Adresse oder

27 Zeit Online (2013).

28 Komponenten/Mechanismen zur effektiven Trennung der Daten und Anwendungen verschiedener VMs.

29 Wojtczuk, R./Beulich, J. (2012); Kortchinsky, K. (2009); Elhage, N. (2011).

30 Bugiel/Nürnberger/Pöppelmann/Sadeghi/Schneider (2011).

31 CSA (2013); Zeit Online (2013).

32 Buchmann (2012).

Zahlungsinformationen des Benutzers erheben. Darüber hinaus werden Benutzername und Kennwort für den wiederholten Zugriff auf personalisierte Online-Dienste für den komfortablen Umgang mit der Seite im Speicher des Smart TVs gespeichert. Eine Nutzung des SmartTVs ohne Konto- und Registrierungsdaten ist in der Regel möglich, aber sobald echte «Smart»-Dienste wie personalisierte Apps genutzt werden sollen, muss häufig eine Anmeldung erfolgen.

b) Nutzungs- und Fernsehverhaltensdaten

Nutzungsdaten entstehen über die Interaktion zwischen den SmartTVs und den Nutzern und enthalten Details über die für oder von den Nutzern auf dem Fernseher aktivierten Inhalte, Apps oder Dienste sowie Informationen über zur Verfügung stehende TV-Kanäle. Diese Informationen umfassen etwa, welche TV-Programme angesehen werden, Anfragen und Suchbegriffe zu Inhalten etwa in der Mediathek, das angeklickte Werbematerial sowie welche und wie lange der Zuschauer Steuerungsaktionen wie «Play», «Stop», «Pause», «Fast Forward» oder ähnliches betätigt hat. Zudem werden Nutzungsdaten über das Browsing-Verhalten oder die Browsing-Historie des Nutzers sowie die durch SmartTV-Sensoren erfassten Video-, Bilder- und Stimmaufnahmen von Hausbewohnern und Besuchern erfasst. Aus den Sensordaten können unter Umständen biometrische Daten wie Gesichtsgeometrie abgeleitet werden. Sie werden zunehmend genutzt um ein personalisierteres TV-Erlebnis zu schaffen, z. B. durch Gesichts- bzw. Stimmerkennung.[33] Nutzungsdaten werden durch den Fernseher und Apps kontinuierlich erfasst und an Dienstanbieter oder Werbetreibende übermittelt, sobald sie sich mit dem Internet verbinden. Auch bei HbbTV werden Nutzungsdaten erfasst und typischerweise schon beim Einblenden, dass HbbTV verfügbar ist, an den Sender übermittelt. Google Analytics und andere Trackingdienstleister wurden in der Vergangenheit ebenfalls genutzt.[34]

c) Gerätspezifische Daten

Hardware-Merkmale des Smart TVs wie der Name des Geräteherstellers, die Modellbezeichnung oder Geräteversion sowie der Typ, die Version des Betriebssystems oder der Firmware werden erfasst. Hinzu kommen Details über die Art der Netzwerkschnittstelle oder Netzwerkverbindung (WLAN, LAN, Bluetooth), die Netzwerkadresse des Fernsehgerätes (MAC- oder IP-Adresse), Informationen über eingebaute Sensorgeräte oder der eindeutige Fernsehgeräte-Identifier («Unique Device ID»). Einbezogen werden die Version des HbbTV-Standards, die das Fernsehgerät unterstützt, oder der HbbTV Status in den Geräteeinstellung (aktiviert / deaktiviert). Weitere gerätspezifische Daten sind Angaben über alle im Heimnetzwerk vorhandenen und an das SmartTV-Gerät angeschlossenen elektronischen Geräte, sowie die notwendigen Zugangsdaten, um sich gegenüber netzwerkfähigen Heimgeräten oder externen Servern zu authentifizieren.

33 Lendino (2014); Yeong Gon et al (2012).
34 Ghiglieri/Oswald/Tews (2013); Ghiglieri (2014).

d) Ableitbare Daten

Eine Auswertung des Nutzungs- und Fernsehverhaltens erlaubt Rückschlüsse auf die politische Einstellung, Hobbys, Bildungsgrad oder den ethnischen Hintergrund des Zuschauers. Zudem lassen sich Rückschlüsse auf Familienstatus sowie Gewohnheiten und Objekte in der unmittelbaren Umgebung des Fernsehgerätes etwa im Wohnzimmer ziehen. Die Aggregation von Browsing-Historie und Korrelationen mit Konto- und Registrierungsdaten können zur Gewinnung weiterer Persönlichkeitsmerkmale und privater Eigenschaften der Zuschauer wie etwa sexuelle Orientierung oder Vorlieben verwendet werden. Aus der Interpretation der gerätespezifischen Daten oder der Netzwerkadresse des Fernsehers können Details über den Standort des Gerätes und somit die des Zuschauers gewonnen werden. Dritte können auf diese Weise nicht nur die Fernseh- und Nutzungsgewohnheiten der Zuschauer ausforschen, sondern diese auch gezielt überwachen.

5. Beeinträchtigungen der Privatheit der Nutzer

Die finanziellen oder politischen Anreize, SmartTV-Daten systematisch zu erfassen und auszuwerten, bewirken in der kommenden «Big Data»-Ära schwerwiegende Folgen für die Privatsphäre des Nutzers.

a) Tracking und Profilbildung

SmartTV-Geräte mit HbbTV-Anwendung verbinden sich zu den Servern der Sender des jeweils auf dem Gerät laufenden Programmes. Mindestens beim Einschalten[35] des Senders wird vom Gerät eine Anfrage an einen Server des Senders gestellt, um den sog. «Red Button», der die Verfügbarkeit von weiteren Onlineinhalten zum gewählten Programm anzeigt, auf dem Bildschirm einzublenden. Viele Sender senden aber periodische Anfragen mit einem Zeitintervall zwischen einer Sekunde und mehreren Minuten.[36] Auf diese Weise ist der Sender in regelmäßigen Abständen – in der Vergangenheit teilweise sogar sekundengenau – darüber informiert, zu welcher Zeit der Nutzer einen Sender eingeschaltet hat. Dies verletzt das Prinzip der Datensparsamkeit und Datenvermeidung. Bei einigen Sendern werden über periodische Anfragen auf den Server des Senders zugleich Trackingskripte von Drittanbietern (z.B. Google Analytics oder etracker) geladen oder Cookies gesetzt. Beides sind Maßnahmen, um das Nutzerverhalten zu tracken und zu analysieren. Die Ergebnisse des Trackings mit Google Analytics erhält der Sender selbst nur in anonymisierter Form. So dürfen keine vollständigen, sondern nur Teile der IP-Adressen an den Sender übermittelt werden.

Dagegen liefert die Verwendung von Cookies dem Sender wesentlich detailliertere Informationen zum Nutzerverhalten. Der Setzung von Cookies kann in vielen SmartTV-Geräten nicht widersprochen werden. Zudem können diese oft gar nicht oder nur umständlich angesehen oder gelöscht werden.[37] So bleiben Cookies für immer auf dem Gerät gespeichert und stellen so eine eindeutige Nutzerkennung dar.

35 Datenschutzfreundlichere Varianten von HbbTV ermöglichen sogar das Laden über das Rundfunksignal. Dies lässt Nutzertracking und Profilbildung nicht zu.

36 Ghiglieri/Oswald/Tews (2013).

37 Ghiglieri/Oswald/Tews (2013).

Da häufig eine Sendeanstalt mehrere Sender verantwortet, wird so auch ein senderübergreifendes Tracking der Nutzer und die Erstellung von detaillierten Nutzerprofilen ermöglicht. Dass die Sender tatsächlich Nutzerprofile erstellen, zeigt die bei manchen Sendern in festen Zeitabständen eingeblendete personalisierte Werbung.[38] Besonders problematisch ist das Tracking des Nutzerverhaltens, weil dies technisch sogar dann möglich ist, wenn der Nutzer die HbbTV-Funktionalität nicht wissentlich anfordert. Unabhängig von Cookies oder Skripten wird in jedem Fall durch eine Verbindung des Smart TV zum Sender die IP-Adresse des Nutzers übertragen, die eine grobe Lokalisierung des Nutzers erlaubt. Da IP-Adressen bei vielen Internetprovidern für 24 Stunden oder länger gleich bleiben, liefert diese damit zugleich die Möglichkeit, den Nutzer in diesem Zeitraum wiederzuerkennen.

b) Massenüberwachung und gezielte Überwachung der Zuschauer

Aus Daten kompromittierter SmartTV-Sensoren (z. B. Video-, Bilder-, und Stimmaufnahmen) lassen sich ohne Wissen und Einverständnis der Nutzer Informationen über Aktivitäten und Verhaltensweisen der Nutzer sowie über die Ausstattung in sensiblen Bereichen des Haushalts ableiten. Dies stellt nicht nur ein Sicherheitsrisiko dar, weil Einbrecher oder aufdringliche Diensteanbieter den Zuschauer On- und Offline gezielt überwachen können. Auch Geheimdienste können die im SmartTV-Ökosystem anfallenden Daten zweckentfremden, um Massenüberwachungsprogramme durchzuführen.

c) Intransparenz der Datenverarbeitung

Mit Smart–TVs erhobene Daten sind personenbezogene Daten. Die Nutzer wissen jedoch oft nicht, dass ihre Fernsehgeräte solche Daten häufig auch ohne konkreten Bedarf erfassen und weiterleiten können. Viele Nutzer von SmartTV-Geräten sind sich nicht einmal der Tatsache bewusst, dass ihr Gerät über eine Verbindung ins Internet verfügt.[39] Zudem ermöglicht die Systemgestaltung des heutigen SmartTV die Erhebung und Verarbeitung dieser Daten ohne Mitwirkung der Betroffenen.[40] Daher verletzt ihre Übermittlung an externe Akteure die Einhaltung des Transparenzprinzips gegenüber den Nutzern.

d) Verlust der Entscheidungsautonomie

Heutige SmartTV-Dienste können schwerwiegende Folgen für die individuelle Entscheidungsautonomie haben. Insbesondere ist es bedenklich, dass die Nutzer aufgrund der Gestaltung der Plattform und der Methoden zur Erhebung und Verarbeitung der Daten keine echten Entscheidungsoptionen erhalten. Dies stellt die Verbraucher vor die nicht akzeptable Wahl, der Datenerhebung entweder zu widersprechen oder die Dienstleistung zu verlieren.[41] Schon das Wissen um die Möglichkeit, SmartTVs und die anfallenden Daten zur gezielten Überwachung einzusetzen,

38 Ghiglieri/Oswald/Tews (2013).

39 Nach PricewaterhouseCoopers (2013), S. 12 wissen 22% der SmartTV-Benutzer nicht, ob ihr Smart –TV mit dem Web verbunden ist; 10% der TV-Haushalte wissen nicht, ob ihr TV-Gerät ein SmartTV ist.

40 DoctorBeet's Blog (2013-a).

41 DoctorBeet's Blog (2014-b).

kann die Entscheidungsautonomie der Nutzer stark einschränken. Sie können ihr Nutzungsverhalten als Reaktion auf das Gefühl der Beobachtung einschränken oder ganz auf die Nutzung eines SmartTVs verzichten. Zudem entsteht das Risiko einer Offenlegung vertraulicher Daten wie der Konto- oder Registrierungsdaten des Zuschauers als Folge von technischem oder menschlichem Versagen oder von Cyber-Angriffen. Damit verbunden ist das Risiko eines millionenfachen Identitätsdiebstahls mit schwerwiegenden finanziellen Schäden für die Nutzer.

6. Technische Schutzmöglichkeiten

Die Erhöhung der Funktionalität und der Verbindungsmöglichkeiten von Unterhaltungselektronik vergrößert die potentielle Angriffsfläche und erhöht die Wahrscheinlichkeit von Datenschutzproblemen. Ein Sicherheits- und Datenschutzproblem bei smarter Unterhaltungselektronik kann unmittelbar zu einem Vertrauensverlust bei Nutzern und einem Reputationsverlust bei Unternehmen führen. Daher ist es notwendig, hohe Transparenz bei der Einführung solcher Geräte für alle Prozesse zu schaffen. Diese reichen von der Aufklärung der Bevölkerung bis zur Entwicklung komplexer technischer Schutzmaßnahmen.

a) Datensparsamkeit

Die Datensparsamkeit ist ein einfaches Mittel, um Gefahren zu minimieren. Datensparsamkeit bedeutet nicht nur, die Anzahl der anfallenden Daten, sondern auch deren Aussagekraft zu minimieren. So sollten nur die Daten übertragen werden, die für eine korrekte Funktionalität benötigt werden. Allerdings besteht ein Interessenkonflikt: Hersteller wollen möglichst genau erfahren, in welcher Umgebung ein Gerät eingesetzt wird. Daher werden Verfahren und Methoden benötigt, die die Interessen aller Akteure in Einklang bringen. Dies können zum einen komplexe technische Lösungen sein, die die Einhaltung von bestimmten Sicherheitsregeln bekräftigen, zum anderen die einfache Blockierung von Datenströmen. Zum Beispiel könnte die einfache Aggregation von Daten und die Weiterleitung dieser Daten an Dienste schon allen Anforderungen gerecht werden. Bei noch sensibleren Daten könnte man kryptografische Verfahren, wie die homomorphe Verschlüsselung, nutzen. Die Aggregation von Daten kann dann beispielsweise mit der Gewissheit durchgeführt werden, dass die Daten selbst für den verarbeitenden Anbieter nicht sichtbar sind, aber dennoch bestimmte Operationen ausführbar bleiben. Ein beispielhaftes System skizieren wir im nächsten Kapitel.

b) Aufklärung der Nutzer

Sie ist ein wichtiges Instrument, um Transparenz und Vertrauen in neue Techniken zu schaffen. Sie umfasst die benutzergerechte Visualisierung und Deutung der Daten. Auch wenig-technikaffine Personen nutzen die Funktionen eines Smart TVs ohne einen versteckten Datentransfer zu erwarten. Die Visualisierung beginnt bei der Sichtbarmachung von Datenströmen zum Internet bis zur Kommunikation unterhalb der Geräte. Häufig sind die Daten ohne Kenntnis über den Inhalt und die Bedeutung der Daten für Nutzer schlecht bewertbar. Die Kommunikation mit einer Fremdpartei kann zwar schon Indiz für eine unberechtigte Verbindungsaufnahme sein. In vielen Fällen jedoch ist es wünschenswert, den Grund und den Inhalt für

eine Kommunikation mit in die Bewertung einfließen zu lassen. Allerdings ist die benutzergerechte Visualisierung im Bereich Smart TV noch nicht so weit fortgeschritten, dass eine flächendeckende Verwendung möglich wäre.

Die Deutung der anfallenden Daten stellt eine größere Herausforderung dar. Wie auch bei Virenscannern ist eine große Datenbank von Signaturen und Mustern notwendig, um bestimmte Übertragungsmuster zu deuten und zu erkennen. Der Unterschied zwischen einer Datenbank mit Vireninformationen und einer Datenbank mit Informationen zum gewünschten Verhalten eines Smart TVs ist, dass Viren Schadprogramme sind, die für jeden ähnlich schädlich eingestuft werden sollten. Bei Geräten, die bestimmte Daten übermitteln, ist es nicht immer für jeden Nutzer klar, was gewünscht oder unerwünscht ist. Die Etablierung einer solchen Datenbasis für Smart TVs ist wünschenswert, bedarf aber weiterer Forschung. Die Erhebung einer solchen Datenbasis birgt allerdings auch Gefahren für jeden einzelnen Nutzer oder Haushalt, da unter Umständen private Nutzungsgewohnheiten veröffentlicht werden könnten. Dazu müssten Methoden und Verfahren evaluiert werden, wie die Generierung ohne Datenschutzprobleme vollzogen werden kann. Ein bestehendes Forschungsproblem ist die Verallgemeinerung solcher Daten, so dass der erzeugende Haushalt keine Informationen zu Nutzungsgewohnheiten preisgeben muss.

c) Aktive Steuermöglichkeit

Sie würde dem Nutzer etwa durch Filterung oder Blockierung ermöglichen, einen unerwünschten Datenstrom zu unterbinden. Die heutigen Filterungs- und Blockierungsmaßnahmen sind häufig nur netzwerkbasiert, wünschenswert wäre jedoch eine inhaltsbasierte Filterung. So könnten etwa HbbTV-Anwendungen von öffentlich-rechtlichen Sendern übertragen und von Privatsendern blockiert werden. Eine Blockierung kann ganze Geräte oder bestimmte Dienste erfassen. In jedem Fall sollte eine geeignete Übertragungsform mit verschlüsselungs- und integritätsgewährleistenden Verfahren genutzt werden. Im Bereich des Internets haben sich HTTPS Verbindungen etabliert, die auch bei SmartTV Diensten genutzt werden sollten.

d) Regelmäßige Aktualisierung

Eine regelmäßige Aktualisierung der Software auf den Geräten ist wichtig, da sie ähnlich leistungsfähig sind wie Computersysteme. Mit der Erhöhung der Konnektivität werden Sicherheitslücken in Smart TVs wahrscheinlicher. Aus diesem Grund müssen Aktualisierungen vom Hersteller durchgeführt und auf alle Smart TV Geräte gebracht werden. Geht man von ähnlichen Lebenszeiten wie bei konventionellen Fernsehgeräten aus, müssen Aktualisierungen über mehrere Jahre bereitgestellt werden. Bei einigen Smartphone Herstellern liegt die Aktualisierungszeit derzeit bei 18 Monaten, was bei Fernsehgeräten deutlich zu niedrig wäre.

e) Benutzerfreundlichkeit

Eine Sicherheitsmaßnahme wird sich vermutlich durchsetzen, wenn sie die Nutzung nicht einschränkt. So ist HTTPS für jeden Benutzer anwendbar, ohne dass sich etwas

an der Benutzbarkeit verändert. Als negatives Beispiel kann man Firewalls anführen: In heutigen Heimroutern sind zwar Firewallwerkzeuge integriert, dennoch haben Nutzer häufig nicht die Kenntnisse zur korrekten Anwendung. Auch die Aktualisierungsmöglichkeit der Smart TV-Geräte muss benutzbar sein. Ein Konsument wird im Regelfall nicht auf die Herstellerwebsite gehen, um dort eine Aktualisierung der Software auf einem Fernsehgerät durchzuführen.

7. Implementierung

Die erläuterten Methoden können bereits an einigen Beispielen gezeigt werden. Allerdings ist ein vollständiger Schutz vor allen Gefahren derzeit nicht erforscht. Viele Gefahren und Möglichkeiten der Datennutzung sind noch unbekannt.

Die Möglichkeit einer noch genaueren Zuschauermessung über HbbTV wurde erstmalig in Publikationen[42] nachgewiesen und mit dem Privacy Protector in [43] prototypisch durch den Nutzer steuerbar gemacht. Auch wenn ein Benutzertracking aus rechtlicher Sicht durchaus als legal eingestuft werden könnte, hat jeder Nutzer das Recht, diese Messung zu erkennen und auch ausschalten zu können. Mit dem Privacy Protector wird eine Konzeptimplementierung für einen kleinen Computer (Raspberry Pi) vorgestellt, die es dem Konsumenten ermöglicht, das Laden von HbbTV Inhalten ohne seine Zustimmung zu unterbinden. Der Raspberry Pi wird dabei zwischen dem Smart TV und dem herkömmlichen Internet-Router angeschlossen. Die Verbindung zwischen Smart TV und Raspberry Pi ist üblicherweise ein Kabelanschluss; die Verbindung zum Internet kann ebenfalls per Kabel oder drahtlosen Adapter bewerkstelligt werden. Das Gerät kann hinter ein Smart TV-Gerät montiert werden und ist damit nicht sichtbar. Nach Inbetriebnahme wird eine HbbTV Anwendung standardmäßig nicht geladen. Dem Benutzer wird auf dem Bildschirm mitgeteilt, dass eine Internetaktivität durch HbbTV blockiert wurde, woraufhin der Nutzer diese mit Drücken des «Green Button» zulassen kann. Technische Details finden sich in.[44] Eine prototypische Implementierung des Systems kann auf den Seiten der TU Darmstadt[45] heruntergeladen werden. In einer weiteren HbbTV-Analyse wurde nachgewiesen, dass eine Nutzermessung auch auf Radiokanälen, die über Satellit übertragen werden, möglich ist.[46] Diese wurde mit einer Erweiterung des oben genannten Systems ebenfalls unterdrückt.

In [47] wird gezeigt, wie eine neue Art der Zuschauermessung datenschutzfreundlich durchgeführt werden kann. Die derzeitigen Verfahren setzen voraus, dass eine Telefonleitung eine Verbindung zwischen Erfassungsunternehmen und Haushalt herstellt. Im vorgestellten Ansatz können auch Internetverbindungen genutzt werden, bei dem eine Zwischeninstanz zur Aggregation der Daten genutzt wird. Die Aggregation gibt nur etwa die Anzahl der Zuschauer über alle Haushalte und nicht Daten über einen speziellen Haushalt weiter. Das Verfahren hat den Vorteil, dass

42 Ghiglieri/Oswald/Tews (2013).
43 Ghiglieri/Tews (2014).
44 Ghiglieri/Tews (2014).
45 http://www.smarthome.sit.tu-darmstadt.de.
46 Ghiglieri (2014).
47 Ghiglieri (2015).

auch andere Geräte wie smarte Stereoanlagen gemessen werden können. Als zusätz. liche Besonderheit bekommt der Nutzer die Möglichkeit, die Daten einzusehen und eine Übertragung vollständig abzulehnen.

Der Datenschutz kann schon mit einer korrekten Anwendung einfacher Best Practice Regeln erhöht werden. So sollten immer verschlüsselte Verbindungen zur Datenübertragung genutzt werden. Weiterhin sollte eine Aktualisierungsstrategie für Smart TV Geräte etabliert werden. Sicherheits- und Datenschutzprobleme aufgrund veralteter oder fehlerhafter Software kann nur wirkungsvoll behoben werden, wenn die Aktualisierung der Fernsehgeräte schnell, sicher und ohne schwierige Handhabungen für die Nutzer durchgeführt werden können.[48] Heutige Smart TV-Geräte erfordern teilweise die Aktualisierung per USB-Stick mit vorherigem Herunterladen von Software aus dem Internet. Auch hier gibt es gute Beispiele, wie es in aktuellen Browsern mit stillen Aktualisierungen nicht zu veralteter Software kommen kann.[49]

In Zukunft sind Systeme notwendig, die etwa wie handelsübliche Router Standard in jedem Haushalt werden. Sie müssen den Datenstrom überwachen und nach gewissen Regeln ungewollte Verbindungen ignorieren und den Nutzer dadurch schützen. Handelsübliche Router können nach heutigem Stand für solche Zwecke nicht eingesetzt werden, da die Hardware im Allgemeinen nicht leistungsfähig genug ist. Die Benutzerfreundlichkeit wird bei diesen Lösungen eine besondere Rolle spielen.

8. Fazit

Trotz einer starken Zunahme internetfähiger Fernsehgeräte bestehen nur unzureichende Sicherheitsmaßnahmen, um Geräte oder sensible Nutzerdaten zu schützen. Gefahren ergeben sich durch Angriffe auf das Fernsehgerät selbst, auf Sensoren wie Kamera und Mikrofon oder eine Kompromittierung der Software. Zudem sind Angriffe auf sensible Nutzerdaten mittels Tracking oder Abhören der Kommunikationskanäle möglich. Die übermittelten Daten erlauben weitgehende Rückschlüsse auf das Nutzerverhalten und spezifische Gewohnheiten. Durch Tracking können gezielt Nutzerprofile erstellt werden, ohne dass dies für die Nutzer transparent oder zu verhindern wäre. Derzeit bestehen keine ausreichenden Schutzmöglichkeiten. Eine konsequente Umsetzung des Prinzips der Datensparsamkeit und transparenter Datenübermittlung könnte Nutzern die heute nicht gewährleistete Entscheidungsautonomie über ihre übermittelten Daten zurückgeben. Ferner könnte die Verwendung kryptographischer Methoden der Verschlüsselung die Kommunikationskanäle schützen. Ein umfassender Schutz ist jedoch nur möglich, wenn die Übermittlung von Nutzerdaten durch einen Privacy Protector überwacht wird. In Zukunft ist die flächendeckende Verwendung solcher Systeme notwendig, die den Datenstrom überwachen und die Nutzer vor unerwünschter Datenübermittlung schützen. Eine zentrale Rolle wird dabei die Benutzerfreundlichkeit spielen, die für eine flächendeckende Verwendung entscheidend ist.

48 Ghiglieri (2014-a); Michéle/Karpow (2014).
49 Ragan, S. (2009).

Danksagung: Diese Arbeit wurde vom Bundesministerium für Bildung und Forschung (ECSPRIDE, Forum Privatheit) und von der Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz des Landes Hessen (CASED) unterstützt. Darüber hinaus möchten wir uns bei den anonymen Gutachtern bedanken, die wesentlich dazu beigetragen haben, diesen Beitrag zu verbessern.

Literaturverzeichnis

Statista (2010): *Wie wird sich der Markt für Smart Home bis 2020 entwickeln?* Online: http://de.statista.com/statistik/daten/studie/183271/umfrage/prognose-zur-entwicklung-von-smart-home-aus-sicht-der-hersteller, Zugriff am 16.11.2014.

Pricewaterhousecoopers (2013): *Media Trend Outlook. SmartTV: Mehrwert für den Konsumenten, mehr Umsatz für die Medienbranche,* Online: http://www.pwc.de/de/technologie-medien-und-telekommunikation/assets/white-paper-SmartTV.pdf.

Statista (2011): *Anzahl der Smart TV-Haushalte in Deutschland im Jahr 2010 und Prognose bis 2016 (in Millionen),* Online: http://de.statista.com/statistik/daten/studie/208236/umfrage/prognose-zur-entwicklung-der-SmartTV-haushalte-in-deutschland, Zugriff am 16.11.2014.

Sattler, C. (2011): *Smart TV: Wer erringt die Portalhoheit auf dem Fernseher?,* Goldmedia Innovation GmbH, Düsseldorf.

Statista (2011)b: *Prognose zur Anzahl der Haushalte mit mindestens einem an das Internet angeschlossenen HbbTV-Gerät von 2011 bis 2016 (in Millionen),* Online: http://de.statista.com/statistik/daten/studie/271953/umfrage/prognose-zur-entwicklung-der-hbbtv-haushalte-in-deutschland, Zugriff am 16.11.2014.

Emarketer (2013): *Connected TVs Reach One in Four Homes,* Online: http://www.emarketer.com/Article/Connected-TVs-Reach-One-Four-Homes/1009581, Zugriff am 16.11.2014.

StrategyAnalytics (2014): *2013 Smart TV Shipments Grew 55 Percent,* Online: https://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5472, Zugriff am 16.11.2014.

ETSI (2012): *ETSI TS 102 796 V1.2.1 (2012-11),* Online: http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.02.01_60/ts_102796v010201p.pdf, Zugriff am 16.11.2014.

Deutsche TV Plattform (2014): *Deutsche TV Plattform,* Online: http://www.tv-plattform.de/images/stories/pdf/marktanalyse_SmartTV_2014_de.pdf. Zugriff am 17.11.2014BLM (2012): *HbbTV beinhaltet Chancen für Lokalfernsehen - SmartTV-Anwendungen können Reichweiten und Umsätze lokaler TV-Anbieter erhöhen,* Online: http://www.blm.de/de/infothek/pressemitteilungen/2012.cfm?object_ID=436, Zugriff am 16.11.2014.

hbbtv-infos.de (2014): *HbbTV® Infoportal,* hbbtv-infos.de, Online: http://www.hbbtv-infos.de, Zugriff am 16.11.2014.

Kuri, J. (2013): *CE Week: Der Kampf um den Second Screen,* in: heise online, Online: http://www.heise.de/newsticker/meldung/CE-Week-Der-Kampf-um-den-Second-Screen-1902324.html, Zugriff am 16.11.2014.

IRT GmbH (2014): *HbbTV mit Second-Screen-Funktion,* IRT Online: http://www.irt.de/no_cache/de/aktuell/news/view/article/hbbtv-with-second-screen-function.html, Zugriff am 16.11.2014.

Auriemma, Luigi (2012): *Samsung devices with support for remote controllers,* Online: http://aluigi.altervista.org/adv/samsux_1-adv.txt, Zugriff am 16.11.2014.

SeungJin, L./Kim, S. (2013): *Smart tv security – #1984 in 21st century,* in CanSecWest, Online: http://cansecwest.com/slides/2013/SmartTV Security.pdf .

Ghiglieri, M. (2014): *Incorrect HTTPS Certificate Validation in Samsung Smart TVs,* Technische Universität Darmstadt, Darmstadt.

Michéle, B./Karpow, A. (2014): *Watch and be Watched: Compromising All Smart TV Generations,* in: 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA.

Grattafiori, A./Yavor, J. (2013): *The Outer Limits: Hacking the Samsung Smart TV,* in: Black Hat US, Las Vegas, NV, USA.

Ghiglieri, M./Oswald, F./Tews, E. (2013): *HbbTV – I Know What You Are Watching,* in: 13. Deutschen IT-Sicherheitskongresses, Bonn.

Ghiglieri, M./Oswald, F./Tews, E. (2013): *HbbTV: Neue Funktionen mit möglichen Nebenwirkungen,* in: FKT - Die Fachzeitschrift für Fernsehen, Film und elektronische Medien, pp. 563-566.

Ghiglieri, M./Tews E. (2014): *A Privacy Protection System for HbbTV in Smart TVs,* in: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA.

Oren,Y./Keromytis, A. D. (2014): *From the Aether to the Ethernet – Attacking the Internet using Broadcast Digital Television,* in: USENIX Security 14, San Diego, CA, USA.

Borgmann, M./Hahn, T./Herfert, M./Kunz, T./Richter, M./Viebeg, U./Vowé, S. (2012): *On the Security of Cloud Storage Services,* in: Technical report SIT-TR-2012-001, Darmstadt.

CSA (2013): *The Notorious Nine: Cloud Computing Top Threats in 2013,* in: CloudSecurityAlliance. Online: https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013, Zugriff am 16.11.2014.

Zeit Online (2013): *Daten von zwei Millionen Vodafone-Kunden kopiert,* in: Die Zeit, Online: http://www.zeit.de/digital/2013-09/vodafone-daten-diebstahl, Zugriff am 16.11.2014.

Bugiel, S./Nürnberger, S./Pöppelmann, T./Sadeghi, A./Schneider, T. (2011): *AmazonIA: When Elasticity Snaps Back,* in: ACM CCS, Chicago, IL, USA.

Buchmann, J. (Hrsg.) (2012): *Internet Privacy: Eine multidisziplinäre Bestandsaufnahme/ A multidisciplinary analysis,* in: Springer (acatech Studie), Heidelberg/Berlin.

Yeong Gon, K. et al (2012): *Multimodal Biometric Systems and Its Application in Smart TV, in Computer Applications for Database, Education, and Ubiquitous Computing,* in: Springer. 219-226., Berlin/Heidelberg.

Lendino, J. (2014): *Panasonic Unveils Voice-Activated TVs With Facial Recognition,* Online: http://www.pcmag.com/article2/0,2817,2429165,00.asp., Zugriff am 16.11.2014Ghiglieri, M. (2014): *I Know What You Watched Last Sunday – A New Survey Of Privacy In HbbTV*, in: Workshop Web 2.0 Security & Privacy 2014 in conjunction with the IEEE Symposium on Security and Privacy, San Jose, CA, USA.

Ghiglieri, M./Oswald, F./Tews, E.: *HbbTV – I Know What You Are Watching,* in: 13. Deutscher IT-Sicherheitskongress des BSI.

DoctorBeet's Blog, (2013): *LG Smart TVs logging USB filenames and viewing info to LG servers,* Online: http://doctorbeet.blogspot.co.uk/2013/11/lg-SmartTVs-logging-usb-filenames-and.html.

DoctorBeet's Blog, (2014): *LG Disables Smart TV features in the EU to force users to accept new oppressive Privacy Policy,* Online: http://doctorbeet.blogspot.de/2014/05/lg-disables-SmartTV-features-in-eu-to.html.

Ghiglieri, M. (2015): *PriMSED - Privacy-Friendly Measurement of Smart Entertainment Devices,* in: 2015 IEEE 12th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA.

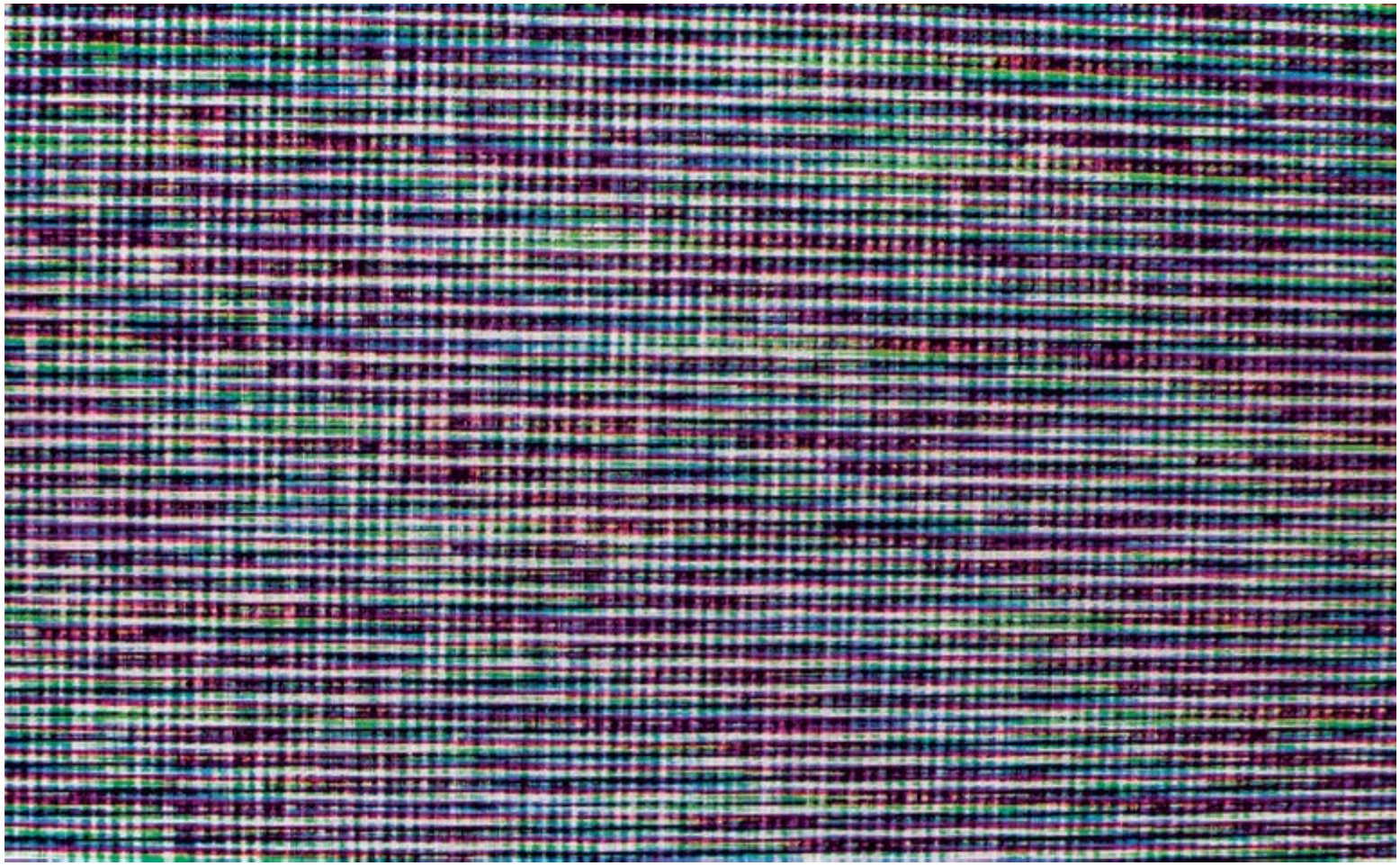
Ragan, S. (2009): *Report: Using silent updates boosts browser security,* Online: http://www.thetechherald.com/articles/Report-Using-silent-updates-boosts-browser-security/5714/., Zugriff am 16.11.2014KVJS-Fachtagung (2012): *My Smart Home is my Castle - Wohnqualität durch benutzerfreundliche Technik,* Online: http://www.bundesanzeiger-verlag.de/betreuung/aktuelles/aktuelle-meldungen/newsdetails/artikel/my-smart-home-is-my-castle-wohnqualitaet-durch-benutzerfreundliche-technik-6789.html., Zugriff am 16.11.2014Wojtczuk, R./Beulich, J. (2012): *Advanced Exploitation of Xen Hypervisor Sysret VM Escape Vulnerability,* 4.9.2012.

Kortchinsky, K. (2009): *Cloudburst – A VMware Guest to Host Escape Story,* in: BlackHat USA.

Elhage, N. (2011): *Virtunoid: A KVM Guest - Host privilege escalation exploit,* in: Black Hat USA.

heise online, *Internet of Things: Mein Kühlschrank als Spammer,* in: heise online, 17. 11. 2014 Online: http://heise.de/-2088336, Zugriff am 17.11.2014.

II. Regulierung der Digitalen Revolution?



PETER SCHAAR

Lässt sich die globale Überwachung einhegen?

Der im Juni 2013 nach Edward Snowdens Enthüllung der gigantischen Abhörung durch die US-amerikanische NSA und das britische GCHQ zu vernehmende globale Aufschrei ist mehr als ein Jahr nach Beginn der Veröffentlichungen weitgehend abgeklungen. Trotzdem – oder gerade deshalb – drängt sich die Frage auf, ob es überhaupt wirksame Mittel gegen die lückenlose Registrierung und Überwachung durch Geheimdienste gibt.

Eines ist jedenfalls klar: Ein Zurück in die analoge Zeit vor dem Internet wird es nicht geben. Wenn wir auf die Segnungen der Informationstechnologie nicht verzichten wollen, werden wir uns damit arrangieren müssen, dass in erheblichem Umfang Daten verarbeitet werden. Illusorisch wäre auch die Hoffnung, die staatlichen Überwachungsaktivitäten auf Null zurückzufahren zu können. Und trotzdem wäre es falsch, den Kopf in den Sand zu stecken und einfach der Dinge zu harren, die da noch kommen mögen. Es gibt durchaus einige Ansätze, die uns helfen können, die Überwachungsschraube zurück zu drehen und unsere Privatsphäre auch in der digitalen Welt besser zu schützen – auf rechtlicher wie auf politischer Ebene.

1. Recht im globalen Raum: Fehlanzeige?

Gesetze entfalten ihre Schutzwirkung grundsätzlich im jeweiligen territorial definierten Geltungsbereich. Im Internet spielen dagegen Landes- oder auch Kontinentalgrenzen technisch keine Rolle. Die Abfrage eines deutschen Internetnutzers, der die Webseite eines deutschen Anbieters aufruft, kann viele Umwege nehmen, auch über amerikanische Netzknoten. Globale Internetunternehmen speichern Daten auf weltweit verteilten Servern. Deshalb ist es unzureichend, stets nur auf die Einhaltung des eigenen, heimischen Rechts zu pochen. Vertreter der amerikanischen und der britischen Regierung hatten offenbar kein Problem mit der Überwachung, soweit ihre Nachrichtendienste beteuerten, sich an – das eigene – Recht und Gesetz zu halten. Diese Versicherung hilft deutschen oder brasilianischen Internetnutzern aber wenig, wenn sie Opfer der Überwachung waren und weiterhin sind. Der Hinweis auf die angebliche Gesetzeskonformität gegenüber dem heimischen Recht blendet die in den letzten hundert Jahren entwickelten Rechtsprinzipien des Völkerrechts weitgehend aus, die gerade nicht mehr territorial beschränkt sind. Auch wenn dabei, etwa in der Allgemeinen Erklärung der Menschenrechte von 1948, Fragen des Umgangs mit Informationen historisch bedingt nicht im Mittelpunkt standen, bieten sie Ansatzpunkte für die Zivilisierung der heutigen, zunehmend globalisierten Informationsgesellschaft.

Hinzu kommt: Gerade bei der Auslandsaufklärung wird systematisch gegen Rechtsvorschriften im Operationsgebiet verstoßen. Selbst wenn sich die NSA an US-Recht hält und der GCHQ britische Gesetze beachtet, können sie durchaus ausländisches – etwa deutsches – Recht brechen. Und sie haben dies in der Tat getan:

Wenn etwa ein ausländischer Geheimdienstcomputer deutsche Nutzer mittels Trojaner infiltriert und überwacht, erfüllt dies den (deutschen) Straftatbestand des Ausspähens von Daten. Auch Geheimdienste, die mittels Telekommunikation übertragene nichtöffentliche Daten deutscher Teilnehmer unter Anwendung von technischen Mitteln abfangen oder sich aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschaffen, begehen eine Straftat. Und auch die Tatsache, dass Spionage nicht gegen Völkerrecht verstößt, stellt Spione keineswegs straffrei, wie das Verbot geheimdienstlicher Agententätigkeit für eine fremde Macht verdeutlicht.

2. Menschenrecht auf Privatheit

Das rechtliche Territorialdilemma lässt sich nur überwinden, wenn endlich wirksame, durchsetzbare Instrumente die Menschenrechte mit Leben füllen. Dies gilt auch und insbesondere für den Datenschutz. Schon seit Jahren fordern daher Datenschützer internationale Standards zum Schutz der Privatsphäre – bislang allerdings ohne durchschlagenden Erfolg. Seit dem Bekanntwerden der umfassenden Überwachungsaktivitäten der amerikanischen NSA und des britischen GCHQ ist aber Bewegung in die internationale Diskussion gekommen.

Die auf Snowden zurückgehenden Berichte riefen einer breiteren Öffentlichkeit wieder in Erinnerung, dass es sich bei dem Datenschutz um ein Menschenrecht handelt. In Artikel 12 der Allgemeinen Erklärung der Menschenrechte von 1948 stellte die Völkergemeinschaft fest: «Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.»

Bereits seit den 1960er Jahren befassen sich die Vereinten Nationen intensiver mit den Konsequenzen der automatisierten Datenverarbeitung. Durch Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte von 1966 wurde der Schutz der Privatsphäre zum verbindlichen Völkerrecht. Die Staaten, die diesen «Zivilrechtspakt» ratifiziert haben, verpflichteten sich damit, diese Rechte zu achten und sie allen in ihrem «Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen ohne Unterschied wie insbesondere der Rasse, der Hautfarbe, des Geschlechts, der Sprache, der Religion, der politischen oder sonstigen Anschauung, der nationalen oder sozialen Herkunft, des Vermögens, der Geburt oder des sonstigen Status zu gewährleisten.»

Im Jahr 1990 beschloss die UN-Generalversammlung Empfehlungen über den Umgang mit personenbezogenen Daten in automatisierten Dateien. Es blieb allerdings den Mitgliedstaaten überlassen, hierzu verbindliche Bestimmungen festzulegen. Insofern hätte es eigentlich außer Frage stehen müssen, dass zumindest die 167 Staaten, die den Zivilrechtspakt ratifiziert haben, darunter alle EU-Mitgliedsländer, die Vereinigten Staaten und die Russische Föderation – nicht jedoch die Volksrepublik China –, sich an die in Artikel 12 der UN-Menschenrechtscharta formulierten Vorgaben gebunden fühlen. Abhilfe könnte ein Zusatzprotokoll zum Artikel 17 des UNO-Paktes für bürgerliche und politische Rechte schaffen. Um ein solches verbindliches völkerrechtliches Protokoll in Kraft zu setzen, genügt die Unterstützung von 20 Staaten – angesichts der 27 EU-Mitgliedstaaten müsste dies

doch zu schaffen sein. Staaten, die sich nicht dazu bekennen, müssten nachweisen, wie sie trotzdem Datenschutz, Privatsphäre und Fernmeldegeheimnis garantieren.

Nachdem es zunächst so aussah, als würde eine entsprechende Initiative der Bundesregierung auf breite europäische und internationale Unterstützung treffen, ruderten jedoch in den folgenden Wochen und Monaten einige der Regierungen zurück, die zunächst ihre Zustimmung signalisiert hatten. Als sich abzeichnete, dass ein derartiges Zusatzprotokoll zum UN-Zivilrechtspakt nur geringe Durchsetzungschancen hatte (und zudem auch im günstigsten Fall eine eher langfristige Angelegenheit wäre), schlugen die Bundesregierung und die brasilianische Regierung, die ebenfalls massiv durch die NSA ausspioniert worden war, einen Resolutionsentwurf der Vollversammlung der Vereinten Nationen vor. Im Mittelpunkt des Erschließungsentwurfs stand die Forderung, das Menschenrecht auf Privatsphäre unabhängig vom Territorialprinzip auch außerhalb der eigenen Landesgrenzen zu wahren.

Dagegen wandten sich Vertreter der Vereinigten Staaten. In einem der Zeitschrift «Foreign Policy» zugespielten Verhandlungspapier der US-Delegation wird großer Wert darauf gelegt, dass nicht jede Überwachung zu verurteilen sei, sondern nur solche, die «gegen Gesetze verstößt». Da sich die USA und Großbritannien – wie auch andere Regierungen – allerdings immer wieder nur auf die eigenen Gesetze beziehen, wäre die Entschließung so zu einem Muster ohne Wert geworden. Auf Grund dieser massiven Intervention wurde die Resolution schließlich teilweise entschärft. So sei die Einbeziehung «extraterritorialer» Spähaktionen – also von einem Staat in den anderen – «ein schwieriger Punkt» gewesen. Immerhin blieb die Aussage, die Überwachung müsse global und nicht nur durch nationales Recht begrenzt werden, Teil der Entschließung. Allerdings ist jetzt nicht mehr von Überwachung generell die Rede, sondern nur noch von «ungesetzlicher Überwachung» und deren «negativem Einfluss». Trotzdem enthält die von der Generalversammlung angenommene Resolution «Das Recht auf Privatheit im digitalen Zeitalter» die deutliche Botschaft: Der Schutz der Privatsphäre ist ein internationales Menschenrecht, das auch und gerade im Zeitalter der globalen Kommunikation weltweit garantiert werden muss. Die Staaten müssen «die vollständige Einhaltung ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen» sicherstellen und Maßnahmen «ergreifen, um Verletzungen dieser Rechte ein Ende zu setzen und die Bedingungen dafür zu schaffen, derartige Verletzungen zu verhindern»

Vielleicht am bedeutsamsten ist, dass das Thema Überwachung nach dem Beschluss der Vollversammlung auf der Tagesordnung der UN-Gremien bleiben soll. So soll die UN-Menschenrechtskommissarin dem Menschenrechtsrat und der Generalversammlung einen «Bericht über den Schutz und die Förderung des Rechts auf Privatheit im Kontext des innerstaatlichen und extraterritorialen Überwachens und/oder Abfangens von digitaler Kommunikation und Sammelns personenbezogener Daten, namentlich in massivem Umfang, samt Auffassungen und Empfehlungen» vorlegen, heißt es in der Resolution.

3. Europäisches Datenschutzrecht: Firewall gegen Überwachung?

Doch so wichtig die einhellige Meinungsbekundung der UN-Mitgliedsstaaten ist – sie reicht bei weitem nicht aus. Notwendig sind vielmehr verbindliche völkerrechtliche Regelungen, die den globalen Überwachungsaktivitäten einen Riegel vorschieben. Selbst wenn die USA, Russland und China, die sich in der globalen Überwachung besonders hervortun, im Bündnis mit autoritären Regimes versuchen, die Verabschiedung international durchsetzbarer Datenschutzstandards zu verhindern, darf sich insbesondere Europa hiermit nicht zufrieden geben.

Auch wenn die modernen Vorstellungen über den Schutz der Privatsphäre zunächst überwiegend in den USA entwickelt wurden, sind sie doch heute in weiten Teilen Europas weitaus stärker verankert als dort. Nicht zu übersehen sind allerdings die großen Differenzen zwischen den europäischen Staaten. Nicht erst der Umgang der britischen Öffentlichkeit mit den Enthüllungen Snowdens belegt, dass staatliche Überwachung in Großbritannien auf weitaus größere Akzeptanz trifft als in Deutschland. So stößt etwa die nahezu flächendeckende Videoüberwachung im städtischen Bereich in Großbritannien kaum auf öffentliche Kritik, während entsprechende Maßnahmen in Deutschland heiß diskutiert werden. Trotz dieser Unterschiede bieten die europäischen Datenschutztraditionen und die in den letzten Jahrzehnten formulierten europäischen Datenschutzstandards und -gesetze durchaus Ansatzpunkte für die Begrenzung der Überwachung. Mit der Europäischen Menschenrechtskonvention von 1953 und mit der Konvention zum Datenschutz von 1981 (Konvention 108) hat der Europarat bereits sehr frühzeitig – und lange vor der Europäischen Union – Maßstäbe zur Gewährleistung der Grundrechte und des Datenschutzes gesetzt.

Anknüpfend an die Allgemeine Erklärung der Menschenrechte der Vereinten Nationen bekennt sich die Menschenrechtskonvention des Europarats zur universellen und wirksamen Anerkennung und Einhaltung dieser Rechte. Und wie diese gesteht Artikel 8 der Menschenrechtskonvention jeder Person das Recht «auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz» zu. Im Unterschied zur Allgemeinen Erklärung der Menschenrechte ist die Europaratskonvention für alle Unterzeichnerstaaten verbindlich. Zwar verpflichten sich die Vertragsparteien explizit nur dazu, die Rechte «allen ihrer Hoheitsgewalt unterstehenden Personen» zuzugestehen. Durch ihren universellen Anspruch sind die Vorgaben der Menschenrechtskonvention jedoch auch im Rechtsverkehr der Staaten untereinander verbindlich und gelten damit auch für Aktivitäten staatlicher Stellen außerhalb des eigenen Territoriums.

Den vom zunehmenden internationalen Datenaustausch ausgehenden Gefährdungen trägt die Datenschutzkonvention des Europarats Rechnung. Für viele Staaten innerhalb und außerhalb Europas war sie die Blaupause für ihr nationales Datenschutzrecht. In ihrer Präambel heißt es, «dass es angesichts des zunehmenden grenzüberschreitenden Verkehrs automatisch verarbeiteter personenbezogener Daten wünschenswert ist, den Schutz der Rechte und Grundfreiheiten jedes Menschen, vor allem das Recht auf Achtung des Persönlichkeitsbereichs, zu erweitern.» Artikel 8 der EU-Grundrechtecharta enthält zudem – anders als das deutsche Grundgesetz – ein explizites Grundrecht auf Datenschutz: «(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten

dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.» Als Teil des am 1. November 2009 in Kraft getretenen Vertrags von Lissabon ist die Grundrechtecharta direkt anwendbares europäisches Recht. Damit ist der Datenschutz in Europa rechtlich erheblich tiefer verankert als etwa in den USA oder im asiatisch-pazifischen Raum.

4. Überwachung auch im «sicheren Hafen»?

Eine entscheidende Rolle spielt die 1995 in Kraft getretene EU-Datenschutzrichtlinie. Sie verpflichtet die Mitgliedstaaten zur Gewährleistung eines hohen Datenschutzniveaus. In allen Mitgliedstaaten sind die Vorgaben der Richtlinie durch nationale Rechtsvorschriften umgesetzt worden, etwa in Deutschland durch das Bundesdatenschutzgesetz. Wie wichtig die EU-Datenschutzrichtlinie ist, belegt die jüngste Entscheidung des Europäischen Gerichtshofs in Luxemburg zu Google. Demnach kann der Suchmaschinenbetreiber dazu verpflichtet werden, Verweise auf Webseiten mit sensiblen persönlichen Daten aus seiner Ergebnisliste zu streichen. Ein solches Recht leitet sich nach Ansicht des Gerichts aus der EU-Datenschutzrichtlinie ab. Demnach ist der Suchmaschinenbetreiber für die Verarbeitung der Daten verantwortlich – und damit auch für die Änderung der Suchergebnisse auf Bitte der Betroffenen.

Die Datenschutzrichtlinie legt fest, dass der Datenexport grundsätzlich nur dann zulässig ist, wenn im Empfängerland ein «angemessenes Datenschutzniveau» gewährleistet wird. Über die Angemessenheit des Schutzniveaus in einem Drittstaat entscheidet die Europäische Kommission. So hat die Kommission die Angemessenheit des Schutzniveaus für jene Unternehmen festgestellt, die sich den mit der US-Regierung ausgehandelten Safe-Harbor-Prinzipien unterwerfen. Zuvor hatte die EU jahrelang mit den USA darüber verhandelt, wie die in die Vereinigten Staaten exportierten personenbezogenen Daten angemessen geschützt werden können. Die US-Regierung weigerte sich standhaft, mit dem europäischen Recht vergleichbare Datenschutzgesetze mit verbindlichen Vorgaben für US-Unternehmen auf den Weg zu bringen. Um gleichwohl den Datenexport in die USA zu erleichtern, einigte sich die EU-Kommission mit der US-Regierung im Jahr 2000 auf das Safe-Harbor-Abkommen. Dessen Grundidee besteht darin, dass auch ohne ein allgemein gültiges US-Datenschutzgesetz ein angemessener Schutz der europäischen Daten für die Verarbeitung durch diejenigen Unternehmen angenommen wird, die sich zur Einhaltung der vereinbarten Prinzipien verpflichten. Die US-Regierung sagte im Gegenzug zu, die Prinzipien bei den Unternehmen durchzusetzen. Die dem sicheren Hafen beigetretenen Unternehmen werden von den europäischen Datenschutzbehörden ähnlich wie Firmen behandelt, die personenbezogene Daten in Europa verarbeiten. So müssen europäische Unternehmen keine Genehmigungen bei den europäischen Datenschutzbehörden einholen, wenn sie Daten an Safe-Harbor-Mitglieder übermitteln wollen. Inzwischen ist Safe Harbor das wichtigste Instrument für den

Transfer personenbezogener Daten in die USA – z. Zt. sind mehr als 4400 Firmen dem sicheren Hafen beigetreten, darunter alle großen US-Internetunternehmen.

Allerdings haben die europäischen Datenschutzbeauftragten von Beginn an kritisiert, dass die Safe-Harbor-Prinzipien deutlich hinter den Ansprüchen des europäischen Datenschutzrechts zurückbleiben. Ein weiterer Kritikpunkt richtet sich dagegen, dass die Unternehmen schon dann die Vorteile des Safe-Harbor-Systems genießen, wenn sie den Beitritt zum «sicheren Hafen» erklärt haben. So bedarf im allgemeinen die Datenübermittlung aus Europa an ein Safe-Harbor-Mitglied keiner Genehmigung durch die zuständige Datenschutzaufsichtsbehörde. Die Unternehmen sind nicht verpflichtet, bereits vor ihrer Aufnahme in die Safe-Harbor-Liste nachzuweisen, dass sie die Anforderungen erfüllen. Zudem können sie sich aussuchen, welche Stelle kontrolliert, ob sie die Bedingungen einhalten. Soweit bekannt, haben sich sämtliche Safe-Harbor-Unternehmen der Aufsicht durch Federal Trade Commission (FTC) unterworfen und kein Einziges der Aufsicht einer europäischen Datenschutzbehörde. Nach den Veröffentlichungen über die NSA-Aktivitäten ist ein weiterer Kritikpunkt in den Mittelpunkt gerückt: Das Safe-Harbor-Abkommen nimmt die Verarbeitung von Daten zu Zwecken der «nationalen Sicherheit» explizit aus. Auf diese Ausnahme berufen sich sowohl die US-Behörden als auch jene Unternehmen, deren umfangreiche Datenweitergabe an die NSA jetzt kritisiert wird – wie etwa Google, Microsoft, Amazon, Apple und Yahoo.

Eigentlich müssten sich US-Sicherheitsbehörden, die etwa gegen einen Terrorverdächtigen ermitteln, im Wege der internationalen Rechtshilfe an die EU-Staaten wenden, wenn sie Daten aus Europa erhalten wollen. Vor der Übermittlung würde dann von den zuständigen europäischen Behörden – in Deutschland: vom Bundesjustizministerium – geprüft, ob die Voraussetzungen für die Datenübermittlung vorliegen. Dieses rechtsstaatlich einwandfreie, aber aufwändige Verfahren wird unterlaufen, wenn die europäischen Daten quasi automatisch, ohne weitere Prüfung, auf Basis von Safe Harbor an ein US-Unternehmen übermittelt werden und von diesem an US-Geheimdienste gelangen. In Europa wächst deshalb der Druck, das Safe-Harbor-Abkommen zu kündigen. So hat sich etwa das europäische Parlament dafür ausgesprochen, das Abkommen neu zu verhandeln. Das Europäische Parlament verlangt seine Aussetzung, und Datenschutzbehörden haben erklärt, das Safe-Harbor-Abkommen nicht mehr als Rechtsgrundlage für die Datenübermittlung in die USA zu akzeptieren.

Bei einem Nachfolgeabkommen zu Safe Harbor wird es entscheidend darauf ankommen, dass – anders als bisher – staatliche Zugriffe auf Daten umfasst werden, die dem europäischen Datenschutzrecht unterliegen oder die aus Europa in die USA übermittelt wurden. Es darf nicht länger hingenommen werden, dass US-Behörden ohne angemessene rechtsstaatliche Sicherungen auf aus Europa stammende Daten zugreifen, diese kopieren und zu Profilen zusammenführen. Eine generelle Ausnahme für die Verarbeitung der Daten zu Zwecken der «nationalen Sicherheit» kann nicht akzeptiert werden.

5. Rechtliche «Daumenschrauben» im EU-Datenschutzrecht

Welche Rolle Europa bei der Durchsetzung internationaler Datenschutzstandards spielt, wird sich auch an dem Schicksal der EU-Datenschutzreform messen lassen. Dabei geht es zum einen um die weitere Harmonisierung der Datenschutzregeln in den EU-Mitgliedstaaten und eine bessere Kooperation der Datenschutzbehörden. Mindestens genauso wichtig ist allerdings eine eher unscheinbare Änderung bezüglich des Anwendungsbereichs des EU-Datenschutzrechts: Bisher können sich Unternehmen wie Google dem europäischen Recht weitgehend dadurch entziehen, dass sie ihre Dienste aus den USA anbieten. In Zukunft würde diese Umgehungsstrategie nicht mehr klappen. Die EU-Kommission hat nämlich die Einführung eines «Marktortprinzips» vorgeschlagen. Danach soll das EU-Datenschutzrecht immer schon dann anwendbar sein, wenn Unternehmen Dienstleistungen oder Waren auf dem europäischen Markt anbieten und dabei in der Europäischen Union personenbezogene Daten erheben. Google und andere in Europa tätige US-Unternehmen müssten sich dann genauso an das europäische Recht halten wie die hier ansässigen Firmen. Die jüngste Google-Entscheidung des Europäischen Gerichtshofs in Luxemburg hat diesem Prinzip Rechnung getragen.

Um der maßlosen Überwachung durch ausländische Behörden entgegenzuwirken, hat das europäische Parlament darüber hinaus die Aufnahme einer weiteren «Daumenschraube» in das EU-Datenschutzrecht vorgeschlagen: In Fällen, in denen Behörden oder Gerichte aus Drittstaaten den Zugriff auf Daten anordnen, die dem europäischen Datenschutzrecht unterliegen, benötigen die betroffenen Unternehmen eine Genehmigung der jeweiligen europäischen Datenschutzbehörde. «Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung (der Daten) Verantwortlichen oder Auftragsverarbeiter verlangen, personenbezogene Daten weiterzugeben, dürfen weder anerkannt noch in irgendeiner Weise vollstreckt» werden, so der Vorschlag des Europäischen Parlaments.

Die neue Vorschrift würde etwa zur Anwendung kommen, wenn das FBI oder die NSA die Herausgabe von in der Google- oder Microsoft-Cloud gespeicherten Daten anordnen. Die von derartigen Datenanforderungen betroffenen Unternehmen sollen verpflichtet werden, dies der in der EU zuständigen Datenschutzaufsichtsbehörde zu melden. Sie dürften die Daten nur dann an US-Behörden herausgeben, wenn die Datenschutzbehörde feststellt, dass die Herausgabe auch nach europäischem oder internationalem Recht zulässig ist. Zudem müssten die Betroffenen sowohl über die Anfrage als auch über die Autorisierung durch die Datenschutzbehörde informiert werden. Die Teilnahme an geheimen Überwachungsprogrammen wäre damit unzulässig.

Sollte die EU allerdings eine derartige Regelung beschließen, wäre ein Konflikt mit den USA vorprogrammiert: Nach US-Recht sind die Unternehmen zu strikter Geheimhaltung bezüglich der Datenherausgabe an Sicherheitsbehörden verpflichtet. Bisher ist es ihnen sogar untersagt, auch nur die Tatsache zu offenbaren, dass es entsprechende Anfragen – etwa der NSA oder des FBI – überhaupt gibt. Ob und wie dieser Konflikt aufgelöst werden kann, ist derzeit nicht abzusehen. Würde Europa allerdings aus wirtschaftlichen Gründen oder wegen des sich aufbauenden politischen Drucks der US-Regierung auf die Durchsetzung seiner datenschutz-

rechtlichen Standards verzichten, wäre der damit einhergehende Vertrauensverlust kaum zu kompensieren. Von großer Bedeutung wird auch sein, wie die Europäische Kommission die Verhandlungen mit der US-Regierung über das transatlantische Freihandelsabkommen TTIP fortführen wird. Es besteht die Gefahr, dass ein solches Abkommen den europäischen Datenschutz erheblich schwächt.

Aus diesem Grund ist auch ein allgemeines Datenschutzabkommen zwischen der EU und den USA dringend erforderlich. Dieses muss garantieren, dass die EU-Bürger in den USA effektive Rechtsschutzmöglichkeiten gegen das Handeln staatlicher Stellen bekommen. Bisher weigert sich die US-Regierung, EU-Bürgern solche Datenschutzgarantien zu geben, auf die sich US-Bürger in Europa selbstverständlich berufen können. Daran hat sich seit Beginn der NSA-Affäre nichts geändert – allen Bekundungen Präsident Obamas zum Trotz, die USA würden zukünftig auch die Rechte von Nicht-Amerikanern im Ausland respektieren. Auch müssen die USA garantieren, dass die auf amerikanischen Servern lagernden personenbezogenen Daten europäischer Provenienz denselben Schutzmechanismen gegen staatliche Zugriffe unterliegen wie die Daten, die aus den USA selbst stammen. Die schon seit Jahren wegen des hinhaltenden Widerstands der US-Seite ins Stocken geratenen Verhandlungen einer «High Level Contact Group» müssen endlich zu einem annehmbaren Abschluss gebracht werden. Ohne ein entsprechendes Ergebnis darf auch Safe Harbor nicht fortgeführt werden – massenhafte Verletzungen des in der Europäischen Grundrechtecharta garantierten Rechts auf Datenschutz darf die EU nicht in Kauf nehmen. Eine Lösung zeichnet sich bisher jedoch nicht ab, weil die US-Seite in all diesen zentralen Fragen nicht zu wesentlichen Zugeständnissen bereit war.

6. Freiheitsrechte, Zivilcourage und Technikgestaltung

Umso weniger kommt die Gesellschaft um die Frage herum, welchen anderen Ausweg aus der Überwachungsspirale es gibt. Von zentraler Bedeutung ist dabei die Frage, wie wir zukünftig mit Risiken umgehen. Kaum jemand wird der These widersprechen, eine hundertprozentige Sicherheit vor Lebensrisiken sei nicht zu erreichen. Gleichwohl strebt unsere postindustrielle Gesellschaft genau danach, wenn es um den Umgang mit Gewalt, Kriminalität und Terrorismus geht. Wenn daher Politiker wie George W. Bush oder auch die deutschen Innenminister Otto Schily, Wolfgang Schäuble und Hans-Peter Friedrich die Sicherheit zu einem Grundrecht oder gar «Super-Grundrecht» erklärten, handelten sie durchaus in Übereinstimmung mit einer Mehrheitserwartung.

Allerdings haben die Enthüllungen Edward Snowdens die öffentliche Wahrnehmung erheblich verändert. Erst jetzt ist deutlich geworden, wie stark nach dem Elften September Freiheitsrechte eingeschränkt wurden. David Lyon beschreibt das Dilemma zutreffend: «Die Macht hat sich in einen globalen, extraterritorialen Raum verzogen, während die Politik, die einst zwischen den Interessen des Einzelnen und der Gemeinschaft vermittelte, an feste Orte gebunden bleibt und nicht auf globaler Ebene zu agieren vermag. Ohne politische Kontrolle wird Macht jedoch zur Quelle großer Unsicherheit, während die Politik in Bezug auf die Probleme und Ängste vieler Menschen offenbar jede Bedeutung verliert.»[1]

1 Baumann/Lyon (2013): Daten, Drohnen, Disziplin, S. 16.

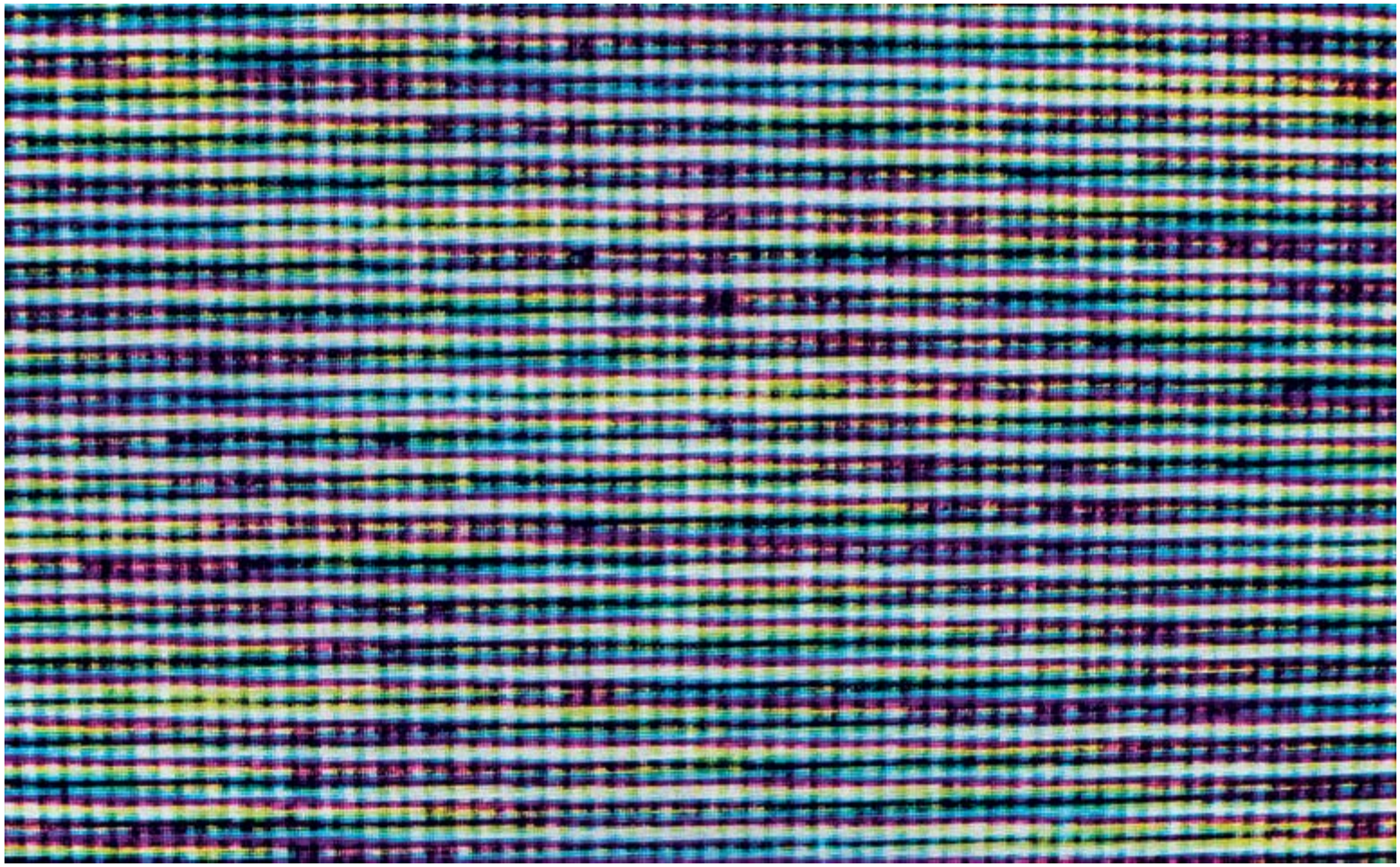
Zunächst ist es deshalb von entscheidender Bedeutung, auch für die geheimdienstlichen Aktivitäten zur Terrorabwehr für viel mehr Transparenz zu sorgen. Die Maßnahmen und Gesetze, die unsere Sicherheit verbessern sollten, gehören dringend auf den Prüfstand. Es kann einfach nicht länger hingenommen werden, dass Sicherheitspolitiker immer wieder behaupten, die umfassenden Überwachungsmaßnahmen hätten Terroranschläge verhindert, ohne dafür den Nachweis zu führen. Beweise für diese Behauptung sind sie nämlich – häufig unter Hinweis auf die Notwendigkeit zur Geheimhaltung – weitestgehend schuldig geblieben. Inzwischen haben Wissenschaftler und unabhängige Datenschutzbehörden den Umgang mit den gesammelten Daten überprüft. Das ernüchternde Ergebnis: Die massenhaften anlasslosen Datensammlungen haben so gut wie keine positiven Auswirkungen auf die Sicherheit gehabt. Wesentlich effektiver sind nach wie vor klassische gezielte Ermittlungen. Zwar können auch dabei Unschuldige ins Visier der Sicherheitsbehörden geraten, aber in sehr viel geringerem Umfang als bei der anlasslosen Massenüberwachung.

Fest steht aber auch: Die Umkehr zu einem verbesserten Schutz unserer Daten wird nicht von selbst kommen. Nur wenn die Überwachung und die von ihr ausgehenden Gefahren stärker ins Blickfeld der Öffentlichkeit und der politischen Debatte rücken, werden sich die Kräfte, die für immer neue Instrumente zur Registrierung und Steuerung unseres Verhaltens eintreten, zurückdrängen lassen. Das Ringen um den Datenschutz ist eine politische Auseinandersetzung. Das Recht steht nicht außerhalb der Gesellschaft, es ist vielmehr Resultat – und zugleich Triebfeder der Entwicklung. Die Verfassungsgerichtsentscheidungen zur Volkszählung, zur Rasterfahndung, zum großen Lauschangriff und zur Online-Durchsuchung sind das Ergebnis gesellschaftlichen Ringens um einen tragfähigen Interessenausgleich zwischen Freiheit und Sicherheit und nicht bloß Ausdruck gelehrter Rechtsexegese. Heute können wir beobachten, dass die Kräfte in der Zivilgesellschaft stärker werden, die die Überwachung nicht mehr als Schicksal hinzunehmen bereit sind. Und auch das hermetische System geheimer Überwachung, das seit 2001 errichtet wurde, zeigt die ersten Risse. Die auf Snowden zurück gehenden Veröffentlichungen haben die Fundamente dieses Gebäudes erschüttert. Seine Grundmauern allerdings stehen nach wie vor. Der Kampf dagegen bleibt also weiter unabdingbar.

Bei alledem darf derjenige nicht vergessen werden, dem wir die Kenntnis über die immensen Menschenrechtsverletzungen verdanken. Edward Snowden ist ein klassischer «Whistleblower», also jemand, der laut pfeift, weil er mit Rechtsbrüchen und unmoralischem Handeln konfrontiert ist. Dass er den Weg über China wählte und dann in Moskau «hängen blieb», tut seiner Leistung keinen Abbruch. Wenn die westlichen Demokratien ihren Ansprüchen und Grundwerten treu bleiben wollen, müssen sie ihm einen gesicherten Aufenthaltsstatus einräumen. Letztlich beweist sich nur am Umgang mit dem einzelnen Menschen, wie ernst es den Verantwortlichen mit den Grund- und Menschenrechten ist – und ob es sich dabei um einen echten Willen oder nur um papierne Bekenntnisse handelt.

Last but not least sollte nicht vergessen werden, dass auch die Technologie und ihr Einsatz keine völlig unbeeinflussbaren Faktoren sind. Konzepte wie «Privacy by Design», also der Berücksichtigung datenschutzrechtlicher Anforderungen bei der Entwicklung von Hard- und Software, zeigen Gestaltungsmöglichkeiten auf. Inwieweit sich solche Konzepte aber mit Leben füllen lassen oder sogar zum selbstver-

ständlichen Standard werden, hängt auch von den politischen und rechtlichen Rahmenbedingungen ab. Deshalb gehört die Technikgestaltung zu den zentralen Komponenten eines modernen Datenschutzrechts, wie es etwa derzeit in der EU diskutiert wird. Datenschutzfreundliche Techniken, mit denen sich personenbezogene Daten vermeiden, anonymisieren und minimieren lassen, könnten auch den Bogen zwischen der technikaffinen Internet-Community, Datenschützern und Bürgerrechtlern schlagen. Deren Anliegen sind zwar nicht deckungsgleich, aber sie überschneiden sich gerade angesichts der überbordenden Überwachung viel stärker, als den meisten Akteuren bewusst ist.



JAN PHILIPP ALBRECHT

EU-Datenschutzreform: Blockade made in Germany

Die Reform des Europäischen Datenschutzrechts wurde als wichtigster Schritt zu einem gemeinsamen digitalen Binnenmarkt und einer vertrauenswürdigen digitalen Wirtschaft und Gesellschaft gefeiert. Bundeskanzlerin Angela Merkel bezeichnete ihre Verabschiedung im Sommer 2013 als «höchste Priorität» und ließ sich dennoch auf Druck des britischen Regierungschefs David Cameron davon abbringen, diese vor der Europawahl 2014 zu verabschieden. Man einigte sich darauf, die Reform stattdessen bis 2015 unter Dach und Fach zu bringen. Doch im Ministerrat verzögerte ihre eigene Bundesregierung die Einigungsprozesse so lang, dass eine endgültige Verabschiedung noch im Jahr 2015 fraglich ist. Eine Verzögerung, die allen in der EU – den Verbraucherinnen und Verbrauchern, den Unternehmen und dem deutschen und europäischen Datenschutz – erheblich schaden wird. Eine Verzögerung, die nur einen Gewinner kennt: Die großen Wettbewerber und Datensammler aus dem Silicon Valley, die damit Zeit gewonnen haben, um nach deutschem Recht rechtswidrige Geschäftsmodelle auf dem europäischen Markt fest zu verankern und die seit 1995 in der EU geltenden Datenschutzstandards durch globale Marktfreiheiten zu untergraben. Der Dank dafür geht an Angela Merkel, die Regierungschefin des größten Mitgliedslandes der EU, die es trotz großer Ankündigungen zugelassen hat, dass es auch über drei Jahre nach Vorlage der Gesetzesvorschläge für ein schlagfertiges EU-Datenschutzrecht keine Verhandlungsposition des Rates gibt. Dabei hat das durch die Bürgerinnen und Bürger der EU direkt gewählte Europäische Parlament bereits vor über einem Jahr einen umfangreich ausgehandelten und von allen Fraktionen getragenen Gesetzestext verabschiedet. Wenn es um die Interessen von Unternehmen und Behörden geht, kann die Verabschiedung europäischer Regeln gar nicht schnell genug gehen. Wenn es aber um die Rechte von Bürgerinnen und Bürgern geht, wird plötzlich alles ganz kompliziert. Dabei liegen die Lösungen bereits längst auf dem Tisch.

1. Der Gesetzesvorschlag

Im Jahr 2007 forderten die europäischen Datenschutzbehörden die EU-Kommission auf, das EU-Datenschutzrecht grundlegend zu reformieren und stärker zu vereinheitlichen. Zwölf Jahre nach dem Inkrafttreten der Datenschutzrichtlinie 95/46/EG war offensichtlich, dass der noch recht generelle gemeinsame Rechtsrahmen zu viele unterschiedliche Interpretationen zuließ und dem anstehenden Ansturm neuer Datenverarbeitungsmöglichkeiten nicht standhalten würde. Es dauerte über zwei Jahre, bis die EU-Kommission auf diese Aufforderung mit einem umfassenden Konsultationsverfahren reagierte. Anlass war das Ende 2009 in Kraft getretene neue Vertragsrecht der Europäischen Union, in dem nicht nur die nun verbindliche Grundrechtecharta den Datenschutz ausdrücklich als Menschenrecht benennt, sondern dem EU-Gesetzgeber in Artikel 16 des EU-Vertrags AEUV auch eine umfassende Regelungs-

kompetenz zum Datenschutz einräumte. Die damals neu ernannte EU-Kommissarin für Justiz und Grundrechte, Viviane Reding, legte auf Grundlage der Konsultationsergebnisse eine ausführliche Mitteilung über die Reform des EU-Datenschutzrechts vor. Das Europäische Parlament reagierte hierauf im Sommer 2011 mit einer sehr eindeutigen und mit breiter Mehrheit getragenen Position: Es bedürfe eines einheitlichen Datenschutzrechts für die Europäische Union, das allen Unternehmen und Behörden im EU-Binnenmarkt einen hohen Datenschutzstandard über dem Niveau von 1995 auferlegt und allen Verbraucherinnen und Verbrauchern weitgehende und durchsetzungsfähige Selbstbestimmungs- und Informationsrechte bei der Verarbeitung ihrer personenbezogenen Daten einräumt. Die Datenschutzbehörden sollten zudem mit einem scharfen Sanktionsmechanismus ausgestattet werden, der das Ausweichen auf schwächere Datenschutzregeln («Forum Shopping») effektiv verhindern würde. Die Position des Europäischen Parlaments war von diesem Zeitpunkt an – neben einer allgemeinen Reaktion aus dem Ministerrat, bei der die Mitgliedstaaten die Notwendigkeit der Reform anerkannten – maßgeblich für die Ausarbeitung eines Gesetzesvorschlags durch die EU-Kommission. Bereits im Januar 2012 wurde dieser der Öffentlichkeit präsentiert und den beiden gesetzgebenden Kammern der EU, dem Parlament und dem Rat, zugeleitet.

2. Die Position des Europäischen Parlaments

Im Europäischen Parlament begann eine der umfangreichsten Gesetzgebungsarbeiten seiner Geschichte. Die zuständigen Ausschüsse führten eine ganze Reihe großer parlamentarischer Anhörungen sowie interparlamentarische Runden zwischen Abgeordneten des Europäischen Parlaments und der nationalen Parlamente durch. Als Berichterstatter des federführenden Innen- und Justizausschusses habe ich in dieser Zeit fast 200 unterschiedliche Interessengruppen getroffen, die ihre Anmerkungen zu den Vorschlägen der EU-Kommission für ein neues Datenschutzrecht einbringen konnten. Ein regelrechter Lobby-Ansturm zum Thema Datenschutz war von den Abgeordneten und allen Beteiligten zu bewältigen. Zu dem im Januar 2013 vorgestellten Berichtsentwurf wurden schließlich nicht weniger als 3.999 einzelne Änderungsanträge zu nahezu jedem Absatz der etwa hundert Artikel umfassenden geplanten EU-Datenschutzverordnung eingereicht! Die zuständigen Obleute der Fraktionen des Europäischen Parlaments (sogenannte «Schattenberichterstatter») schnürten in über fünfzig stundenlangen Sitzungen aus diesem Berg von Änderungswünschen ein umfassendes Kompromisspaket. Die Abgeordneten waren von dem Willen getragen, den 500 Millionen Bürgerinnen und Bürgern der Europäischen Union zu zeigen, dass die Europäische Union im Sinne aller Betroffenen einen ausgeglichenen Rahmen für das Zusammenleben in einer grenzenlos gewordenen digitalisierten Welt schaffen kann. Das Ergebnis, dass im Oktober 2013 im federführenden Ausschuss und im April 2014 im Plenum des Europäischen Parlaments beschlossen wurde, zeigt den großen Erfolg dieser Arbeit: Fast alle Abgeordneten stimmten am Ende dem gefundenen Kompromiss und damit dem neuen EU-Datenschutzrecht zu. Aber sie mussten mit Bedauern feststellen, dass trotz ihres großen Einsatzes, die Verhandlungen zwischen dem Parlament und dem Rat der Europäischen Regierungen nicht bereits im Oktober 2013 begannen und die Mitgliedstaaten bis zur Europawahl im Juni 2014 nicht ein einziges Kapitel der Reform zum Abschluss führten.

3. Der Überwachungsskandal

Nachdem im Juni 2013 bekannt wurde, dass der ehemalige US-Geheimdienstmitarbeiter Edward Snowden ganze Berge hoch vertraulicher Dokumente über die Überwachungsmaßnahmen des amerikanischen Nachrichtendienstes NSA an investigative Journalisten weitergegeben hatte, erhielt die Debatte über die Notwendigkeit schärferer Regeln zum Schutz und der Kontrolle personenbezogener Daten eine völlig neue Dimension. Zwar war schon seit dem Aufkommen der sozialen Netzwerke um das Jahr 2007 verstärkt über die richtige Antwort auf die zu erwartende Flut personenbezogener Daten diskutiert worden. Allerdings erhielt das Thema erst mit dem Bekanntwerden der umfassenden und anlasslosen Überwachung der Internetkommunikation durch die Geheimdienste demokratischer Rechtsstaaten, der USA und Großbritanniens, die Aufmerksamkeit der allgemeinen Öffentlichkeit. Plötzlich wurde wirklich für alle offensichtlich, dass die Massenerhebung sogenannter Meta-Daten (Verbindungs- oder Verkehrsdaten) die Erstellung weitreichender Persönlichkeitsprofile zuließ und der Zugriff staatlicher Behörden eine Gewissheit war. Erstmals erhielt die bis dahin weit verbreitete positive Einstellung zur Digitalisierung der Kommunikation einen massiven Dämpfer. Bisher glaubten die Menschen, dass die Massen an Daten nur vor dem Zugriff Unbefugter geschützt werden müssten und niemand einen Nachteil durch deren Verarbeitung zu befürchten habe, solange er oder sie sich nicht verdächtig gemacht hatte. Nun riefen selbst Konservative und Wirtschaftsliberale nach einer Begrenzung der Datenerhebung und -verbreitung. Dies beeinflusste die Verhandlungen zur Datenschutzreform. Obwohl zu diesem Zeitpunkt bereits zahlreiche Kompromisse im Europäischen Parlament ausgehandelt und auch Bestimmungen zum Schutz vor drittstaatlichen Behörden getroffen waren, sorgte der Geheimdienst-Skandal für ein Zusammenrücken der politischen Entscheidungsträger mit Blick auf ein hohes und verlässliches Datenschutzniveau in der EU. Wenn schon keine schärferen Regeln für die Arbeit der Geheimdienste zu erreichen waren, sollten die Betroffenen zumindest eine bessere Kontrolle darüber erhalten, welche Daten überhaupt erhoben würden.

4. Die EuGH-Urteile zur Vorratsdatenspeicherung und zum Löschungsanspruch

Am 8. April 2014 urteilte zudem der Europäische Gerichtshof (EuGH) über die Vereinbarkeit einer anlasslosen Datensammlung mit den Grundrechten auf Datenschutz und Privatsphäre aus der Grundrechtecharta. In seinem lang erwarteten Richterspruch hielt er überraschend die gesamte EU-Richtlinie zur Vorratsdatenspeicherung aus dem Jahr 2006 für unvereinbar mit den Grundrechten und erklärte sie von Anfang an für nichtig. Die Luxemburger Richter begründeten dies vor allem mit der Anlasslosigkeit der Speicherung von personenbezogenen Daten, in diesem Falle von Telefonverkehrsdaten. Angesichts der Vielzahl von Datensammlungen in der EU wird das Urteil zahlreiche Gesetzesänderungen veranlassen. Es schränkt zudem die Möglichkeiten der EU und ihrer Mitgliedstaaten ein, künftig umfangreiche Datenerhebungen zuzulassen. Dennoch sind viele mitgliedstaatliche Regelungen zur Speicherung von Telekommunikationsdaten entgegen der Vorgaben dieses Urteils (im Rahmen der so genannten ePrivacy-Richtlinie) noch immer in Kraft. Auch müssen die bereits beschlossenen und geplanten Maßnahmen

zur Speicherung und Auswertung von Bank- und Passagierdaten auf den Prüfstand gestellt werden, wogegen sich Konservative in Parlament und Rat trotz eindeutiger Rechtslage noch immer sträuben.

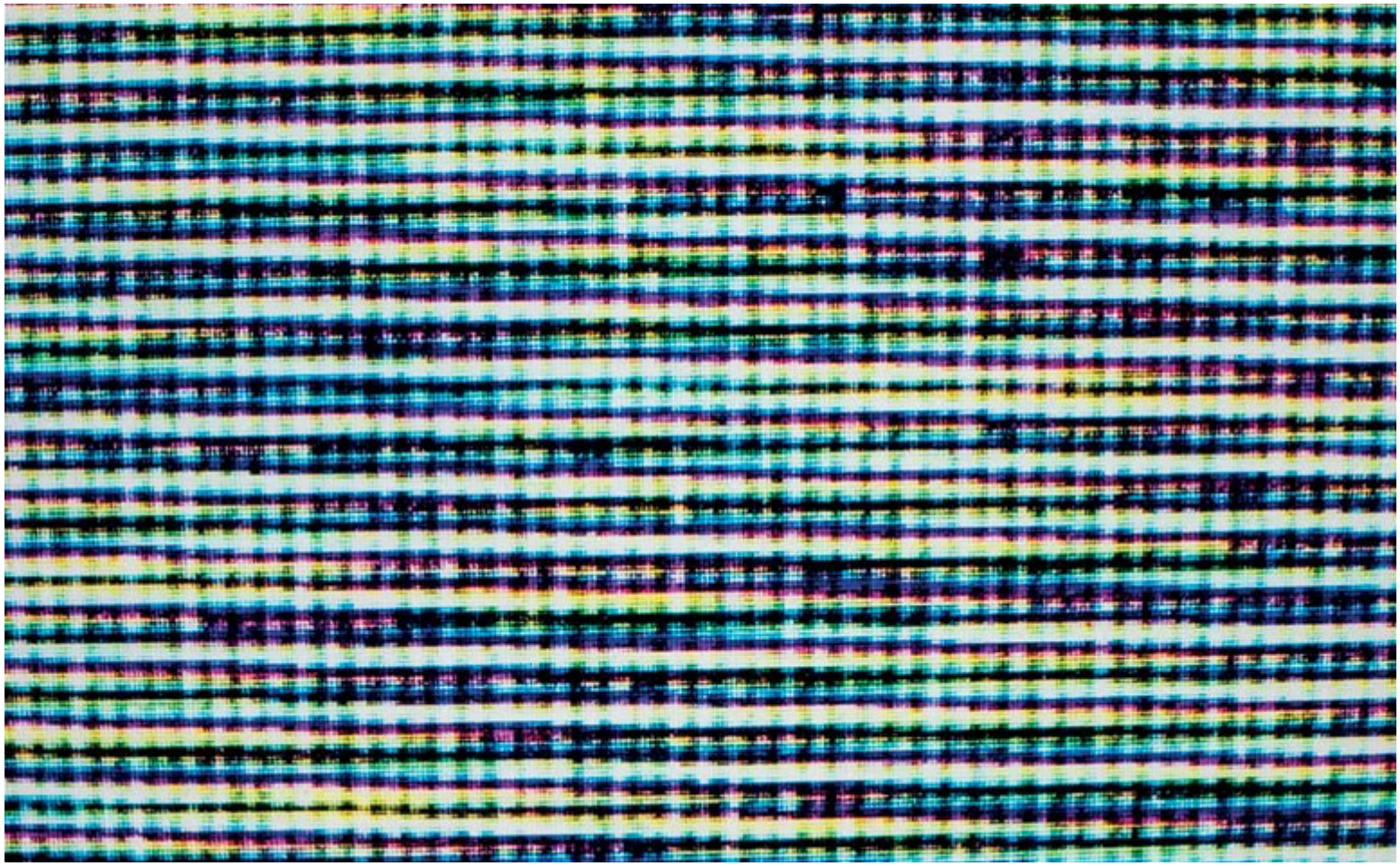
Im Mai 2014 folgte ein weiteres aufsehenerregendes Urteil des EuGH zur Anwendbarkeit der EU-Datenschutzrichtlinie von 1995 auf Internetsuchmaschinen wie Google sowie zum Verhältnis des Grundrechts auf Datenschutz zur Gewerbe-, Informations- und Meinungsfreiheit. Der Gerichtshof urteilte, dass auch Suchdienste an das Datenschutzrecht gebunden sind, wenn sie für die Suchergebnisse personenbezogene Daten selbst verarbeiten. Hier kann im Wege der Abwägung zwischen den Persönlichkeitsrechten auf Datenschutz ein Anspruch auf Löschung dieser Daten das öffentliche Interesse an der Informations- und Meinungsfreiheit überwiegen: das sogenannte «Recht auf Vergessenwerden». Daher hat dieses Urteil nur geringe Auswirkungen auf den Fortgang der EU-Datenschutzreform, da diese Rechtslage auch unter den neuen Bestimmungen weitestgehend erhalten bleiben wird. Die Gerichte werden auch weiterhin gehalten sein, zwischen dem neuen EU-Datenschutzrecht sowie anderen Bestimmungen zum Grundrechtsschutz abzuwägen.

5. Die Trilog-Verhandlungen

Die Position des Europäischen Parlaments liegt nun bereits seit über einem Jahr auf dem Tisch und enthält für alle im Verlaufe des Jahres aufgetretenen Debatten eine Reihe von Antworten, deren Umsetzung dringend geboten wäre. Nach zähen und langen Auseinandersetzungen im Ministerrat über ganz grundsätzliche Fragen von Form und Verfahren im neuen EU-Datenschutzrecht widmen sich nun auch die Mitgliedstaaten der Kompromissfindung in den konkreten Datenschutzbestimmungen. Dass dies nicht über Nacht zu erreichen ist, wissen gerade auch die Abgeordneten im Europäischen Parlament. Deshalb erwarten nun alle, dass es im Juni 2015 ein Verhandlungsmandat für die Ratspräsidentschaft geben wird, die daraufhin die Verhandlungen im so genannten Trilog eröffnen kann. An einem Tisch mit den Vertreterinnen und Vertretern von Parlament und Kommission müssen sie sich dort auf eine gemeinsame Version der Gesetzestexte einigen. Das Parlament geht in diese Verhandlungen angesichts der Breite der Unterstützung für seine Position mit hohem Selbstbewusstsein. Um eine Einigung noch im Jahr 2015 zu erreichen, müsste der Ministerrat die Forderungen des Parlaments weitgehend bereits in seiner Verhandlungsposition übernehmen. Je mehr Unterschiede die Ministerinnen und Minister zur Parlamentsposition aufmachen, desto langwieriger und mühsamer wird der weitere Einigungsprozess. Auch die EU-Kommission zeigte bereits von Beginn an klare rote Linien auf, bei deren Überschreitung sie intervenieren und damit eine einstimmige Einigung im Rat erzwingen könnte. Dabei drängt die Zeit für eine Verabschiedung der EU-Datenschutzreform nun mehr denn je: Während die Europäische Union noch an ihrem neuen Datenschutzrecht feilt, versucht die US-Regierung bereits, im Rahmen der Verhandlungen zum transatlantischen Handels- und Investitionsabkommen TTIP eine Anerkennung ihrer teilweise nicht einmal gesetzlich normierten Regeln durchzusetzen.

Wenn es den Regierungsspitzen in der EU wirklich um den Schutz der Interessen und Rechte ihrer Bürgerinnen und Bürger geht, dann müssen sie dafür sorgen, dass es vor der Jahresmitte 2015 zu einer endgültigen Einigung im Ministerrat

kommt und die dort abgestimmte Position keine weitgehenden Abweichungen vom Beschluss des Europäischen Parlaments enthält. Ansonsten müssen sie – gerade auch die deutsche Bundesregierung – für den angerichteten Schaden eines praktisch bedeutungslosen Datenschutzrechts verantwortlich gemacht werden. Und nicht nur das: Sie werden damit auch das Ziel verfehlen, mit der Schaffung einheitlicher EU-Datenschutzregeln einen wichtigen Schritt hin zu einem digitalen europäischen Binnenmarkt zu gehen. Ein Schritt, der schon heute eher eine fatale Untätigkeit zu Lasten der eigenen Wirtschaft und Verbraucherinnen und Verbraucher beseitigen würde, als einen Vorsprung im globalen Wettbewerb zu bewirken. Daher muss die EU-Datenschutzreform besser heute als morgen verabschiedet werden.



STEFAN KÖPSELL

Dezentralität, Diversität und Redundanz – Bausteine für eine bürgerorientierte Netzwelt

Dieser Beitrag beschäftigt sich mit der Frage, wie die Internet-Infrastruktur zu gestalten oder zu verändern wäre, damit diese eine Überwachung nicht mehr begünstigt, sondern erschwert und so die Freiheit der Nutzer stärkt. Dabei werden die Aspekte Dezentralität, Diversität und Redundanz betrachtet.

1. Begriffe

a) Dezentralität

In dezentralen oder verteilten Systemen werden *zentrale* Elemente vermieden. Dabei können bezüglich der (De-)Zentralität verschiedene Aspekte betrachtet werden. Häufig wird an eine räumlich Verteilung gedacht, das heißt physische Systemkomponenten befinden sich an geographisch unterschiedlichen Orten. Einen anderen wichtigen Aspekt stellt die Kontrollstruktur dar, das heißt die Frage, ob es eine zentrale Entität gibt, die das System kontrolliert. Schließlich kann betrachten werden, ob eine einzelne Entität allein für den Entwurf, die Implementierung, Herstellung oder Betrieb des Systems verantwortlich ist.

b) Diversität

In diversen Systemen werden *gleiche* Systembestandteile *unterschiedlich* realisiert. Die Gleichheit bezieht sich dabei typischerweise auf die nach Außen zur Verfügung gestellten Schnittstellen. So ist es leicht möglich, für die Umsetzung einer bestimmten Funktionalität unterschiedliche Komponenten zu verwenden. Die Unterschiede in der Realisierung können wiederum eine Reihe verschiedener Aspekte umfassen. Naheliegend ist hier zunächst, daß die betreffenden Komponenten durch unterschiedliche Hersteller produziert oder im Falle von Software programmiert werden. Ein weiterer Aspekt wäre die Herstellung unter Verwendung unterschiedlicher Maschinen und Herstellungstechnologien, im Falle von Software unter Verwendung unterschiedlicher Programmiersprachen. Darüber hinaus können die betreffenden Komponenten von unterschiedlichen Entwicklern entworfen worden sein, so daß komplett unterschiedliche Lösungsansätze umgesetzt würden. Die Entwickler können dabei wiederum unterschiedliche Werkzeuge (etwa in Form von Software) verwendet haben.

c) Redundanz

Hiermit ist gemeint, daß wichtige Systembestandteile mehrfach vorhanden sind, so daß der Ausfall einer einzelnen Komponente nicht zum Komplettausfall des Gesamtsystems führt. Im folgenden soll der Zusammenhang zwischen diesen drei Konzepten auf das Internet als der bestimmenden digitalen Kommunikationsinfrastruktur angewendet. Dabei soll untersucht werden, ob und wie Strukturen im freiheitsgewährleistenden Sinne entwickelt und ausgelegt werden könnten.

2. Zentrale Strukturen des Internets

Das Internet wird hin und wieder als „Netz der Netze“ bezeichnet. Damit ist durchaus nicht nur die herausragende Bedeutung des Internet gemeint, tatsächlich ist das Internet ein Netz von Netzen, genauer ein Netz sogenannter «autonomer Systeme». Ein autonomes System ist dabei ein Netz, das unter der administrativen Kontrolle einer einzelnen Institution steht, typischerweise eines Internet Service Providers (ISP). Diese autonomen Systeme sind zusammengeschaltet, so daß die Daten eines Nutzers *A* aus dem autonomen System 1 an einen Nutzer *B* aus dem autonomen System 3 übermittelt werden können (siehe Abbildung). Dabei ist es nicht zwingend notwendig, daß eine direkte Verbindung zwischen den autonomen Systemen 1 und 3 existieren muß. Vielmehr besteht eine Stärke der Internet-Architektur darin, daß ein geeigneter Weg gefunden wird. Ausgehend von diesem prinzipiellen Aufbau des Internet könnte man zunächst vermuten, daß das Internet ein stark dezentrales System ist, also sehr viele autonome Systeme mit zahlreichen Verbindungspunkten (Gateways) miteinander verbunden sind.

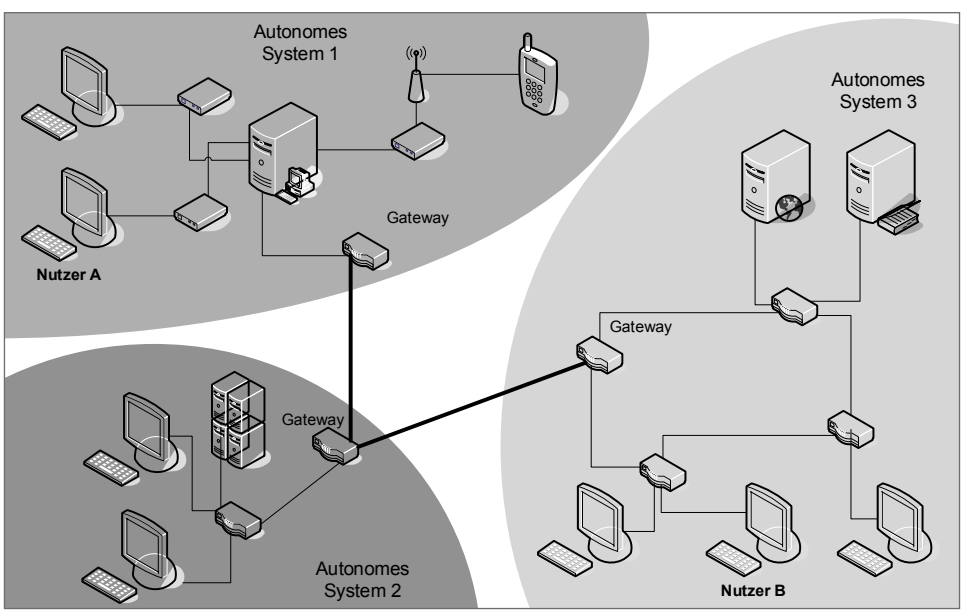


Abbildung : Das Internet als «Netz-der-Netze»: Verbindungen zwischen autonomen Systemen ermöglichen den weltweiten Datenaustausch.

Dies ist allerdings nicht der Fall. Stattdessen bestehen eine Reihe sogenannter «Austauschpunkte», an denen eine Vielzahl von autonomen Systemen angeschlossen ist. Der Datenaustausch zwischen den autonomen Systemen läuft dann über diese Austauschpunkte. Der Großteil des weltweiten Datenaustausches läuft daher über eine relativ kleine Zahl zentraler Stellen.

Eine ähnliche Zentralisierung kann man auch bei den Endpunkten der für die Internet-Kommunikation verwendeten Unterseekabel feststellen. So befinden sich beispielsweise viele Kopfstationen der transatlantischen Unterseekabel in England. Die Zentralisierung der Austausch- und Endpunkte unterstützt die Überwachbarkeit, da das Belauschen der Kommunikation an einigen wenigen Punkten Einblick in einen Großteil der im Internet übertragenen Daten vermittelt. So wurde im Zuge der Snowden-Enthüllungen bekannt, daß die NSA durch Zusammenarbeit mit dem BND (Operation „Eikonal“[1]) eine Überwachung des großen deutschen Internet-Austauschpunktes (DE-CIX) in Frankfurt durchführt, dort Daten abgreift und mit Hilfe des britischen Geheimdienstes GHCQ und dem System „Tempora“ die Unterseekabel überwacht, die in England enden[2].

3. Monopolistische Strukturen

Neben der physischen Zentralität der aktuellen Architektur des Internets fördern weitere Faktoren die Überwachbarkeit. Diese hängen eng mit der fehlenden Diversität und der sich daraus ergebenden Zentralität der Kontrollstrukturen zusammen. Hier sind die Beispiele beliebter Internet-Dienste wie etwa Online Social Networks oder die Internet-Suche zu nennen. In beiden Fällen besteht eine starke Dominanz eines einzigen Anbieters. Im Falle der Online Social Networks ist dies Facebook und im Falle der Internet-Suche (zumindest in Deutschland) ist dies Google. Zwar betreiben beide Anbieter Rechenzentren in den verschiedensten Gebieten der Welt - insofern handelt es sich um physisch verteilte Dienste – allerdings gibt es eben nur jeweils eine Instanz (Facebook bzw. Google, beide USA), die die Kontrolle über den Dienst hat. Diese zentralen Instanzen können nicht nur Kenntnis von allen über die jeweiligen Dienst ausgetauschten Daten erlangen, sie können auch kontrollieren, welche Daten, Nachrichten oder Informationen über den Dienst ausgetauscht werden und diese auch manipulieren.

Aber nicht nur im Bereich der Internet-Dienste fehlt es an Diversität. Auch im Bereich der Netzinfrastruktur gibt es beispielsweise mit der Firma Cisco (USA) einen Ausrüster, der mit einem Marktanteil von über 60 Prozent[3] einen Großteil der verwendeten Geräte stellt. Im Bereich der in PCs, Notebooks oder auch Servern verbauten Prozessoren besitzt Intel (USA) einen Marktanteil von ca. 80 Prozent und bei den Desktop-Betriebssystemen hat Microsoft (USA) einen Marktanteil von über

1 Georg Mascolo, Hans Leyendecker, John Goetz: “Codewort Eikonal - der Albtraum der Bundesregierung”, Süddeutsche Zeitung (online), 4. Oktober 2014, http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432 (abgerufen: 2. Juni 2015).

2 Ewen Macaskill, Julian Borger, Nick Hopkins, Nick Davies, James Ball: “GCHQ taps fibre-optic cables for secret access to world’s communications”, The guardian, 21. Juni 2013.

3 http://www.inside-it.ch/articles/29907 (abgerufen: 12. Dezember 2014).

80 Prozent[4]. Die Liste ließe sich mit vielen weiteren Beispielen fortsetzen, in denen die Produkte eines einzigen Herstellers oder Entwicklers einen sehr hohen Marktanteil haben. Das Problem dieser „Monokulturen“: die Hersteller oder Entwickler üben die Kontrolle über die betreffenden Teile der Informations- und Kommunikationstechnik (IKT) - Infrastruktur aus. So muß man darauf vertrauen, daß weder Intel noch Microsoft mit der NSA zusammenarbeiten und nicht mit in der Hardware (Prozessor) oder Software (Betriebssystem) eingebauten Hintertüren auf die durch die Endnutzer_innen gebrauchten Systeme wie Rechner oder Notebooks zugreifen. In diesem Falle würde selbst Verschlüsselung nichts nutzen, da die Nachrichten, Daten oder Information auf den Endgeräten in unverschlüsselter Form vorliegen müssen, damit der Nutzer des Gerätes diese wahrnehmen kann. Aber selbst wenn Hersteller nicht mit Geheimdiensten oder anderen Cyber-Kriminellen zusammenarbeiten würden, erleichtern Monokulturen im Bereich der IKT-Infrastruktur den Angreifern das Belauschen und Manipulieren der Kommunikation durch Veränderung der eingesetzten Hard- oder Software. Der Angreifer muß sich nur mit wenigen verschiedenen Technologien und Produkten auseinandersetzen und entsprechende Manipulationsmöglichkeiten finden. Gäbe es im Bereich der IKT-Infrastrukturen eine größere Diversität, würde der Aufwand stark steigen.

Daß Geheimdienste tatsächlich Hard- oder Software manipulieren, um ihre Ziele zu erreichen, ist spätestens durch die Snowden-Enthüllungen bekannt. So wurde etwa berichtet,[5] daß die NSA Cisco-Router[6] auf dem Transportweg abfängt und mit einer Hintertür ausstattet, bevor die Geräte an den Empfänger weitergeschickt werden. Auf diese Weise ist es der NSA möglich, sämtliche über den betreffenden Router abgewickelte Kommunikation zu belauschen und zu manipulieren. Geht man davon aus, daß IKT-Infrastrukturen wie etwa das Internet und die damit verbundene Benutzung von IT-Geräten heutzutage einen wichtige Voraussetzung für die Meinungsbildung und politische Einflußnahme und somit letztlich für den Fortbestand unserer freiheitlich-demokratischen Grundordnung sind, so ist es bedenklich, daß diese wichtige Infrastruktur zu großen Teilen unter ausländischer Kontrolle steht.

4. Abbau der Redundanz

In den letzten Jahren zeigt sich der klare Trend, vormals redundante Systeme unter dem Gesichtspunkt von Kosteneinsparungen auf ein einziges System zu reduzieren oder in ein einziges System zu integrieren. Als Beispiel seien die drei unterschiedlichen Informations- und Kommunikationskanäle Telefon, Fernsehen und Internet genannt: Waren diese früher unterschiedliche Systeme, die schlimmstenfalls teilweise dasselbe Kabel nutzten, aber nicht auf dieselbe Vermittlungsinfrastruktur angewiesen waren, so findet heute mit den „All-IP“-Lösungen eine Verschmelzung

4 http://de.statista.com/statistik/daten/studie/157902/umfrage/marktanteil-der-genutzten-betriebssysteme-weltweit-seit-2009/ (abgerufen: 2. Juni 2015).

5 Gleen Greenwald: „No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State“, Hamish Hamilton, Mai 2014.

6 Ein Router ist eine Netzkomponente, die, ähnlichem einem Vermittlungsrechner im Telefonnetz, die Daten auf dem richtigen Weg vom Sender zum Empfänger weiterleitet.

der drei Dienste statt. Da sie alle IP-basiert arbeiten, führt ein Ausfall der verwendeten IP-Komponenten wie etwa der Vermittlungsstelle oder des DSL-Modems zu einem gleichzeitigen Ausfall aller drei Kommunikationskanäle. Eine Redundanz der IKT-Infrastruktur wäre insbesondere wichtig, sollten Abstimmungen zukünftig über das Internet erfolgen. Andernfalls wäre es einem Angreifer leicht möglich, die IKT-Infrastruktur zu stören und so Möglichkeiten zur Abstimmung zu unterbinden.

Der gesamte Bereich des Cloud Computing missachtet die Leitlinien der Dezentralität, Diversität und Redundanz. Daten, die früher lediglich verteilt auf den Rechnern der Nutzer_innen gespeichert waren, finden sich heute an zentraler Stelle bei den Cloud-Anbietern wie etwa Apple, Google, Microsoft oder Amazon, alle in den USA. Je schlechter die Daten gegen unberechtigte Kenntnisnahme geschützt sind, desto leichter wird die Überwachung - und heute ist das unsichere Speichern von Daten in der Cloud eher die Regel als die Ausnahme[7]. Aber nicht nur Daten werden ausgelagert, sondern auch die Ausführung der Programme. Bei Ausfällen bei den Cloud-Anbietern sind regelmäßig sehr viele Dienste und Nutzer_innen betroffen[8]. Die Situation dürfte sich in Zukunft mit dem sogenannten „Internet der Dinge“ (Internet of Things, IoT) weiter verschlimmern, da es im Wesentlichen auf eine Nutzung der Cloud als Kommunikationsplattform, Datenspeicher und Ausführungsumgebung setzt. Grundgedanke des „Internets der Dinge“ ist, daß zukünftig alle physischen Objekte vernetzt sein werden – die Überwachbarkeit dehnt sich somit von der virtuellen auf die physische Welt aus.

5. Auswege?

Aber wie kann man die aktuelle Situation in Richtung zu mehr Dezentralität, Diversität und Redundanz verbessern? Es erscheint schwer vorstellbar, daß sich an den vorhandenen „Monokulturen“ grundsätzlich etwas ändert. Zu dominant sind die ausländischen Entwickler und Hersteller, zu groß erscheinen die Kosten, um für mehr Diversität zu sorgen. So hat etwa Samsung in den Bau einer einzigen neuen Chip-Fabrik mehr als 11 Milliarden Euro investiert![9] Das deutsch-französische Projekt „Quaero“[10], daß sich zum Ziel gesetzt hatte, eine europäische Suchmaschine als Konkurrenz zu Google aufzubauen, wurde nach Millioneninvestitionen 2013 endgültig für beendet – sprich gescheitert – erklärt. Versuche, eine dezentrale Variante von Facebook zu schaffen, wie etwa Diaspora[11], Frendica[12] oder Safebook[13]

7 http://www.heise.de/security/meldung/Unzaehlige-Apps-speichern-private-Daten-unsicher-in-der-Cloud-2671988.html (abgerufen: 2. Juni 2015).

8 www.heise.de/newsticker/meldung/Weitere-Stoerungen-bei-Apples-Cloud-Diensten-2678590.html, http://www.heise.de/newsticker/meldung/Internetdienste-nach-Amazon-Stoerung-mit-Schluckauf-1942704.html (abgerufen: 2. Juni 2015).

9 http://www.heise.de/newsticker/meldung/Samsung-baut-neue-Chip-Fabrik-fuer-mehr-als-11-Milliarden-Euro-2411823.html (abgerufen: 12. Dezember 2014).

10 http://www.quaero.org/ (abgerufen: 3. Juni 2015).

11 https://diasporafoundation.org/ (abgerufen: 3. Juni 2015).

12 http://friendica.com/ (abgerufen: 3. Juni 2015).

13 L. A. Cutillo, R. Molva, T. Strufe: “Safebook: A privacy-preserving online social network leveraging on real-life trust,” IEEE Communications Magazine, vol.47, no.12, pp.94– 101, Dezember 2009.

sind unter theoretischen Gesichtspunkten interessant, haben aber noch keine nennenswerte Bedeutung gewonnen.

a) Freifunk-Bewegung

Trotz der Schwierigkeiten versuchen Bürger_innen, die Abhängigkeit von wenigen Herstellern und Anbietern zu durchbrechen. So hat sich die Freifunk-Bewegung[14] zum Ziel gesetzt, eine dezentrale und freie Kommunikationsinfrastruktur zu schaffen, die nicht unter der Kontrolle einiger weniger Unternehmen steht. Dabei vernetzen die Teilnehmer ihre WLAN-Router miteinander, um anderen den Zugang zu ihren WLAN-Routern zu ermöglichen. Ein ähnliche Idee verfolgen viele Projekte weltweit wie beispielsweise auch das Projekt „qaul.net – "[15]. Technisch sind die vorgeschlagenen Ideen durchaus umsetzbar. Allerdings scheitert eine stärkere Verbreitung in Deutschland an rechtlichen Hürden: Hier ist insbesondere die sogenannte «Störerhaftung» zu nennen, aber auch die geplanten Änderungen am Telemediengesetz. Im Kern geht es darum, daß jemand, der anderen Zugang zu seinem WLAN ermöglicht, für deren Handlungen haftbar gemacht werden kann. Möchte man also an Initiativen wie dem Freifunk teilnehmen, entsteht das Risiko von Schadensersatzforderungen in unbekannter Höhe, wenn das zur Verfügung gestellte WLAN mißbraucht wird. Durch politische Entscheidungen und Gesetzesänderungen wäre es aber sehr wohl möglich, die Entwicklung von dezentralen und diversitären, also freien Netzen zu unterstützen. Allerdings würde dann auch eine staatliche Kontrolle dieser Netze wesentlich erschwert.

b) Öffnung von Schnittstellen

Im Bereich von Internet-Diensten scheint die Überwindung von Monokulturen deutlich schwieriger. Eine staatlich betriebene Schaffung von Alternativen etwa im Bereich von Suchmaschinen, Online Social Networks oder ähnlichem wäre nur mit großem finanziellen Aufwand möglich und zudem der dauerhafte Erfolg fraglich. Allerdings besteht auch hier die Möglichkeit eines regulatorischen Eingreifens: So könnte man Regelungen schaffen, die Anbieter von marktdominierenden Diensten zwingen, Schnittstellen anzubieten, so daß neue Anbieter ihre Dienste mit den existierenden Diensten verbinden können. Dies würde helfen, Lock-In-Effekte zu vermeiden. Würde beispielsweise WhatsApp[16] als eines der dominierenden Text-Messaging-Systeme gezwungen werden, Schnittstellen für andere Text-Messaging-Systeme zu schaffen, könnten Nutzer_innen auf sichere, dezentrale und weniger überwachungsgeneigte Dienste ausweichen, ohne befürchten zu müssen, nicht mehr erreichbar zu sein. Statt eines harten Schnitts wäre ein sanfter Wechsel von einem Dienst zu einem anderen möglich.

c) Hardware-Monopole

Betrachtet man den Bereich der Endgeräte und der dafür verwendeten Hardware, so scheint ein Überwinden der Monopolstellung einiger weniger Unternehmen

14 http://freifunk.net/ (abgerufen: 3. Juni 2015).
15 http://qaul.net/ (abgerufen: 2. Juni 2015).
16 https://www.whatsapp.com/ (abgerufen: 3. Juni 2015).

noch deutlich unwahrscheinlicher. Die enormen Kosten für Entwicklung und Herstellung eigener deutscher oder europäischer Hardware stehen dem entgegen. Zudem müsste eine wirksame Umsetzung der Idee der Diversität konsequent verfolgt werden. In der Halbleiterindustrie geht es nicht nur um den Entwurf und die Herstellung der Mikrochips, sondern auch um Diversität bei den verwendeten Maschinen. So haben aktuelle wissenschaftliche Untersuchungen[17] Wege aufgezeigt, wie sich Prozessoren während der Produktion gezielt so manipulieren lassen, daß diese eine für den Angreifer nützliche Funktionalität, etwa eine Hintertür, enthalten, die gleichzeitig von außen nur schwer oder gar nicht feststellbar ist. Diese Hintertüre kann dann wieder zur Überwachung oder Manipulation der IKT-Infrastruktur oder der Endgeräte verwendet werden.

Auch der Markt von Produktionsmitteln für die Chip-Herstellung ist von ausgeprägten Monokulturen geprägt. So besitzt der Hersteller ASML, ein Ausrüster im Bereich der Lithographiesysteme, einen Marktanteil von mehr als 80%[18]. Auch hier verursachen die enormen Kosten eine Konzentration auf wenige Anbieter, so betrugen die Ausgaben für Forschung und Entwicklung bei ASML im Jahre 2014 mehr als. 1 Mrd. Euro[19]. Es stellt sich die Frage, ob im Bereich der Hardware-Herstellung eine gegebenenfalls staatlich geförderte europäische Alternative zu den amerikanisch dominierten Firmen vorstellbar wäre. In jedem Fall würde dies den politischen Willen zur Unabhängigkeit erfordern und mit enormen Anfangskosten verbunden sein.

d) Vereinfachung der Fertigungsprozesse

Eine interessante Alternative, deren Potential heute nur schwer abzuschätzen ist, ergibt sich aus der Vereinfachung von Fertigungsprozessen, so daß diese auch von Bürger_innen in Eigenregie durchgeführt werden können. Hier sind etwa die Maker-Bewegung[20] und die 3D-Druck-Technologie zu erwähnen. Werden in der physischen Welt in absehbarer Zeit ähnliche Schwellen überschritten werden, wie in jüngster Vergangenheit in der digitalen (virtuellen) Welt? So war es noch vor wenigen Jahrzehnten nicht vorstellbar, daß einzelne Bürgerinnen erfolgreich in Konkurrenz zu etablierten Medien aus dem Bereich Zeitung, Fernsehen oder Radio treten. Mit den durch das Internet geschaffenen Möglichkeiten in Form von Blogs, Podcasts oder You-Tube-Kanälen ist dies heute möglich und längst Realität. Werden also künftig Einzelne in der Lage sind, konkurrenzfähig physische Dinge herzustellen, die heute nur durch große Firmen oder Konzerne produziert werden können? Sollte dies durch den wissenschaftlich-technologischen Fortschritt ermöglicht werden, ist durchaus vorstellbar, daß die Diversität im Bereich der Hardwarekomponenten der IKT-Infrastruktur deutlich zunimmt.

17 http://www.heise.de/security/meldung/Forscher-beschreiben-Chip-Sabotage-ab-Werk-1961412.html (abgerufen: 12. Dezember 2014).

18 http://www.wsj.com/articles/SB10001424127887323809304578428850807241388 (abgerufen: 2. Juni 2015).

19 http://www.asml.com/asml/show.do?lang=EN&ctx=51431&dfp_fragment=technology_1 (abgerufen: 4. Juni 2015).

20 http://make-germany.de/ (abgerufen: 2. Juni 2015).

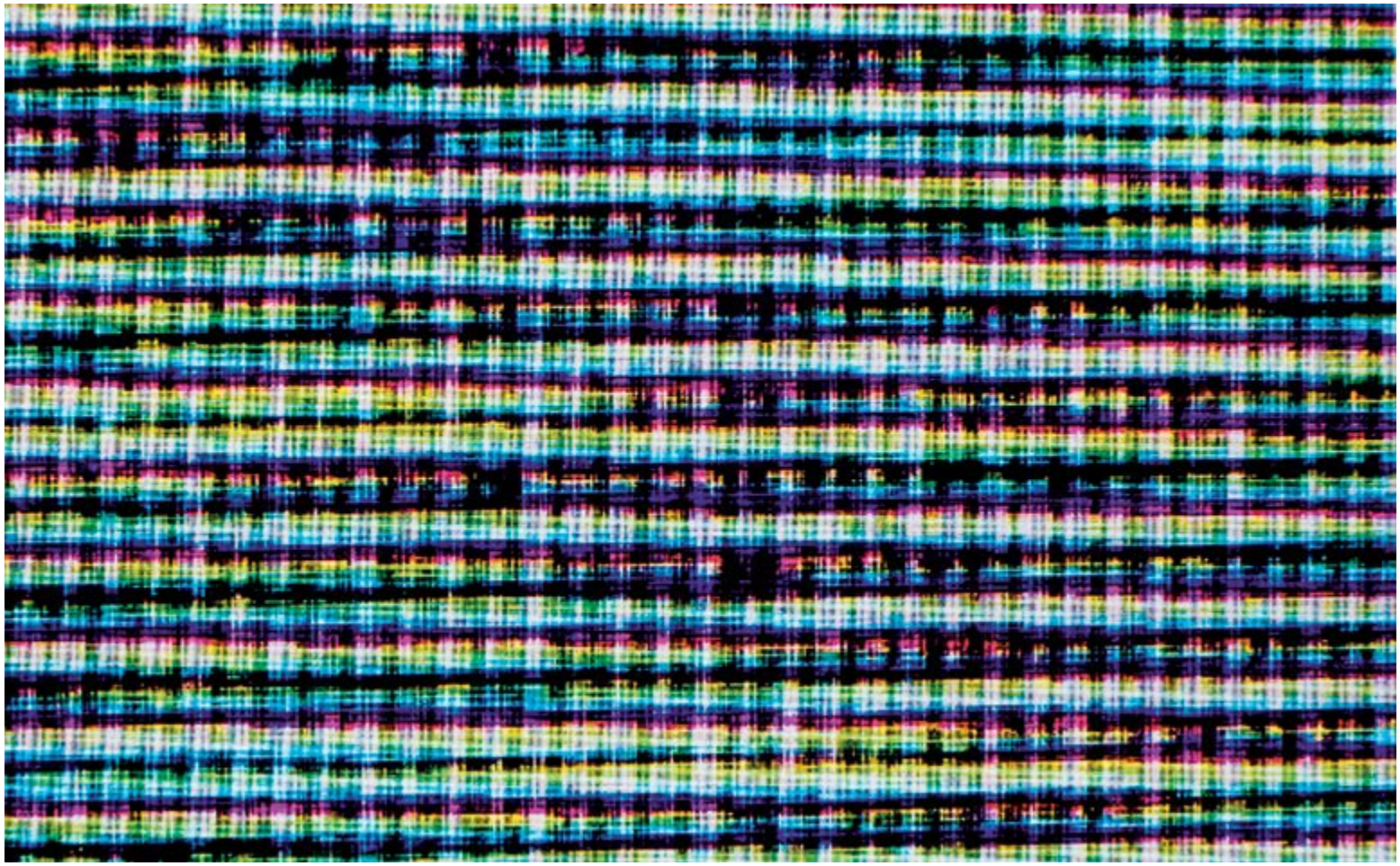
e) Zwangsrouter

In jedem Fall sollten aus politisch regulatorischer Sicht unnötige Hindernisse für mehr Diversität beseitigt werden. Ein aktuelles Beispiel ist das Thema „Zwangsrouter“: Aktuell weigern sich einige Internet Service Provider, ihren Kunden die Zugangsdaten für den Internet-Anschluß mitzuteilen, so dass diese Kunden gezwungen werden, den vom Provider bereitgestellten Router zu verwenden. Bedenkt man, daß wöchentlich neue gravierende Sicherheitslücken in diesen Routern bekannt werden[21] und die Hersteller oder Internet Service Provider diese nur zögerlich oder gar nicht beseitigen, so wird damit der Überwachbarkeit geradezu Vorschub geleistet. Gäbe es entsprechend klare gesetzliche Vorgaben, daß Kunden von Internet Service Providern die benötigten Zugangsdaten mitzuteilen sind, könnten Betroffene wenigstens auf sicherere Produkte wechseln.

f) Fazit

Zusammenfassend kann man feststellen, daß die heutigen zentralen und wenig diversen Strukturen im Bereich der Informationstechnologie und insbesondere im Bereich des Internets die Überwachbarkeit und Manipulierbarkeit fördern. Änderungen an diesen negativen Gegebenheiten gibt es zwar in Ansätzen, es ist aus heutiger Sicht aber zweifelhaft, ob diese langfristig erfolgreich sein werden. Dies hängt in starkem Maße von den durch die Politik gesetzten Zielen und den daraus resultierenden Rahmenbedingen ab.

21 www.heise.de/security/meldung/Kritische-Luecke-in-etlichen-Routern-2655271.html, www.heise.de/security/meldung/Und-taeglich-gruesst-die-D-Link-Luecke-2628562.html, www.heise.de/security/meldung/D-Link-Patch-ergaenzt-Sicherheitsluecken-durch-neue-Luecke-2607642.html, http://www.heise.de/security/meldung/D-Link-Luecke-klafft-seit-November-weitere-Geraete-betroffen-2563782.html (abgerufen: 2. Juni 2015).



LEONHARD DOBUSCH

Probleme digitaler Plattformregulierung zwischen Verboten, Geboten und Entflechtung

1. Regulierungsforderungen aus der Politik

Das Internet des Jahres 2014 ist geprägt von großen Plattformen und den von ihnen forcierten digitalen Ökosystemen.[1] Wenige zentrale Akteure – allen voran Apple, Amazon, Google, Facebook und Microsoft[2] – dominieren mit ihren Angeboten und Algorithmen wie sich das Internet für die große Masse der InternetnutzerInnen darstellt. In dem Maße, in dem Arbeit und Freizeit, Privates und Berufliches mehr und mehr durch deren digitale Dienstleistungen vermittelt wird, wächst auch deren Bedeutung und Einfluss in den verschiedensten Bereichen einer zunehmend digitalen Gesellschaft.

Mit dieser Entwicklung geht auch ein wachsendes Unbehagen über den festgestellten oder potentiellen Missbrauch der marktbeherrschenden Stellung von Plattformbetreibern einher. Die Liste der Vorwürfe und Bedenken ist lang. Auf Seiten wie *Fairsearch.org* oder *Focusontheuser.eu* wird beispielsweise Google Bevorzugung eigener Dienste im Rahmen seiner Suchmaschine vorgeworfen. Facebook sorgte für Schlagzeilen, weil es im Rahmen von erst im Nachhinein offengelegten Experimenten Stimmungslagen und sogar Wahlverhalten seiner NutzerInnen beinflusst hatte.[3] Amazon wiederum sah sich 2014 mit einer Beschwerde des Börsenvereins des Deutschen Buchhandels beim Kartellamt konfrontiert, in der ihm «erpresserisches Vorgehen gegenüber Verlagen» vorgeworfen wurde.[4] Und auch Apple muss sich regelmäßig Kritik an restriktiven Vorgaben und intransparenten Begutachtungsverfahren in seinem App-Store anhören,[5] jüngst zum Beispiel rund um In-App-Käufe.[6]

Ähnlich vielfältig wie die Vorwürfe über Marktmachtmissbrauch sind auch die Reaktionen politischer Entscheidungsträger. Allein in Deutschland reicht die

1 Zum Thema Ökosystemisierung: Bahr et al. (2012): Schönes neues Internet? Chancen und Risiken für Innovation in digitalen Ökosystemen. Stiftung neue Verantwortung, Policy Brief 05/2012.

2 Aktuelle Zahlen und Analyse dieser Unternehmen: Dolata (2014): Märkte und Macht der Internetkonzerne: Konzentration – Konkurrenz – Innovationsstrategien. SOI Discussion Paper 2014-04.

3 Dobusch, L. (2014): Algorithm Regulation #7: Experimenting with Algorithms for Business and Research, http://governancexborders.com/2014/06/29/algorithm-regulation-7-experimenting-with-algorithms-for-business-and-research/.

4 http://www.spiegel.de/kultur/literatur/boersenverein-legt-beschwerde-beim-bundeskartellamt-ein-a-977153.html.

5 https://www.techinasia.com/plea-apple-improve-app-store-review-process/.

6 http://europa.eu/rapid/press-release_IP-14-847_de.htm.

Bandbreite an Regulierungsvorschlägen von der Forderung nach einem Verbot von Persönlichkeitsprofilen (Innenminister Thomas de Maiziére)[7] über ein Gebot zur Offenlegung von Algorithmen (Justizminister Heiko Maas)[8] bis zur Entflechtung von Plattformbetreibern (Wirtschaftsminister Sigmar Gabriel).[9] Folgt man Gabriel, stehe sogar die gesamte marktwirtschaftliche Ordnung zur Disposition, weil «Vertragsfreiheit und der freie Wettbewerb zur Schimäre zu werden [drohen], wo die Ungleichheit zwischen den Wirtschaftssubjekten absurde Ausmaße annimmt, wo in neufeudaler Selbstherrlichkeit auftretende Monopolisten sich rechtsstaatlichen Regeln entziehen und notwendige Informationen verweigern.»

Die meisten Regulierungsvorschläge haben gemeinsam, dass sie auf die europäische Ebene abzielen. Und EuGH-Urteile wie die jüngste Entscheidung zum sogenannten «Recht auf Vergessen»[10] zeigen doch, dass europäische Regulierung durchaus folgenreich sein kann. So sah sich Google durch die EuGH-Entscheidung genötigt, binnen kurzer Zeit Suchergebnisse zu entfernen, die potentiell Persönlichkeitsrechte verletzen. Dieses Beispiel zeigt jedoch auch, welche Tücken mit unzureichender Regulierung verbunden sein können. So wird mangels klarer Vorgaben des europäischen Gesetzgebers die Abwägung, ob eine Entfernung auch wirklich angemessen ist oder das Recht Dritter auf Informationsfreiheit verletzt, an ein privates Unternehmen wie Google delegiert. Schon länger gibt es ähnliche Formen privater Rechtsdurchsetzung im Bereich des Urheberrechts, wo Suchresultate auf (vermeintlich) raubkopierte Inhalte gelöscht oder Videos mit (vermeintlich) urheberrechtsverletzendem Inhalten blockiert werden.[11]

Die prinzipielle Regulierbarkeit auch großer und grenzüberschreitend tätiger Plattformbetreiber wirft so die Frage nach geeigneten Regulierungsformen und -praktiken auf. Um diese beantworten zu können, müssen jedoch zuerst die Ursachen für die marktbeherrschende Stellung der oben genannten Unternehmen ergründet werden. Erst dann lässt sich nämlich beurteilen, welche Verbote, Gebote oder Entflechtungsmaßnahmen überhaupt geeignet sind, nachhaltig für mehr Wettbewerb und Innovationsoffenheit in verschiedenen digitalen Märkten zu sorgen.

2. Ursachen der Marktmacht großer Plattformbetreiber

Die marktbeherrschende Stellung einzelner Unternehmen sowie ihr Missbrauch sind in einer kapitalistischen Marktwirtschaft nichts ungewöhnliches. Ganz im Gegenteil, mit dem Kartellrecht existiert ein eigener Rechtsbereich der sich explizit diesem Problemkreis widmet und die Ausnutzung einer marktbeherrschenden

7 http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/thomas-de-maiziere-will-persoenlichkeitsprofile-im-internet-verbieten-13164149.html.

8 http://www.spiegel.de/wirtschaft/unternehmen/google-heiko-maas-fordert-offenlegung-von-algorithmus-a-991799.html.

9 http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/sigmar-gabriel-konsequenzen-der-google-debatte-12941865.html.

10 EuGH, Urteil v. 13.05.2014, Az. C-131/12.

11 Zum Beispiel https://netzpolitik.org/2012/private-rechtsdurchsetzung-via-google-mehr-loschungen-neuer-suchalgorithmus/ bzw. https://netzpolitik.org/2012/wikipedia-bbc-cnn-uvm-auf-microsofts-copyright-loschlisten/.

Stellung zu verhindern sucht. Entscheidend für kartellrechtliche Maßnahmen ist dabei nicht schon die Existenz großer Marktmacht, sondern deren Missbrauch. Das ist auch der Grund, warum Initiativen wie Focusontheuser.eu Google die marktmissbräuchliche Bevorzugung eigener Dienstleistungen nachzuweisen versuchen. Wenn ich im folgenden drei zentrale Ursachen – nämlich Skalen-, Netzwerk- und Koordinationseffekte[12] – für die Marktmacht großer Plattformbetreiber im Internet anführe, sind diese zwar nicht völlig neu. Allerdings sind sie im Kontext digital-globalisierter Märkte allgegenwärtiger und auch jenseits klassischer Felder wie beispielsweise der Daseinsvorsorge von Bedeutung.

Positive Skaleneffekte treten immer dann auf, wenn eine größere Zahl an produzierten bzw. verkauften Einheiten mit sinkenden Stückkosten einher geht. Gerade bei digitalen Gütern sind derart sinkende Grenzkosten die Regel. Die Kosten für die Erstellung und Vermarktung eines digitalen Musikstücks oder eines Films sind zum größten Teil fix, die Kosten für die Produktion einer zusätzlichen Einheit gehen gegen Null. Für Plattformanbieter gilt das genauso. Der Aufbau und Betrieb einer Plattforminfrastruktur wie YouTube oder Facebook ist kostspielig, zusätzliche NutzerInnen sorgen hingegen kaum für zusätzliche Kosten.

Vielmehr steigern zusätzliche NutzerInnen über *Netzwerkeffekte* sogar den (Nutzen-)Wert der Plattform. Facebook ist deshalb so ein attraktives soziales Netzwerk, weil viele andere Menschen ebenfalls Facebook nutzen. Ein Konkurrent mit identischem Angebot an Features und Usability wäre deshalb keine ernstzunehmende Bedrohung für Facebook. Nicht immer sind Netzwerkeffekte derart offensichtlich wie im Fall von Facebook, aber auch in allen anderen bisher genannten Plattformen spielen sie eine entscheidende Rolle für deren Attraktivität. Weil die meisten Menschen Smartphone Apps über Apples AppStore und Googles PlayStore beziehen, kommen auch die App-Entwickler nicht an diesen Stores und ihren intransparenten und restriktiven Nutzungsbestimmungen vorbei. Umgekehrt sind transparentere und offenere Alternativen wie zum Beispiel der Open-Source-Store F-Droid wegen ihres eingeschränkten Angebots für die Mehrzahl der NutzerInnen keine Option. Und auch bei Google und Amazon haben wir es mit Netzwerkeffekten zu tun: die Qualität ihrer Such- und Empfehlungsalgorithmen basiert zumindest teilweise auf der Auswertung einer sehr großen Zahl von Nutzerinteraktionen. Auch hier gilt also, dass Qualität und Nutzen des Dienstes auch von der Zahl der Nutzenden abhängt.

Die dritte Ursache für Marktmacht großer Plattformbetreiber, die *Koordinationseffekte*, folgen aus ihrem rechtlichen, in der Regel transnationalen Kontext und der damit verbundenen Unsicherheit bzw. Komplexität. Während digitale Dienstleistungen zumindest technologisch unmittelbar global erbracht werden können, sind sie weiterhin einer Vielzahl an unterschiedlichen nationalen Regelungen unterworfen und tangieren eine Unmenge an Rechtspositionen wie Grundrechte, Persönlichkeitsrechte oder Urheberrechte. Ein wesentlicher Grund für die Attraktivität großer Plattformen ist nun, dass sie die rechtliche Unsicherheit und den Aufwand

12 Allgemeine Diskussion von Mechanismen derart pfadabhängiger Entwicklungen, Dobusch, L., Schüßler, E. (2013): Theorizing Path Dependence: A Review of Positive Feedback Mechanisms in Technology Markets, Regional Clusters and Organizations. In: Industrial and Corporate Change, 22 (3), 617-647.

für die Klärung der Rechte reduzieren, indem Sie verschiedene Anspruchsberechtigte koordinieren. Besonders fortgeschritten ist in dieser Hinsicht Googles bzw. YouTubes Content-ID-Verfahren.[13] Einerseits schützt ein Upload eines musikalisch hinterlegten Videos auf YouTube im Unterschied zum eigenen Blog wirksam vor einer Abmahnung. Andererseits erlaubt der Upload Rechteinhabern Ansprüche anzumelden und so auch nutzergenerierte Inhalte zu monetarisieren. Je undurchdringlicher das Dickicht an nationalen rechtlichen Bestimmungen und je höher die Transaktionskosten herkömmlicher Rechteklärung sind, umso attraktiver und zugleich alternativloser wird die Nutzung proprietärer Plattformen wie YouTube, Facebook oder im Bereich der Fanfiction von Amazon.

3. Notwendigkeit und Möglichkeit regulatorischer Einschränkung von Marktmacht?

In den politischen Regulierungsdebatten spielen die Ursachen für die marktbeherrschende Stellung jedoch bislang kaum eine Rolle. Zwar wird die Marktmacht von Plattformbetreibern als potentielles Problem bis hin zur «Gefahr eines digitalen Totalitarismus» (Gabriel)[14] erkannt und nach der Kartellbehörde gerufen. Konkrete Regulierungsvorschläge bleiben aber im Ungefähren. Allgemein kämpfen politische Regulierungsversuche derzeit mit zwei Problemen: der Dynamik der technologischen Entwicklung und der Wirkungslosigkeit klassisch-kartellrechtlicher Instrumente wie Preiskontrollen oder Zerschlagung.

Die politische Zurückhaltung bei regulatorischen Interventionen im Bereich digitaler Technologien hängt stark mit deren rascher technologischer Entwicklung zusammen. Warum Facebook regulieren, wenn es doch gerade erst Myspace und dieses wiederum Friendster als führendes soziales Netzwerk abgelöst hat? Vielfach wird deshalb die Notwendigkeit einer Regulierung überhaupt verneint: im Unterschied zu den «natürlichen» Monopolen im Bereich von Eisenbahn-, Strom- und Gasnetzen handle es sich bei den neuen, digitalen nur um «serielle Monopole».[15] Beispiele wie die seit über 20 Jahren andauernde Dominanz von Microsoft Windows und Office zeigen jedoch, dass nach einer Phase des Wettbewerbs durchaus gefestigte und hochprofitable Marktführerschaft stehen kann, die wie im Fall von Microsoft diese Position auch durchaus missbraucht.[16]

Aber auch die «Serialität» verschiedener marktbeherrschender Unternehmen bedeutet nicht, dass deshalb deren Dominanz unproblematisch wäre. Auf Grund der beschriebenen Skalen-, Netzwerk- und Koordinationseffekte ist die Wettbewerbsintensität im Plattformbereich klar vermindert. Es bleibt die Herausforderung, dass sich Plattformdominanz sehr rasch herausbilden kann - im Fall von Googles Android-Betriebssystem gerade einmal binnen zwei Jahren. Dagegen schreiten

13 http://governancexborders.com/2014/10/21/algorithm-regulation-9-youtube-and-the-comeback-of-copyright-registration.

14 http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/sigmar-gabriel-konsequenzen-der-google-debatte-12941865.html.

15 Liebowitz S.J./Margolis, S.E. (2001): Winners, Losers & Microsoft. Competition and Antitrust in High Technology. Oakland: Independent Institute.

16 Economides, N. (2001): The Microsoft Antitrust Case. Journal of Industry, Competition and Trade, 1(1), 7-39.

politische Regulierungsprozesse vergleichsweise langsam voran. Auch wenn eine stärkere Regulierung politisch gewollt ist, erweist sich das klassische kartellrechtliche Repertoire von Strafzahlungen und Entflechtungen als vergleichsweise stumpf. So würde eine «Entflechtung» von Facebook oder Google an den Skalen-, Netzwerk- und Koordinationseffekten, die mit den Produkten «Soziales Netzwerk» bzw. «Online-Suche» zwangsläufig verbunden sind, nichts ändern. Strafzahlungen können zwar ein bestimmtes missbräuchliches Verhalten unterbinden, ändern aber strukturell wenig an der marktbeherrschenden Stellung eines Unternehmens. Das Verbot einzelner Nutzungspraktiken wie beispielsweise die Erstellung von Persönlichkeitsprofilen stößt wiederum dort an ihre Grenzen, wo genau mit der Zusammenführung personenbezogener Daten Komfortvorteile für NutzerInnen verbunden sind und diese deshalb weitreichende Einverständniserklärungen abgeben.

So bleibt die Frage, ob neue digitale Plattformen nicht auch neue regulatorische Instrumenten verlangen. Die Forderung von Justizminister Maas, Google zur Offenlegung seiner Suchalgorithmen zu zwingen, könnte ein innovatives Regulierungsinstrument sein. Der Vorschlag verkennt jedoch, dass es sich bei Suchalgorithmen nicht um statische Formeln sondern um kontinuierliche algorithmische Praktiken[17] handelt und dass völlige Algorithmentransparenz mit Funktionalitätseinbußen einher gehen dürfte.

4. Ansatzpunkte für eine Regulierung digitaler Plattformen

Eine wirkungsvolle Regulierung marktbeherrschender Plattformbetreiber erfordert dreierlei: Erstens bedarf es einer flexiblen und weitgehend unabhängigen Regulierungsbehörde für digitale Märkte auf europäischer Ebene, die zweitens mit großer Flexibilität bezüglich konkreter Regulierungsinstrumente ausgestattet wird. Drittens gilt es jene rechtlichen Rahmenbedingungen zu verändern, die Plattformdominanz begünstigen. Ziel muss es sein, die Ursachen einer marktbeherrschenden Stellung, also die Skalen-, Netzwerk- und Koordinationseffekte, möglichst unmittelbar zu verändern.

Im Bereich der Skalen- und Netzwerkeffekte bestünde die Möglichkeit, Plattformbetreiber zur Öffnung ihrer Datenbasis für Drittanbieter zu zwingen. Im Falle von Google würde das bedeuten, nicht den Algorithmus sondern den Suchindex gegen ein behördlich gedeckeltes Nutzungsentgelt für Dritte zu öffnen. Neue Wettbewerber müssten dann nicht erst enorme Summen in den Aufbau eines Index investieren, sondern könnten sich vor allem auf die Entwicklung und Vermarktung alternativer Suchalgorithmen konzentrieren.

Im Bereich softwarebasierter Plattformen wie Microsoft Windows oder Apples iOS könnte die Verpflichtung eingeführt werden, den plattformkonstituierenden Quellcode offen zu legen. Das Beispiel Android darf hier als Beleg gelten, dass zwar auch Open-Source-Plattformen von einzelnen Betreibern - in diesem Fall Google - dominiert werden können, es allerdings für Wettbewerber immer die Möglichkeit von kompatiblen Konkurrenzangeboten gibt - in diesem Fall die Amazon-Fire-Reihe.

Die größte regulatorische Herausforderung stellen wahrscheinlich soziale Netzwerke wie Facebook und in Teilen YouTube dar, die starke direkte Netzwerk-

17 http://governancexborders.com/2013/01/14/algorithm-regulation-4-algorithm-as-a-practice.

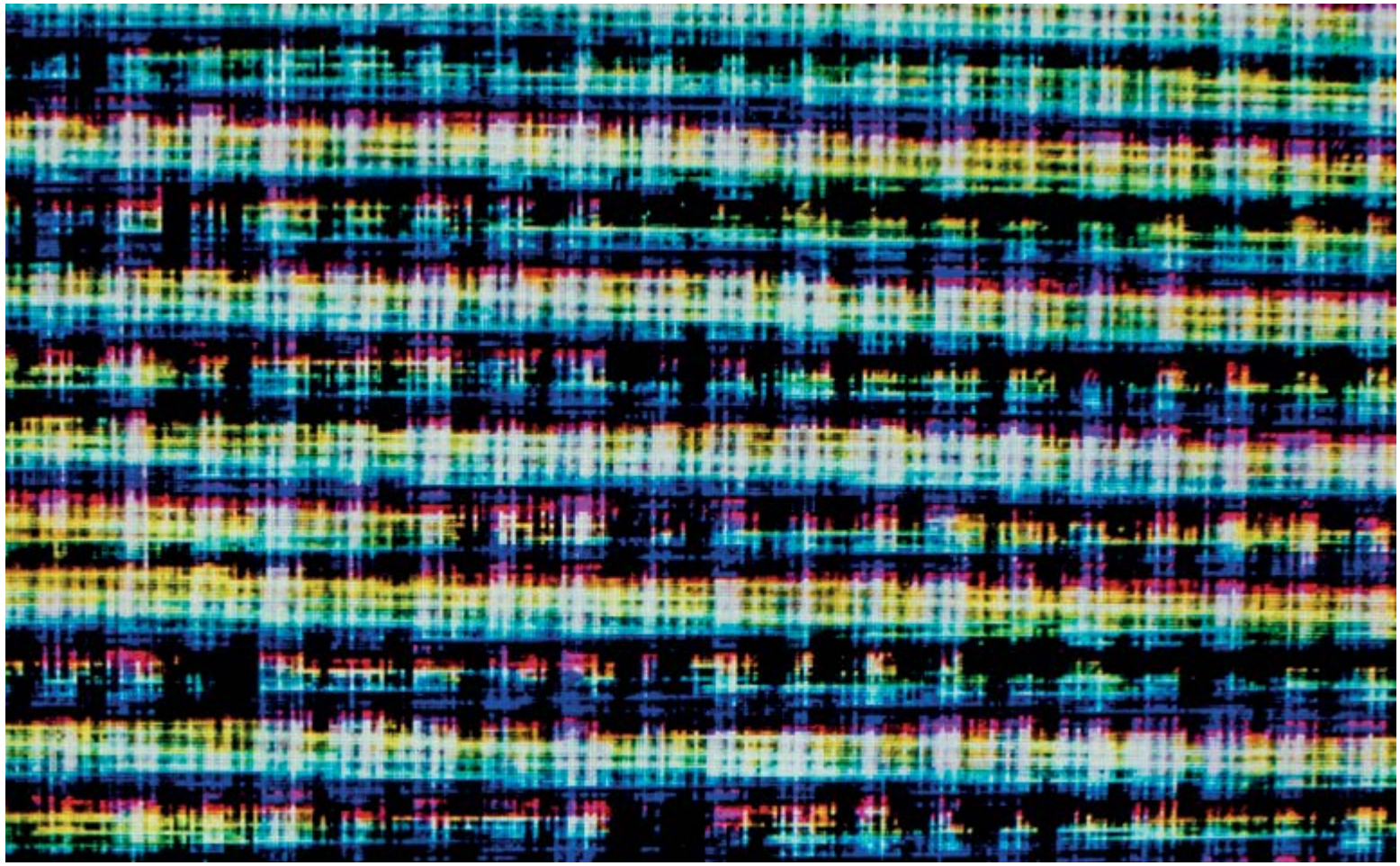
effekte aufweisen. Hier könnte ein Gebot zur Öffnung bestimmter Schnittstellen dafür sorgen, dass bestimmte Funktionalitäten und Dienstleistungen auch durch Drittanbieter erbracht werden können. Im Fall von Facebook wäre es beispielsweise bei einer offenen Schnittstelle auf die eigene Timeline Drittanbietern möglich, eine ungefilterte oder nach anderen Algorithmen gefilterte Timeline anzubieten.

Koordinationseffekte, die vor allem im Fall von Inhalteanbietern wie YouTube oder Amazon eine entscheidende Rolle für die Plattformattraktivität spielen, ließen sich darüber hinaus durch Harmonisierung und Flexibilisierung im Bereich des Urheberrechts reduzieren. Derzeit sind nur große Plattformbetreiber in der Lage, die innereuropäische Vielfalt an rechtlichen Bestimmungen und Ausnahmen zu bewältigen. Ein harmonisiertes einheitliches europäisches Urheberrecht könnte helfen, Koordinationseffekte zu senken. Und wenn für die Verwendung geringfügiger Teile bestehender Werke ähnlich dem Fair-Use-Prinzip des US-Copyrights keine Rechteklärung mehr erforderlich wäre, könnten sie auch außerhalb großer kommerzieller Plattformen risikolos zugänglich gemacht werden. Ähnliches gilt auch für Datenschutzbestimmungen, wobei diesbezüglich der europäische Regulierungsdiskurs bereits weiter fortgeschritten ist.

5. Fazit

Wer die Marktmacht großer Plattformanbieter regulatorisch begrenzen möchte, muss sich mit den Ursachen für deren marktbeherrschende Stellung auseinandersetzen. Erst wenn die steigende Bedeutung von Skalen-, Netzwerk- und Koordinationseffekten in transnational-digitalen Märkten erkannt wird, können innovative Regulierungsinstrumente wirksam gegensteuern. Je nach Plattform sind dafür unterschiedliche Ansatzpunkte maßgeblich. Gemeinsamer Nenner einer wirksamen Regulierung von Plattformen ist aber die Verpflichtung zu größerer Offenheit für die Mitnutzung der Plattformstrukturen und -daten durch kommerzielle und nichtkommerzielle Mitbewerber.

III. Die Herausforderung für Freiheit und Demokratie



ULRIKE ACKERMANN

Digitale Revolution – Eine Herausforderung für die Freiheit

1. Einleitung

Es hat einige Zeit gedauert, bis endlich eine breitere Diskussion über die Chancen und Risiken der digitalen Revolution, ihre Folgen für unser Alltagsleben, für die Demokratie sowie für die politische, wirtschaftliche und vor allem individuelle Freiheit begonnen hat. Die euphorische Begeisterung über das web 2.0 ist inzwischen einem regelrechten Katzenjammer gewichen. Anfangs wurde das Netz als Reich und Instrument der Freiheit gefeiert, entstanden ohne festen Plan, ohne maßgeblichen Eingriff der Regierungen und weltweit genutzt von Bürgern, die mit seiner Hilfe gegen Autokraten aufbegehrten. Es ermöglichte ganz neue Formen der Partizipation und der demokratischen Kontrolle. Der weltweite Zugang und Austausch von Wissen war und ist tatsächlich ein gigantischer, revolutionärer Akt, den die digitalen Technologien möglich machen. Vom Zugewinn individueller Souveränität war die Rede, den das Netz und die damit verbundenen Apparaturen uns bescheren.

Zugleich aber erlaubt diese Technologie eine bisher nicht vorstellbare Anhäufung von Daten über jeden Einzelnen, die auf staatlicher oder privatwirtschaftlicher Seite gesammelt, ausgewertet und für unterschiedlichste Zwecke genutzt werden. Die Debatte über Big Data ist seit den Enthüllungen von Edward Snowden in Sachen NSA kräftig in Gang gekommen. Die Begeisterung einstiger Internet-Pioniere wie Jaron Lanier (USA) oder Sascha Lobo ist längst großer Skepsis und Kritik gewichen. Diese vermählt sich dann zuweilen mit kulturkonservativen Elementen, die in der digitalen Revolution ein die abendländische Kultur zerstörendes Teufelwerk sehen. Schnittflächen damit findet aber auch die Kritik von links, die einen Sieg des Neoliberalismus ausmachen will, der mit seinem ungezügelten Fortschrittswahnsinn, konzentriert im digital-militärischen Komplex die Menschheit in die Hölle treiben würde. Die Skepsis hat aber auch bedächtigere Zeitgenossen so weit getrieben, dass sie wie Hans Magnus Enzensberger dazu raten, das Smartphone zu entsorgen und gegenüber der digitalen Welt die größte nur mögliche Enthaltsamkeit zu üben.

Ist das Internet tatsächlich eine gefährliche Krake, die uns die bisher verteidigte Privatsphäre raubt und die Chancen der Selbstbestimmung schmälert, wie es Kulturkritiker in deutschen Feuilletons befürchten? Oder eröffnet es im Gegenteil ganz neue Möglichkeiten individueller Selbstentfaltung und Freiheitsgewinne für jeden, die wir in diesem Ausmaß bisher überhaupt noch nicht kannten? Wie verändert sich unser Verständnis von und unser Umgang mit Privatheit im Zuge der digitalen Revolution? Wenn sich virtuelle und reale Kommunikation vermischen und vervielfachen, müssen dann neue Spielregeln geschaffen werden? Wie wandeln sich die Strukturen der Öffentlichkeit? Und wie gestaltet sich das Verhältnis von privater und öffentlicher Sphäre neu? Die gesellschaftliche Debatte darüber hat begonnen.

Die Politik allerdings ist bisher von den rasanten Entwicklungen überfordert und hoffnungslos im Nachtrab. Und die Wissenschaft macht sich gerade erst daran zu untersuchen und zu verstehen, wie die digitale Revolution die Parameter unseres alltäglichen Lebens verschiebt und welche Folgen sie für den politischen Raum und die Demokratie zeitigen.

Aus Sicht der Bürger und Nutzer eröffnet die digitale Revolution ungeahnte Ressourcen, die es ermöglichen, den Horizont des alltäglichen, lokal verankerten Lebens aufzubrechen und sich in neuen, selbst gewählten Kontexten zu reflektieren und zu verwirklichen – nie waren die Chancen für «Lebensexperimente» (J. S. Mill) besser als heute. Nutzen die Menschen diese neuen Chancen? Wie verändert dies unsere Sozialbeziehungen? Welche neuen Kulturtechniken des selbstbestimmten Lebens müssen die Menschen womöglich erlernen? Zugleich regt sich bei den Nutzern auch Abwehr gegenüber den medialen Informationsfluten und neuen sozialen Transparenzzwängen, die ihr Privatleben plötzlich kolonialisieren.

2. Privatheit unter Druck

Jedenfalls gerät Privatheit als Hort der individuellen Freiheit im Zuge der digitalen Revolution unter massiven Druck, und zwar von drei Seiten aus:

a) Privatheit unter Druck des Staates

Der Staat, der über seine Bürger so viel wie nur möglich wissen will, um als großer Sozialingenieur zu planen, zu schalten und zu walten: unter anderem für das gute Funktionieren der Sozialsysteme und des Gesundheitswesens und natürlich für die Sicherheit seiner Bürger. Auf der Ebene der Gesetzgebung haben die Eingriffe ins Privatleben zu Gunsten der Sicherheit in den letzten Jahren bereits massiv zugenommen. Die Liste ist lang: Lauschangriff, Online-Durchsuchung, Vorratsdatenspeicherung. Auch wenn der EuGH die EU-Richtlinie dazu gerade verworfen hat, weil sie die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten nicht geachtet habe, hält er an einer maßvollen und abgewogenen Vorratsdatenspeicherung fest. Es gibt aber noch weit mehr Eingriffe wie den Kennzeichen-Abgleich, die Aufweichung des Bankgeheimnisses, Rasterfahndung, Mauterfassungssystem, Volkszählung, Videoüberwachung, Ausgabe von Personenkennziffern, Sammlung von genetischen und biometrischen Daten, Ausweisdokumente mit biometrischen Fotos und genetischen Fingerabdrücken, staatliche Sperrung von Internetseiten sowie die Verwendung privater Tagebuchaufzeichnungen als Prozessindizien und so weiter und so fort. Spätestens seit dem Terroranschlag am 11. September 2001 in New York und Washington sind diese massiven Einschränkungen der Privatsphäre zu beobachten. Sie zeugen von einem längerfristigen Mentalitätswandel weg vom Wert der Freiheit und hin zum Wert der Sicherheit. Doch nicht nur der Staat bringt die Privatsphäre in die Bredouille.

b) Privatheit unter Druck der Internet-Monopolisten

Suchmaschinen, soziale Netzwerke, virtuelle Kaufhäuser wie Google, Facebook, Whatsapp, MySpace, YouTube, Ebay oder Amazon gründen ihr Geschäftsmodell auf der Sammlung, Auswertung und Verkauf der privaten Daten ihrer Nutzer. Zudem

arbeiten sie freiwillig oder unter Zwang mit staatlichen Behörden zusammen, wie nicht zuletzt der Wechsel des Spitzenpersonals zwischen staatlichen Überwachungsdiensten und der Internet-Branche eindrücklich zeigen. Es gelingt den Konzernen mit diesen Datenmengen, individualisierte Profile der Nutzer zu erstellen und ihre Vorlieben, Meinungen und Orientierungen zu erfassen. Diese Erfassung dient einer ausgefeilten Marktforschung zum Zwecke personalisierter Werbung - die bei den jugendlichen Usern zum Teil recht beliebt ist.

c) Privatheit unter Druck der Nutzer

Und hier kommen wir zur dritten Seite, die die Privatsphäre unter Druck setzt: nämlich die User selbst, die bereit sind, für eine Gratis-Nutzung der sozialen Netzwerke und Internet-Dienste ihre persönlichen Daten preiszugeben. Details und Fragmente ihres privaten Lebens sind quasi die Währung, mit der sie die kostenlose Nutzung bezahlen. So etwa auf Timeline, einer Chronik, in der biographische Details des eigenen Lebens in einer Facebook-Rubrik für jedermann einsehbar präsentiert werden, also eine Art öffentliches Tagebuch. Mit dem Like-button, den die User anklicken, hinterlassen sie im Netz Spuren über ihre Vorlieben, bevorzugten Marken, ihren Bücher-, Zeitungs- oder Musikgeschmack oder ihre bevorzugten Filme. In der Zusammenschau der Daten ergibt sich ein recht scharfes Profil der Person, die sich im Netz bewegt. Offensichtlich lockt und verführt das Netz und vor allem die sozialen Netzwerke, sich viel stärker virtuell zu inszenieren und zu präsentieren als in der realen Welt. Das beliebte Versenden der Selfies dokumentiert diesen neuen Exhibitionismus, der zugleich ein Voyeurismus ist. Die öffentliche Inszenierung des Privaten via Webcams ist so vielfältig wie die Akteure selbst. Das eigene Zimmer, ehemals von niemand einsehbarer Rückzugsort wird gleichsam zur Bühne, die die Welt betrachten soll, etwa auf Seiten wie www.zimmerschau.de. Dieser Mentalitätswandel geht mit einer radikalen Veränderung der Kommunikationsgewohnheiten im öffentlichen und privaten Raum einher.

3. Privatheit im liberalen Zeitalter

Um diesen Wandel besser zu verstehen und zu beleuchten, soll daran erinnert werden, was Privatheit und Privatsphäre im analogen Zeitalter, also vor der digitalen Revolution, bedeutet haben. Die klassische Definition lieferten 1890 angesichts neuer technischer Innovationen wie der Fotografie, dem Aufkommen von Tonaufnahmegeräten oder dem Entstehen der Boulevardpresse die beiden amerikanischen Richter Samuel Warren und Louis Brandeis. Sie forderten ein «right to be alone». Es ist ein klares Abwehrrecht, nämlich das Recht, in Ruhe gelassen zu werden, in der eigenen Privatsphäre vor der Einmischung anderer und von sozialer Kontrolle frei zu sein.

a) Grundrechtlicher Schutz

Dieses Prinzip fand Eingang in die unveräußerlichen Grundrechte zum Schutz der Würde des Menschen wie sie in den ersten beiden Artikeln des Grundgesetzes oder etwa in Artikel 12 der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen festgehalten sind. Dort heißt es: «Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beein-

trächtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.» Auch in Artikel 10 des Grundgesetzes zum Brief-, Post- und Fernmeldegeheimnis ist dieses Prinzip kodifiziert. In der Kontroverse um staatliche Überwachungsmaßnahmen hat die Rechtsprechung des Bundesverfassungsgerichts zur Unverletzlichkeit der Wohnung das Grundrecht des Artikels 13 ebenfalls ungewöhnlich ausführlich formuliert. All dies sind Abwehrrechte des Individuums zum Schutz seiner Privatsphäre gegenüber dem Staat. Und spätestens seitdem das Bundesverfassungsgericht im Volkszählungsurteil 1983 das Grundrecht auf «Informationelle Selbstbestimmung» begründet hat, ist der Daten- und Privatsphärenschutz eine Aufgabe, die die Politik verbindlich zu lösen hat. Bereits 1969 hatte das Gericht von der Privatsphäre als einem schützenswerten Innenraum gesprochen, in dem der Bürger «sich selbst besitzt», sich zurückziehen kann, in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt.

b) Vom liberalen Staat zum Wohlfahrtsstaat

Die Trennung zwischen öffentlicher und privater Sphäre verbunden mit der Überzeugung, dass letztere die Basis für individuelle Freiheit und Selbstbestimmung ist, gehört zu den Prämissen des modernen Liberalismus. Die ursprünglich vom Bürgertum erkämpfte Privatsphäre hat sich aber seit Ende des 19. Jahrhunderts aufgrund des Aufstiegs der Massenmedien und der Tendenz der Kommerzialisierung privat-intimer Information erheblich gewandelt. Erst recht steht die Privatsphäre unter Beschuss, seitdem moderne Bürokratien immer ausufernder routinemäßig und massenhaft persönliche Daten der Bürger erheben. Der klassisch liberale Staat kümmerte sich vornehmlich um die physische Sicherheit der Menschen, die Durchsetzung des Vertragsrechts und der Eigentumsrechte und hatte wenig Bedarf, allzu viel über seine Bürger zu wissen. Das lag natürlich auch an den lange nicht vorhandenen technischen Möglichkeiten. Der moderne Wohlfahrtsstaat hingegen, der sich um die Gesundheit, den Wohlstand und die Produktivität der Bevölkerung kümmert, erhebt zu diesem Zweck detaillierteste persönliche Informationen seiner Bürger – zu ihrem Besten versteht sich. Dies ist gewissermaßen der Preis für Sicherheit, Für- und Vorsorge des Staates von der Wiege bis zur Bahre, den er seinen Bürgern abverlangt.

c) Schutz des Kernbereichs der Privatheit

Zugleich können wir über die Jahrzehnte einen Strukturwandel der Information beobachten. Die Revolution der Informationstechnologie hatte in den 1960er und 1970er Jahren weitreichende Folgen für die administrative Handhabung der öffentlichen und privaten Datenerfassung, z. B. in Form der sogenannten Amtshilfe. Das Konzept der Informationellen Selbstbestimmung reagiert dezidiert auf diese Entwicklung, um der Entstehung eines Überwachungsstaats Einhalt zu gebieten. In den letzten Jahren hat das Bundesverfassungsgericht in mehreren seiner Entscheidungen im Kontext des Privatsphärenschutzes immer wieder auf den «unantastbaren Kernbereich privater Lebensgestaltung» gepocht. Privatsphäre ist zu einem Wert geworden, der einen normativen Kern hat. Die Trennung von Privatsphäre und Öffentlichkeit, politischem und wirtschaftlichen Raum ist in diesem Sinne konstitutiv für eine Demokratie, für die Freiheit ihrer Bürger und deren individuelle Entfaltungsmöglichkeiten.

4. Vom Sinn der Privatheit als individuellem Schutzraum

Im geschützten privaten Bereich, jenseits sozialer Kontrolle, jenseits politischer Korrektheit oder wirtschaftlicher Erwägungen und überformender gesellschaftlicher Diskurse lässt es sich frei denken und imaginieren. Es ist ein kreativer Raum, aus dem Kraft und Ideen für die eigene Lebensgestaltung zu schöpfen sind. Ein Raum im übrigen, der erlaubt, jenseits von Konformitätsdruck unabhängige Vorstellungen zu entwickeln, um sie in der Öffentlichkeit und im Widerstreit der Meinungen einzubringen. Der amerikanische Rechtswissenschaftler und Privatsphärenforscher Alan Westin definierte 1967 in seinem Buch «Privacy and Freedom» die Privatsphäre als «den Anspruch von Individuen, für sich selbst zu bestimmen, wann, wie und in welchem Umfang Informationen über sie gegenüber anderen kommuniziert werden.» Westin unterscheidet hierbei vier grundlegende Zwecke, welchen die Privatsphäre dient: (1) Autonomie, (2) emotionaler Ausgleich, (3) Reflexion und (4) beschränkte, das heißt selbst ausgewählte Kommunikation. Privatsphäre markiert zudem einen Lebensbereich, der nicht politisch verantwortet werden muss. Erst dies ermöglicht eine selbstbestimmte Lebensgestaltung und «Lebensexperimente» (J. S. Mill). Alle diese hier skizzierten Funktionen der Privatsphäre, also Autonomie, emotionaler Ausgleich, Reflexion und beschränkte Kommunikation, beruhen auf Vertrauen. Wer sich nicht sicher sein kann, was mit seinen Daten geschieht, so beispielsweise das Bundesverfassungsgericht, der würde sich präventiv konform verhalten. Hier haben wir die Verbindung zwischen dem Konzept der Privatsphäre, der Freiheit und des Gesetzes. Denn nur eine gesetzlich garantierte Privatsphäre kann unter der Bedingung allgegenwärtiger Datenverarbeitung das nötige Vertrauen herstellen, das Voraussetzung für die Autonomie und Freiheit des Individuums, der Bürger ist.

5. Freiheitsgewährleistung durch Trennung zwischen Öffentlichkeit und Privatheit

Für die alten Griechen, denen wir die Anfänge des Rechtsstaats und der Demokratie verdanken, war das staatsbürgerliche Engagement in der Polis der ultimative Horizont menschlicher Tugend; die Person erfüllte sich einzig im Staatsbürger, der sich der Gemeinschaft der Polis zu unterwerfen hatte. Das war die alte politische Freiheit, welche Privatsphäre und die moderne individuelle Freiheit noch nicht kannte. Platons Vorstellung vom Staat gründet in einem Modell der Inklusion: der totale Wächterstaat, der eben nicht die Unterscheidung zwischen Öffentlichkeit und Privatheit und die Möglichkeit des freien Wechsels kennt, sondern die Differenz zwischen privat und öffentlich im Interesse seiner Macht und Herrschaft über seine Bürger nicht zulassen will. Erst über die Jahrhunderte gewann die Idee der Privatheit als Hort der individuellen Freiheit an Bedeutung und wurde hart erkämpft, bis sich allmählich eine Trennung der Sphäre des Öffentlichen von der Sphäre des Privaten durchsetzte. Sie ist bis heute konstitutiv für demokratische Gesellschaften, die immer wieder gegen Anfeindungen verteidigt werden muss. John Stewart Mill schreibt in seinem berühmten Essay «Über die Freiheit» von 1859: «Abgesehen von den besonderen Lehrsätzen individueller Denker ist aber in der Welt überhaupt eine wachsende Neigung zu spüren, die Macht der Gesellschaft über das Einzelne,

sowohl durch die Macht der öffentlichen Meinung wie sogar durch Gesetzgebung, ungebührlich auszudehnen.» Eindrücklich hat er bereits im 19. Jahrhundert ebenso wie sein Zeitgenosse Alexis de Tocqueville vor der Gefahr der sozialen Tyrannei und des Konformismus gewarnt. Angesichts der Lobpreisungen der neuen Kollektive der gegenwärtigen Mediengesellschaft in Gestalt der Internetcommunities ist die Freiheitsschrift von Mill immer noch eine hochaktuelle, zur Skepsis anregende Lektüre.

Die Aufhebung der Trennung von privater und öffentlicher Sphäre ist auch ein Kennzeichen moderner Diktaturen. Die Überwachung der Bevölkerung ist ein wesentliches Herrschaftsinstrument, begleitet von der Politisierung des gesamten sozialen und privaten Lebens. Wenn alles sichtbar wird und transparent sein soll, kontrolliert nicht allein der Staat, auch die gegenseitige soziale Kontrolle wird immens gesteigert und der Gleichschritt im Kollektiv gefördert. Konformität und Uniformität sorgen dann für Ruhe im Land, in dem alles, was abweicht, anders und eigenwillig ist, zugunsten der Stabilität getilgt werden muß.

6. Transparenz – ein trügerisches Versprechen

Im Zuge der digitalen Revolution ist das Wort «Transparenz» zum trügerischen Versprechen geworden: wir haben nun den gläsernen Bürger, aber auch den mit seinen privaten Daten zahlenden gläsernen User und Konsumenten. Inzwischen ist ein allgegenwärtiger Zwang zur Transparenz auszumachen. Und die Neigung zur Selbstdarstellung im Netz liefert der ständigen Dauerbeobachtung Vorschub, so dass Soziale Netzwerke zu «Assessment-Centern der alltäglichen Lebensführung» mutieren. Nicht nur die gegenseitige soziale Kontrolle wächst, sondern auch die Neigung, es den anderen gleichzutun. Es handelt sich also um neuartige Prozesse der Vergemeinschaftung und Kollektivierung, die z. B. Jaron Lanier von einem «Maoismus des Internets» sprechen lassen. Wir haben es also mit einem höchst ambivalenten Prozess zutun: Einerseits können in der Produktion virtueller Identitäten in der sozialen Wirklichkeit der Netz-Gesellschaft spielerisch neue Rollen erprobt, über Raum und Zeit hinweg ein Netzwerk von Bekanntschaften gepflegt und neue soziale Kontakte geknüpft werden. Eine wahrlich grenzenlose Kommunikation ist damit möglich geworden. Andererseits ist mit diesem Gewinn an Kommunikationsfreiheit ein massiver Verlust an Privatheit einhergegangen. Sphären der Privatheit verändern sich und konstituieren sich je nach Kommunikationszusammenhang neu, teilen sich und lösen sich wieder auf. Vom Zeitalter der Post Privacy ist inzwischen schon die Rede – was von Teilen der Netz-Gemeinde ausdrücklich begrüßt (Spackeria).

Der Wandel der Mentalitäten und Verhaltensweisen geht einher mit dem Wandel der Bedeutung von Privatheit. War der Begriff im analogen Zeitalter vornehmlich auf Abgrenzung und Unzugänglichkeit ausgerichtet, so ist Privatheit heute viel stärker an Teilhabe, also Partizipation orientiert. Der Sozialphilosoph Isaiah Berlin hat in seinen «Vier Versuchen über die Freiheit» in Anknüpfung an Immanuel Kant zwischen der negativen und positiven Freiheit unterschieden. Die negative Freiheit ist Freiheit von etwas, Freiheit von Zwang, Freiheit von sozialer Kontrolle. Positive Freiheit meint hingegen die Freiheit zu etwas. Sie verfügt also per se über ein partizipatives, auf Interaktion ausgerichtetes Moment. Es geht also angesichts

der Herausforderungen der digitalen Revolution darum, zwischen negativer Freiheit und den daraus abgeleiteten Schutzrechten des Individuums gegenüber den kollektivierenden Effekten positiver Freiheit und den daraus abgeleiteten Teilhaberechten abzuwägen.

7. Positionen der Parteien zum Datenschutz

Angesichts des NSA-Skandals und anderer staatlicher Überwachungsmethoden, der Datensammelwut der Internet-Monopolisten und der bereitwilligen Preisgabe der Daten auf Seiten der User stellt sich die Frage: brauchen wir mehr Datenschutz, wo ist er angesiedelt und wer setzt ihn durch? Was ist Aufgabe der Politik, des Staates und was ist Angelegenheit der IT-Unternehmen? Was ist demgegenüber Sache der Nutzer und Bürger? Soll der Staat gar die Bürger vor sich selbst schützen?

Das Spannungsverhältnis von starkem Datenschutz und staatlicher Regulierung einerseits sowie schwachem Schutz und Selbstregulierung andererseits war Gegenstand einer Inhalts- und Diskursanalyse der Programme und Verlautbarungen der deutschen Parteien, die wir am J. S. Mill Institut durchgeführt haben. Dafür haben wir acht sogenannte Frames für die Analyse des politischen Diskurses entwickelt. Sie dienen der Messung der Einstellungen auf einer Skala, die von einer positiven Einschätzung des Internets bis zu großer Skepsis gegenüber dem Internet reicht:

(1) Das Internet als Chance, d.h. das Internet und besonders die sozialen Netzwerke sind eine begrüßenswerte Errungenschaft, die es zu sichern gilt,
(2) Eigenverantwortung, d.h. der Nutzer trägt durch umsichtiges Verhalten selbst die Verantwortung für den Schutz seiner Daten und seine Privatsphäre,
(3) Freier Markt, d.h. das Datenschutzproblem löst sich am besten durch die Mechanismen des freien Marktes, d.h. der Selbstregulierung,
(4) Abwägung, d.h. der Schutz der Privatsphäre ist mit anderen gesellschaftlichen Gütern und Interessen in Ausgleich zu bringen,
(5) Problem Wirtschaft, d.h. Anbieter der Netzwerke sind kommerziell orientierte Großunternehmen, welche die Privatsphäre kommerzialisieren,
(6) Politikversagen, d.h. die Politik hat eine Verantwortung zum Schutz der Privatsphäre in Sozialen Netzwerken, der sie bisher nicht gerecht wird,
(7) Individuelle Überforderung, d.h. der Nutzer ist machtlos gegenüber und orientierungslos in dem überkomplexen System und kann sich daher nicht selbst schützen,
(8) Skepsis gegenüber dem Internet, d.h. die Verbreitung von Sozialen Netzwerken geht einher mit erheblichen Risiken, die schwer zu kontrollieren sind.

Unsere Untersuchung hat zu Tage gefördert, dass CDU/CSU und FDP ein optimistisches Narrativ über den digitalen Wandel und dessen großes Potential propagieren, das sich am besten ohne die Einmischung der Politik und neuen Regulierungen entfalten könne. SPD, Grüne und Linkspartei betonen in ihrem Gegennarrativ die Risiken eines unkontrolliert ablaufenden digitalen Wandels. Kern der Debatte ist das Thema Selbstbestimmung und Autonomie. Für die CDU/CSU und FDP steht der selbstbestimmte Nutzer im Vordergrund, der in eigener Verantwortung selbst entscheidet, was er preisgibt. Staatliche Regulierung sei in diesem Felde deshalb unnötig. Zugleich wägen sie zwischen Privatsphäre und anderen Gütern ab: etwa dass Unternehmen aufgrund strenger Datenschutzregeln Deutschland

als Wirtschaftsstandort negativ bewerten könnten. SPD, Grüne und Linkspartei hingegen sehen die Nutzer prinzipiell überfordert und trauen ihnen nicht zu, autonom und eigenverantwortlich ihre Privatsphäre zu schützen. Der politische Streit kreist also darum, wer die Verantwortung für den Schutz der Privatsphäre zu tragen hat: Nutzer, Unternehmer oder der Staat?

Die Vorschläge zur Regulierung reichen denn auch vom Selbstdatenschutz bis zur EU-Regulierung. Pikanterweise verkehren sich die Positionen der Parteilager auf Länderebene in Abhängigkeit davon, ob die politischen Akteure die Regierungs- oder die Oppositionsrolle innehaben. Das hängt schlichtweg damit zusammen, dass Regierende, die ihr Volk lenken und führen wollen, alles tun werden, um so viel wie möglich über ihr Volk in Erfahrung zu bringen. Das ist im Übrigen der Preis, den die Bürger zahlen, wenn ein stark ausgebauter Sozialstaat seine Bürger von der Wiege bis zur Bahre betreut und im Zuge dieser Fürsorge alle verfügbaren Daten erheben will: der Staat als gut informierter Sozialingenieur und oberster Hüter der Sicherheit. Untersuchungen belegen zudem, dass die Chance großflächiger Datenerhebung und –auswertung offenbar Lust auf mehr macht und letztlich eine Ausweitung der Kontrolle zur Folge hat. Für die politischen Akteure heißt: je größer ihre politische Macht und je verwobener diese mit der Verwaltung des Staates ist, desto geringer wird ihre Interesse am Datenschutz der Bürger sein.

8. Mögliche Regelungen zum Schutz der Privatsphäre

Haben die Bürger historisch ihre Freiheitsrechte gegen den Staat erstreiten müssen, so hat sich die Problemlage im Zuge der digitalen Revolution verändert: die Privatsphäre müssen die Bürger nicht nur gegen Übergriffe des Staates, sondern auch gegenüber monopolistischen Großunternehmen wie Google, Facebook etc. verteidigen. Zugleich ist der Staat laut Grundgesetz verpflichtet, die Persönlichkeitsrechte und die Privatsphäre seiner Bürger zu schützen. Da die großen Internetunternehmen seit Jahren propagieren, das Konzept der Privatsphäre sei völlig überholt, stellt sich die Frage, wie der Staat schützend eingreift, um das Recht auf informationelle Selbstbestimmung und Wahlfreiheit zu gewährleisten. Dazu könnten Datenschutzregulierungen zählen wie das Kopplungsverbot von Service und Datenhandel, das die Nutzung von Internetdiensten ohne erzwungene Weitergabe personenbezogener Daten ermöglichen würde. Ein «Recht auf Vergessen» und die Pflicht zur Löschung ist ebenso vorstellbar wie ein Profilbildungsverbot oder zumindest wirksame «Opt-in»- und «Opt-out»-Regelungen. Auch liegt es im Aufgabenfeld des Staates, für mehr Wettbewerb zu sorgen. Zudem würde die rechtliche Einklagbarkeit von Datenschutzstandards, deren Verletzungen mit Gewinn abschöpfenden Sanktionen belegt wären, die Position der Nutzer gegenüber den Anbietern erheblich stärken. Wirksamer Datenschutz hätte zudem auch noch eine einhegende Wirkung auf den Staat selbst.

Beim Datenschutz handelt es sich also um ein Anliegen und zugleich eine große aktuelle Herausforderung des Liberalismus. Mehr Datenschutz vom Staat zu fordern, bedeutet in diesem Fall gerade nicht, die Bürger in paternalistischer Manier zu entmündigen, sondern mit dem Schutz ihrer Privatsphäre jenen Raum zu sichern, der die Möglichkeit bietet für Selbstbestimmung und Autonomie jedes Einzelnen.

9. Der Kampf um die EU-Datenschutzregulierungen

Sinnvoll ist es in jedem Fall, Datenschutzstandards auf europäischer Ebene einzuführen. Die Kommission hat 2012 eine EU-Datenschutzgrundverordnung vorgelegt, über die in sogenannten Trilog-Verhandlungen zwischen Parlament, Kommission und Rat Einigkeit hergestellt werden muss. Zunächst muss sich jedoch noch der Ministerrat einigen. Gegenstand der Verhandlungen sind: das Recht auf Vergessen, ein leichterer Zugang zu den eigenen Daten, Einwilligung in Datenverarbeitung und Widerspruchsrecht, die Pflicht, Nutzer innerhalb von 24 Stunden über Datenverlust zu informieren, «Privacy by design» und «Privacy by default» (d.h. technische Lösungen zum Schutz gegen Unbekannte oder Hacker bzw. restriktive Voreinstellungen der Unternehmen für den Schutz der Privatsphäre, z.B. keine automatische Einwilligung) oder die Einrichtung einer europaweiten Ansprechstelle für Nutzer.

Das Parlament hat folgende Änderungen vorgenommen: Aus dem Recht auf Vergessen wird ein weniger scharfes Löschungsrecht. Die Datenweitergabe an Drittstaaten wird nur auf der Grundlage von EU-Recht erlaubt. Sanktionen gegen Datenverstöße wurden verschärft (bis zu 5% des Unternehmensumsatzes statt 2%). Eine implizite Einwilligung durch Nutzung soll nicht mehr genügen. Die Transparenzpflicht wird zur Unterbindung versteckter Klauseln verschärft. Eine Profilbildung wird durch Anforderungen an Zweckbindung der Daten und Einwilligungen beschränkt. Die 24-Stunden-Frist wird gestrichen. Nationale und europaweite Ansprechstelle werden verzahnt. Die einheitliche europäische Datenschutzbehörde soll unabhängiger werden und mehr Einfluss erhalten.

In den Verhandlungen in Brüssel im Ministerrat orientieren sich Beamte des deutschen Innenministeriums offensichtlich an einer Minderheitsposition im juristischen Diskurs. Vertreten wird sie u.a. von Jochen Schneider, Ausschussvorsitzender zum Informationsrecht im Deutschen Anwaltsverein. Das Recht auf informationelle Selbstbestimmung in der digitalen Ökonomie sei ein «Hemmnis für modernen Datenschutz». Das «Verbot der Datenverarbeitung» käme einem «Verbot der Kommunikation» gleich. Die Argumentation verweist auf das Spannungsverhältnis von Privatsphäre und Meinungsfreiheit, will den Konflikt aber zugunsten der Meinungsfreiheit auflösen und den Schutz der persönlichen Daten damit unterlaufen. So hat im übrigen auch schon mehrfach Google im Hinblick auf die Nutzer argumentiert. Vergleichbares hört man auch in der Debatte um Urheber- und Leistungsschutzrechte der Zeitungsverlage. Wenn diese Haltung die deutsche Verhandlungsposition in Brüssel bestimmt, nimmt es nicht Wunder, dass die Verhandlungen zugunsten eines strengeren europäischen Datenschutzes im Ministerrat stocken.

Auch der im EU-Parlament zuständige Verhandlungsführer für die neue EU-Datenschutzgrundverordnung, Jan Philipp Albrecht, wirft der Bundesregierung in seinem gerade erscheinenden Buch «Finger weg von unseren Daten! Wie wir entmündigt werden» vor, mit «verdeckten Karten ein falsches Spiel» zu spielen und «wahrheitswidrig» behauptet zu haben, die EU-Datenschutzverordnung würde das deutsche Datenschutzniveau absenken. Sie möchte den Bereich behördlicher Datenverarbeitung von der neuen EU-Regelung ausnehmen, aber wohl weniger, weil dies das Schutzniveau in Deutschland gesenkt, sondern eher gehoben hätte;

schließlich sind auch Behörden in den Datenaustausch und -handel involviert. Die Bundesregierung hätte sich auch gegen das Prinzip des «Erlaubnisvorbehalts» ausgesprochen, das seit 30 Jahren eine verfassungsrechtlich abgesicherte Grundlage des Privatsphärenschutzes sei. Die deutsche Strategie sei eine Art Marktliberalisierung gekoppelt mit nebulösen Selbstregulierungspflichten. In internen Beratungen hätten deutsche Beamte angegeben, dass «den Menschen in Deutschland der Datenschutz gar nicht mehr so wichtig sei». Außerdem wirft Albrecht der Bundesregierung vor, die eigenen Ministerien und den Bundestag «absolut ungenügend» eingebunden zu haben.

In unserem diesjährigen Freiheitsindex 2014, den das John-Stewart-Mill-Institut alljährlich erhebt, ist das Internet und das Verhältnis der Bürger zu den Folgen der digitalen Revolution Schwerpunktthema. Wir wollen mit dessen Ergebnissen dazu beitragen, Kriterien für eine digitale Selbstbestimmung zu entwickeln, die die individuelle Freiheit und Privatsphäre schützen, jedoch ohne sie einem staatlichen oder wirtschaftlichen Paternalismus zu unterwerfen. Erforderlich ist dazu nicht nur eine Verbesserung des Datenschutzes, sondern auch Elemente des Nutzerselbstschutzes. Mit einer Abkehr vom Gratisprinzip wäre etwa zu vermeiden, dass private Daten umstandslos als Zahlungsmittel dienen.

10. Schluss

Es gibt natürlich noch viele Aspekte der digitalen Revolution, auf die ich hier aus Zeitgründen nicht weiter eingehen kann: etwa die völlige Umwandlung der Medienlandschaft, also ein gigantischer Zugewinn an Foren der politischen Meinungsbildung, zugleich aber die Fragmentierung des öffentlichen Diskurses und der Verlust der Deutungshoheit etablierter Medien. Erfüllt sich in diesen Entwicklungen die liberale Hoffnung einer Optimierung der Politik nach den Maßstäben von Vernunft und demokratischer Kontrolle? Wie viel Transparenz und Partizipation sind gut? Wie verträgt sich das Strukturprinzip des Internets mit den Strukturen unserer modernen Repräsentativdemokratie? Wie verändern sich das Verständnis und die Bedeutung von Privateigentum, insbesondere im Hinblick auf das geistige Eigentum und die Frage der Urheberschaft?

Es wird in Zukunft vor allem darum gehen, die Wahrnehmung und das Bewusstsein für die Möglichkeit digitaler Selbstbestimmung und Mündigkeit zu schärfen: auf Seiten der Nutzer des Internets, also den Bürgern, ebenso wie bei den politischen Entscheidungsträgern und wirtschaftlichen Akteuren. Der immense Strukturwandel im Verhältnis von Öffentlichkeit und Privatheit im Zuge der digitalen Revolution verändert unser Alltagshandeln, Selbstverständnis und unsere Mentalitäten grundlegend und rasant. Die Analyse und Deutung dieser Wandlungsprozesse wird weiterhin im Fokus unserer Forschung stehen. Es geht nicht zuletzt darum, ob diese revolutionären Entwicklungen uns einen Zugewinn an Freiheit bescheren oder bisherige Freiräume und Handlungsoptionen einschränken. In jedem Fall liegt es im Ermessen unserer jeweiligen individuellen Freiheit, wie wir uns im Internet bewegen. Über Regeln, die diese Freiheit auch unter den sich ständig verändernden Bedingungen schützen, müssen wir uns immer wieder neu verständigen.

Literatur

Ulrike Ackermann, *Eros der Freiheit, Plädoyer für eine radikale Aufklärung,* Stuttgart 2008.

Jan Philipp Albrecht, *Finger weg von unseren Daten! Wie wir entmündigt werden,* München 2014.

Isaiah Berlin, *Vier Versuche über die Freiheit,* Frankfurt 1995.

Byung-Chul Han, *Transparenzgesellschaft,* Berlin 2012.

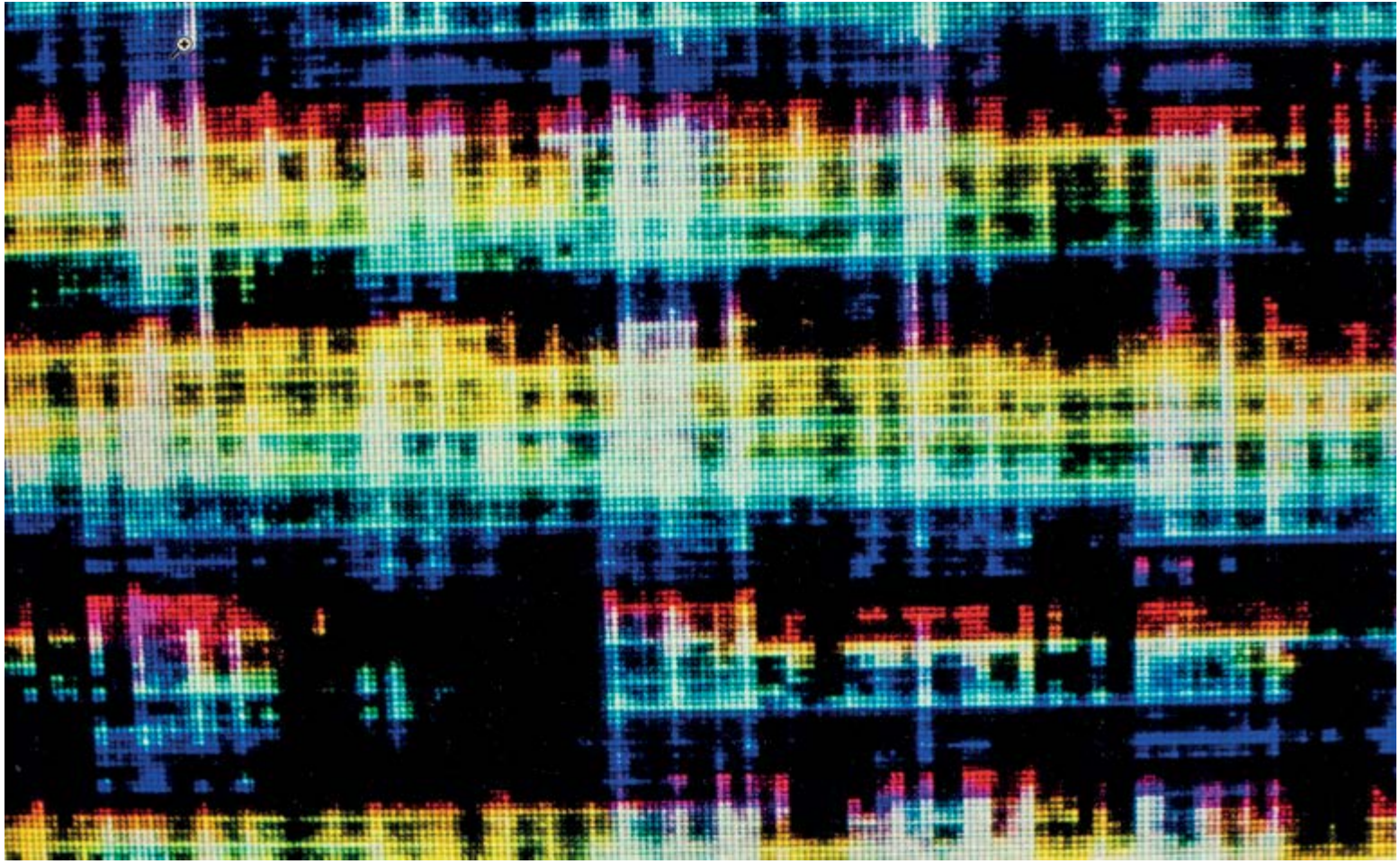
Uwe Ebbinghaus, Stefan Schulz, Thomas Thiel, *Machtprobe mit dem Silicon Valley,* Frankfurter Allgemeine Zeitung vom 12.3.2014.

Jaron Lanier, *Warum die Zukunft uns noch braucht,* Berlin 2012.

John Stewart Mill, *Über die Freiheit,* 1859.

Samuel Warren/ Louis Brandeis, *The Right to Privacy,* in: Harvard Law Review 4/5, 1890, S.193-222.

Alan Westin, *Privacy and Freedom,* New York 1970.



MARION ALBERS

Zukunftsszenarien polizeilicher Überwachung

Dieser Beitrag erörtert aus rechtlicher Perspektive die Überwachung durch Sicherheitsbehörden und hier vor allem durch Polizeien. Einige Schlagworte sind in der Öffentlichkeit bekannt: zunehmende Ausweitung der Ermittlungsmethoden wie etwa der Videoüberwachung, Internet-Aufklärung oder Online-Durchsuchungen, eine zunehmende Vernetzung der Sicherheitsbehörden unter anderem durch Gemeinsame Dateien wie die Anti-Terror-Datei und nicht zuletzt der NSA-Skandal.

Im ersten Abschnitt soll ein übergreifender Rahmen geschaffen werden. Denn technische Möglichkeiten aufgrund der Digitalisierung oder des Internets liefern keine ausreichende Erklärung für die Veränderungen sicherheitsbehördlicher Ermittlungs-, Datenverarbeitungs- oder Datenaustauschformen. Die Genese und der Einsatz von Techniken sind ebenso wie die Nutzung des Internets immer auch in soziale Zusammenhänge eingebettet. Daher ist die Erläuterung der übergreifenden Sicherheitsarchitektur notwendig, die den Kontext für polizeiliche oder nachrichtendienstliche Aktivitäten liefert und die sich von den überkommenen Mustern der Gefahrenabwehr einerseits und der Strafverfolgung andererseits längst gelöst hat. Diese neue Sicherheitsarchitektur ist zugleich der Hintergrund für die im zweiten Abschnitt thematisierten Zukunftsszenarien. Der Fokus richtet sich hierbei auf neue polizeiliche Konzepte wie die prädiktive Polizeiarbeit, auf neue technikermöglichte Ermittlungsmethoden sowie die Verknüpfung so erlangter Daten, auf technikgestützte Vernetzungen der Sicherheitsbehörden und auf die globalisierte Überwachung. Mit all dem steht eine freiheits- und menschenrechtsorientierte Regulierung vor erheblichen Herausforderungen.

I. Wandel der Sicherheitsarchitektur

Die überkommene Sicherheitsarchitektur unterliegt seit den 1970er Jahren einem grundlegenden, nachhaltigen und dynamisch fortschreitenden Wandel. Die wesentlichen Stichworte lauten: Prävention wird zur Leitidee. Polizeiliche Kompetenzen werden in das Vorfeld der Gefahrenabwehr und der Strafverfolgung ausgedehnt; qualitativ neue Ermittlungsmethoden erweitern das bisherige Instrumentarium. Im föderalen System werden die Bundespolizeien mehr und mehr ausgebaut. Neben dem Bundes- und dem Zollkriminalamt entwickeln sich die Nachrichtendienste zu «Informationsschaltstellen» im Netzwerk der Sicherheitsbehörden. All dies führt dazu, dass die inhaltlichen und organisatorischen Differenzierungen, die das rechtsstaatliche Markenzeichen der überkommenen Sicherheitsarchitektur waren, jedenfalls nicht mehr in der traditionellen Form existieren und neue freiheitssichernde Muster benötigt werden.

1. Bausteine der traditionell-rechtsstaatlichen Sicherheitskonzeption

Die traditionellen rechtsstaatlichen Sicherheitskonzeptionen, hinter denen das bürgerlich-liberale Gesellschaftsmodell mit seinen Charakteristika und Grenzen steht, bauen darauf auf, dass Aufgaben und Institutionen inhaltlich und organisatorisch differenziert und zugleich eingegrenzt werden. Für die Gefahrenabwehr sind neben den Ordnungsbehörden prinzipiell die Polizeien der Länder zuständig. Die Aufgabe richtet sich auf die Abwehr von Schäden für die Integrität der Rechtsordnung und individueller Rechtsgüter. Polizeiliches Handeln setzt Gefahrensituationen voraus. Diese liegen nur vor, wenn hinreichende Tatsachen und Kausalitätserfahrungen den Schluss erlauben, dass bei ungehindertem Fortlauf Schäden entstehen. Aus Prognosesicherheits- und Effektivitätsgründen werden die Eingriffs- und Abwehrmaßnahmen zeitlich so nah wie möglich an den befürchteten Schadenseintritt herangerückt. Personen sind nach Verantwortlichkeitskriterien in Anspruch zu nehmen, also beispielsweise, weil ihr Verhalten die Gefahr verursacht. Jemand, der nicht verantwortlich ist, darf nach der traditionellen Konzeption nur unter sehr engen Voraussetzungen mit polizeilichen Maßnahmen belastet werden.

Die Strafverfolgung obliegt demgegenüber der Staatsanwaltschaft, der die Polizei als Hilfsorgan untergeordnet ist, sowie – nach Anklageerhebung – den Strafgerichten. Im Fokus stehen nicht künftige Gefahren, sondern Sanktionen für in der Vergangenheit begangene Straftaten. Die Einleitung eines Ermittlungsverfahrens setzt den Anfangsverdacht einer begangenen oder begonnenen Straftat voraus, also eine konkrete Tatsachenbasis, die den Schluss erlaubt, dass eine Straftat stattgefunden hat. Die Ermittlungsmaßnahmen sind auf eine konkrete Straftat bezogen, für die ein Anfangsverdacht bestehen muss. Verdächtige müssen eingriffsintensivere Maßnahmen dulden als bloße Zeugen.

Den Nachrichtendiensten, also den Ämtern für Verfassungsschutz, dem Militärischen Abschirmdienst und dem Bundesnachrichtendienst, sind Informationsaufgaben im Hinblick auf den Schutz der freiheitlich-demokratischen Grundordnung, die Sicherheit der Streitkräfte oder die außen- und sicherheitspolitischen Interessen der Bundesrepublik zugewiesen. Diese Behörden greifen nicht selbst in relevante Geschehen ein. Sie sind nach der überkommenen Konzeption auf die Aufgabe der Information der Bundes- oder der Landesregierungen beschränkt, die eher als übergreifend-generalisierte Wissensvermittlung ausgestaltet war. Vor diesem Hintergrund sah man weitreichende Ermittlungs-, Datenerhebungs- und Datenverarbeitungsbefugnisse der Nachrichtendienste als gerechtfertigt an: die Einschreitschwellen waren niedrig, eine Überwachung von Personen im Umfeld der für relevant erachteten Aktivitäten möglich und Instrumente der heimlichen Datenbeschaffung üblich. Deswegen wurden Nachrichtendienste vormals scharf gegen Polizei und Staatsanwaltschaft abgegrenzt.

2. Die Karriere der Prävention

Diese durch inhaltliche und institutionelle Differenzierungen, durch Einschreitschwellen wie Gefahr und Verdacht sowie durch eine begrenzte Inanspruchnahme der Bürger und Bürgerinnen gekennzeichnete Sicherheitsarchitektur hat sich inzwischen deutlich verändert. Dazu hat die Veränderung der Kriminalitätsformen beige-

tragen. Beispiele hierfür sind der Terrorismus der 1970er Jahre oder die organisierte Kriminalität mit ihren übergreifend-langfristigen, Legalität und Illegalität verflechtenden Zielen und Organisationsstrukturen. Überdies erscheinen Gefahren in der «Risikogesellschaft» nicht mehr als naturgegeben, sondern als Folge mangelnder Vorsorge. Prävention, also das «Zuvor-Kommen», wird zur Leitidee. Sie zielt darauf, absehbare oder auch nur denkbare Schäden und Gefahrenlagen bereits an deren Quellen zu verhindern. Sie setzt anders als die Gefahrenabwehr nicht mehr so spät, sondern so früh wie möglich an. Niemand hat diese Leitidee für die Polizei deutlicher formuliert als Horst Herold, der ehemalige Präsident des Bundeskriminalamts, der vor dem Hintergrund der Verwissenschaftlichung der Polizeiarbeit und der beginnenden elektronischen Datenverarbeitung die Vision eines Systems hatte, «das befähigt, Problemen zuvorzukommen, bevor sie zutage treten, erst recht, bevor sie bedrohlich werden».[1]

Prävention hat Vorteile, aber auch Nachteile. Negative Folgen resultieren daraus, dass sich die alten für Gefahrenabwehr und Strafverfolgung begründeten Einschreitschwellen auflösen.[2] Das Präventionsinstrumentarium ist wegen der zahlreichen Gefahrenquellen breit gefächert; Einschreitschwellen werden unter Umständen weit vorverlagert. Es erscheint legitimierbar, dass Bürger und Bürgerinnen auch dann Überwachungen, Inpflichtnahmen, Einflussnahmen oder Risikobeurteilungen hinnehmen müssen, wenn sie selbst dafür keinen Anlass gegeben haben.[3] Prävention birgt eine Dynamik: Sie lässt sich immer noch erweitern, immer weiter vorverlagern und immer weiter verbessern. Zumindest als Prinzip kennt sie keine immanenten sachlichen, personellen, räumlichen oder zeitlichen Grenzen.

3. Die Praxis der Polizei

Die Praxis der Polizei hat die Idee der frühzeitig ansetzenden Kriminalprävention recht schnell aufgegriffen und «operative» Konzepte forciert. Die operative Betrachtung stellt Überlegungen und Ziele in den Mittelpunkt, die über die einzelne Situation, die Abwehr einer konkreten Gefahr oder die Aufklärung eines konkreten Verdachts, hinausgehen. Gerade im Bereich der organisierten Kriminalität, so ist das operative Konzept erläutert worden, komme es nicht darauf an, einige bestimmte Taten beweiskräftig zwecks Strafverfolgung festzustellen oder einige weitere Straftaten präventiv zu verhindern. Wichtig sei vielmehr die umfassende Unterbindung der Aktivitäten einer kriminellen Organisation. Ansatzpunkt ist daher nicht eine Einzelfallaufklärung, sondern die Aufdeckung übergreifender Zusammenhänge und krimineller Strukturen. Man führt – im Sinne einer «network-detection» – Erkenntnisse nicht nur täter-, sondern auch milieu-, umfeld- und kontaktbezogen zusammen und versucht, Querverbindungen zu erkennen. Das erfordert «proaktive» Vorfeldermittlungen und heimliche Ermittlungsmethoden ebenso wie die umfassende Sammlung und mehrdimensionale Auswertung von Informationen und Daten zu organisations- oder milieubezogenen Ermittlungsergebnissen, zu übergreifenden

1 Herold (1972): 134 (Hervorh. im Orig.).

2 Ausführlich zum «Präventionsdilemma» Albers (2012).

3 Näher dazu Grimm (1991): 198 ff. Für das Recht der inneren Sicherheit Huster/ Rudolph (2008): 17 ff.

Strukturanalysen oder zu Lagebildern. Dies ähnelt den Arbeitsweisen der Nachrichtendienste, die ihrerseits aufgrund einer Vielzahl gesammelter Erkenntnisse strukturelle Analysen oder Lagebilder erarbeiten, in denen einzelne Daten oder Ereignisse als Mosaikstein erscheinen, vielfältig verwendet und immer wieder neu bewertet werden. Mit solchen Ansätzen hat sich die polizeiliche Tätigkeit von dem traditionellen Konzept der differenzierten Wahrnehmung der Aufgaben Gefahrenabwehr, Strafverfolgung oder nachrichtendienstliche Information der Regierungen entfernt, in das Vorfeld von Gefahren oder Straftatverdachtslagen ausgegriffen und Methoden eingesetzt, die zuvor allein die nachrichtendienstlichen Tätigkeiten kennzeichneten.

4. Gesetzliche Gestaltung der neuen Sicherheitsarchitektur

Nicht zuletzt vor dem Hintergrund dieser polizeilichen Praxis sind seit den 1980er Jahren alle Polizeigesetze und die Strafprozessordnung fundamental verändert worden.[4] Institutionell hat die Polizei an Bedeutung gewonnen, insbesondere gegenüber der im Strafverfolgungsbereich eigentlich leitenden Staatsanwaltschaft. Neben Gefahrenabwehr und Strafverfolgung sind die Straftatenverhütung und die Verfolgungsvorsorge als neue Aufgaben gesetzlich verankert worden. Die Straftatenverhütung deckt das relativ unbestimmte und weit reichende Vorfeld von Gefahren, die Verfolgungsvorsorge für die Straftatenverfolgung das Vorfeld des Verdachts ab. In diesem Vorfeld sind Ermittlungen unterhalb der Gefahrenschwelle, Maßnahmen ohne Vorliegen eines Straftatverdachts, die Sammlung von Daten über Personen, bei denen man erwartet, dass sie künftig Straftaten begehen werden, Analysen struktureller Zusammenhänge einer «kriminellen Szene» oder die Erarbeitung übergreifender Lagebilder möglich. Dies wird um Vorverlagerungen des materiellen Strafrechts ergänzt: Insbesondere im Bereich organisierter oder terroristischer Kriminalität stehen mittlerweile auch die Vorbereitungs-, Unterstützungs- oder Organisationshandlungen im Vorfeld der eigentlichen Rechtsgutverletzung unter Strafe.

Konsequenterweise sind in allen Polizeigesetzen und in der Strafprozessordnung im Laufe der Zeit die Ermittlungs- und Datenverarbeitungsermächtigungen deutlich erweitert worden. Die neuen Ermittlungsmethoden spiegeln häufig die neuen technischen Möglichkeiten wider. Oft funktioniert dies im Wege einer Massendatenerfassung mit entsprechend hohe Streubreite, d. h. viele unbeteiligte Personen werden miterfasst. Die Maßnahmen reichen von der Raster- und Schleierfahndung über die Videoüberwachung öffentlicher Räume und die akustische oder optische Überwachung von Wohnräumen, die automatische Kennzeichenerfassung oder die Ausschreibung zur polizeilichen Beobachtung bis hin zur Telekommunikations- und Internet-Überwachung. Gerade dieser letzte Bereich ist für Ermittlungen eine sehr ergiebige Quelle und wird zunehmend ausgebaut. Unter bestimmten Voraussetzungen zulässig sind etwa die Erhebung von Telekommunikationsverkehrs- und -nutzungsdaten, die Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten, der verdeckte Eingriff in informationstechnische Systeme (sog. Online-Durchsuchung) oder die Internet-Aufklärung etwa in sozialen Netzwerken. In seiner berühmten Entscheidung zur Online-Durchsuchung hat das Bundesverfassungsgericht an diese zwar hohe, an die Internet-Aufklärung jedoch denkbar niedrige

4 Ausführlich Albers (2001): 97 ff.

Anforderungen gestellt. Die insgesamt nicht überzeugende Begründung lautete unter anderem, dass man im Internet ohnehin kein Vertrauen in die Authentizität seines Kommunikationspartners haben dürfe.[5] Allgemein bekannt ist außerdem die Diskussion um die Vorratsdatenspeicherung: Provider und Diensteanbieter sollen die Verkehrsdaten länger als für ihre Zwecke erforderlich speichern, damit Sicherheitsbehörden unter bestimmten Voraussetzungen darauf zugreifen können. Die Vorratsdatenspeicherung ist auch ein Beispiel für das zunehmende Zusammenspiel von Datensammlungen Privater und staatlichen Zugriffen. Die jeweiligen gesetzlichen Ermittlungsermächtigungen sind also zahlreich. Sie haben allerdings recht differenzierte Voraussetzungen, manchmal auch deshalb, weil das Bundesverfassungsgericht entsprechende Anforderungen aufgestellt hat.

Im Rahmen des Wandels der Sicherheitsarchitektur haben sich darüber hinaus die Datenverarbeitungs- und Datenaustauschmöglichkeiten stark erweitert und verändert. Obwohl sie mindestens genauso wichtig sind wie die Ermittlungsmethoden oder die Datenerhebungsmöglichkeiten, werden sie in den öffentlichen Debatten ebenso wie bei der Regulierung vernachlässigt. Die rechtlichen Grundlagen sind hier oft unangemessen generalisierend, vage und weit gefasst. Demgegenüber kommt es entscheidend darauf an, in welche Zusammenhänge erhobene Daten gestellt werden, wie sie verändert und verknüpft werden, welche Informationen aus ihnen gewonnen werden, wie sie bewertet werden und an welche Stelle sie weiter übermittelt und dann neu verarbeitet werden. Dies wird im Zuge der Digitalisierung der Kommunikation und der Vernetzung der Sicherheitsbehörden noch deutlicher, und künftig müssen die Datenflüsse, -veränderungen und -verknüpfungen sowie die daraus resultierende Informations- und Wissenserzeugung in bestimmten Kontexten angemessene Aufmerksamkeit erhalten.

Die neue Rolle der Polizeien wird durch die Stärkung der Bundespolizeien mitbestimmt. Das Bundeskriminalamt, das zu Beginn seiner Tätigkeit als eine vorwiegend Informationen sammelnde und auswertende Serviceeinrichtung für die Länderpolizeien verstanden wurde, wird mit seinem heutigen Organisations- und Aufgabenprofil als eine multifunktionale «Intelligence-Behörde»[6] bezeichnet. Es fungiert als Zentralstelle, die Daten sammelt und auswertet, zentrale Dateien und Informationssysteme betreibt und auch darüber hinaus «kriminalistische Expertise» bündelt. Zudem ist es Schaltstelle für die internationale Zusammenarbeit. Seine Rolle wird weiter durch die Aufgaben auf dem Gebiet der Strafverfolgung in bestimmten Kriminalitätsbereichen und durch die präventiven Aufgaben bei der Bekämpfung des internationalen Terrorismus geprägt. Aus dem früheren Bundesgrenzschutz ist die Bundespolizei mit einer gewissen Aufgabenvielfalt geworden. Eine erhebliche Bedeutung hat inzwischen auch der Zoll. Vor dem Hintergrund der mit dem grenzüberschreitenden Warenverkehr vermittelten strategischen Position sind den Zollbehörden Aufgaben etwa im Bereich des illegalen Technologie- oder Waffentransfers, des Rauschgifthandels, der Geldwäsche und der Terrorismusfinanzierung zugewiesen worden. Zollfahndungsämtern und dem Zollkriminalamt stehen weitreichende Datenerhebungs- und -verarbeitungsbefugnisse zu. In der Vernetzung der Sicherheitsbehörden spielt der Zoll ebenfalls eine prominente Rolle.

5 BVerfG, Urt. vom 27.02.2008, 1 BvR 370/07: Rn. 311.

6 Abbühl (2010): 353 ff.

Nachrichtendienste treten zu diesem Bild nicht nur deshalb hinzu, weil es zwischen Nachrichtendiensten und Polizeien zunehmende Aufgabenüberschneidungen gibt, unter anderem wegen des Ausbaus der Staatsschutzdelikte. Maßgebliche Veränderungen bewirken die wachsenden Formen institutionalisierter informationeller Zusammenarbeit. Über ihre klassische Rolle der Regierungsinformation hinaus sind auch die Nachrichtendienste mittlerweile zu «Informationsschaltstellen» im Verbund der Sicherheitsbehörden geworden.

5. Die gegenwärtige Sicherheitsarchitektur als Basis von Zukunftsszenarien

Im Sicherheitsrecht haben sich die traditionell-rechtsstaatlichen Differenzierungen von Aufgaben und Institutionen ebenso relativiert wie die durch Gefahr oder Verdacht markierten Grenzen für sicherheitsbehördliche Eingriffe und die Inanspruchnahme von Personen. Gefahrenabwehr und Strafverfolgung sind um die deutlich weiter ausgreifenden Aufgaben der Straftatenverhütung und die Strafverfolgungsvorsorge ergänzt, das materielle Strafrecht ist um Vorbereitungs- und Organisationsdelikte erweitert worden. Unter bestimmten rechtlichen Voraussetzungen sind Vorfeldermittlungen ohne Gefahrenlage, die Verdachtsgewinnung im Vorfeld eines Straftatverdachts, der Einsatz zahlreicher heimlicher Ermittlungsmethoden, die Sammlung von Daten über potenzielle künftige Straftäter, die Inanspruchnahme Unbeteiligter, Analysen struktureller Zusammenhänge zwischen erfassten Personen oder die Erarbeitung übergreifender Lagebilder zulässig und Bestandteil polizeilicher Praxis. Institutionell ist die «Polizei» heute ein Netzwerk von Länder- und zunehmend ausgebauten Bundespolizeien. Mehr und mehr hat man insgesamt mit sicherheitsbehördlichen Netzwerken zu tun, in die Polizeien, andere Behörden mit Ordnungsaufgaben und vor allem auch die Nachrichtendienste eingebettet sind. Diese Sicherheitsarchitektur ist inzwischen weitgehend verfestigt. Sie bietet den Hintergrund für Zukunftsszenarien. Dabei sind die Digitalisierung ebenso wie die Internetvermitteltheit der Kommunikation entscheidende Faktoren.

II. Zukunftsszenarien

Die in diesem Abschnitt im Mittelpunkt stehenden Szenarien sind zum Teil bereits eingeleitet und werden die Zukunft der Sicherheitsbehörden prägen. Die Aufmerksamkeit gilt neuen polizeilichen Konzepten wie der «prädiktiven Polizeiarbeit», neuen technikermöglichten Ermittlungs-, Verknüpfungs- sowie Auswertungsmethoden, technikgestützten Vernetzungen der Sicherheitsbehörden und der globalisierten Überwachung.

1. Neue polizeiliche Konzepte, insbesondere: prädiktive Polizeiarbeit

Prädiktive, also die vorhersagende Polizeiarbeit umreißt als aktuelles Stichwort neue polizeiliche Konzeptionen, die Präventionsstrategien in Gestalt einer weit vorverlagerten Prognose kriminalitätsrelevanter Ereignisse weitertreiben. Das sich in den USA bereits verbreitende «predictive policing»[7] wird derzeit in Deutschland aufgegriffen und diskutiert.[8] Mehr noch als bei der im Kern handlungsorientierten Prävention der vergangenen Jahrzehnte richtet sich dabei der Blick auf Datenverarbeitungs-, Datenanalyse- und Wissensgewinnungsinstrumentarien, die mit den Entwicklungen der Techniken und Netze ermöglicht werden. Prädiktive Polizeiarbeit ist insofern ein Bündelungsbegriff, der verschiedene Ansätze wie Data Mining-Strategien, Crime Mapping, Netzwerkanalysen oder «Big Data»-Visionen aufnehmen kann. Die integrierende Vision lautet erneut: eine Straftat hat noch gar nicht begonnen und die Polizei ist schon da.

Prädiktive Polizeiarbeit ist außerordentlich voraussetzungsvoll. Die – regelmäßig von privaten Unternehmen entwickelten – Datenverarbeitungs-, Datenanalyse- und Wissensgewinnungstechniken und -programme, die sie ermöglichen sollen, stehen selbst noch am Anfang. Die ersten Einsatzfelder betreffen überschaubare Kontexte: Bestimmte Delikte, etwa Eigentumsdelikte in Form von Einbruchsdiebstählen, stehen im Vordergrund. Auswertungen sind auf begrenzte Räume bezogen, etwa auf die verschiedenen Bezirke einer Stadt. In ein leistungsfähiges Datenverarbeitungs- und -analyseprogramm werden zahlreiche Daten aus unterschiedlichen Zusammenhängen und längeren Zeitperioden eingespeist. Dazu gehören etwa die bekannten Einbruchsdiebstähle der vergangenen zwanzig Jahre, genauer Ort, genaue Zeit, Art der Begehung, Ergebnisse der jeweiligen Ermittlungen, Vorkommnisse an Gewalttätigkeiten in dem Bezirk, Drogenhandelsplätze und deren Veränderungen, Gestaltung und Veränderungen des lokalen Umfelds im Laufe der Zeit, Bevölkerungsfluktuation, statistische Einkommensverhältnisse in dem Bezirk, Erkenntnisse aus Ermittlungen in sozialen Netzwerken – eben alles, was an Daten zur Verfügung steht und was irgendwie relevant sein könnte. Automatische Programme und Algorithmen analysieren die Daten in unterschiedlicher Form. Im einfachsten Fall könnten sie eine regelmäßige zeitliche Häufung von Einbruchsdiebstählen in bestimmten Gegenden anzeigen, die die Vorhersage erlaubt, dass im Falle künftiger Einbruchsmeldungen in derselben Gegend weitere Einbrüche passieren werden, so dass hier verstärkte

7 Siehe dazu näher Perry/ McInnis/ Price/ Smith/ Hollywood (2013).

8 Siehe etwa mit differenzierter Beurteilung Gluba (2014). Siehe auch die Antwort der Bundesregierung in BT-Drucksache 17/11582.

polizeiliche Kontrollen stattfinden sollten. Ausgefeiltere Analyseprogramme sollen insbesondere zuvor unbekannte Muster und Trends herauskristallisieren und bei komplexeren Daten- und Datenverarbeitungsgrundlagen würden die Vorhersagen selbst von Algorithmen errechnet und Auswertungsergebnisse geliefert. «Intelligente» Programme wären so konzipiert, dass sie aus neu eingespeisten Daten ebenso wie aus Ergebnissen lernten und ihre eigenen Strukturen und Abläufe anpassten.

Ebenso wie Prävention kann prädiktive Polizeiarbeit mit positiven und mit negativen Folgen verbunden sein. Für sich genommen bietet es zahlreiche Vorteile, wenn kriminelle Aktivitäten tatsächlich treffsicherer prognostiziert und polizeiliche Ressourcen effektiv eingesetzt werden könnten. Aber der Einsatz der «intelligenten» Datenverarbeitungs-, -analyse- und -auswertungsprogramme erzeugt im Schatten zugleich Probleme, Defizite und potenzielle Nachteile. Der dynamisch wachsende, aus sich heraus praktisch nicht mehr begrenzte Datenbedarf – «alles kann ja irgendwann und irgendwie mal wichtig sein»[9] – ist einer der hier zu nennenden Faktoren. Der Kern der Problematik besteht jedoch darin, dass die eingesetzte Software weitaus mehr ist als eine äußerlich bleibende Technologie. Nicht nur hinter ihrer Auswahl, sondern auch hinter ihrer Ausgestaltung und den Programmierungsschritten stecken bestimmte Theorien, Modelle und Hypothesen über Kriminalität. Bei den in den USA für Eigentumsdelikte erprobten Programmen sind dies etwa die «Near Repeat Theory» oder das «Risk Terrain Modeling».[10] Je komplexer die Software wird, desto mehr verbergen sich in ihr Werte und Meinungen, Unsicherheiten und Zweifel, Entscheidungsprozesse, (Vor-)Entscheidungen und Weichenstellungen. Software ist insofern ein «eingefrorener Diskurs». Aber zugleich installiert sie «relativ unveränderliche, als selbstverständlich hingenommene Protokolle in der alltäglichen Informationspraxis von Organisationen, vereinheitlicht die Formen der Interpretation von Ereignissen, beeinflusst die Art und Weise der Entscheidungsfindung und standardisiert solche Entscheidungen über Zeit und Raum hinweg».[11]Eine einprogrammierte Lernfähigkeit kann (Fehl-)Annahmen korrigieren, aber die Problematik auch noch steigern.

Prädiktive Polizeiarbeit greift über die punktuellen einzelfallbezogenen Perspektiven und über die entsprechenden sachlichen, zeitlichen und personellen Einschreitschwellen der klassischen Sicherheitskonzeptionen hinaus. Sie lässt auch bisherige Datenschutzmechanismen als partiell veraltet erscheinen, soweit diese allein personenbezogene Daten und deren Erhebung sowie die Erhebungsmethoden für problematisch halten. Künftig muss sich mehr Aufmerksamkeit auf den Einsatz und auf die Handhabung von Datenverarbeitungsprogrammen und auf die damit verbundenen Folgen richten. Da dies den Kernbereich der Polizeiarbeit

9 Extrabreit (1981), Polizisten.

10 Der Near Repeat Theory liegt u.a. folgende Annahme zu Grunde: Sobald in einer bestimmten Gegend Delikte wie Einbruchsdiebstähle verübt werden, gibt es eine erhöhte statistische Wahrscheinlichkeit, dass kurz nach einem Ausgangsdelikt weitere ähnliche Delikte in dieser Gegend oder in der näheren Umgebung begangen werden. Das Risk Terrain Modeling legt zu Grunde, dass Kriminalität eine Funktion einer dynamischen Interaktion zwischen sozialen, physikalischen und verhaltensbezogenen Faktoren ist, die an bestimmten Orten stattfindet, und dass auf dieser Basis für bestimmte Bereiche bestimmte Risikofaktoren identifiziert und kartografiert werden können. Vgl. insgesamt Ferguson (2012): 277 ff.

11 Leyshon/ Thrift (1999): 453 (Übersetzung von Marion Albers).

betrifft, wird man neue Formen der – gegebenenfalls indirekten – Regulierung sowie neue Formen institutionalisierter und öffentlicher Kontrolle finden müssen.

2. Neue technikermöglichte Ermittlungs- und Datenverarbeitungsformen

Digitalisierung und Netzvermitteltheit der Kommunikation ermöglichen unter quantitativen und qualitativen Aspekten neue Formen der Ermittlung und der Datenverarbeitung. Anschaulich hierfür ist die Videoüberwachung: Aus einem ehemals punktuell und gezielt genutzten Instrument hat sich eine im privaten mehr noch als im öffentlichen Raum weit verbreitete und namentlich in Großbritannien nahezu flächendeckend eingesetzte Überwachungstechnik entwickelt. Die Videoüberwachung durch Bundes- oder Länderpolizeien erfolgt in Deutschland im Rahmen der grenzziehenden gesetzlichen Ermächtigungen. Allerdings können die Polizeibehörden unter wiederum rechtlich begrenzten Voraussetzungen auf Aufzeichnungen privater Personen oder Unternehmen zugreifen. Erst die Kombination polizeilicher Videoüberwachungen und polizeilicher Zugriffsmöglichkeiten auf private Videoüberwachungen ergibt daher ein vollständiges Bild von der Überwachungsreichweite. Darüber hinaus ist die Videoüberwachungshard- und -software deutlich weiterentwickelt worden. Ursprünglich beschränkte sie sich auf die Übertragung der Bilder einer unter Umständen starren Überwachungskamera auf einen Monitor im Beobachtungsraum. Heute ermöglichen Programme und Algorithmen fließende Zoomgrade und das simultane Abprüfen unterschiedlichster Aspekte, Beobachtungen nach Differenzierungskriterien wie Geschlecht oder Hautfarbe, eine Verhaltens- und Gesichtserkennung, die Herausfilterung auffälliger Verhaltensweisen oder eine Bewegungsverfolgung.[12] Rundum drehbare Mikrokameras ergänzen sich in ihrem Beobachtungsradius. Die Aufzeichnungen können verknüpft werden und so lässt sich eine bestimmte Person auf ihrem Weg durch die Stadt verfolgen. «Smarte» Auswertungsprogramme können sich anschließen und deren Ergebnisse wiederum die Überwachung modifizieren. Und nicht zuletzt können bei Vorliegen der technischen Voraussetzungen Aufzeichnungs- und Auswertungsdaten aus Videoüberwachungen ebenso vielfältig mit anderweitigen Daten zusammengeführt wie anderweitige Daten (etwa Fotos aus sozialen Netzwerken) in die Videoüberwachungsprogramme eingespeist werden können. Wie bei den Überlegungen zum prädiktiven Konzept zeigt sich, dass es zu kurz greift, allein einzelnen Ermittlungsmethoden und den punktuellen polizeilichen Datenerhebungseingriffen Aufmerksamkeit zu schenken. Datenverknüpfungen, Datenauswertungsformen, Datenkreisläufe und Datenverarbeitungsprogramme als vorweggenommene Entscheidungs- und Bewertungsverfahren sind gleichermaßen wichtig. Beschreibungen und Beurteilungen werden so schwierig, weil man immer sowohl einen bestimmten Datenverarbeitungsschritt fokussieren als auch die gesamten Verarbeitungsprozesse und -zusammenhänge im Blick haben muss.

12 Ausführlicher Held (2014): 15 ff.; Gouaillier/ Fleurant (2009): 26 ff.

3. Technisierte Vernetzung der Sicherheitsbehörden

Die informationelle Vernetzung der Sicherheitsbehörden ist ein wesentliches Kennzeichen der neuen Sicherheitsarchitektur. Moderne Infrastrukturen und Datenverarbeitungstechniken machen ihre gegenwärtige Gestalt erst möglich. Neben den vielfältigen Formen wechselseitigen Datenaustauschs sind inzwischen zahlreiche Zentraldateien und Verbunddateien institutionalisiert, die bei einer Stelle geführt werden und in die die daran beteiligten Stellen nach vielfältigen, partiell gestuften Vorgaben selbst Daten einpflegen und aus denen sie Daten abrufen.[13] Solche Dateien stärken noch einmal die Rolle der Bundespolizeien, bei denen sie regelmäßig geführt werden; Beispiele sind das polizeiliche Informationssystem INPOL beim Bundeskriminalamt oder das Zollinformationssystem INZOLL beim Zollkriminalamt. Projektbezogene gemeinsame Dateien und gemeinsame Dateien in bestimmten Sachbereichen wie die «Antiterrordatei» oder die Rechtsextremismusdatei treten hinzu. Automatisierte zentrale gemeinsame Dateien verdichten die Datenlage zu bestimmten Personen, Objekten oder Sachverhalten. Sie zeichnen sich aber immer auch durch ein eigenständiges, technisch mitgeprägtes Datenformat und durch eine spezifische, meist durchaus hohe Selektivität der Datenbasis aus, die sich auf die jeweilige Wissenserzeugung der datennutzenden Sicherheitsbehörde auswirkt. Anschaulich ist etwa das Problem, inwieweit bewertende personengebundene Hinweise, wie etwa «geisteskrank» oder «gewalttätig», in gemeinsame Dateien eingespeist werden sollen, obwohl Bewertungsgrundlagen und -kontext nicht unbedingt mitgespeichert werden können, so dass die abrufende Behörde die Bewertung möglicherweise fehlinterpretiert. Umgekehrt werden aber auch Freitextfelder kritisiert, weil sie Raum für unbegrenzte Eingaben zu Personen gewährten. Vor diesem Hintergrund werden gemeinsame Dateien teilweise auf die Funktion knapper Nachweise beschränkt, die einen anderweitigen näheren Datenaustausch zwischen den Sicherheitsbehörden anbahnen können.

Die einzelnen Datenverarbeitungsschritte, nämlich welche Behörde unter welchen Voraussetzungen welche Daten eingeben und abrufen darf, werden in gesetzlichen Grundlagen, Verordnungen und teilweise als Verschlusssache eingestuften Errichtungsanordnungen relativ detailliert geregelt. Das Kernproblem, welche Folgen gemeinsame Dateien und die Art der dort gespeicherten Datensätze für die behördliche Wissenserzeugung in den Kontexten haben, in die die Daten dann fließen, kann allerdings nicht mit isolierend-punktuellen, sondern nur mit übergreifenden, prozess- und kontextbezogenen Perspektiven erfasst werden. Solche Perspektiven sind auch wichtig für die rechtliche Beurteilung. Gemeinsame Dateien dürfen beispielsweise nicht dazu führen, dass Nachrichtendienste, die persönliche Daten nach Maßgabe relativ niedriger Einschreitschwellen und in weitem Umfang heimlich erheben dürfen, die so erlangten Daten unbeschränkt in eine gemeinsame Datei mit der Folge einspeisen, dass Polizeien darauf zugreifen können, obwohl für sie höhere Hürden bei der Datenerhebung gelten.

Die technisierte Vernetzung der Sicherheitsbehörden erfordert also komplexe rechtliche und informationstechnische Architekturen. Dies wird umso anspruchsvoller, je mehr Behörden beteiligt sind und je mehr man mit transnationalen

13 Zum Überblick etwa BT-Drucksache 17/14735: 9 ff.

Verbunddateien zu tun hat. Beispielsweise hat die Trennung zwischen Polizeien und Nachrichtendiensten in wichtigen anderen Mitgliedstaaten der Europäischen Union keine Tradition, so dass insoweit gar kein Anlass gesehen wird, den Datenaustausch differenziert zu gestalten. Die daraus resultierenden Abstimmungsprobleme werden mit der zunehmenden Europäisierung des Sicherheitsbereichs noch wachsen.

4. Globalisierte Überwachung

Edward Snowden hat enthüllt, in welch globalem und flächendeckendem Umfang Nachrichtendienste das Kommunikationsverhalten überwachen.[14] Dabei wird ausgenutzt, dass jede Person unter den heutigen Kommunikationsbedingungen weit reichende Datenspuren hinterlässt. Verschlüsselungstechniken scheinen wenig zu helfen. Das Datenschutzrecht steht auf sämtlichen Regelungsebenen – international, europäisch, national – vor neuen Fragen.

Die Überwachung durch ausländische Nachrichtendienste ist dabei auch, aber keineswegs allein mit internationalem Recht erfassbar. Auf allen Regelungsebenen ergeben sich vielmehr spezifische Anknüpfungspunkte, die allerdings weiter ausarbeitungsbedürftig sind. Diskutiert wird über Rechte aus den menschenrechtlichen Verträgen, unter anderem aus Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte oder Art. 12 der Allgemeinen Erklärung der Menschenrechte. Deren Anwendbarkeit setzt jedoch die Ausübung von Hoheitsgewalt als traditionellem Merkmal territorialer Herrschaft voraus, und das führt bei globalen Überwachungsmaßnahmen der US-amerikanischen National Security Agency NSA zu einigem Begründungsaufwand. Hinsichtlich des TEMPORA-Programms und der Überwachungsmaßnahmen des britischen Geheimdienstes kommt eine Verletzung insbesondere des Art. 8 oder auch des Art. 10 der Europäischen Menschenrechtskonvention (EMRK) in Betracht. Für deren Überprüfung ist der Europäische Gerichtshof für Menschenrechte (EGMR) zuständig und entsprechende Verfahren sind dort anhängig.[15] Hinsichtlich der Überwachungsaktivitäten der NSA bestehen im Rahmen der Europäischen Union (EU) zumindest mittelbare Kontrollmöglichkeiten. Das gilt etwa im Hinblick auf das Erfordernis, dass die Übermittlung personenbezogener Daten in die USA als Drittstaat dort ein angemessenes Datenschutzniveau voraussetzt. Aufgrund der «Safe-Harbor»-Absprache zwischen den USA und der EU hatte die Europäische Kommission zwar im Jahre 2000 festgestellt, dass aus EU-Sicht ausreichende Datenschutzstandards in den USA bestehen würden.[16] In Kenntnis der NSA-Überwachung und des sonstigen Umgangs mit persönlichen Daten lässt sich diese Sicht jedoch nicht halten. Zu diesem Problemkomplex steht eine Entscheidung des Europäischen Gerichtshofs (EuGH) an.[17]

14 Näher etwa Rosenbach/ Stark (2014).

15 Big Brother Watch and others against the United Kingdom, Aktenzeichen 58170/13; Bureau of Investigative Journalism and Alice Ross against the United Kingdom, Aktenzeichen 62322/14.

16 Entscheidung der Kommission vom 26. Juli 2000, ABl. L 215: 7.

17 Rechtssache C-362/14 (Schrems/Data Protection Commissioner). Es handelt sich um ein Vorabentscheidungsersuchen des High Court of Ireland, der danach fragt, ob die unabhängige Datenschutzbehörde zwingend an die Safe-Harbor-Einschätzung der Kommission gebunden ist oder im Lichte tatsächlicher Entwicklungen eigene Ermittlungen anstellen darf.

Dies zeigt zum Abschluss, dass die technik- und netzvermittelte Globalisierung der Kommunikation dazu führt, dass auch die sicherheitsbehördlichen Aktivitäten nicht mehr allein mit Blick auf die nationale Ebene und auf nationale Polizeien und Nachrichtendienste zu beobachten sind. Überwachungsmechanismen sind in bestimmtem Umfang ihrerseits globalisiert. Auch damit stellen sie uns vor neue Herausforderungen.

Literatur

Abbühl, Anicee (2010), *Der Aufgabenwandel des Bundeskriminalamts,* 2010, Stuttgart u. a.

Albers, Marion (2001), *Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge,* Berlin.

Albers, Marion (2012), *Das Präventionsdilemma,* in: Weichert/Schmidt (Hrsg.), Datenschutz, Berlin, 102 ff.

Extrabreit (1981), *Polizisten,* in: *Welch Ein Land ! - Was Für Männer:* (Song 4), Album (Vinyl), erschienen auf dem Label Reflektor Z (0060.431), Hamburg.

Ferguson, Andrew Guthrie (2012), *Predictive Policing and Reasonable Suspicion,* in: Emory Law Journal Vol. 62, 259 ff.

Gluba, Alexander (2014), *Predictive Policing – eine Bestandsaufnahme,* Hannover.

Gouaillier, Valérie/Fleurant, Aude-Emmanuelle (2009), *La vidéosurveillance intelligente: promesses et défis* (auch auf englisch verfügbar: *Intelligent Video Surveillance: Promises and Challenges),* Québec.

Grimm, Dieter (1991), *Verfassungsrechtliche Anmerkungen zum Thema Prävention,* in: ders., *Die Zukunft der Verfassung,* Frankfurt a. M., 197 ff.

Held, Cornelius (2014), *Intelligente Videoüberwachung,* Berlin.

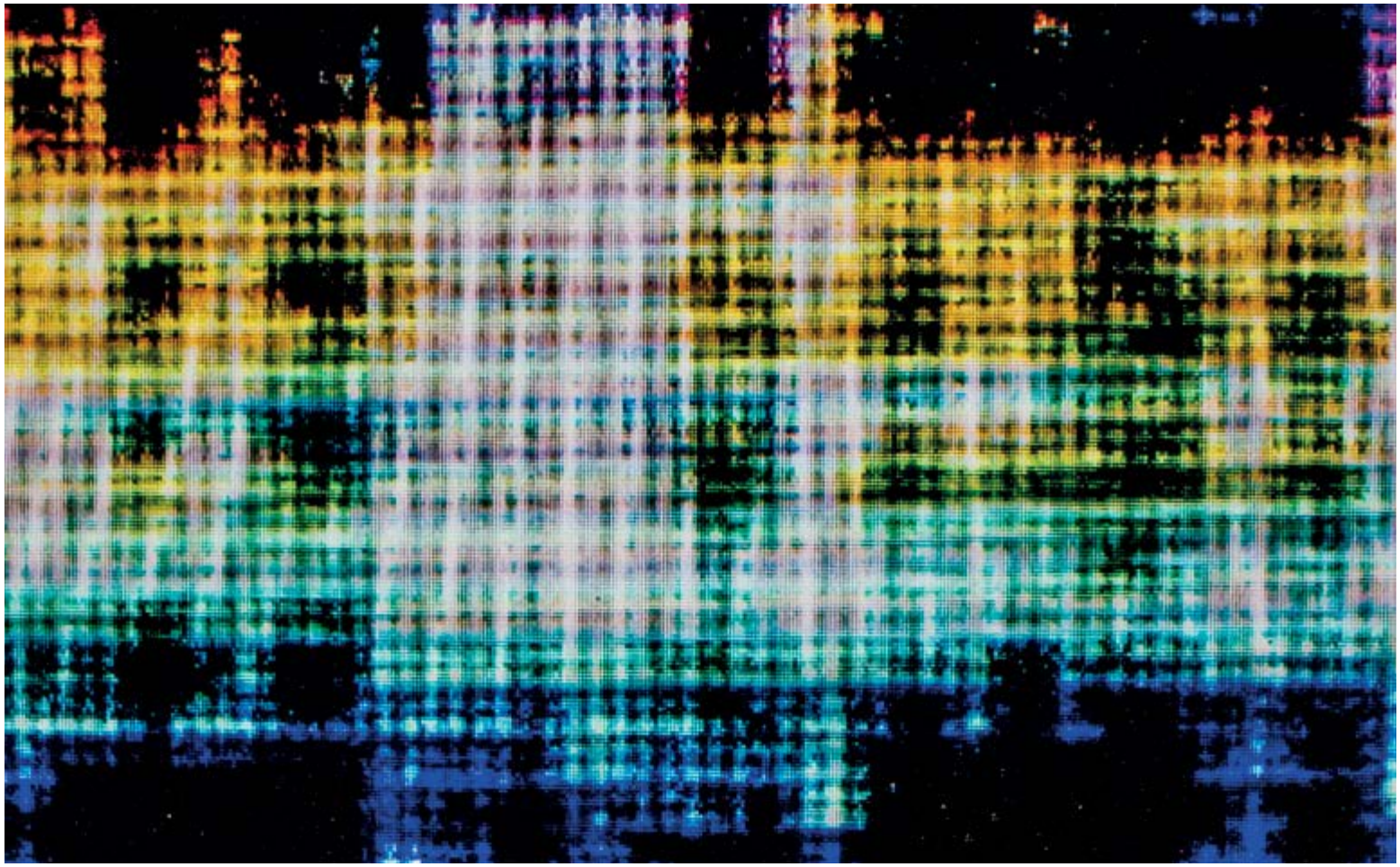
Herold, Horst (1972), *Gesellschaftlicher Wandel – Chance der Polizei?,* Die Polizei Bd. 63, 133 ff.

Huster, Stefan/ Rudolph, Karsten (2008), *Vom Rechtsstaat zum Präventionsstaat,* in: dies. (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, Frankfurt a.M., 9 ff.

Leyshon, Andrew/ Thrift, Nigel (1999), *Lists come alive: electronic systems of knowledge and the rise of credit-scoring in retail banking,* Economic and Society Vol. 28, 434 ff.

Perry, Walter L./ McInnis, Brian/Price, Carter C./Smith, Susan C./Hollywood, John S. (2013), *Predictive Policing,* Santa Monica, CA u. a.

Rosenbach, Marcel/ Stark, Holger (2014), *Der NSA-Komplex: Edward Snowden und der Weg in die totale Überwachung,* München.



JOHANNES NÄDER

Weder Fluch noch Segen – Die digitale Schwelle als Herausforderung der demokratischen Gesellschaft

«The right net brings freedom and the wrong net brings tyranny.»
Eben Moglen, FOSDEM 2011

1. Das janusköpfige digitale Zeitalter

Wer in Zukunft eine Mentalitätsgeschichte des frühen 21. Jahrhunderts schreibt, wird an zwei Ereignissen der vergangenen Jahre nicht vorbeikommen, die jeweils stellvertretend für verbreitete Auffassungen von der digitalen Realität stehen: Da ist zum einen der «arabische Frühling», jene Reihe revolutionärer Erhebungen mit völlig unterschiedlichem Ausgang, in deren Verlauf die Demonstrierenden gezielt Plattformen wie Twitter, Facebook und Youtube zur Vernetzung, Information und zur Beeinflussung der Öffentlichkeit einsetzten. Als in den letzten Januartagen des Jahres 2011 Zehntausende auf dem Tahrir-Platz in Kairo zusammenströmten, um gegen das autoritäre Regime zu protestieren, konnten sich Menschen in aller Welt mit Hilfe dieser Dienste detaillierte Eindrücke vom Geschehen in Ägypten verschaffen. Schnell verbreitete sich unter Netzenthusiasten die Deutungstradition vom demokratischen, demokratisierenden Internet, an dem jeder teilhaben kann und das erfolgreich Gegenöffentlichkeit von der Subkultur bis zur Revolution zu konstituieren vermag. Diktaturen würden es im digitalen Zeitalter schwer haben, denn dem Internet im Allgemeinen und sozialen Netzwerken im Besonderen sei ihr Demokratisierungspotenzial inhärent. So wenigstens hofften viele, und auch wenn diese Idee nach der zuvor gescheiterten iranischen «Facebook-Revolution» alles andere als unumstritten war, schien sie sich im «arabischen Frühling» zunächst eindrucksvoll zu bewahrheiten.[1]

Das andere mentalitätsgeschichtlich bedeutende Ereignis ist die Aufdeckung der weltweiten Überwachungs- und Spionageaktivitäten amerikanischer und britischer Geheimdienste durch den Whistleblower Edward Snowden seit dem Frühjahr 2013. Zwar war die dunkle Seite der weltweiten Vernetzung nichts völlig Neues. Seit langem hatten Netzaktivisten die Einschränkungen informationeller Selbstbestimmung kritisiert und auf die erweiterten Überwachungs- und Kontrollmöglichkeiten in den digitalen Netzen hingewiesen. Kaum jemand hatte aber damit gerechnet, dass die westlichen Demokratien tatsächlich zu einer solchen Entgrenzung ihrer Sicherheitsorgane, zu dermaßen umfassenden Grundrechtsverletzungen bereit sein könnten. Selbst Aktivisten mussten sich an die Vorstellung gewöhnen, dass ihre schlimmsten Befürchtungen von der Realität übertroffen wurden: Offenbar sind mehrere

1 Morozov (2011).

Geheimdienste technisch dazu in der Lage, die schier unglaublichen Datenmengen eines full take – den überwiegenden Teil der digitalen Kommunikation der Menschheit – nicht nur zu speichern, sondern auch gezielt auszuwerten.

Wer eben noch begeistert von der «Twitter-Revolution» geschwärmt hatte, den trafen Snowdens fortlaufende Enthüllungen hart. Ließen sich vielleicht noch Erklärungen für das Scheitern fast aller arabischer Revolutionen finden, so blieb mit jedem veröffentlichten NSA- oder GCHQ-Dokument für eine grundsätzliche, ungebrochene Begeisterung über die digitale Technologie weniger Raum. Der Medienjournalist Sascha Lobo traf den Nerv einer Generation, indem er bekannte: «Das Internet ist nicht das, wofür ich es so lange gehalten habe. Ich glaubte, es sei das perfekte Medium der Demokratie und der Selbstbefreiung. […] Auf eine Art hat es sich gegen mich gewendet und mich verletzt. […] Das Internet ist kaputt.»[2]

Wer indes schon immer in tiefem Pessimismus auf digitale Technologien geblickt hatte, konnte sich jetzt endgültig bestätigt fühlen: Der technologische Fortschritt mit all seinen Apps und Diensten würde nicht zu Gerechtigkeit und Wohlstand, zu Menschenrecht und Demokratie führen, weil das Internet seiner Natur nach eigentlich Opium für das Volk ist, ein Instrument stillschweigender Kontrolle und Manipulation, eine Technologie der Herrschenden.

2. Gefährlicher Technikdeterminismus

Im Technikpessimismus und im Technikoptimismus begegnen wir zwei verbreiteten Haltungen, die man gegenüber den uns umgebenden digitalen Technologien einnehmen kann: Der Optimist sieht diese Technologien als inhärent gut an, als Motoren gesellschaftlicher Emanzipation, individueller Freiheit und politischer Partizipation, die möglichst große Verbreitung finden sollten. Der Pessimist hingegen beharrt darauf, die Menschen seien in ihrem vordigitalen Zustand (was auch immer damit gemeint sein mag) souveräner und freier gewesen. Dem Internet sei es anzulasten, dass diese Souveränität und Freiheit zunehmend eingeschränkt und letztlich unweigerlich zerstört werde.

Auch wenn diese Haltungen auf den ersten Blick konträr erscheinen mögen, teilen sie doch eine unausgesprochene Grundannahme über das Wesen der Technik oder wenigstens über das Wesen des Internets und über seine Bedeutung für menschliches Zusammenleben: Die «digitale Revolution», so diese Grundannahme, sei wie eine Naturgewalt über die Menschheit gekommen und präge sie nun zum Guten oder zum Schlechten, jedenfalls aber unerbittlich und unhintergehbar. Gesellschaftliche Entwicklung finde in einem medientechnisch abgesteckten Rahmen und nach medientechnisch fixierten Regeln statt, die dem menschlichen Zugriff weitgehend entzogen seien. Digitalität und Internet taugen in dieser Perspektive als Erklärungsmuster für nahezu beliebige gesellschaftliche Phänomene, ob Revolutionen oder Überwachungsexzesse, Veränderungen des Arbeitsmarktes oder unserer Konsumgewohnheiten, Aufmerksamkeitsdefizite und Effizienzsteigerungen.

Diese mediendeterministische Weltsicht ist im Kern irrational, weil sie ausschließlich einseitige Kausalitäten anerkennt. Sie interessiert sich dafür, wie die Gesellschaft von den neuen Medien geprägt wird, geht aber nicht der Frage nach,

2 Lobo (2014).

wie die Gesellschaft diese Medien geprägt hat und es weiterhin tut. Sie beschwört die Kennzeichen und Auswirkungen eines medialen Epochenwechsels, müht sich aber nicht, die zur Rede stehenden Technologien zu erklären und historisch einzuordnen. Weitgehend im Dunkeln bleibt, was das Internet eigentlich ist, und erst recht, wie die digitalen Netze sich entwickeln, verbreiten und verändern. Die Fixierung auf einzelne Dienste (WWW, Facebook, WhatsApp) und irreführende Metaphern («Daten-Autobahn») sowie die Neigung zu kurzschlüssigen Wirkungszuschreibungen («Twitter-Revolution») verhindern ein tieferes Verständnis der uns umgebenden digitalen Technologien.

Technikoptimismus und Technikpessimismus sind deswegen gleichermaßen bequem und gefährlich: Beide Haltungen tendieren dazu, Digitalität und Internet als Ergebnisse einer zwangsläufigen mediengeschichtlichen Entwicklung zu verstehen, die hinsichtlich ihrer gesellschaftlichen Auswirkungen zwar unterschiedlich beurteilt werden können, an sich aber als alternativlos zu akzeptieren sind. Ob man staatliche Überwachung nun als logische Konsequenz oder als Missbrauch der digitalen Netze betrachtet, ob man diese Netze als natürliche Protest- oder als Herrschaftsinstrumente sieht: Wer so denkt, hat immer nur die Wirkungsseite der heutigen Netzinfrastrukturen im Blick. Er übersieht, dass diese Infrastrukturen keineswegs aus dem Nichts kommen, sondern in einem spezifischen historischen Kontext entstanden sind. Er vergisst, dass sie in ihrer Entwicklung immer wieder gezielten Einflüssen politischer, wirtschaftlicher und ideologischer Natur ausgesetzt waren. Gleichzeitig glauben Optimisten und Pessimisten an eine gewisse Zwangsläufigkeit und Zielgerichtetheit technologischer Entwicklung: Sie lassen aus dem Blick, dass unsere digitalen Infrastrukturen ganz anders aussehen könnten und dass sie mit Sicherheit zu einem späteren Zeitpunkt auch anders aussehen werden. Vor allem verweigern sich Optimisten wie Pessimisten der Einsicht, dass diese Entwicklung von den Interessen unterschiedlicher Akteure bestimmt ist. Damit geben sie jede Hoffnung auf, die digitale Medienrealität nachhaltig beeinflussen zu können.

3. Zur Logik des medialen Wandels

Wer hingegen einen rationalen Blick auf den digitalen Wandel und seine Bedeutung wagen möchte, dem verbietet sich die Hingabe an digitale Utopien oder Dystopien. Angemessener ist es, einem Vorschlag des Netztheoretikers Evgeny Morozovs folgend, die Haltung eines radikalen Technikagnostizismus anzunehmen und nüchtern zu fragen: Wie funktionieren eigentlich unsere digitalen Netze, Dienste, Medien, Protokolle – all das, was wir landläufig als «das Internet» bezeichnen – technisch, ökonomisch, institutionell? Wie haben sie sich entwickelt? Wem nützt und wem schadet es, dass diese einzelnen Technologien genau so funktionieren und nicht anders? Stellen sie sich in ihrer jetzigen Form eher «in den Rahmen des Emanzipations- oder in den des Versklavungsprojektes»?[3] Welche Entwicklungen, Veränderungen und Alternativen sind denkbar? Und was davon ist sinnvoll, was gefährlich? Für eine solche nüchtern-rationale Sichtweise plädiert auch der französische Philosoph Régis Debray, der sich scharf gegen jeglichen Technikdeterminismus wendet: «Es geht nun aber nicht darum, zu beklagen, zu exorzisieren oder zu

3 Morozov (2014).

erbauen. Wir werden der technologischen Zukunft nicht dadurch Herr, dass wir uns von ihr abwenden. Die Verantwortung besteht darin, ihre Logik zu verstehen, um möglichst viele ihrer Auswirkungen vorwegzunehmen.»[4]

Sucht man nach der Logik des gegenwärtigen medialen Wandels, so stößt man auf drei Tendenzen:

a) Durchdringung mit vernetzter Technologie

Wir erleben eine beispiellose Durchdringung unserer Gesellschaft mit digitaler, vernetzter Technologie. Die meisten Menschen hantieren täglich, viele sogar fast ununterbrochen mit Geräten, die ihnen permanent ermöglichen, Kontakt zu anderen Geräten und Menschen aufzunehmen, Informationen abzurufen, zu organisieren, bereitzustellen, auszutauschen, zu verarbeiten und zu kategorisieren. Bereits heute sind zahlreiche Apparaturen unserer Umgebung an diese Netzwerke angebunden – Ampeln und Autos, Unterhaltungstechnik und Überwachungskameras, selbst Stromzähler und Kühlschränke. Vernetzung und Datenverarbeitung sind nicht nur die Basis für digitale Dienstleistungen, sondern integrieren sich tief in Arbeit und Freizeit, Politik und Verwaltung, Wirtschaft und Finanzen, Kommunikations- und Nachrichtenwesen, Bildung, Wissenschaft und Kriegsführung. Zukünftig wird diese Vernetzung voraussichtlich noch umfassender sein und nicht nur Menschen und technische Geräte betreffen, sondern auch die meisten Gegenstände, von denen wir umgeben sind. In diesem «Internet der Dinge» werden alltägliche Abläufe nicht mehr zu erledigen sein, ohne dass wir mit digitalen Netzwerken interagieren oder zumindest Spuren in ihnen hinterlassen. Die digitale Schwelle, wie wir sie heute erleben, ist der Eintritt der Menschheit in einen beispiellosen Zustand der Technisierung und Vernetzung.

b) Speicherung und Verarbeitung von Informationen

Die digitalen Technologien eröffnen ungeahnte Möglichkeiten der Speicherung, Übertragung und Verarbeitung von Informationen: Es entstehen mehr und mehr innovative Geräte, Anwendungen und Dienste und damit immer neue Szenarien der Interaktion mit anderen Menschen und Gegenständen unseres Alltags. Wir können uns jederzeit schier unendlicher Wissensbestände bedienen und über größte Entfernungen nahezu in Echtzeit kommunizieren. Mit ein und demselben Gerät arbeiten wir, erledigen Einkäufe oder Behördengänge, lesen, tauchen in mehr oder weniger virtuelle Welten ein, produzieren Selfies oder Kunst und steuern andere Geräte. Wir unterhalten und informieren uns und andere, erhalten auf unsere Interessen abgestimmte Tipps, knüpfen Kontakte und sind jederzeit über das Wetter auf dem Laufenden. Die anspruchsvollsten und die banalsten Aufgaben lassen sich zusammenfassen, vereinfachen, beschleunigen, automatisieren oder rationalisieren. Die erstaunlichen Möglichkeiten der digitalen Technologien scheinen uns geradezu zu neuen, kreativen Lösungen herauszufordern; sie versprechen uns gesteigerte Effizienz, bessere Übersicht, mehr Kontrolle, größeres Wissen und oft auch spielerische Leichtigkeit und mehr Spaß bei der Erledigung unserer Projekte und Aufgaben. Diese Möglichkeiten und diese Versprechen sind verführerisch und faszinierend;

4 Debray (2003): 246.

Gefühle der Allmacht und der Allgegenwärtigkeit bannen uns mit einer geradezu metaphysischen Anziehungskraft. Es ist diese euphorisierende Wirkung, durch die digitale Technologien eine derart große Verbreitung finden konnten und die den nüchternen, technikagnostischen Blick zu einer Herausforderung geraten lässt: Wer die Logik der digitalen Medien ergründen will, muss ihre Faszination verstehen lernen, ohne sich ihr hinzugeben.

c) Komplexität und Technikunmündigkeit

Unsere medientechnischen Infrastrukturen werden zunehmend komplex. Ob man eine Zeitung in digitaler Form auf einem E-Book-Reader liest oder die Papierausgabe durchblättert, macht aus der Sicht der Lesenden auf den ersten Blick nur einen kleinen Unterschied. Im Inneren des Gerätes sowie in entfernten Backbones, Servern und Netzwerken laufen aber zahlreiche Datenverarbeitungs- und Übertragungsprozesse ab, die den Lesenden in aller Regel nicht bewusst sind und erst recht nicht verstanden, hinterfragt oder unterbunden werden können. Verborgen bleibt nicht nur, wie ein E-Book abgerufen oder eine E-Book-Seite aufgebaut wird, sondern auch, welche nicht vom Nutzer intendierten Prozesse im Gang sind: Wird sein Nutzungsverhalten überwacht, protokolliert und ausgewertet? Bleiben ihm bestimmte Inhalte verborgen oder werden sie manipuliert? Können sie über das Netzwerk sogar jederzeit gegen seinen Willen gelöscht werden? Welche Akteure kommen als Verantwortliche in Frage und welche Möglichkeiten haben sie jeweils: der Verleger, ein Distributor wie Amazon, Internet-Provider, Drittunternehmen, Konkurrenten, Behörden, Geheimdienste? Das Beispiel veranschaulicht die Bedeutung zunehmend komplexer Technologie für einen Bereich, den wir schlechthin als konstituierend für unser demokratisches Gemeinwesen ansehen: die publizistische Öffentlichkeit. Es fällt nicht schwer, sich auszumalen, welche Rolle die Komplexität digitaler Technologien in anderen Bereichen spielen mag – etwa in der Medizintechnik, dem Straßenverkehr, in der Kommunikation über «soziale Netzwerke», im Smart Home oder beim alltäglichen Einkauf. Selbst wenn unsere digitalen Geräte und Apps ein höheres Maß an Effizienz, Sicherheit, Überblick, Organisation und Autonomie mit sich bringen mögen: Wer sie nutzt oder von ihnen abhängt, ohne sie technisch zu verstehen, erlebt einen Kontrollverlust. Je komplexer die zu nutzende Technologie ist, desto intensiver arbeiten die Hersteller daran, die Geräte und ihre Interfaces immer nutzerfreundlicher, intuitiver und leichter bedienbar zu gestalten. Arbeitsschritte werden zusammengefasst und automatisiert, Prozesse verschwinden aus dem Blickfeld der Nutzer und betroffenen Personen. Anders als noch vor wenigen Jahren muss man heute kein Geek mehr sein, um ein Betriebssystem zu installieren. Auch wer seinen Browser, Google und das Internet nicht auseinanderhalten kann, ist in der Lage, alle drei zu benutzen. Microsofts Ankündigung aus den 1990er Jahren, Computer würden bald «so unauffällig wie Waschmaschinen werden – Black Boxes also, deren Innereien besagte Endbenutzer nichts mehr anzugehen brauchen»,[5] ist längst Wirklichkeit geworden, auch wenn Microsoft daran ironischerweise weniger Anteil hatte als sein größter Konkurrent. In einer durchtechnisierten, nutzerfreundlichen Welt fallen Medien-

5 Kittler (1998): 119.

nutzungskompetenz und Medienwissen auseinander: Um mit den hunderttausend Black Boxes dieser Welt zu interagieren, muss man sie zwar bedienen können, braucht dazu aber weder besondere technische Fertigkeiten noch das geringste Medienwissen. Deswegen – weil das benötigte Medienwissen nicht mehr mit den komplexen Technologien Schritt hält – gehen technischer Fortschritt und individuelle Technikunmündigkeit Hand in Hand.

4. Pessimismus ist nicht angebracht

Unser nüchterner Blick auf den digitalen Wandel scheint den Technikpessimisten also Recht zu geben: Der technische Wandel unserer Zeit führt zu einer tiefen Durchdringung der Gesellschaft mit komplexer vernetzter Technologie, die zwar wunderbar einfach zu bedienen, aber für die meisten Menschen hinsichtlich ihrer Funktionalität und möglicher Nebenwirkungen nicht mehr durchschaubar und erst recht nicht beherrschbar ist. Die Segnungen der heutigen digitalen Netzwerke, Smartphones, Smart Homes und des Internets der Dinge bezahlen wir mit neuer Unmündigkeit und einem Kontrollverlust, der weit über den Bereich der Kommunikation hinausgeht. Fatalerweise wird der Kontrollverlust trotzdem nur selten als solcher wahrgenommen. In aller Regel fühlen wir uns bei der Handhabung unserer neuen Medien und digitalen Technologien nicht schwächer, sondern stärker, weil sie uns als Werkzeuge der Selbstermächtigung begegnen.

Vernünftigerweise sollten wir uns eingestehen, dass keine der geschilderten Tendenzen umkehrbar ist. Wir werden natürlich nicht verhindern, dass unsere medientechnischen Infrastrukturen allgegenwärtiger, technologisch komplexer und einfacher handhabbar werden. Zu großartig sind die Versprechungen und Erwartungen, die sich mit dem technischen Fortschritt verbinden. Heidegger formulierte dies 1955 zwar in völlig anderem Kontext, aber doch so prägnant wie allgemeingültig: «Es wäre töricht, blindlings gegen die technische Welt anzurennen. Es wäre kurzsichtig, die technische Welt als Teufelswerk verdammen zu wollen. Wir sind auf die technischen Gegenstände angewiesen, sie fordern uns sogar zu einer immerzu steigenden Verbesserung heraus.»[6] Gleiches gilt für unsere vernetzten Digitaltechnologien: Es gibt kein Zurück in die Welt der handgeschriebenen Briefe und des sorgsam gehüteten Wissens, und selbst, wer sich wenigstens als Individuum allen digitalen Verlockungen verweigern möchte, wird bald an seine Grenzen kommen – im Zweifel durch seine soziale und ökonomische Exklusion.

Ist unser Weg in eine faszinierende, aber von Kontrollverlust und Unmündigkeit geprägte Zukunft also unumkehrbar vorgezeichnet? Als Medienagnostiker können wir uns mit dieser deprimierenden Perspektive nicht zufrieden geben. Auch wenn die Technologien der digitalen Vernetzung momentan offenbar Überwachung, Zensur, Monopolisierung und das Ende aller Privatheit mit sich bringen, könnte dies eher an ihrer aktuellen Verfassung und unserer verfehlten Haltung zu ihnen liegen als an ihrer «Natur». Wir mögen die technologische Entwicklung nicht umkehren können, aber wir sind auch nicht verpflichtet, sie in all ihren Erscheinungen und Wirkungen passiv hinzunehmen. Und tatsächlich bleiben uns grundsätzlich ja

6 Heidegger (1955): 22.

Möglichkeiten, Alternativen zur heutigen Medienrealität zu entwickeln: Nicht mit der realitätsfernen Ignoranz des Technikverächters, aber auch nicht in unmündiger Scheu vor scheinbar unantastbaren Technologien, Institutionen und Infrastrukturen. Einige denkbare Ansätze und erforderliche Schritte möchte ich im Folgenden skizzieren.

5. Abschied von vertrauten Denkmustern

Zunächst ist es unerlässlich, liebgewordene Denkmuster in Bezug auf die digitalen Medien über Bord zu werfen. Dazu gehört das deterministische Denken in all seinen Facetten: Die Vernetzung der Welt führt nicht zwingend zu mehr Partizipation, reiferen Bürgern, besserer Demokratie, besser verfügbarem Wissen oder einer glücklicheren Gesellschaft. Sie ebnet aber auch nicht unausweichlich den Weg für tyrannische Herrscher, manipulative Unternehmen oder allmächtige Institutionen. Letzteres wird nur geschehen, wenn wir intransparenten Akteuren fraglos die Gestaltung und die Kontrolle der Technik überlassen, mit der wir uns in jedem Moment umgeben und die wir mit Informationen über alle Details unseres Lebens füttern. Ersteres kann nur möglich sein, wenn wir die Entwicklung der Medientechnik, aber auch ihre juristischen und institutionellen Rahmenbedingungen und deren Kontrolle als eine gesellschaftliche Aufgabe begreifen – eine Aufgabe, die nicht jede und jeder Einzelne leisten kann, deren Bedeutung aber möglichst von jedem verstanden werden sollte und die gerade in unseren technorevolutionären Zeiten nicht auf der Strecke bleiben darf.

Wenigstens ebenso gefährlich wie Resignation und Euphorie ist die auch nach Snowden noch verbreitete Überzeugung, digital vernetzte Medien seien nichts als Werkzeuge, die man benutzen oder denen man sich verweigern könne, ohne dadurch persönliche und gesellschaftliche Risiken einzugehen. Dahinter mag technisches Unverständnis oder eine tiefere Verachtung gegenüber allem Technischen stehen, die Faszination der Innovation und die Bereitschaft, sich ihrem Sog um jeden Preis hinzugeben, vielleicht auch schlichte Selbstüberschätzung: Wer glaubt, all die medientechnischen Helferlein, die uns auf Schritt und Tritt ihre Dienste anbieten, beherrschen oder ignorieren zu können, der liefert sich ihnen aus. Wer meint, man müsse «soziale Netzwerke», Smartphones, Apps, SmartTVs und den Gmail-Account nur richtig konfigurieren und adäquat nutzen, um sich vor Verletzungen der Privatsphäre zu schützen, der verkennt nicht nur die technische und wirtschaftliche Logik vieler Geräte und Dienste. Er unterschätzt ebenfalls die Einflussmöglichkeiten und die Interessenlagen staatlicher, wirtschaftlicher und privater Akteure. Und selbst Heideggers viel zitierter Vorschlag, die undurchsichtige Eigenmächtigkeit der Technik notgedrungen anzuerkennen, sich aber in Gelassenheit zu üben und in kritischem «Nachdenken» eine innere Distanz zu wahren, wirkt in unserem überwachten Zeitalter kaum praxistauglich. Was Heidegger 1955 noch nicht ahnen konnte: Die Nutzung digitaler Technologie betrifft unsere Kommunikation ganz direkt – und zieht damit auch unser Denken in ihren Bann. So ist es mindestens fraglich, ob wir heute noch «die technischen Gegenstände im Gebrauch so nehmen [können], wie sie genommen werden müssen», dabei aber «diese Gegenstände zugleich auf sich beruhen lassen als etwas, was uns nicht im Innersten und Eigentlichen

angeht.»[7] Zweifellos sind Wachsamkeit und das Bewusstsein für Risiken im Umgang mit digitalen Medien unverzichtbar. Medienkompetenz darf sich aber nicht auf die reine Nutzung vorhandener Medientechnologien reduzieren lassen, denn der individuelle Kontrollverlust ist den neuen Medien inhärent und kann nicht allein durch eine wachsame, kluge Verwendung, nicht allein durch Kompetenz im Umgang mit diesen Medien kompensiert werden. Außer einer kritischen Prüfung unserer bisherigen Denkmuster bezüglich der neuen Medien bedarf es deswegen auch einer mündigeren Haltung gegenüber den digitalen Netzen und Technologien. Es gilt, dem individuellen Kontrollverlust mit einer kollektive nErmächtigung zu begegnen. Diese Ermächtigung kann aber nur gelingen, wenn sie an zwei Stellen gleichermaßen ansetzt: Medienwissen sowie Technikgestaltung und -kontrolle.

6. Ermächtigung durch Medienwissen

Wenn wir künftig auf Schritt und Tritt mit komplexer Medientechnik interagieren, wird ein in der Breite der Gesellschaft verankertes Medienwissen nötig, das wesentlich weiter reicht als bis zu den Privatsphäre-Einstellungen von Facebook. Es geht dabei einerseits um grundlegende informationstechnische Kenntnisse, die nötig sind, um technische Aspekte der neuen Medien wenigstens ansatzweise verstehen und beurteilen zu können: Wie unterscheiden sich Ende-zu-Ende-verschlüsselte E-Mails von vermeintlich privaten Facebook-Nachrichten? Befinden sich bestimmte Daten lokal und zudem gut geschützt auf dem heimischen Rechner oder unverschlüsselt in der Cloud? Wird eine bestimmte Anwendung entfernt oder lokal ausgeführt? Welche Konsequenzen bringt der Versuch mit sich, eine Nachzensur einmal veröffentlichter digitaler Daten zu ermöglichen? Worin besteht der fundamentale Unterschied zwischen proprietärer und Freier Software? Wem solche Grundkenntnisse fehlen, der wird immer nur die undurchsichtige Oberfläche und den schönen Schein der digital vernetzten Welt sehen, ohne sich ein kritisches Urteil bilden zu können.

Genauso brauchen wir jedoch medientheoretisches Grundlagenwissen, also ein grundsätzliches Verständnis für die historische und aktuelle Entwicklung von Medientechnologien, für ihre offensichtlichen und weniger offensichtlichen Funktionen und für deren direkte und indirekte Auswirkungen auf Individuen, Kultur und Gesellschaft. Schließlich muss sich unser Medienwissen auch auf die Akteure beziehen, die an der Entwicklung und Kontrolle der digitalen Infrastrukturen beteiligt sind: Unternehmen, staatliche Institutionen, internationale Organisationen. Bestehende Interessen- und Machtkonstellationen im Bereich der digitalen Netzwerke und Dienste zu erkennen, zu ergründen und auf den Prüfstand zu stellen, ist eine zentrale Voraussetzung verantwortlichen, mündigen Medienhandelns.

7 Ebd.

7. Die offene Gesellschaft braucht offene Medien

Damit ist es aber nicht getan. Mit dem nötigen Grundlagenwissen ausgestattet, müssen wir zudem einen gesellschaftlichen Kontroll- und Gestaltungsanspruch gegenüber den digitalen Infrastrukturen erheben. Dabei wird eine demokratische, offene Gesellschaft eine Medieninfrastruktur zum Ziel haben, die nachprüfbar nicht schon auf technologisch-infrastruktureller Ebene Vermachtung mit sich bringt oder Souveränitätsverluste zementiert. Hier sollen nur einige elementare Orientierungspunkte benannt werden:

a) Ungehinderte Teilhabe

Die Verfügbarkeit digitaler Ressourcen gewinnt an Bedeutung für den Erwerb und Austausch von Wissen und damit für eine gesellschaftliche, politische und ökonomische Partizipation. Gleichberechtigte Teilhabe darf nicht kleineren oder größeren gesellschaftlichen Gruppen vorbehalten bleiben. Neben der flächendeckenden Verfügbarkeit geeigneter Netzwerkzugänge ist vor allem eine grundsätzliche Neutralität der technischen Infrastrukturen gegenüber den Inhalten von Bedeutung: «Überholspuren», Priorisierungen einzelner Dienste und jegliche technische Maßnahmen zur Filterung und Zensur von Inhalten verletzen eine solche Netzneutralität. Dieses Szenario bezieht sich nicht nur auf die unteren Schichten der digitalen Netze, sondern in ähnlicher Weise auch auf zentralistische Dienste, die in höheren Netzwerkschichten operieren.

b) Zensurfreiheit

Eine kritische Öffentlichkeit, die ihrer Verantwortung als Machtkorrektiv gerecht werden will, ist auf einen von staatlicher oder privatwirtschaftlicher Zensur freien Austausch angewiesen. Eine Zensur ist umso einfacher, je zentralistischer die Netzwerkarchitektur gestaltet ist; dagegen erschweren dezentrale Architekturen Zensurbestrebungen. Eine erhebliche Gefahr für den ungehinderten Meinungsaustausch sind die einfachen technischen Filtermöglichkeiten in digitalen Netzwerken, die längst nicht mehr nur in China als deep packet inspection, sondern im Namen von Urheberrechts- und Jugendschutz auch in den westlichen Demokratien genutzt werden.

c) Wahrung der Privatsphäre

Selbst da, wo Überwachung nicht zu unmittelbarer Repression oder offensichtlichen Benachteiligungen führt, bringt sie chilling effects mit sich, also Selbstbeschränkungen hinsichtlich der Ausübung verfassungsmäßiger Rechte, die man sich aus Scheu vor möglichen Konsequenzen auferlegt. Daher müssen alle Menschen mit digitaler Technik kommunizieren und interagieren können, ohne Kommunikationsinhalte oder Verkehrsdaten für Dritte verfügbar zu machen. Ende-zu-Ende-Verschlüsselung und Privacy by Design/Default können dazu ebenso einen Beitrag leisten wie die gesetzliche Verankerung eines starken und durchsetzungsfähigen Datenschutzes. Auch Pseudonymität und Anonymität ermöglichen ein höheres Schutzniveau.

d) Offenheit der technischen Infrastrukturen

Wo in der Gesellschaft neue Machtstrukturen auftauchen, brauchen wir gesellschaftliche Kontrollmechanismen. Die komplexen digitalen Netzwerke, die unsere Welt durchdringen, sperren sich jedoch gegen jegliche Kontrolle, solange sie in weiten Teilen intransparent sind und selbst für den Blick und für die Verbesserungsvorschläge der technisch Kundigen verschlossen bleiben. Transparente und offene Hardware, Freie Software und offene Standards sind deswegen die grundlegende Voraussetzung für eine gesellschaftliche Kontrolle und Gestaltung der digitalen Infrastrukturen.

8. Für eine rekursive Gesellschaft

Es wären zahlreiche weitere Handlungsfelder zu nennen, auf denen unter den veränderten medialen Bedingungen um Mündigkeit, Souveränität und Gerechtigkeit zu ringen ist. Ihr gemeinsamer Angelpunkt ist die Gestaltung medialer Infrastrukturen durch sich ergänzende rechtliche und technische Maßnahmen. So können etwa nationale Datenschutzregeln erst dann wirksam werden, wenn ihre Missachtung durch den verbreiteten Einsatz leistungsfähiger Verschlüsselungstechnologie verhindert wird. Dieses notwendige Zusammenwirken von Technik und Recht hatte der Datenschutz- und Datensicherheitsforscher Andreas Pfitzmann bereits im Jahr 1998 im Blick, als er statt einer unbeobachteten eine unbeobachtbare Kommunikation forderte: «In Zukunft wird es nötig sein, die Technikgestaltung durch Recht zu beeinflussen und nicht nur den Umgang mit Technik.»[8]

Noch einen Schritt weiter geht der Medienanthropologe Christopher Kelty mit seinem Konzept einer «rekursiven Öffentlichkeit», die Technikgestaltung nicht nur als Aufgabe für die Politik, sondern als wesentliches Element bürgerschaftlicher Partizipation und Machtkontrolle begreift: «A recursive public is a public that is vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its own existence as a public; it is a collective independent of other forms of constituted power and is capable of speaking to existing forms of power through the production of actually existing alternatives.»[9]

Keltys Konzept zielt auf zivilgesellschaftliche Aktivistinnen und Initiativen, welche die elementare Bedeutung offener, unvermachteter Medieninfrastrukturen für sich selbst und für die offene Gesellschaft erkannt haben und die sich deswegen für solche Infrastrukturen engagieren. Ein Paradebeispiel dafür ist tatsächlich die von Kelty untersuchte Free-Software-Bewegung. Doch auch wenn deren Bedeutung für die digitale Medienrealität der Gegenwart erheblich ist, bleibt sie eine begrenzte Community, definiert durch ähnliche Zielvorstellungen hinsichtlich der medientechnischen Infrastrukturen und durch gemeinsame Grundsätze, die von breiten gesellschaftlichen Mehrheiten bisher keineswegs verstanden, anerkannt oder geteilt werden. Ähnlich steht es um zahlreiche rekursive Partikularöffentlichkeiten, die engagiert für Netzneutralität, informationelle Selbstbestimmung, unbeobachtete Kommunikation und Zensurfreiheit streiten. Dauerhafter Erfolg kann ihnen nur

8 Pfitzmann (1998): 132.

9 Kelty (2008): 3.

beschieden sein, wenn viele Menschen ihr Engagement als notwendig und wichtig erachten, wenn also das zuvor beschriebene Medienwissen zu einem selbstverständlichen Kernbestandteil des allgemeinen Bildungskanons wird: Affirmative Beliebigkeit in der Verwendung und Behandlung von Medientechnik ist in demokratischen Bildungsinstitutionen fehl am Platze. Stattdessen muss Bildung Interesse wecken, Wissen vermitteln und die kritische, engagierte Auseinandersetzung mit Technologien und neuen Kulturtechniken fördern.

Medienbildung wird so zu einem integralen Bestandteil politischer Bildung und zur notwendigen Grundausstattung einer Gesellschaft, die in allen Bereichen zunehmend auf digitale Technologien angewiesen ist. Medienwissen ist die Voraussetzung dafür, dass sich Bürgerinnen und Bürger entscheiden können, die Gestaltung dieser medientechnischen Existenzgrundlagen nicht länger intransparenten Dritten zu überlassen, sondern sich technisch und netzpolitisch zu engagieren. Diese Bildung, dieses Engagement sind die wichtigsten Anforderungen, vor die uns die digitale Vernetzung der Welt stellt: Wir brauchen eine rekursive Gesellschaft.

Trotz vereinzelter guter Ansätze scheint eine solche Gesellschaft heute in weiter Ferne zu liegen. Wenn es aber zutrifft, dass die «digitale Revolution» in ihrer gesellschaftsverändernden Wirkung der industriellen Revolution um Nichts nachsteht, dann gerät uns die Entwicklung einer rekursiven Gesellschaft tatsächlich zu einer gewaltigen Herausforderung, vergleichbar vielleicht nur der sozialen Frage und dem Kampf um Demokratie und Aufklärung während der letzten zwei Jahrhunderte: Denn die digitalen Infrastrukturen sind in ihrem jetzigen Zustand längst nicht neutral, transparent und offen. Gerade weil die digitale Vernetzung unsere Welt erschüttert und verändert, weil sie bestehende Macht- und Besitzverhältnisse in Frage stellt und neue zu schaffen vermag, ist die Entwicklung dieser Infrastrukturen vielfältigen Interessen und Einflussversuchen ausgesetzt. Nichts hätte uns dies drastischer vor Augen führen können als die Enthüllungen Edward Snowdens.

Es ist an uns, mit diesen Erkenntnissen angemessen umzugehen: Sehen wir über sie hinweg, wohl ahnend, dass andere die Gelegenheit zur Formung und Kontrolle der digitalen Infrastrukturen nicht verstreichen lassen? Resignieren wir in hilfloser Verweigerung oder Anpassung? Suchen wir Trost in der alten, trügerischen Euphorie, die uns angesichts von Innovation und Fortschritt überfällt? All dies wäre so nutzwie aussichtslos. Wenn wir dauerhaft verhindern wollen, dass die Fundamente der offenen Gesellschaft an der digitalen Schwelle untergraben werden, haben wir uns der digitalen Frage als einer zentralen Herausforderung unserer Zeit zu stellen, auch wenn sie keine einfachen und schnellen Antworten verträgt.

Literatur

Debray, Régis (1993): *Einführung in die Mediologie*. Bern/Stuttgart/Wien.

Heidegger, Martin (1959): *Gelassenheit*. Stuttgart.

Kelty, Christopher M. (2008): *Two Bits. The Cultural Significance Of Free Software*. Durham, London.

Kittler, Friedrich (1998): *Hardware, das unbekannte Wesen*. In: Sybille Krämer (Hg.): *Medien, Computer, Realität. Wirklichkeitsvorstellungen und neue Medien*. Frankfurt a.M., S. 119-132.

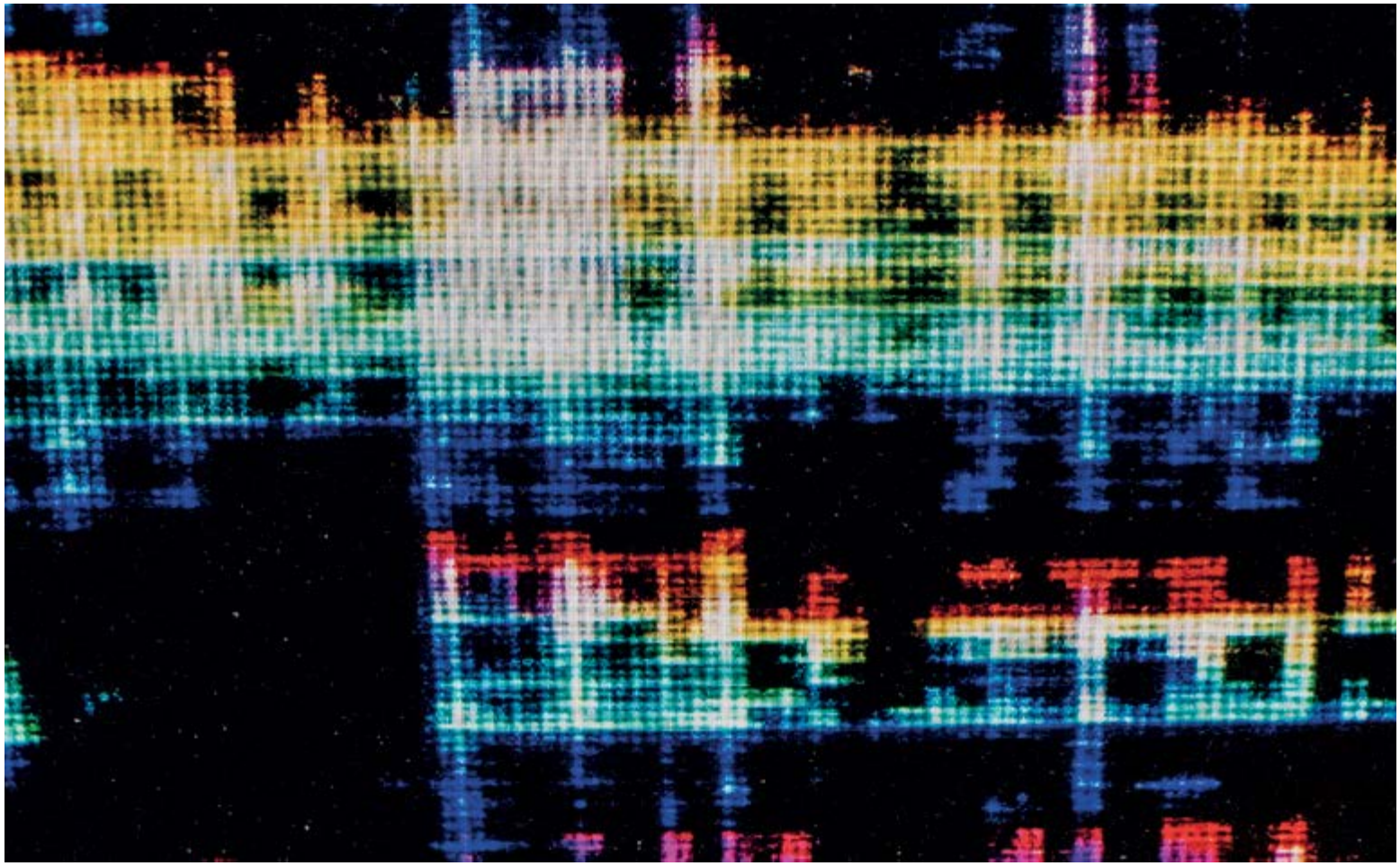
Lobo, Sascha (2014): *Die Digitale Kränkung des Menschen. Abschied von der Utopie*. in: FAZ, 11.Januar 2014.
Online: http://www.faz.net/aktuell/feuilleton/debatten/abschied-von-der-utopie-die-digitale-kraenkung-des-menschen-12747258.html.

Moglen, Eben (2011): *Why Political Liberty Depends on Software Freedom More Than Ever*. Rede bei FOSDEM 2011 in Brüssel am 5. Februar 2011.
Online: http://www.softwarefreedom.org/events/2011/fosdem/moglen-fosdem-keynote.html.

Morozov, Evgeny (2011): *The Net Delusion*. New York.

Morozov, Evgeny (2014): *Wider digitales Wunschdenken*. FAZ, 7.2.2014. Online: http://www.faz.net/aktuell/feuilleton/debatten/evgeny-morozov-antwortet-auf-martin-schulz-wider-digitales-wunschdenken-12790285.html.

Pfitzmann, Andreas (1998): *Warum brauchen wir Technik? Zum Verhältnis von Technik und Recht*. In: Bettina Sokol (Hg.): *20 Jahre Datenschutz. Individualismus oder Gemeinsinn?* Düsseldorf, S. 131–135.
Online: https://www.ldi.nrw.de/mainmenu_Service/submenu_Tagungsbaende/Inhalt/20_Jahre_Datenschutz/20_Jahre_Datenschutz1.pdf.



YVONNE HOFSTETTER

Big Data: Von der Analyse riesiger Datenmengen zur Steuerung des Menschen

Die digitale Wirtschaft konfrontiert die Zivilgesellschaft mit Big-Data-Geschäftsmodellen der Überwachung, Analyse und manipulativen Beeinflussung menschlichen Verhaltens. Das geschieht durch die massenweise Erhebung und Analyse riesiger Datenmengen unter zunehmendem Einsatz künstlicher Intelligenz für die Optimierung und Steuerung unseres Alltags. Doch den Apologeten der Big-Data-Industrie unterläuft ein Denkfehler: Sie degradieren den Menschen zum «Rohstoffträger» persönlicher Daten und bloßen Objekt ihres Wirtschaftens. Tatsächlich ist der Mensch Wirkursache des finanziellen Erfolgs und der wachsenden Macht globaler Technologiegiganten: Ein Aufruf für die Rechte der Person in Zeiten von Big Data.

Der britische Installationskünstler Luke Jerram (*1974) ist bekannt für seine 3D-Glasskulpturen. Ihm gelingt ein schwieriges Kunststück: die Visualisierung von Daten, etwa langer Zahlenreihen. Diese monochrome Ausdrucksweise dient Wissenschaftlern zur Kodierung von Phänomenen aus Natur, Wirtschaft oder Technik. Manchmal entbergen sich die als Daten verschleierten Geheimnisse unseres Lebens und werden unter aller Augen als katastrophales Ereignis sichtbar: als Vulkanausbruch, Erdbeben, Tsunami oder Börsencrash. Zu Jerrams Werken zählt deshalb auch die dreidimensionale Indexkurve der New York Stock Exchange mit ihren Finanzcrashs.[1] Gegossen in Glas, wirkt der Börsenindex wie ein gedrechseltes Werkstück, wie ein übertrieben ornamentierter Zierfuß eines historischen Möbelstücks. Dabei ist Jerrams Kunstwerk auch eine Metapher dafür, wie die moderne Mathematik unseren Alltag bestimmt. In der Vergangenheit half die Mathematik, das Universum zu erklären. Mit Big Data ist sie dazu übergegangen, die Welt neu zu gestalten – man könnte sagen, die Zukunft zu manipulieren. Die Mathematik erlaubt Terra Forming, und einzelne Industrien, darunter elektronische Börsen, geben bereits heute beredt Auskunft darüber, womit wir bald in größerem Ausmaß rechnen müssen.

1. Die Entstehung von Big Data in der militärischen Aufklärung

Big Data ist keine neue Technologie. Seit fast zwanzig Jahren werden Big-Data-Systeme zur militärischen Aufklärung und Lageanalyse genutzt. Ein bekanntes Beispiel ist das AWACS-Flugzeug. Mit seinen Sensoren erfasst das «fliegende Auge» alle Luftfahrzeuge eines Luftraums in Echtzeit. Erfassung heißt: Man sieht einen Plot auf einem Radarbildschirm, der sich bewegt. Das allein genügt dem Militär noch nicht. Es will mehr wissen: Ist das erfasste Luftfahrzeug zivil oder militärisch, um welchen Flugzeugtyp handelt es sich, welche Bewaffnung führt es mit? Ist ein

1 Jerram, Luke. 2012. Crash! Glass Stock Exchange Sculptures. Bristol: Luke Jerram.http://www.lukejerram.com/projects/stock_exchange_sculptures (abgerufen am 15.08.2014).

Aufklärungssystem gut konstruiert, findet es eine Antwort auf genau diese Fragen. Dazu «fusioniert» es alle vorhandenen Rohdaten: Geschwindigkeit des überwachten Flugzeugs, Radarrückstrahlfläche und zivile Flugpläne. «Multi-Sensor-Datenfusion», kurz: Datenfusion, heißt ein solch leistungsfähiges Computerprogramm, ein anderer Begriff für «Algorithmus». Beschrieben ist jener Algorithmus in der Sprache der Mathematik und realisiert mit künstlicher Intelligenz. Nur künstliche Intelligenz kann riesige Datenmassen in Echtzeit analysieren. Hat die intelligente Maschine eine Antwort gefunden: «Das erfasste Luftfahrzeug ist ein russischer Sukhoi-Su-24s-Kampfjet, Status: Feindlich», fehlt noch ein letzter Schritt im Prozess: die Entscheidung, was denn nun zu tun sei. Soll man den russischen Kampfjet unbehelligt lassen? Soll man ihn abschießen? In gut durchdachten Datenfusionssystemen wird auch diese Entscheidung, die sogenannte Kontrollstrategie, von einer intelligenten Maschine berechnet und automatisch ausgelöst. Datenfusionssysteme mit ihrem Dreiklang «überwachen – analysieren – steuern» sind deshalb nicht nur für Aufklärungsaufgaben nützlich, sondern als Basistechnologie etwa für die Selbststeuerung autonomer Drohnen oder für die automatische Zuweisung eines Ziels zu einer Waffe geeignet. Wäre das Luftabwehrsystem, mit dem russische Rebellen den zivilen Flug Malaysian Airlines 17 am 17. Juli 2014 vermutlich abgeschossen haben, mit einer leistungsfähigen Datenfusion und maschinellen Kontrollstrategie ausgerüstet gewesen, hätte das System den zivilen Airliner nicht nur automatisch als nichtmilitärisch identifizieren, sondern den Abschuss der todbringenden Rakete maschinell blockieren können. Das war die ursprüngliche, eigentliche Idee der Architekten der Datenfusion Mitte der Neunzigerjahre: Intelligente Maschinen zu bauen, die Entscheidungsträger unterstützen. Intelligente Auto-»Piloten», die in stressbelasteten Situationen eine systematische, nachvollziehbare und «bessere» Entscheidung als der Mensch treffen würden.

2. Big data heute: massenhaft persönliche Daten

Was also ist neu an Big Data 2014? Natürlich hat es in den vergangenen Jahren technische Fortschritte gegeben. Damit sind durchaus nicht Verbesserungen bei den Algorithmen für die Datenfusion gemeint. Neu an Big Data 2014 sind die infrastrukturellen Bedingungen: Seit 2010 steigen die verfügbaren Massen unstrukturierter Daten wie Bilder, Texte oder Videos gewaltig an. Der Grund: die exzessive Nutzung mobiler Technologien wie Smartphones und Tablet-PCs. Und die Qualität der Datenberge ist eine andere. Die heute verfügbaren Daten stammen nicht mehr von Objekten, wie das bei der militärischen Überwachung der Fall ist, sondern von Menschen, von Personen. Sie bestehen aus einem ganz überwiegenden Teil aus «personenbezogenen Daten», so die korrekte juristische Bezeichnung für unsere Daten. Werden wir in der Folge etwas weniger formal und benutzen den Begriff der persönlichen Daten. Eine weitere Neuerung bei Big Data 2014 ist die Verfügbarkeit massiv paralleler Supercomputer für jedermann. Sehr vereinfacht gesagt, ist ein Algorithmus – auch der Datenfusionsalgorithmus – ein Berechnungsverfahren. Das Wort sagt es bereits: Ein Algorithmus hat mit Rechnen zu tun, also mit Mathematik. In der Welt von Big Data spielt die Mathematik die fundamentale Rolle schlechthin. Denn um aus unstrukturierten Daten Erkenntnisse zu gewinnen, müssen Strukturen erst modelliert werden. Bevor ein Mathematiker – nennen wir ihn allgemeiner einen

Data Scientist – Daten überhaupt analysieren kann, muss er sich vorweg die Frage stellen, was er aus den Daten herauslesen möchte, wie also sein Modell aussehen und was das Ziel seiner Berechnungen sein soll. Und diese Berechnungen müssen schnell gehen. Genau diese Schnelligkeit hat die Computerindustrie vor rund fünf Jahren für den breiten Markt hergestellt, als die Produzenten grafischer Prozessoren, die ursprünglich für die wie real wirkenden Darstellungen von Computerspielen gedacht waren, einen neuen Anwendungsbereich entdeckten: das parallele Berechnen tausender Variablen von umfangreichen Gleichungen auf ihren Grafikkarten.

3. Was Data Scientists mit Daten tun

Stellen wir uns einen Data Scientist vor, dem man historische Wechselkursdaten von Währungen aus den vergangenen zehn Jahren übergibt. Für einen internationalen Konzern soll er eine Maschine bauen, die das Wechselkursrisiko für den Konzern minimiert. Dazu muss unser Data Scientist unter vielem anderem verstehen, wie der Währungsmarkt funktioniert, damit seine Maschine eine Prognose über das wahrscheinliche Verhalten von Währungen berechnen kann, auf die sich der Konzern später verlassen wird. Also beginnt unser Data Scientist zunächst damit, ein Interaktionsmodell jenes Lebensbereichs zu erstellen, den wir als «Währungsmarkt» bezeichnen. Er identifiziert die Marktteilnehmer, darunter Zentralbanken, Geschäftsbanken, Broker, international tätige Firmen und auch Spekulanten, und definiert die Variablen, die die Wechselkurse bestimmen. Solche Variablen sind die Entwicklung der Leitzinsen, die aktuelle wirtschaftliche Situation, die gehandelten Währungsvolumina, die Marktstrategien der Marktteilnehmer, auch Transaktionskosten oder -steuern. Manche Variablen kann er beobachten und direkt aus seinen Datenbergen auslesen. Andere Variablen sind nicht beobachtbar, sie sind «latent». Er überlegt, wie die Variablen zusammenhängen, ob sie sich gegenseitig beeinflussen oder miteinander korreliert sind. Bis hierher können Sie, lieber Leser, auch noch Mathematik betreiben. Es ist jener philosophische Teil der Mathematik, bei dem der Wissenschaftler in einem Ohrensessel sitzt, an seiner Pfeife zieht, stumm gen Himmel schaut und – langsam nachdenkt.

Der nächste Schritt ist allerdings nur für Insider. Das fertige Interaktionsmodell muss in ein mathematisches Modell übersetzt werden. Die Variablen des Interaktionsmodells werden neu beschrieben – eben in jener Beschreibungssprache, die sich Mathematik nennt. Die Variablen werden in Formeln transkribiert, bis schließlich eine gewaltige Gleichung entsteht, die den Währungsmarkt beschreibt. Ist die Gleichung «korrekt», sollte sie in der Lage sein, das historische Verhalten des Währungsmarktes, wie es in den Datenmassen enkodiert ist, widerspruchsfrei zu erklären und dem Data Scientist anzuzeigen, unter welchen Bedingungen etwa Trends auftreten. Genügt das mathematische Modell den Ansprüchen des Data Scientists, geht er noch einen Schritt weiter: Er will aus der – nun richtig verstandenen – Vergangenheit auf die Zukunft schließen. Seine Hypothese ist: Die Zukunft ist in der Menge der historischen Daten verborgen. Ähnlich geht auch die Wettervorhersage vor: Wenn Sie wissen wollen, wie das Wetter morgen und übermorgen wird, müssen Sie auf das Wetter heute, vielleicht noch auf das von gestern schauen.

Für die Prognose helfen dem Data Scientist Verfahren der künstlichen Intelligenz weiter, genauer: Maschinen, die lernen können. In einer Trainingsumgebung aus Supercomputern präsentiert der Data Scientist seiner lernenden Maschine die Beobachtungen, die er aus den historischen Datenmassen gewonnen hat. Aufgabe der Maschine, bei der es sich oft um einen Optimierungsalgorithmus handelt, ist es nun, die beste Strategie zu berechnen, mit der man das Wechselkursrisiko des Konzerns minimieren kann, eben eine Kontrollstrategie, von der schon vorher die Rede war.

Wird die intelligente Maschine in den operativen Einsatz entlassen, wird sie nicht mehr länger die Trainingsdaten des historischen Währungsmarktes beobachten und daraus ihre Schlüsse ziehen. Ab jetzt überwacht sie die neuesten Wechselkurse, wie sie in Echtzeit von Preistickern übertragen werden. Ihre Entscheidungen, erlernt durch die millionenfache Suche nach der optimalen Risikostrategie, beeinflusst unmittelbar das Betriebsergebnis des Konzerns. Ihre Kontrollstrategie gestaltet das Betriebsergebnis aktiv mit, weil sie Verlustrisiken durch Währungsschwankungen in Echtzeit ausgleicht. Das ist das Terra Forming, die Beeinflussung der Zukunft, die Big Data mit ihren Datenbergen, mathematischen Modellen und Supercomputern erst seit einigen Jahren im großen Stil ermöglicht.

Spannend an der Arbeit des Data Scientist ist, dass er sein Handwerkszeug auf jeden beliebigen Lebensbereich anwenden kann. Ob Währungsmärkte, industrielle Wertschöpfungsketten, Waffensteuerungen, Aufklärungssysteme oder den Alltag des Bürgers – wer die modernen Big-Data-Schlüsseltechnologien beherrscht und ausreichend Datenmaterial gesammelt hat, gehört zum Kreis jener Expertokraten, die unsere gesellschaftliche Zukunft gestalten und über ein nicht zu unterschätzendes Machtpotential verfügen. Was einst historisch gesehen in den Händen hoheitlicher Institutionen lag, gut gehütet unter rechtsstaatlicher Aufsicht, hat längst den Kommerz erreicht. «Proliferation» nennt sich dieser Vorgang. Er meint die Wucherung von Wissen aus einem Sektor heraus in andere Sektoren und Industrien hinein. Doch wie hat es soweit kommen können?

4. Die erste Kommerzialisierungswelle in der Finanzindustrie

Seit sich Mathematiker und Physiker aus dem Militär nach dem Fall des Warschauer Pakts in den Neunzigerjahren ein neues Betätigungsfeld suchten und es als «quantitative Analysten» an den Börsen fanden, verbreitet sich das Wissen um die Datenfusion. Statt feindlicher Flugzeuge überwacht man Aktienkurse, Fundamentaldaten und Firmennachrichten, fusioniert alles zu einer Lage und überlässt einer Kontrollstrategie die Entscheidung, wann und in welcher Höhe eine Kauforder zu tätigen ist. Seit dem Jahr 2006 nahm der «algorithmische Handel» jedoch eine besondere Wendung, und aus Big Data wurde Big Speed. Heute ist der amerikanische Börsenhandel zu mehr als siebzig Prozent von Hochfrequenzalgorithmen dominiert.[2] Beim Hochfrequenzhandel wickeln Maschinen mit Maschinen im Mikrosekundenbereich

2 Wenning, Brenda. 2013. The TABB Group estimates that HFT accounts for 73% of all trades on American stock exchanges. New York, NY: AdviceIQ. http://quantlabs.net/blog/2013/02/the-tabb-group-estimates-that-hft-accounts-for-73-of-all-trades-on-american-stock-exchanges/#sthash.C4XMyKMN.dpuf (abgerufen am 15.08.2014).

Handelsaufträge ab. In ihrem maschinellen Paralleluniversum ist der Mensch nur Statist, Beobachter eines unverständlichen Auf und Ab von Wertpapierkursen in einem, wie institutionelle Händler beunruhigt feststellen, «perversen System.» Denn in der Welt der Maschinen geht vieles schief. Programmierfehler in den Algorithmen führen zu «blitzartigen Kursstürzen», den Flash Crashs, oder längeren Stillständen an den Börsen.[3] Als ob dies nicht genüge, manipulieren einige Marktteilnehmer mit ausgefeilten Algorithmen Wertpapierkurse ganz bewusst, wie es auch am 6. Januar 2014 geschah, als der Goldpreis fiel und der Handel kurz ausgesetzt wurde.[4] Terra Forming an der Börse: Wertpapierkurse, wenn sie durch Algorithmen manipuliert sind, haben mit der Realwirtschaft nicht das Geringste zu tun und wirken sich doch global auf alle Märkte aus.

5. Die zweite Kommerzialisierungswelle: Big Data 2014 trifft auf den Konsumenten

Die zweite Kommerzialisierungswelle von Big Data erfasst jeden einzelnen Konsumenten, jedes Individuum. Dabei sitzen die Nutzer von Computern, Smartphones und Tablet-PCs einem gewaltigen Irrtum auf: Sie glauben, bei Big Data ginge es nur um das Sammeln ihrer persönlicher Daten. Dafür stelle ihnen das Internet eine riesige Datenbank für Fotos, E-mails oder Urlaubsgeschichten zur Verfügung. Wäre das so, wir hätten kein Problem und müssten keine Debatte über die Zukunft des freien Menschen führen. Doch hinter dem Bildschirm entsteht ein Ökosystem millionenschwerer intelligenter Maschinen, die unsere bekannte Welt aus den Angeln heben. Heute beschränken sich intelligente Maschinen nicht mehr auf die unterbrechungsfreie Beobachtung von Objekten des Wirtschaftens. Neu ist, dass sich die Überwachung durch Maschinen nun auf Personen erstreckt - in einem bisher ungeahnten Ausmaß. Maschinen überwachen unser Verhalten und unsere Verhältnisse, klauben daraus unseren digitalen Zwilling zusammen, prognostizieren unsere Zukunft – und steuern nach, wo sie es für nötig halten. Das ist das erklärte Ziel des «Geschäftsmodells Überwachung». Noch hat es sich nicht in dem Umfang durchgesetzt, wie es sich Big-Data-Protagonisten wünschen. Doch viel Zeit bleibt nicht, um Gegenmaßnahmen zu ergreifen. Zu verführerisch sind die Verheißungen der schönen, neuen Kontrollgesellschaft, die uns Selbstoptimierung und ein bequemes Leben versprechen. Ihre Verlockungen sind die Falle, die dann zuschnappt, wenn wir uns einen kurzfristigen persönlichen Vorteil von der Totalüberwachung erhoffen.

Häufig bleibt dem Konsumenten verborgen, wo er mit intelligenten Maschinen in Berührung kommt. Bei Big Data ist er manchmal Nutzer und Nutznießer intelligenter Kontrollstrategien, wenn er etwa ein teilautonomes Auto fährt oder sich auf intelligente Haustechnik verlässt. Er selbst ist nicht Betreiber intelligenter Maschinen, aber er liefert ihnen seine Daten. Dazu dient das Internet als Kommunikationsinfrastruktur. Das Internet verbindet die Konsumenten mit der Maschinenintelligenz. Dabei ist ein Trend feststellbar: Die Erhebung persönlicher Daten

3 Johnson, Neil et al. 2013. Abrupt rise of new machine ecology beyond human response time. In: Nature, Scientific Reports 3, 2627. New York, NY: Nature Publishing Group.

4 Nanex Research. 2014. First Gold Halt of 2014. Boston, MA: Nanex LLC. http://www.nanex.net/aqck2/4522.html (abgerufen am 15.08.2014).

findet immer öfter nicht-kooperativ statt. Emails, Blogeinträge, Familienfotos geben wir noch mit unserem Einverständnis weiter. Doch der Trend geht dahin, dass wir nicht nur von Polizeibehörden und Geheimdiensten, sondern immer mehr von privaten Wirtschaftsunternehmen ohne unser Einverständnis, sogar gegen unseren Willen überwacht werden. Die «magische Brille» eines globalen Technologieanbieters ist ein gutes Beispiel für die nicht-kooperative Datenerhebung. Ein Brillenträger, der uns heimlich filmt und abhört und seine Aufzeichnungen öffentlich im Internet verfügbar macht, macht sich nach deutschem Recht strafbar, §§ 201, 201a Strafgesetzbuch. Es ist zu Recht fraglich, wie strafrechtliche oder urheberrechtliche Vorschriften durchsetzbar bleiben sollen, wenn die «magische Brille» zu demselben Massenphänomen wie das Smartphone wird?

Das Beispiel macht deutlich, worum es bei Big Data, bei der digitalen Wirtschaft überhaupt, geht: Um einen wahren Umsturz. Das «Alte» hält der Revolution nicht mehr stand. Traditionelle Geschäftsmodelle wanken über alle Industrien und Branchen hinweg. Und von der übergreifenden Unruhe, von dem Zwang zum Paradigmenwechsel, bleiben weder Grundrechte noch Rechtsordnung noch die Gesellschaft insgesamt verschont. Big Data beschränkt sich nicht nur auf einzelne Branchen und Sektoren. Big Data betrifft die gesamte Zivilgesellschaft. Denn was trotz seiner Heilsversprechen, darunter wie so oft und durchaus zu Recht das des wirtschaftlichen Wachstums, problematisch ist: Big Data bringt unser Menschenbild ins Wanken. Es ist das Menschenbild, das die Mütter und Väter unseres Grundgesetzes in Art. 1 mit Ewigkeitsgarantie festgeschrieben haben: «Die Würde des Menschen ist unantastbar.» Big Data setzt die Menschenwürde aufs Spiel und damit unsere demokratisch-freiheitliche Gesellschaftsordnung.

6. Der Angriff auf das europäische Menschenbild und die Demokratie

Immanuel Kant (1724-1804) hat dem Menschenbild, das dem Grundgesetz für die Bundesrepublik Deutschland zugrunde liegt, einen theoretischen Rahmen verliehen. Weil der Mensch in der Lage sei, vernünftig zu handeln, unterscheide er sich von seinen Mitgeschöpfen. Der Mensch sei zwar Teil der Schöpfung, steche aber durch seine Fähigkeiten zu Verantwortung, Gewissen, Moral daraus hervor. Als «Krone der Schöpfung» sei er Subjekt, die übrige Schöpfung sei Objekt und dem Menschen unterworfen. Tatsächlich spiegelt sich dieser Dualismus auch in unserer Rechtsordnung: der Mensch ist «Rechtssubjekt», er ist Träger von Rechten und Rechtspflichten. Eingebettet ist die Subjektivität des Menschen in die Menschenwürde. Aus ihr gehen die Freiheitsrechte hervor, wie sie das Grundgesetz garantiert, darunter das verantwortungsvolle, vernünftige Herrschaftsrecht über die Objekte der Schöpfung, ebenso das Recht auf die «negative Freiheit» – das Recht, in Ruhe gelassen zu werden – mit ihrem Recht auf Privatsphäre.

Genau diese Dichotomie von (Rechts-)Subjekt und Objekt ist es, die die Big-Data-Industrie verleugnet. «(Persönliche) Daten sind der Rohstoff des 21. Jahrhunderts», das Öl, das neue Gold der Wirtschaft, sagt uns die Big-Data-Industrie. Big Data nimmt den Menschen nicht als Subjekt wahr, sondern als Objekt, als Rohstoffträger, der ausgebeutet und um seine Daten gebracht werden muss. So erklärt sich leicht, warum Big Data unter der aktuellen Rechtslage zu millionenfachen Rechtsverstößen führt. Big Data erkennt den Subjektcharakter von Personen

nicht an; sie sind nicht mehr als Objekte seiner Geschäftsmodelle. Konsumenten sind die Ware der Big-Data-Industrie, nicht ihre Kunden. Besondere Freiheitsrechte gelte es deshalb nicht zu beachten.

Ähnliches trifft für den Demos, das «Volk», zu, das ein Vielfaches des einzelnen Bürgers ist. Denn die Big-Data-Industrie zielt nicht nur darauf ab, unser Menschenbild umzubauen, sondern auch zentrale Funktionen unserer Gesellschaft zu verändern. Dazu gehört auch unsere demokratische Staatsform. Darüber müssen wir nicht einmal spekulieren. «Die Demokratie ist eine alte Technologie»,[5] sagen uns die Internetgiganten, man müsse etwas Neues ausprobieren und einen Staat etwa wie ein Startup-Unternehmen führen. Wer jemals ein Unternehmen geleitet hat, weiß, dass nur autokratische Strukturen schnelle Entscheidungen ermöglichen, um Marktanteile zu gewinnen oder ein Unternehmen aus einer Schieflage zu bringen. Die Demokratie ist hier eher hinderlich, und so sind demokratisch geführte Unternehmen selten über die Erprobungsphase hinaus gekommen.

Die Weltmachtsfantasien globaler Technologiegiganten werden durch die Akkumulation von Daten und die Schlüsseltechnologien der Datenfusion beflügelt. Beides, Daten und Schlüsseltechnologien, in einer Hand vereint, bedeutet Macht. Auch das ist neu an Big Data 2014: Trotz zunehmender staatlicher Überwachung findet diese Machtkonzentration nicht bei demokratisch legitimierten Staaten, sondern in privaten Wirtschaftsunternehmen statt. Im Sommer 2013 installierte Amazon ein Team für maschinelles Lernen und warb viele in Deutschland verfügbare Experten an. Im Dezember 2013 gab Facebook bekannt, es setze künftig auf künstliche Intelligenz, «um aus all den Inhalten, die Facebook-Nutzer einstellen, klug zu werden.»[6] Am eindeutigsten, jedenfalls aus der Sicht von Technologieexperten, agiert jedoch Google. Seit Dezember 2013 hat Google mit dem Kauf von Militärrobotern, adaptiven Rauchmeldern, maschinellen Lernverfahren, Drohnen und Satelliten genug Überwachungs-Knowhow, Hardware und künstliche Intelligenz erworben, um mit smarten Geräten künftig direkt bis in unsere Häuser und unsere Intimsphäre vorzudringen. Gefragt werden wir nicht. Als «Internet der Dinge» sollen uns die Gegenstände unseres Alltags engmaschig überwachen mit dem Versprechen, unser Leben zu optimieren. Konkret bedeutet das: Kontrollstrategien werden uns optimale Handlungsempfehlungen geben oder eine optimierte Entscheidung gleich selbst ausführen. Das ist bequem: Eine Entscheidung, die ein anderer für uns trifft, müssen wir nicht mehr selbst treffen. Das sei gut für die Menschen, so der Internetgigant, punktum. Dabei ist ein solcher Top-Down-Approach, ein «hierarchisches Diktat», das genaue Gegenteil von Demokratie, die sich aus der Willensbildung durch den Souverän «von unten», aus Wahlfreiheit statt Alternativlosigkeit und der Kontrolle der Handelnden speist.

5 Hencken, Randolph. 2014. In: Mikrogesellschaften. Hat die Demokratie ausgedient? Capriccio. Video, veröffentlicht am 15.5.2014. Autor: Joachim Gaertner. München: Bayerischer Rundfunk.

6 Isaac, Mike. 2013. Facebook Steps Up Artificial-Intelligence Efforts With New Research Lab. New York, NY: Dow Jones & Company, Inc: AllThingsD. http://allthingsd.com/20131209/facebook-steps-up-artificial-intelligence-efforts-with-new-research-lab/ (abgerufen am 15.08.2014).

7. Unsere Kulturgeschichte inspiriert die Lösung des Konflikts

Dumm nur, dass es in einer solchen Kontrollgesellschaft mit der Freiheit des Einzelnen nicht mehr weit her ist. Wenn wir nicht rasch einen gesellschaftlichen Konsens finden, wie wir die intelligenten Maschinen der digitalen Ökonomie beherrschen, werden wir in Kürze bald selbst von ihnen beherrscht. Wenn wir uns den digitalen Technologien, ihren mathematischen Modellen und Algorithmen unterwerfen, werden sie unser Leben determinieren und nicht mehr wir selbst!

Ist guter Rat also teuer?

Nicht unbedingt. Denn die Werteverwirrung durch die Big-Data-Industrie ist nicht neu und hat einen Vorläufer in unserer Kulturgeschichte. In der Objektivierung des Menschen drückt sich der «alte» Denkfehler einer Ideologie aus, mit der die Gesellschaft schon in der Vergangenheit konfrontiert wurde. Es ist der grundlegende Irrtum des Kapitalismus, der den Menschen seinem Wirtschaften unterordnen will.

Unsere Industriegeschichte kann die Lösung für den Konflikt mit Big Data anregen und den Schlüssel zu einer guten Mensch-Maschine-Zukunft bergen. In 2014 ist der Mensch aus 1914 in aller Munde. Er ist uns ganz nah, dieser Mensch aus 1914; auch er befindet sich im Zeitalter der Beschleunigung, weil gerade der Motor erfunden wurde und die Dampflok Geschwindigkeiten von hundert Stundenkilometer erreicht. Der Mensch wird urban, er zieht in die Städte, dorthin, wo die «erste maschinelle Revolution» stattfindet, die Dampfmaschinen rauchen und die Essen dröhnen. Diese erste maschinelle Revolution bringt ein neues Gut hervor: Es ist das Gut der geteilten Arbeit an den Fließbändern. Begleitet wird die erste maschinelle Revolution von einer Ideologie, der des «ersten Kapitalismus». Kapital und Produktionsgüter akkumulieren sich in den Händen weniger, während die große Mehrheit der Menschen nur mit einem einzigen Mittel am Wirtschaftsprozess teilnimmt: mit ihrer menschlichen Arbeit. Es bildet sich die Arbeiterklasse, und schnell wird klar, dass genau sie es ist, die nicht vom wachsenden Wohlstand der Gesellschaft profitiert. Exzesse sind an der Tagesordnung, darunter Zwölfstundentage, Kinderarbeit und unerträgliche hygienische Arbeitsverhältnisse. Zu Beginn der ersten maschinellen Revolution am Anfang des letzten Jahrhunderts gibt es noch keine Regeln.

Dabei ist die menschliche Arbeit ebenso wenig eine Ware des Wirtschaftens, wie es unsere persönlichen Daten sind. Die menschliche Arbeit sticht aus dem Universum der Güter hervor. Denn die menschliche Arbeit ist ganz existenziell mit dem Menschen selbst verbunden. Sein ganzes Leben ist auf seine Arbeit verwiesen; ohne Arbeit wird er kaum seine Existenz sichern können. Und weil die menschliche Arbeit so ursprünglich und existenziell zum Menschen gehört wie kein anderes Objekt des Wirtschaftens («Im Schweiße deines Angesichts sollst du dein Brot essen», wie die Bibel sagt) «erbt» die menschliche Arbeit etwas von der Subjektivität der menschliche Person. Das erklärt, warum es folgerichtig war, die Arbeit im Laufe des 20. Jahrhunderts zu humanisieren. Die menschliche Arbeit ist nicht dazu da, ausgebeutet zu werden. Sie erbt den ethischen Charakter der menschlichen Person und hat damit einen ganz besonderen Stellenwert, einen «ethischen Wert». Diesem Wert muss die Gesellschaft gerecht werden: durch angemessene Löhne, menschenwürdige Arbeitszeiten und -bedingungen. In

unseren westlichen Kulturen haben wir diese Anforderungen bis heute weitgehend umgesetzt.

Mit einer vergleichbaren Situation sind wir zu Beginn des 21. Jahrhunderts konfrontiert. Dabei hält die «zweite maschinelle Revolution», die der intelligenten Maschinen, eine wirkliche Neuerung in der Menschheitsgeschichte bereit. Ab jetzt nimmt der Mensch nicht nur mit seiner menschlichen Arbeit, sondern auch mit seinen persönlichen Daten am Wirtschaften teil. Tatsächlich sind wir Menschen die Wirkursache der Big-Data-Geschäftsmodelle. Unsere persönlichen Daten ermöglichen es, dass Internetgiganten zu reichen, mächtigen Institutionen aufsteigen. Die menschliche Arbeit ist existenziell für den Menschen. Dasselbe trifft auf persönliche Daten zu. In ihren persönlichen Daten kommt die ganze Existenz einer Person zum Ausdruck. Sie dienen uns dazu, uns zu verwirklichen und unser Recht auf Kommunikation geltend zu machen, wie es grundlegend für eine Gesellschaft ist. In persönlichen Daten kommen die sozialen Beziehungen einer Person zum Ausdruck, ihre politischen Meinungen, wie, wann und wo sie sich bewegt, was sie liebt oder ablehnt. Wer die persönlichen Daten eines Menschen zusammensetzt, erhält ein Spiegelbild der Person, den digitalen Zwilling, der, wenn er von Datenfusionsalgorithmen analysiert, kategorisiert, standardisiert und prognostiziert wird, zum «virtuellen Zombie» wird. Zieht der virtuelle Zombie seine Kreise, wird er etwa unbeobachtet, unwissentlich und ungewollt an Versicherungen, Banken oder Arbeitgeber weiterverkauft, bekommt das Wort «Schicksal» eine ganz neue Bedeutung für den Menschen. Der «virtuelle Zombie» eines Menschen kann verhindern, dass er eine Autoversicherung, einen Kredit, die notwendige Operation oder einen Arbeitsplatz erhält. Exzess neu interpretiert: Die Determinierung der Zukunft einer Person durch die Big-Data-Industrie und nicht durch die Person selbst ist ein so unerträglicher Verstoß gegen die Selbstbestimmung des Menschen, dass klar ist: Nicht nur unsere menschliche Arbeit, auch unsere Daten «erben» die Subjektivität der menschlichen Person. Genau wie die menschliche Arbeit verdienen sie deshalb einen ganz besonderen Schutz.

Auch heute gilt:

Es fehlen Regeln für das neue, das digitale Zeitalter. Die Indizien haben wir bereits benannt: Es kommt zu millionenfachen Rechtsbrüchen, so dass wir uns fragen müssen, ob unsere Rechtsordnung obsolet ist, wo sie gegen Big Data nicht mehr durchsetzbar zu sein scheint, und welche neuen Regeln sie benötigt, um die Rechte der Person wieder ganz herzustellen.

8. Die Zivilgesellschaft muss handeln

Freiheit geht immer Hand in Hand mit Verantwortung, und die Menschenwürde verwirklicht sich zuerst bei jedem Einzelnen. Wer verhindern will, dass seine Zukunft künftig von intelligenten Kontrollstrategien besiegelt wird, muss die Datenzufuhr unterbrechen. Keine Daten, wenige und unvollständige Daten bedeuten eine schlechte Lageanalyse und eine unwirksame Kontrollstrategie. Wer auf Basis einer Lageanalyse mit unvollständigen Daten optimiert oder manipuliert werden soll, wird das sehr schnell bemerken. Deshalb ist es wenig angebracht, den Aufruf von

Hans Magnus Enzensberger, man möge sein Mobiltelefon wegwerfen, zu ironisieren.[7] Eine Demokratie lebt von Alternativen, nicht von der alternativlosen Unterordnung des Menschen unter die Technik.

Auch der Staat ist in der Pflicht und, mehr noch, grundgesetzlich dazu aufgerufen, die Menschenwürde zu schützen. Wer die Alternative zur digitalen Abstinenz wählt, darf für seine Entscheidung nicht diskriminiert werden oder Nachteile erleiden. Die Alternative der digitalen Abstinenz ist nichts weniger als die Realisierung der negativen Freiheit. Wer sich hingegen für die vollumfängliche Teilnahme an Big Data entscheidet und seine Daten bereitwillig zur Verfügung stellt, darf nicht ausgebeutet werden. Die Subjektivität persönlicher Daten verleiht ihnen einen Wert. So wie Menschen nicht ohne Lohn arbeiten, so wenig sollten persönliche Daten kostenlos erhoben werden. Eine Gesellschaft, die eine finanzielle Kompensation für persönliche Daten verlangt, wird Big-Data-Geschäftsmodelle der Überwachung, die wenig Aussicht auf Erfolg haben, gar nicht erst ausbrüten. Hinzukommen muss das Recht auf die Kontrolle persönlicher Daten. Das Recht auf Löschung, wie sie der EuGH in seinem Google-Urteil vom 13. Mai 2014 ausgesprochen hat,[8] ist hier nur ein erster Schritt. Wer persönliche Daten als Wirkursache für sein gewinnbringendes Geschäftsmodell nutzt, muss Auskunft geben, was er mit den Daten vorhat, wo und wie lange er sie speichert, welche Schlüsse er aus ihnen zieht und ob und wohin er sie weiterverkauft. Das Recht des Datensubjekts muss dem Recht auf freie Entfaltung der Big-Data-Industrie, die als Instrument der Ökonomie der Person stets untergeordnet sein muss, klar vorgehen.

Der letzte Aufruf richtet sich an die Data Scientists. Wer hört nicht ihren Aufschrei, ihre Modelle, Algorithmen und Datenanalysen seien wertfrei, und ihnen läge nichts ferner als der Angriff auf den freiheitlichen Menschen? Das ist wahr, tatsächlich hindert aber nichts die findigen Entrepreneurs und Manager unseres Jahrzehnts daran, den Data Scientists Technologien «abzujagen» und gegen die Menschenwürde einzusetzen. Deshalb muss gelten: Wir brauchen nicht weniger Technologie, sondern bessere Technologie. Unsere Algorithmen, Datenanalysen und Kontrollstrategien müssen bereits per Design «Benimmregeln» implementieren, die schon auf «Maschinenebene» mehr Grundrechtsschutz der einzelnen Person gewährleisten.

Technik und wirtschaftliche Entwicklung müssen dem Menschen dienen, nicht umgekehrt. Wer diese Reihenfolge beherzigt, kann die Rahmenbedingungen setzen, die selbst Big Data zähmen. Was jedoch zählt, ist der entschiedene Wille, am freiheitlichen Menschen unseres Grundgesetzes festzuhalten. Darum sollte sich die gesellschaftliche Debatte drehen – um einen Technologieethos und die

7 Enzensberger, Hans Magnus. 2014. Wehrt Euch! Frankfurt: Frankfurter Allgemeine Zeitung. http://www.faz.net/aktuell/enzensbergers-regeln-fuer-die-digitale-welt-wehrt-euch-12826195.html (abgerufen am 05.03.2014).

8 Gerichtshof der Europäischen Union. 2014. Pressemitteilung Nr. 70/14 vom 13.05.2014: Der Betreiber einer Internetsuchmaschine ist bei personenbezogenen Daten, die aufvon Dritten veröffentlichten Internetseiten erscheinen, für die von ihm vorgenommene Verarbeitung verantwortlich. Luxemburg: Gerichtshof der Europäischen Union. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf (abgerufen am 18.08.2014).

Frage, wie weit Big-Data-Technologien gehen dürfen. Sie können und wollen, aber müssen nicht so weit reichen, den freiheitlichen Menschen zu zerstören. Denn auch mit einer Big-Data-Regulierung ist die Gefahr längst nicht gebannt: Der «Posthumane», der technisch aufgerüstete Mensch, der den Homo sapiens überflügeln soll, steht schon in den Startlöchern und profitiert von Milliarden amerikanischer Forschungsgelder. Nach Big Data gilt er als die größte intellektuelle Herausforderung unseres Jahrhunderts. Die Freiheit, wir tragen sie in zerbrechlichen Gefäßen.

Autorinnen und Autoren

Dr. **Ulrike Ackermann,** Politikwissenschaftlerin und Publizistin, ist Professorin an der privaten SRH Hochschule Heidelberg. Dort gründete sie und leitet das John-Stewart-Mill-Institut für Freiheitsforschung und gibt die Werke von Mill heraus. Ihr Institut veröffentlicht den jährlichen *«Freiheitsindex Deutschland»*. Neben zahlreichen anderen Veröffentlichungen erschien 2009 ihr Buch *«Eros der Freiheit»*.

Dr. **Marion Albers** ist Professorin für Öffentliches Recht, Informations- und Kommunikationsrecht, Gesundheitsrecht und Rechtstheorie an der Universität Hamburg. Sie studierte Rechtswissenschaften, Soziologie, Politologie und Ökonomie in Berlin und Bielefeld, habilitierte zum Thema «informationelle Selbstbestimmung» und war Mitarbeiterin am Bundesverfassungsgericht. Albers war als Sachverständige Mitglied in der Enquête-Kommission des Deutschen Bundestages *Ethik und Recht der modernen Medizin.*

Jan Philipp Albrecht ist GRÜNER Europabgeordneter seit 2009, stellvertretender Vorsitzender des Innen- und Justizausschusses des Europaparlaments sowie dessen Berichterstatter für die geplante EU-Datenschutzverordnung. Albrecht war Sprecher der GRÜNEN Jugend, studierte Rechtswissenschaften und ist Gründungsmitglied des Instituts für Solidarische Moderne. 2014 erschien sein Buch *«Finger weg von unseren Daten! Wie wir entmündigt und ausgenommen werden»*.

Dr. **Leonhard Dobusch** ist Juniorprofessor für Organisationstheorie an der FU Berlin. Er studierte Wirtschaftswissenschaften und Rechtswissenschaften in Linz. 2014 gab er gemeinsam mit Valie Djordjevic *«Generation Remix: Zwischen Popkultur und Kunst»* heraus.

Prof. Dr. **Hannes Federrath** leitet die Abteilung *Sicherheit in verteilten Systemen* an der Fakultät für Informatik an der Universität Hamburg. Zu seinen Forschungsschwerpunkten gehören Datenschutz und Anonymität im Netz sowie Informationssicherheit auch für mobile Systeme.

Marco Ghiglieri ist bei der Technischen Universität Darmstadt tätig.

Yvonne Hofstetter studierte Rechtswissenschaften, ist Geschäftsführerin der *Terramark Technologies GmbH*, München, und Essayistin. Im Herbst 2014 erschien bei Bertelsmann ihr Buch *«Sie wissen alles - Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen»*.

Dr. Ing. **Stefan Köpsell** arbeitet am Lehrstuhl für Datenschutz und Datensicherheit der TU Dresden. Er ist einer der Hauptentwickler des AN.ON-Projektes, promovierte 2010 über die praktische Umsetzung dieses Anonymisierungsdienstes und hat zahlreiche Publikationen auf nationalen und internationalen Konferenzen veröffentlicht.

Benjamin Lange arbeitet beim Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt.

Johannes Lichdi ist Rechtsanwalt in Dresden und war unter anderem von 2004 bis 2014 Rechtspolitischer Sprecher der Fraktion Bündnis 90 / Die Grünen im Sächsischen Landtag.

Johannes Näder studierte Kultur-, Literatur- und Geschichtswissenschaft und legte eine Untersuchung zur Transformation des wissenschaftlichen Publizierens im Digitalzeitalter vor. Privat und beruflich engagiert er sich für ein bürgerrechtsfreundliches Internet und für eine freiheitliche Netzpolitik.

Marcel Rosenbach ist beim *Spiegel* stellvertretender Ressortleiter für Wirtschaft und berichtet seit Jahren über Sicherheits- und Netzthemen. Gemeinsam mit Holger Stark veröffentlichte er 2011 das Buch «*Staatsfeind WikiLeaks*» *und 2014 «Der NSA-Komplex – Edward Snowden und der Weg in die totale Überwachung».*

Peter Schaar war von 2003 bis 2013 Bundesbeauftragter für den Datenschutz und Informationsfreiheit und ist heute Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz EAID in Berlin. 2007 erschien sein Buch *«Das Ende der Privatsphäre - Der Weg in die Überwachungsgesellschaft»* und 2014 die Schrift *«Überwachung total - Wie wir in Zukunft unsere Daten schützen».*

Hervais Simo ist beim Fraunhofer-Institut für Sichere Informationstechnologie Darmstadt tätig.

Matthias Spielkamp ist Partner beim Think Tank *iRights.lab,* arbeitet als Journalist, Referent und Berater in Berlin und ist Vorstandsmitglied der deutschen Sektion von *Reporter ohne Grenzen.* Er ist Gründungsredakteur und Projektleiter von *iRights. info – Urheberrecht in der digitalen Welt,* das 2006 mit dem *Grimme-Online-Award* ausgezeichnet wurde. Als Journalist schreibt er vor allem über die Themen Urheberrecht, Internet-Politik und soziale und gesellschaftliche Aspekte der Digitalisierung - online, für Magazine, Tages- und Wochenzeitungen.

Holger Stark ist seit 2013 Korrespondent des *Spiegel* in Washington. Gemeinsam mit Marcel Rosenbach veröffentlichte er 2011 das Buch *Staatsfeind WikiLeaks und 2014 «Der NSA-Komplex – Edward Snowden und der Weg in die totale Überwachung».*

Dr. **Michael Waidner** ist Hochschullehrer für Informatik. Er arbeitete bei IBM und ist Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie in Darmstadt, zudem Direktor des Center of Advanced Security Research Darmstadt (CASED) und Leiter des BMBF-Kompetenzzentrums European Center for Security an Privacy by Design (EC SPRIDE).