Jahrbuch Netzpolitik 2014

Jahrbuch Netzpolitik 2014

netzpolitik.org

Hrsg. Markus Beckedahl, Anna Biselli und Andre Meister

Jahrbuch Netzpolitik 2014
1. Auflage, Buch, Dezember 2014

Herausgeber: Markus Beckedahl, Anna Biselli und Andre Meister
Redaktion: Markus Beckedahl, Anna Biselli und Andre Meister
Paul Berschick, Susanne Eiswirt, Justin Hanney,
Matthias 'wetterfrosch' Mehldau, Nadine Schildhauer
Titelbild: Melanie Twele
Satz: Anna Biselli

Verlag: epubli Berlin
ISBN: 978-3-7375-1489-7 (E-Book)
ISBN: 978-3-7375-1490-3 (Print)
URL: https://netzpolitik.org/jahrbuch-2014/

Inhalt

Editorial 9

Gebrauchshinweise 11

..... Überwachung – Grundrechtsbruch in vielen Formen

1 Hurra, die Vorratsdatenspeicherung ist weg! Ganz sicher? 14
Anna Biselli

2 Nicht-lizenzierte Exporte: Deutsche Unternehmen verdienen Millionen mit Überwachungstechnologien 17
Ben Wagner und Claudio Guarnieri

3 Die Radikalisierung der Innenminister 24
Matthias Monroy

4 Algorithmen Allmächtig? Freiheit in den Zeiten der Statistik 36
Kai Biermann

5 Metadaten: Wie dein unschuldiges Smartphone fast dein ganzes Leben an den Geheimdienst übermittelt 43
Dimitri Tokmetzis

6 Die NSA-Station im 22. Wiener Gemeindebezirk 49
Erich Moechel

..... Überwachung – Widerstand und Gegenwehr

7 Warum protestiert eigentlich niemand? 58
Anne Roth

8 Der NSA-Skandal und die globale Gegenwehr 62
Ben Hayes und Eric Töpfer

9 Immunität für Snowden? Warum wir die Rechte von Whistleblowern stärken sollten 73
Jochai Benkler

10 Hack Back! Ein Do-it-yourself-Guide für alle, die keine Geduld haben, auf Whistleblower zu warten 79
@GammaGroupPR

11 Nehmt euch die Kontrolle über eure privaten Daten zurück! 88
Hannes Mehnert

12 Vor Windows 8 wird gewarnt 93
Rüdiger Weis

13 I Was Looking To See If You Were Looking Back At Me To See Me Looking Back At You 101
Katharina Meyer

..... Geheimdienste – Kontrollieren, reformieren, abschaffen?

14 Grenzen für Überwacher statt grenzenlose Überwachung 109
Peter Schaar

15 Die Aufsicht über Geheimdienste - Ein demokratischer Lackmustest 121
Volker Tripp

16 Modelle zu Reform und Abschaffung der Geheimdienste 125
Markus Reuter und Michael Stognienko

..... TTIP, CETA, TISA – ACTA in neuem Gewand

17 „Framing“: Wie sich die ACTA-Gegner durchgesetzt haben 135
Katrin Tonndorf

18 TTIP und TISA: Die USA wollen Datenschutz wegverhandeln 139
Ralf Bendrath

..... Infrastruktur – Neutrales, schnelles Netz für alle?

19 Wikipedia Zero und Netzneutralität: Wikimedia wendet sich gegen das offene Internet 149
Raegan Mac Donald

20 Chronisch unterversorgt: Die netzpolitische Dimension des Breitbandausbaus 152
Christian Heise, Christian Herzog und Jan Torge Claussen

..... Open * – Open Data, Open Access, Open Source und Co.

21 Sehr geehrte Damen und Herren Abgeordneten, tun Sie endlich etwas für offene (Verwaltungs-)Daten! 157
Christian Heise

22 Open Access: Auf dem Weg zur politischen Erfolgsgeschichte? 165
Jeanette Hofmann und Benjamin Bergemann

23 Open the Snowden Files! Das öffentliche Interesse am freien Zugang zu den Dokumenten des NSA-Gate 180
Krystian Woznicki

24 Freie Software in München: Fakten sind stärker als Fiktion 188
Matthias Kirschner

Medienmarkt und -politik – Von analog zu digital

25 Die Entwicklung des Medienmarktes – zwischen Insolvenzen, Oligopolisierung und Aufbruch 193
Christian Humborg und Benedict Wermter

26 Öffentlich-Rechtlich und offen lizenziert: Creative Commons in ARD & Co 200
Leonhard Dobusch

27 Der gläserne Leser – Wie Amazon unsere Lesegewohnheiten ausspäht 203
Daniel Leisegang

28 Recht auf Vergessen – Kommentare zum Urteil des Europäischen Gerichtshofs 210
Joe McNamee, Jan Schallaböck und Thomas Stadler

Soziale Netzwerke – Chancen und Probleme

29 #Icebucketchallenge: Soziales Groß-Experiment in Sachen Selbstdarstellung 218
Julius Endert

30 Waffen und Brüste: Kultureller Imperialismus und die Regulierung von Sprache auf kommerziellen Plattformen 222
Jillian C. York

31 Rechtsextremismus in Sozialen Netzwerken 229
Johannes Baldauf

Das große Ganze

32 Die Hearings der neuen EU-Kommissare aus netzpolitischer Sicht 234
Angela Sobolciakova

33 Vom Internet der Dinge, algorithmischer Gesetzgebung und dem Ende der Politik 237
Kirsten Fiedler

34 Partizipation als Kontrollinstrument: Internet Governance in Zeiten Snowdens 241
Arne Hintz und Stefania Milan

35 Netzpolitik 2014: Von der Neuformatierung politischer Strukturen 246
Julia Krüger

Abspann

Zehn Gründe, netzpolitik.org zu unterstützen 250

Abkürzungen 252

Liebe Leserinnen und Leser des Jahrbuchs Netzpolitik 2014,

es geht voran. Zumindest in einigen Bereichen. Netzpolitik ist spätestens seit diesem Jahr kein exotisches Randgruppenthema mehr, sondern rückt als ein sich entwickelndes Politikfeld ins Zentrum der Politik.

Das dominierende Thema aus 2013 blieb uns auch in diesem Jahr erhalten: Die Komplettüberwachung der digitalen Welt geht genauso weiter wie die Enthüllungen von Edward Snowden und glücklicherweise weiteren Whistleblowern. Nach dem Fokus auf die Geheimdienste der USA und Großbritannien durch die Dokumente des Whistleblowers rückte dieses Jahr der Bundesnachrichtendienst in den Vordergrund.

Der Deutsche Bundestag hat einen Untersuchungsausschuss zum Thema eingerichtet, dennoch kommen die großen Enthüllungen weiterhin von den Medien. Das Anzapfen riesiger Datenströme aus Glasfaserkabeln an Internet-Knotenpunkten wie in Frankfurt hat jetzt einen Namen: Eikonal. Nicht nur durchsucht der Geheimdienst dort Millionen und Abermillionen Kommunikationsdaten, sondern leitet auch Daten an die NSA und andere Dienste weiter. Verantwortlich für die Einrichtung waren zwei Pfeiler der heutigen Großen Koalition: Frank-Walter Steinmeier und Thomas de Maizière.

Das erklärt wahrscheinlich auch die – freundlich ausgedrückt – mangelnde Unterstützung des Untersuchungsausschusses durch die Bundesregierung. Abgeordnete bekommen Dokumente später als BND-Mitarbeiter, dann auch nur geschwärzt und dürfen nicht darüber reden. Zeugen haben Erinnerungslücken und wollen am liebsten nur nicht-öffentlich aussagen. Quellen von uns werden vom Kanzleramt direkt mit Strafanzeige bedroht, wenn sie uns und anderen Medien Dokumente aus dem Umfeld des Geheimdienst-Untersuchungsausschusses leaken, um Licht ins Dunkel zu bringen. Und wir werden für unsere Berichterstattung von der Bundestagspolizei überwacht.

Davon lassen wir uns nicht einschüchtern, gehen juristisch dagegen vor und machen selbstverständlich weiter. Immerhin kamen schon einige interessante Details ans Tageslicht, darunter geheime Gesetzes-Interpretationen des BND: Da gibt es zum Beispiel die Weltraum-Theorie – wenn der BND Satelliten abhört, gelten keine deutschen Gesetze, ist ja im Weltraum – und die Funktionsträger-Theorie – wenn Deutsche im Ausland für eine ausländische Organisation kommunizieren, gelten keine Grundrechte, Beispiel EU-Kommissar Oettinger. Hoffentlich zieht der Bundestag Konsequenzen und nimmt die Geheimdienste per

Gesetzesänderung an die Leine. Bisher sind politische Konsequenzen auf den größten Überwachungsskandal der Menschheitsgeschichte leider ausgeblieben.

Dauerbrenner-Thema bleibt natürlich auch die Netzneutralität. Das freie und offene Internet, wie wir es kennen und lieben, wird weiterhin von Telekommunikations-Anbietern und der Politik attackiert. Die Deutsche Bundesregierung hat es immer noch nicht geschafft, dieses elementare Grundprinzip des Internets gesetzlich festzuschreiben und Provider nutzen diese Unsicherheit, um Fakten zu ihren eigenen Gunsten zu schaffen.

Auf EU-Ebene hat das Europaparlament im Frühjahr den Vorschlag der EU-Kommission zur Netzneutralität deutlich verbessert und sich für eine starke Netzneutralität ausgesprochen. Derzeit unterlaufen die Mitgliedsstaaten diesen Wunsch, bei den intransparenten Verhandlungen im Rat nutzen Telekom-Lobbyisten ihren Einfluss, ihre Gelddruck-Wünsche durchzusetzen. Das Thema wird uns noch weiterhin begleiten, an ein Happy End ist derzeit leider nicht zu denken.

Auch der neue Digital-Kommissar aus Deutschland scheint sich dieser Linie anzuschließen. Günther Oettinger, ehemaliger Ministerpräsident des Landes Baden-Württemberg, war die netzpolitisch überraschendste Personalie der neuen EU-Kommission. Wie schon als Energie-Kommissar, übernahm er innerhalb kurzer Zeit Sprechblasen von Industrie-Lobbys. Das bedeutet noch viel Arbeit für uns in den nächsten fünf Jahren – auch für unsere Freunde und Partner bei European Digital Rights (EDRi) in Brüssel. Als ob es mit der Datenschutzreform, den Freihandelsabkommen CETA und TTIP sowie der kommenden Urheberrechtsreform nicht schon genug zu tun gäbe. Immerhin hat der Europäische Gerichtshof die Richtlinie zur Vorratsdatenspeicherung gekippt – hoffen wir, dass sie tot bleibt.

Neben dem Digital-Kommissar hat Deutschland jetzt auch eine Digitale Agenda! Was zwischenzeitlich als netzpolitischer Masterplan hochstilisiert wurde, erwies sich jedoch spätestens bei der Präsentation als Bettvorleger. Die einhellige Meinung, nicht nur von uns Dauerkritikern: Unterambitioniert und voller Konjunktive. Da war selbst der Koalitionsvertrag innovativer und konkreter. In der Öffentlichkeit bleibt nur „50 MBit/s bis 2018“ hängen – selbst im globalen Vergleich deutlich unterambitioniert und das Ganze soll auch noch auf dem Rücken der Netzneutralität realisiert werden.

Uns dürfte also auch im Jahr 2015 nicht langweilig werden. Nicht, dass das bisher so gewesen wäre. Schon seit 2004 berichten wir über die Themen der digitalen Gesellschaft, in diesem Jahr feierten wir unser zehnjähriges Bestehen: 10 Jahre netzpolitik.org! Vielen Dank an alle für die schöne Konferenz und Party im Oktober in Berlin.

An dieser Stelle bedanken wir uns auch für die neuen Auszeichnungen: den Grimme Online Award in der Kategorie Spezial und einen Lead Award in Bronze in der Kategorie Independent des Jahres (Online).

Neu in diesem Jahr war endlich ein frisches Design für das Blog, das auch für mobile Nutzung ausgelegt ist. Zusätzlich gibt es mittlerweile einen wöchentlichen Newsletter mit allen relevanten Infos. Und wir haben immer noch mehr Ideen als Zeit und Ressourcen zur Realisierung – das würden wir gerne ändern.

Im vergangenen Jahr haben wir uns etwas neu erfunden: Mit der Einführung eines Modells der freiwilligen Leserfinanzierung haben wir ein Experiment gestartet. Wir wollten mehr recherchieren und uns unabhängig von Klicks und Reichweite auf die Themen konzentrieren, die wir für notwendig erachten. Gleichzeitig wollen wir unsere Berichterstattung ausbauen, um der Politik besser auf die Finger schauen zu können – auf Bundesebene wie auch in der EU. Nach eineinhalb Jahren stellen wir fest, dass das in unserem Fall überraschend gut funktioniert. Dank unserer Leserinnen und Leser konnten wir eine weitere Stelle schaffen und haben jetzt als drittes festes Redaktionsmitglied Anna Biselli an Bord, die neben vielen anderen Dingen entscheidend dazu beigetragen hat, dieses Jahrbuch zu verwirklichen. Und wenn alles gut läuft und die Unterstützung weiterhin so konstant wächst, können wir uns demnächst wieder erweitern.

Das tut auch dringend Not. Viele unserer Themen explodieren und wir können uns über mangelnde Arbeit nicht beschweren – ganz im Gegenteil. Viele Themen, die wir als wichtig, notwendig und unterberichtet empfinden, gehen leider unter, weil wir zu wenig Zeit dafür haben. Das wollen wir ändern und hoffen auf eure Unterstützung. Unter https://netzpolitik.org/spenden gibt es verschiedene Wege, uns und unsere Arbeit durch eine Spende oder einen Dauerauftrag zu unterstützen. Zehn gute Gründe dafür findet ihr am Ende des Buches.

Wir bedanken uns bei allen Leserinnen und Lesern und allen, die uns Informationen zusenden oder unsere Inhalte verteilen. Und natürlich bei allen Spenderinnen und Spendern: Nur dank eurer Unterstützung können wir unsere Redaktion weiter ausbauen und unabhängig bleiben.

Wir freuen uns auf 2015 und wünschen viel Spaß beim Lesen des Jahrbuch Netzpolitik 2014!

Markus Beckedahl, Anna Biselli und Andre Meister

Gebrauchshinweise

Beim Zusammenstellen und Redigieren des diesjährigen Jahrbuches ist uns etwas aufgefallen, das wahrscheinlich auch euch auffallen wird: Jeder Beitrag ist anders. Das klingt wie eine banale, beleidigend offensichtliche Feststellung, denn schließlich haben ja über 40 Personen ihr geschriebenes Wort beigesteuert. Es stellte uns jedoch vor Herausforderungen – während die eine primär in der sachlichen Welt der Wissenschaft zu Hause ist, merkt man dem anderen den Anwaltsberuf oder das Aktivistsein an. Und während manche von NutzerInnen schreiben, wenden sich einige lieber dem Leser im Allgemeinen zu.

Wir finden, das ist gut so und haben uns dagegen entschieden, die Texte „auf Linie" zu bringen. Das würde ihnen und der Vielfalt unserer Autorinnen und Autoren nicht gerecht. Und wir wollen euch dazu ermutigen, unser Jahrbuch nicht einfach von vorn bis hinten in einem durchzulesen und danach im Schrank verstauben zu lassen. Es ist deshalb auch nicht chronologisch geordnet, sondern in Themenblöcke unterteilt und so bietet es sich auch an, zu Themen nachzuschlagen und in zehn Jahren noch einmal zu schauen, wie es um das Thema „Open Data" im Jahre 2014 stand.

Was uns noch auffiel: Auch wenn in diesem Jahr viele verschiedene wichtige netzpolitische Entscheidungen getroffen und Entwicklungen zu beobachten waren, ist das Thema, das unsere Autorinnen und Autoren am meisten beschäftigt zu haben scheint, das der Überwachung. Hier wird eine Diskrepanz deutlich, die etwas Positives und etwas Negatives mit sich bringt. Auf der Negativseite droht die Gefahr, das andere Themen aus dem Fokus geraten, untergehen und ganz nebenbei folgenschwere politische Entscheidungen getroffen werden, während die Zivilgesellschaft damit beschäftigt ist, gegen die Überwachung ihrer Kommunikation zu kämpfen. Auf der Positivseite ist es jedoch ermutigend, zu sehen, dass die Aufmerksamkeit gegenüber den Problemen der Massenüberwachung nicht abgenommen hat – nur der Blick hat sich, vor allem in Deutschland, Richtung Inland verschoben. Das finden wir wichtig und daher geben wir dem Thema auch den Raum, den es fordert, während wir unser Bestes tun, die anderen nicht aus den Augen zu verlieren. Womit wir wieder am Anfang sind: Ohne die Vielfalt unserer Autorinnen und Autoren sowie Mitstreiterinnen und Mitstreiter wäre das kaum möglich.

Ein letzter Hinweis: Dieses Buch ist CC BY-SA 3.0 lizenziert und kann unter Namensnennung unter den gleichen Bedingungen weitergeben, ge-remixt und weiterentwickelt werden – egal ob in der DRM-freien E-Book-Variante oder als etwa

250 Seiten ausgedruckte Digitalpolitik aus dem Jahre 2014. Wir würden uns freuen, wenn ihr diese Möglichkeit nutzt und auf dem Buch aufbaut. Fühlt euch auch ermutigt, es denjenigen ans Herz zu legen, die vielleicht nicht bereits täglich netzpolitik.org verfolgen und auf dem Laufenden sind. Lest es, tragt es weiter, macht was draus.

Und jetzt: Viel Spaß beim Lesen!

Eure Jahrbuch-Redaktion

1 Hurra, die Vorratsdatenspeicherung ist weg! Ganz sicher?

von **Anna Biselli**

Der Europäische Gerichtshof (EuGH) hat am 8. April 2014 entschieden, dass die EU-Richtlinie zu Vorratsdatenspeicherung nicht mit der Wahrung der Grundrechte vereinbar ist. Datenschützer aus Österreich und Irland hatte die Richtlinie angegriffen vor dem Europäischen Gerichtshof angegriffen. Die Richter entschieden in ihrem Urteil, die Richtlinie sei gänzlich ungültig und stellten fest …

> […], dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta einhalten musste.

Die Vorratsdatenspeicherung ist damit ohne die Möglichkeit einer Nachbesserung aufgehoben, was Deutschland sehr entgegenkommen dürfte, da nun keine Verhängung von Zwangsgeldern innerhalb einer Übergangsfrist mehr droht, auf die die EU-Kommission geklagt hatte. Deutschland hatte nämlich bis heute keine nationale Umsetzung der nun vergangenen Richtlinie durchgeführt.

Ein neuer Versuch, die Richtlinie „verfassungskonform" wiederauferstehen zu lassen, ist jedoch nicht vollständig vom Tisch. Zum einen könnte die EU-Kommission eine Neuauflage in Angriff nehmen, diese müsste jedoch auch von Parlament und Rat angenommen werden, was angesichts der jetzigen Situation schwierig werden dürfte. In Deutschland ist man noch uneinig, ob und wie man jetzt trotzdem eine Vorratsdatenspeicherung einführen könnte. Justizminister Heiko Maas sagt:

> Die Grundlage für die Vereinbarung im Koalitionsvertrag ist entfallen […] Es besteht jetzt kein Grund mehr, schnell einen Gesetzentwurf vorzulegen.
>
> Wir werden das Urteil jetzt sorgfältig auswerten. Dann werden wir mit unserem Koalitionspartner neu über das Thema Vorratsdatenspeicherung reden müssen. Wir werden das weitere Verfahren und die Konsequenzen ergebnisoffen besprechen.

Innenminister De Maizière ist ein wenig direkter und fordert nach der Urteilsbekanntgabe eine „verfassungsgemäße Neuregelung“, was uns bereits eine Ahnung davon beschert, dass man nun versuchen wird, durch geschicktes Hin- und Herbiegen die Bedingungen des EuGH mit einer möglichst umfassenden Speicherung überein zu bringen.

Tatsächlich bleiben Möglichkeiten für eine kleine VDS unter dem „Quick Freeze“-Ansatz. Dabei können Daten bei Verdacht auf ein Verbrechen temporär sichergestellt werden. Das Urteil stellt hier als Bedingung, dass es eine Einschränkung geben müsse – auf die „Daten eines bestimmten Zeitraums und/oder eines bestimmten geografischen Gebiets und/oder eines bestimmten Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte“ oder „auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten“. Diese Definition ist so vage, dass der Verdächtigten- und Betroffenenkreis schnell ziemlich groß und universell werden kann.

Auch die Mindestspeicherfrist ist nicht ganz vom Tisch, der EuGH bemängelt nämlich primär, dass es keine objektiven Kriterien gebe, die eine Speicherfrist von sechs bis 24 Monaten rechtfertigten. Die prinzipielle Möglichkeit, diese zu finden oder die Zeiträume plausibel zu kürzen, wird nicht ausgeschlossen.

Weiterhin finden sich noch andere theoretisch erfüllbare Bedingungen für eine Verfassungskonformität: Es bräuchte „materiell- und verfahrensrechtliche Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung“. Zugriff und Nutzung müssten „strikt auf Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung“ beschränkt sein und die Definition von „schweren Verbrechen“ müsse konkretisiert werden.

Darüberhinaus findet sich die Forderung nach einem Richtervorbehalt, wobei man doch in der Vergangenheit oft genug demonstriert bekam, dass dieser oftmals wie ein Blankostempel umgesetzt wird. Andere Punkte beinhalten fristgerechte vollständige Löschung, einen besseren Missbrauchsschutz und eine sorgfältigere Datenaufbewahrung. Dabei wird bemängelt, …

> […], dass die fraglichen Daten [nicht] im Unionsgebiet auf Vorrat gespeichert werden, so dass es nicht als vollumfänglich gewährleistet angesehen werden kann, dass die Einhaltung der in den beiden vorstehenden Randnummern angesprochenen Erfordernisse des Datenschutzes und der Datensicherheit, wie in Art. 8 Abs. 3 der Charta ausdrücklich gefordert, durch eine unabhängige Stelle überwacht wird.

Der am meisten zu bedauernde Punkt ist jedoch, dass der EuGH die Sinnhaftigkeit der VDS zur Strafverfolgung eingesteht.

> [Es] ist festzustellen, dass angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die nach dieser Richtlinie auf Vorrat zu speichernden Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und insoweit daher ein nützliches Mittel für strafrechtliche Ermittlungen darstellen. Die Vorratsspeicherung solcher Daten kann somit als zur Erreichung des mit der Richtlinie verfolgten Ziels geeignet angesehen werden.

Solche Eingeständnisse spülen den Überwachungsfreunden ihre alten Argumente in die Hände. Die klagen über Schwierigkeiten bei der Verbrechensbekämpfung, wie etwa der Vorsitzende des Bundes Deutscher Kriminalbeamter via Twitter:

> Ein sehr schwarzer Tag für Europa. Hoffentlich knickt de #Maizière jetzt nicht ein. #VDS wird täglich dringender.

Fazit: Das Urteil ist zu begrüßen und geht in seinen substantiellen Punkten über die Vorabempfehlung von Generalanwalt Villarón hinaus, aber es lässt weiterhin Schlupflöcher. Es heißt wohl, zu hoffen, dass nicht alles, was juristisch möglich wäre, auch bis ins Letzte ausgenutzt werden wird. Der Anwalt Meinhard Starostik, der 2010 die Beschwerden gegen die Vorratsdatenspeicherung vor dem Bundesverfassungsgericht erfolgreich vertreten hat, fürchtet, dass jetzt erst recht eine Diskussion entstehen werde, „wie eine ‘richtige’ grundrechtekonforme Vorratsdatenspeicherung aussehen könnte“. Heribert Prantl kommentierte dazu in der Süddeutschen Zeitung:

> Die Entscheidung des EuGH ist ein Grund zur Freude. Sie weckt die Hoffnung, dass der Schutz der Menschen in der digitalen Welt vielleicht doch funktioniert [...] Der Datenschutz ist das Grundrecht der Informationsgesellschaft. Er darf kein Gnadenrecht sein. Die drei großen Gerichte haben das verstanden. Die deutsche Politik sollte folgen.

Und sollte sie das nicht tun, muss zur Not der Kampf gegen die nächste Reinkarnation der VDS von vorn beginnen, bis alle Lücken ausgefüllt sind.

Dieser Beitrag erschien zuerst am 8. April 2014 auf netzpolitik.org.

Anna Biselli kommt aus der Welt der Informatik und hat gemerkt, dass sie der netzpolitische Kontext dabei nicht loslässt. Deshalb bewegt sie sich jetzt zwischen den Welten und schreibt in der einen Hälfte ihres Lebens bei netzpolitik.org während sie in der anderen zu Datenschutz im Software Engineering forscht. Und oft merkt sie, dass man die beiden Hälften gar nicht so genau trennen kann.

2 Nicht-lizenzierte Exporte: Deutsche Unternehmen verdienen Millionen mit Überwachungstechnologien

von **Ben Wagner** und **Claudio Guarnieri**

Der Staatstrojaner „made in Germany“ Gamma FinFisher wurde ohne Lizenz aus Deutschland exportiert. Das geht aus Analysen der kürzlich geleakten Dokumente und einer parlamentarischen Anfrage hervor. Deutsche Unternehmen verdienen Millionen damit, Überwachungstechnologien an Menschenrechtsverletzer auf der ganzen Welt zu exportieren.

Von Mexiko über Mosambik bis Pakistan gibt es umfangreiche Beweise dafür, dass Regierungen auf aller Welt Überwachungstechnologien wie FinFisher verwenden, um ihre Bürger auszuspionieren. Das hat Forscher wie uns veranlasst, die Quellen zu betrachten: Wer stellt diese Technologien her? Wer profitiert vom Verkauf? Deutschland ist ein Hauptexporteur dieser Technologien und, da die Privatsphäre der digitalen Kommunikation ein heißes Eisen der deutschen Öffentlichkeit ist, ist das Land als Akteur in diesem Bereich noch weiter ins Zentrum gerückt.

Aufgrund eines Abgleichs von Informationen eines massiven Datenlecks Mitte August[1] mit den Ergebnissen einer aktuellen parlamentarischen Anfrage[2] in Deutschland ergibt sich der Verdacht, dass die Mehrheit der von deutschen Unternehmen hergestellten Überwachungstechnologien unter dem Tisch – das heißt ohne Lizenz – gekauft und verkauft wurden. Die deutsche Regierung verlangt Lizenzen für den Verkauf von Gütern, die als „Dual-Use-Güter“ betrachtet werden, also für Güter, die sowohl im zivilen als auch im militärischen Bereich verwendet werden können.

Im Zentrum der Untersuchung steht das britisch-deutsche Unternehmen Gamma International, Hersteller der FinFisher-Überwachungswerkzeuge. Ahnungslose Überwachungsziele laden FinFisher in der Regel herunter, ohne es zu wissen, indem sie auf einen vermeintlich harmlosen Link oder E-Mail-Anhang klicken. Einmal installiert, erlaubt es dem Nutzer, auf alle gespeicherten Informationen zuzugreifen und selbst verschlüsselte Kommunikation zu überwachen. Tastenanschläge werden aufgezeichnet, Skype-Unterhaltungen aufgenommen und Kameras und Mikrofone können aus der Ferne aktiviert werden.

Kürzlich stellten Bundestagsmitglieder eine parlamentarische Anfrage[3] bezüglich des Verkaufs von Überwachungstechnologien an ausländische Regierungen.

In der Antwort stellte die Regierung fest, dass sie deutschen Unternehmen in den letzten zehn Jahren Ausfuhrlizenzen für Überwachungstechnologien an mindestens 25 Länder genehmigt hat – viele davon mit Vorgeschichten voller Menschenrechtsverletzungen. Zwischen 2003 und 2013 wurde Überwachungstechnik in folgende Länder exportiert: Albanien, Argentinien, Chile, Indien, Indonesien, Katar, Kosovo, Kuwait, Libanon, Malaysia, Marokko, Mexiko, Norwegen, Oman, Pakistan, Russland, Saudi-Arabien, Schweiz, Singapur, Taiwan, Türkei, Turkmenistan, USA und Vereinigte Arabische Emirate. Die Grünen-Abgeordnete Agnieszka Brugger veröffentlichte sämtliche Fragen und die offiziellen Regierungsantworten auf ihrer Website.

Der deutsche Exportmarkt

Die Antworten der Bundesregierung sind schwer zu interpretieren, da die Unterlagen jedes IT-System erwähnen, welches „Bestandteile" von Überwachungstechnologien enthält. Zum Beispiel ein komplettes nationales Telefonsystem, das für insgesamt zehn Millionen US-Dollar verkauft wird, kann einen Überwachungsbestandteil zum Preis von zwei Millionen US-Dollar enthalten, aber das Produkt wird in den öffentlichen Unterlagen als exportiertes Produkt, welches lizenzierte Überwachungstechnologien enthält, im Wert von zehn Millionen Dollar aufgeführt.

Auf der Basis von Gesprächen mit zuständigen Regierungsbeamten und Individuen des Privatsektors sowie den zahlreichen geleakten Dokumenten ist es möglich, einen relativ genauen Wert des Anteils dieser Technologien zu erhalten, der tatsächlich Überwachungstechnologien entspricht. Eine vorsichtige Schätzung geht davon aus, dass ein Fünftel der IT-Gesamtsysteme genau genommen Überwachungstechnologien sind – der Rest sind typische IT-Systeme. Zum Beispiel hat Deutschland im Jahre 2010 IT-Systeme, die Überwachungssysteme enthalten, im Wert von fast zwölf Millionen Euro exportiert. Wir schätzen also, dass von diesen aufgeführten IT-Systemen genau genommen nur knapp 2,5 Millionen Euro Exporte von Überwachungstechnologien sind, während der Rest typische IT- oder Telekommunikationssysteme sind.

Diese Zahlen ermöglichen das Diagramm der deutschen Exporte der Überwachungstechnologie von 2010 bis 2013, das in Abbildung 1 zu sehen ist.

Wichtig ist, dass die deutsche Regierung ausdrücklich bestreitet, von Gamma einen Exportlizenzantrag für deren Produkt FinFisher nach Bahrain oder Äthiopien erhalten zu haben. In den offiziellen Angaben der Bundesregierung tauchen auch keine Exporte in Länder wie Bangladesch, die Niederlande, Estland, Australien, die Mongolei, Bahrain oder Nigeria auf, obwohl es zahlreiche Belege gibt, dass FinFisher in diese Länder verkauft wurde.

Auf der Grundlage der geleakten FinFisher-Daten und der Analyse von Privacy International[4] gehen wir davon aus, dass Gamma diese Überwachungstechnolo-

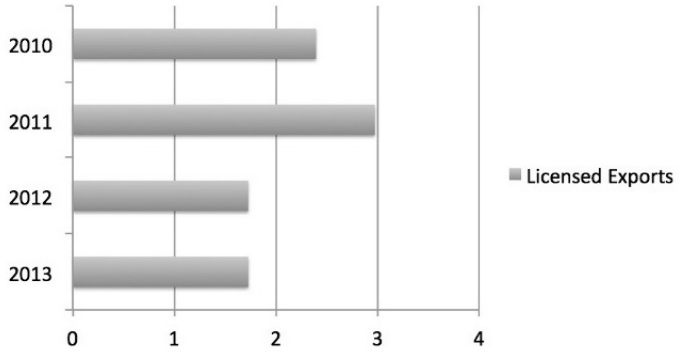

Abbildung 1: Exporte von Überwachungstechnologie aus Deutschland in Millionen Euro

gien ohne Lizenz exportiert hat. Diese Behauptung beruht auf zahlreichen Dokumenten, wie Gamma mit Technologien handelt, und der aktuellen Erklärung der britischen Regierung, dass sie von Gamma per Gesetz fordert, eine Lizenz für FinFisher zu erlangen, wenn das Unternehmen es von Großbritannien aus exportieren wolle.

Bestehende Kenntnisse und Recherchen ergeben, dass Gamma aus Großbritannien und Deutschland heraus operiert, und erhärten den Verdacht des Exports dieser Technologien aus Deutschland. Und Deutschland hat wiederholt abgestritten, Gamma eine Lizenz für den Verkauf in verschiedene Länder ausgestellt zu haben, bei denen wir von der Nutzung FinFishers wissen. Das führt uns zu der Schlussfolgerung, dass FinFisher ohne Lizenz aus Deutschland exportiert wurde.

Was bedeutet das für den deutschen Handel mit Überwachungstechnologien? Nun, die lizenzierten Überwachungstechnologieexporte erscheinen geradezu winzig im Vergleich zu den nicht-lizenzierten Exporten von FinFisher, von anderen Überwachungsprodukten gar nicht zu reden. Gamma verkauft im Moment mehr Überwachungstechnologie als alle lizenzierten Exporte zusammen. In Abbildung 2 sieht man einen Vergleich von lizenzierten und nicht-lizenzierten deutschen Überwachungsexporten.

Und das ist nur ein einziges Unternehmen – es gibt in Deutschland wahrscheinlich weitere, die dieser Geschäftsstrategie folgen. Obwohl eine exakte Summe der nicht-lizenzierten deutschen Überwachungsexporte schwer zu berechnen ist, sollte es nicht überraschen, dass Experten des Branchenführers ISS World ihre globale Industrie auf drei bis fünf Milliarden Dollar schätzen. Die deutliche Lücke zwischen den lizenzierten und nicht-lizenzierten Teilen der Überwachungstechnik-Industrie zeigt die Notwendigkeit einer zügigen und klaren internationalen Regulierung.

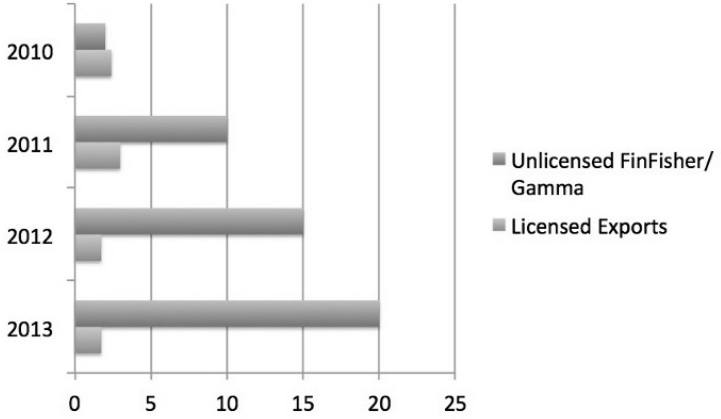

Abbildung 2: Exporte von Überwachungstechnologie aus Deutschland in Millionen Euro

Bestehende deutsche Regelungen für Überwachungstechnikexporte

Die deutsche Regierung schreibt in ihren Antworten auf die parlamentarische Anfrage auch, dass sie weiter darauf hinwirken will, Überwachungstechnologien, die Menschenrechte gefährden, stärker zu regulieren. Das ist eine positive Entwicklung, die ein Verständnis für die Ernsthaftigkeit des Themas widerspiegelt. Angesichts dieser neuen Informationen und dem Wunsch einiger Parteien, dieses Thema mit Priorität zu behandeln, können wir hoffen, dass weitere Änderungen vorgenommen werden, die die Lieferung von noch mehr gefährlichen Technologien an repressive Regime verhindern können.

Die Lage ist jedoch nicht völlig einseitig. So hat Deutschland etwa die Ausfuhr von „Interception Management System"-Software (IMS), vergleichbar mit „Lawful Interception Management System" der deutschen Firma Utimaco, in den Iran im Jahr 2008 verhindert und vor Kurzem vorgeschlagen, dass auch in die Türkei keine Überwachungstechnik mehr exportiert werden soll.

Die Antworten der Bundesregierung zeigen, dass der Markt stark von Großaufträgen mit einzelnen Ländern abhängig ist. Saudi-Arabien und die Türkei waren 2006 und 2007 die größten Einzeldeals. Es ist schwer zu erahnen, auf welche Verträge sich diese Exporte genau beziehen, aber sie passen in das generelle Muster der zunehmenden Internetüberwachung, die seit 2005 kontinuierlich ausgebaut wird, um mit größeren Datenmengen umgehen zu können. Zum Beispiel hatte Tunesien Probleme, worauf hin dort 2007 die Überwachungstechnik Deep Paket Inspection (DPI) eingeführt wurde.

Die Politik der Überwachungsregulierung

Interessanterweise sehen SPD und Grüne in Deutschland die Regulierung von Überwachungstechnologien als wichtiges politisches Thema an, für das es sich zu kämpfen lohnt. Sowohl die Grünen als auch die Sozialdemokraten wollen das Thema besetzen, was wohl der Grund dafür war, dass eine parlamentarische Anfrage gestellt wurde. Obwohl die Politisierung von Menschenrechtsfragen sich nicht immer als hilfreich herausgestellt hat, ist es interessant zu beobachten, dass es einen politischen Wettbewerb zwischen deutschen Parteien über die Frage gibt, wer Überwachungstechnik besser regulieren kann?

In jedem Fall zeigen die FinFisher-Dokumente, dass der Hersteller Gamma aktuell davon ausgeht, dass ihm jetzt oder in naher Zukunft Ausfuhrkontrollen in Deutschland auferlegt werden und bittet seine Kunden daher um zusätzliche Informationen. Dies deutet darauf hin, dass offenbar Ausfuhrbestimmungen für Überwachungstechnologien wirksam geworden sind, bevor sie gesetzlich verankert wurden, da sogar einige der berüchtigtsten Unternehmen bereits reagieren, um sicherzustellen, dass sie die Auflagen erfüllen.

Lobbyarbeit für Veränderungen

Es wird eindeutig noch weitere Änderungen in diesem Bereich geben. Die Bundesregierung erkennt die Notwendigkeit, weitere Überwachungstechnologien, die Menschenrechte verletzen, zu regulieren, die bisher noch nicht im Wassenaar-Abkommen aufgeführt sind. Zum Beispiel nennt sie explizit „Überwachungsbeobachtungszentralen“, die die Überwachung von E-Mails, SMS, Internetverbindungen und VoIP-Anrufen in einer Zentrale bündeln, da diese Technologie missbraucht werden kann und zusätzliche Regulierung benötigt.

Der bevorzugte Ansatzpunkt zur Verhandlung dieser Änderungen der Ausfuhrbestimmungen ist das Wassenaar-Abkommen, ein nicht bindendes Abkommen zwischen Staaten, das bestimmte „Dual-Use-Technologien“ international reguliert. Wassenaar enthält im Grunde eine lange „Kontrollliste“ der Technologien, von denen alle Mitgliedsstaaten glauben, sie könnten missbraucht werden. Jeder einzelne Mitgliedsstaat in der EU implementiert diese Entscheidung dann in seinen nationalen Exportbestimmungen. Diese Listen werden jährlich bei einer großen Mitgliederkonferenz aktualisiert. Es dauert in der Regel ein Jahr, bis diese Änderungen innerhalb der nationalen Gesetze der verschiedenen Wassenaar-Mitgliedsstaaten in Kraft treten.

Wie viele andere Menschenrechtsverteidiger glauben wir, dass das Wassenaar-Abkommen die stärkste Plattform für die deutsche Regierung bietet, sich für diese Änderungen einzusetzen und sie hat gegenüber dem Bundestag wiederholt bestätigt, dies umfassend zu tun. Die bessere Regulierung von Überwachungstechnologien sei „von hoher politischer Bedeutung“ für die Wassenaar-

Mitgliedsstaaten, genauso wie für die Europäische Kommission, die diesem Bereich eine „hohe Priorität“ zuweist.

Deutschland drängt darauf, so schnell wie möglich ein neues Wassenaar-Abkommen auf EU-Ebene umzusetzen. „Herbst 2014“ ist eine eher optimistische Prognose, auch wenn die Bundesregierung auf verschiedenen Ebenen Schritte eingeleitet hat, um den Prozess zu beschleunigen. Wie glaubwürdig dieser Zeitplan ist, bleibt abzuwarten, nach Jahren der Untätigkeit ist er aber zumindest ein deutliches politisches Signal der Bundesregierung.

Der Gesamtzusammenhang

Über Überwachungstechnologien hinaus hat SPD-Chef und Wirtschaftsminister Sigmar Gabriel erklärt, er wolle das Exportkontrollrecht in allen Bereichen strenger interpretieren[5]. Die Werkzeuge dafür existieren seit einiger Zeit in Form der „Politische Grundsätze der Bundesregierung“, die von der rot-grünen Regierung im Jahre 2000 entwickelt, aber selten strikt durchgesetzt wurden. SPD-Minister Gabriel hat diese Prinzipien nun einfach strikter interpretiert, um eine Vielzahl an Waffenexporten aus Deutschland zu stoppen. Zusätzliche Vorschriften für missbrauchsanfällige Überwachungstechnologien passen also sehr gut in seine Agenda. Gleichzeitig wurde Gabriel in der Presse und von der Grünen Partei kritisiert, weil er nicht dokumentieren konnte, dass er tatsächlich einen konkreten Antrag auf Export von Überwachungstechnologien abgelehnt hat.

Hier, wie in anderen Fällen auch, ist der Kampf ist in erster Linie eher politisch als inhaltlich. Es ist zu begrüßen, dass nun zwei politische Parteien beim Thema Regulierung von Überwachungstechnik miteinander konkurrieren. Beide haben klare, konkrete Absichten verkündet, die SPD als Regierungspartei war jedoch noch nicht in der Lage, diese vollständig zu dokumentieren. Was vielleicht am bemerkenswertesten ist: Die deutsche Regierung verfolgt weiterhin den Anspruch, eine führende Stimme in der internationalen Debatte über die Regulierung von Überwachungstechnologien zu werden. Es wird sich zeigen, ob sie tatsächlich in der Lage ist, dieses Versprechen zu erfüllen. Aber die aktuellen Anzeichen sind vielversprechend.

Dieser Beitrag erschien zuerst am 5. September 2014 auf netzpolitik.org sowie auf englisch bei Global Voices.

Anmerkungen

[1] https://netzpolitik.org/2014/gamma-finfisher-gehackt-werbe-videos-von-exploits-und-quelltext-von-finfly-web-veroeffentlicht/

[2] http://www.agnieszka-brugger.de/fileadmin/dateien/Dokumente/Abruestung/Ruestungsexporte/20140808_Antwort_KA_Spaehsoftware_Drs182067_1.pdf

[3] http://dip21.bundestag.de/dip21/btd/18/020/1802067.pdf

[4] https://www.privacyinternational.org/blog/six-things-we-know-from-the-latest-finfisher-documents

[5] https://netzpolitik.org/2014/bericht-wirtschaftsministerium-verhaengt-exportstopp-fuer-ueberwachungstechnologien/

Ben Wagner forscht und forschte zu Meinungsfreiheit, Überwachungstechnologie und Internet Governance, unter anderem am Centre for Internet & Human Rights an der European University Viadrina, die TU Berlin und der Vrije Universiteit Brussel. Er war Post Doc an der University of Pennsylvania und Visiting Fellow bei Human Rights Watch, der Humboldt Universität und dem European Council on Foreign Relations.

Claudio Guarnieri ist Hacker und unabhängiger Sicherheitsforscher. Er arbeitete als Malware-Analyst und -Forscher bei Rapid7 Labs. Er ist Open-Source-Entwickler und erstellte Cuckcoo Sandbox, eine verbreitetes Malware-Analyse-System. Er engagiert sich auch für Bürgerrechte und hat mit CitizenLab an vielen Veröffentlichungen über FinFisher und andere Anbieter von Überwachungstechnik gearbeitet.

3 Die Radikalisierung der Innenminister

von **Matthias Monroy**

Zweifellos sind die in Nordafrika und dem Nahen Osten kämpfenden Djihadisten ein bedrohliches Phänomen. Außer Acht gerät aber, dass wegen dieser als „ausländische Kämpfer" („foreign fighters" bzw. „foreign terrorist fighters") bezeichneten, bewaffneten Missionare im Namen des Korans weitreichende Grundrechtseingriffe auf den Weg gebracht werden. Sie haben eine ähnliche Dimension wie die „Anti-Terror-Gesetze" nach dem 11. September 2001. Trotzdem verlaufen die im Eiltempo durchgepeitschten Maßnahmen weitgehend unterhalb des Radars von Bürgerrechtsgruppen und NetzaktivistInnen.

Weitreichende Grundrechtseingriffe, neue polizeiliche Kompetenzen und Informationssysteme wegen „ausländischer Kämpfer"

Was die Bundesregierung zur Kontrolle „ausländischer Kämpfer" und einer „Radikalisierung" in der Pipeline hat, erläuterte das Bundesinnenministerium im August[1], im September[2] und zuletzt im November[3] in Antworten auf eine Kleine Anfrage. Der CDU/CSU ist das noch zu wenig, weshalb beide Fraktionen „Eckpunkte für einen besseren Schutz vor Djihadisten und ihren Anhängern in Deutschland" veröffentlicht haben[4]. Die Abgeordneten wollen noch mehr Grundrechtseinschränkungen und nennen das „rechtsstaatliche Mittel nachschärfen". Ähnlich hatte es der Bundesinnenminister Thomas de Maizière (CDU) formuliert, als er im Sommer davon sprach dass „eine Reihe von Maßnahmen von Bund und Ländern notwendig" seien. Hierfür seien auch „Rechtsänderungen" zu erwarten. De Maizière bezog sich auf Gespräche auf Ebene der Europäischen Union und der Vereinten Nationen.

Im September hat der Sicherheitsrat der Vereinten Nationen die Resolution 2178[5] beschlossen, in der eine „akute und zunehmende Bedrohung, die von ausländischen terroristischen Kämpfern ausgeht", festgeschrieben wird. Die UN-Resolution und die darin enthaltenen Forderungen waren zuvor mit der EU-Kommission, dem US-Heimatschutzministerium und in den informellen Treffen der „G6+1" der sechs einwohnerstärksten EU-Staaten erörtert worden, an denen seit sieben Jahren auch die USA teilnehmen.

Der Rat der Europäischen Union postulierte im Dezember vier prioritäre Bereiche, mit denen die Mitgliedstaaten zur Handlung aufgefordert werden: Prävention, Ermittlung und Aufspüren von Reisebewegungen, strafrechtliche Reak-

tion sowie die Zusammenarbeit mit Drittländern. Auch der Europäische Auswärtige Dienst (EAD) hat ein Strategiepapier mit den EU-Mitgliedstaaten zu „ausländischen Kämpfern“ abgestimmt, das im Oktober in der Anti-Terror-Ratsarbeitsgruppe positiv behandelt und dem Rat für Außenbeziehungen übergeben wurde. Laut der Bundesregierung fasse das unveröffentlichte Papier „die zahlreichen internen wie externen Aspekte“ zusammen und enthalte konkrete Handlungsempfehlungen. Im EAD sind weitreichende Kompetenzen im Bereich der Außen-, Verteidigungs-, Sicherheits- und Entwicklungspolitik zentriert.

Viele der EU-Maßnahmen gehen auf Initiativen des „Anti-Terrorismus-Koordinators“ der EU, Gilles de Kerchove, zurück[6]. Auf dem ersten EU-Innenministertreffen unter italienischer Ratspräsidentschaft wurde im Juli ein „Aktionsplan gegen die Bedrohung durch zurückkehrende Dschihadisten“ verabredet. Laut Medienberichten hätten daran Deutschland, Frankreich, Belgien, Großbritannien, Italien, Schweden, Spanien, Dänemark und die Niederlande teilgenommen. Auf dem gleichen Treffen erneuerten die Minister die „Strategie zur Bekämpfung von Radikalisierung und Anwerbung für den Terrorismus“[7]. Im Sommer hatte die EU ihre „Überarbeitete Strategie der EU zur Bekämpfung von Radikalisierung und Anwerbung für den Terrorismus“ verabschiedet[8]. Demnächst wird der Rat der Europäischen Union die „Strategie für die innere Sicherheit“ erneuern[9]. Auch dort werden etliche Vorschläge zur Bekämpfung „ausländischer Kämpfer“ aufgeführt.

Mittlerweile ist das ganze Ausmaß von Gesetzesänderungen, weiteren Datensammlungen und neuen Zusammenarbeitsformen sichtbar geworden. Hier eine Übersicht[10]:

Entzug von Reisepässen und Personalausweisen

In der UN-Resolution 2178 werden die 193 UN-Mitgliedstaaten aufgefordert, auf ihren Hoheitsgebieten die Rekrutierung, den Transport, die Durchreise, Finanzierung, Organisierung und Ausrüstung von Terroristen oder terrorbereiten Personen zu verhindern. Die Forderung könnte unter anderem durch den Entzug von Ausweisdokumenten umgesetzt werden. Das derzeitige deutsche Passgesetz erlaubt dies für Reisepässe im Falle einer „Gefährdung der inneren oder äußeren Sicherheit“. So war es in der Vergangenheit bereits in einigen Fällen bei „mutmaßlichen Salafisten“ angewandt worden, inzwischen greifen die Behörden immer öfter darauf zurück. Laut dem Personalausweisgesetz sei das Entziehen des Personalausweises Polizei- und Meldebehörden aber nicht erlaubt. Auf einer Sondersitzung beschlossen die Innenminister im Oktober, dass unverzüglich Gesetzesänderungen vorzulegen seien. Bund und Länder sollten ein vorläufiges Ersatzpapier ausstellen, das nicht zur Ausreise berechtigt. Der Bundesinnenminister nennt dies ein „Grundrechte schonendes und effektives Mittel“. Nun solle die Anti-Terror-Gesetzgebung dahingehend verschärft werden, dass bereits eine

geplante Ausreise zur Beteiligung an schweren Gewalttaten im Ausland strafbar wäre. Unklar ist, wie diese Planung nachgewiesen werden soll und ab wann diese als gesichert gilt.

Neue Kategorie im Schengener Informationssystem (SIS II)

In der EU-Polizeidatenbank soll eine neue Kategorie für „ausländische Kämpfer" oder „gesuchte Djihadisten" eingerichtet werden, um diese bei der Ein- oder Ausreise in die EU überhaupt erkennen zu können und dann besonderen Maßnahmen zu unterziehen (etwa einem Reiseverbot). Personen würden dort zur Fahndung ausgeschrieben, auch etwaige Passentziehungen könnten dort gespeichert werden. Alle Mitgliedstaaten sind aufgerufen, die neue Kategorie dann extensiv und systematisch zu nutzen. Allerdings müsste zuvor der entsprechende EU-Ratsbeschluss zum SIS II und die nachfolgende Verordnung geändert werden. Aus dem Bundesinnenministerium vernimmt man jedoch, dass sich die Maßnahmen auch „unterhalb der Schwelle von Rechtsänderungen" abspielen könnten.

Heimliche Fahndung mithilfe des Schengener Informationssystems (SIS II)

Diese „verdeckte Kontrolle" bzw. „verdeckte Registrierung" ist im Schengener Durchführungsübereinkommen geregelt. Personen und Sachen können von einer Polizeidienststelle ausgeschrieben werden. Bei „Grenzkontrollen und sonstigen polizeilichen und zollrechtlichen Überprüfungen" wird der ausschreibenden Stelle übermittelt, wann und wo die Kontrolle erfolgte. Die Betroffenen erfahren davon nichts. Auch der Anlass der Überprüfung, Reiseweg und Reiseziel, Begleitpersonen oder Insassen sowie mitgeführte Sachen werden gespeichert. Fahrzeuge können auch unter einem Vorwand durchsucht werden. Schon jetzt steigt die unbemerkte Verfolgung durch das SIS II rapide an. Nun ist geplant, die Maßnahme auch gegen „ausländische Kämpfer" zu nutzen, eine weitere, deutliche Zunahme ist also zu erwarten. In Deutschland ist dies bereits belegt: Waren im Januar 2014 noch 548 Personen zur heimlichen Fahndung ausgeschrieben, sind es im Oktober bereits 710.

Systematische Kontrollen von Staatsangehörigen der EU-Mitgliedstaaten an Außengrenzen

Der Schengener Grenzkodex[11] schreibt fest, dass Angehörige der Schengen-Staaten an den EU-Außengrenzen nicht systematisch kontrolliert werden dürften. Zulässig ist lediglich eine „Mindestkontrolle" (Feststellung der Identität, Überprüfung der Echtheit und Gültigkeit des Reisedokuments und Abgleich mit Fahndungsdateien). Um „ausländische Kämpfer" an den Außengrenzen überhaupt feststellen zu können, bedürfte es aber systematischer Kontrollen. Eigentlich wäre auch hierfür die Änderung des Schengener Grenzkodexes Voraussetzung. Diskutiert wird, die eigentlich vorgeschriebenen, nicht-systematischen

Kontrollen ohne Rechtsänderungen einfach kreativ umzuinterpretieren. Dann könnten beispielsweise Männer in einem bestimmten Alter aus bestimmten Herkunftsländern kontrolliert werden. Entsprechende Kriterien müssten aber definiert und festgeschrieben werden. Eigentlich würde es sich dann doch um eine systematische Kontrolle handeln.

Systematische Kontrolle der Reisedokumente von Staatsangehörigen der EU-Mitgliedstaaten an Außengrenzen

Bislang werden Ausweisdokumente von Angehörigen der EU bei der Ein- und Ausreise in die EU nur oberflächlich besehen. Es wird lediglich untersucht, ob vorgezeigte Dokumente echt sind. Eine Abfrage polizeilicher Datenbanken erfolgt ebenfalls nicht systematisch. Das soll sich ändern und sei nach Einschätzung vieler Regierungen auch legal. Möglicherweise wird auch hier phantasievoll uminterpretiert: Systematische Kontrollen könnten sich etwa nur auf bestimmte Reisewege (etwa die Türkei, die als Transitland vieler „ausländischer Kämpfer" gilt) fokussieren. Auch hierfür müsste der Schengener Grenzkodex geändert werden.

Europäische Fluggastdatensammlung trotz Ablehnung des EU-Parlaments

Die Regierungschefs der EU-Mitgliedstaaten haben den Rat und das Europäische Parlament jetzt aufgefordert, eine europäische Fluggastdatendatensammlung zu PNR-Daten (Passenger Name Records) einzurichten, um verdächtige Reisebewegungen von „ausländischen Kämpfern" aufzuspüren. Bei allen Flügen in die EU würden dann sämtliche Daten, die vor dem Flug in Buchungs- und Abfertigungssystemen anfallen, an die Grenzbehörden des Ziellandes übermittelt werden. Den Mitgliedstaaten würde es frei stehen, die Informationen auch bei Flügen innerhalb der EU auszutauschen. Hierzu gehören ausführliche Kontaktangaben sowie die Reiseroute, das ausstellende Reisebüro, Kreditkarteninformationen oder Essenswünsche (insgesamt bis zu 60 Datenfelder). Die Informationen sollen mindestens fünf Jahre gespeichert werden. Viele Mitgliedstaaten hatten den Richtlinienentwurf wegen zu hoher Kosten, aber auch aus Datenschutzgründen kritisiert. Der deutsche Bundesrat forderte, das EU-PNR-System nach Maßgabe des Urteils des Bundesverfassungsgerichtes zur Vorratsdatenspeicherung zu prüfen, denn die Daten würden „ohne Anlass" gespeichert werden. Das Europäische Parlament hatte die Datensammlung nicht weiter beraten, nachdem der Entwurf zur neuerlichen Behandlung in den Innenausschuss rücküberwiesen worden war. Trotzdem wollen die Regierungen der Mitgliedstaaten jetzt die Gunst der Stunde nutzen, um die Abgeordneten doch zum Abschluss des Abkommens zu bewegen. Die deutsche Regierung unterstützt die Einführung eines EU-PNR-Systems ausdrücklich[12].

Mehr Austausch von „erweiterten Fluggastdaten“

Auch ohne PNR-Abkommen werden vor Abflügen längst Fluggastdaten weitergegeben. Es handelt sich dabei um die sogenannten erweiterten Fluggastdaten (API). Hierzu gehören alle Daten des genutzten Reisedokuments sowie Daten zum Verkehrsmittel (Flugnummer und Airline, Abflug- und Zielort). Diese werden für gewöhnlich nur bei interkontinentalen Flügen verarbeitet. Nun wird geprüft ob die API-Daten auch bei Flügen innerhalb der EU genutzt werden könnten. Sie könnten das EU-PNR-Abkommen insofern ergänzen, als dass der Tausch von Fluggastdaten bei Flügen innerhalb der EU dann nicht mehr freiwillig wäre. Entsprechende Prüfungen werden nun vom EU-Netzwerk der Flughafenpolizeien AIRPOL vorgenommen.

Änderung des deutschen Passgesetzes zur Weitergabe von „erweiterten Fluggastdaten“

Inmitten der Auseinandersetzungen um den Ausstieg Großbritanniens aus zahlreichen EU-Abkommen im Bereich Innen- und Justizpolitik kündigte die britische Regierung an, auf der Übermittlung von API-Daten zu bestehen. Zahlreiche europäische Airlines gäben diese angeblich an die Einreisebehörden Großbritanniens weiter, deutsche Anbieter jedoch nicht. Daher drohen beispielsweise der Lufthansa Landeverbote. Die Bundesregierung will deshalb das deutsche Passgesetz und das Personalausweisgesetz ändern[13]. Zwar dürften Beförderungsunternehmen laut dem Passgesetz personenbezogene Daten „aus der maschinenlesbaren Zone des Passes elektronisch auslesen und verarbeiten“, wenn sie aufgrund internationaler Abkommen oder Einreisebestimmungen hierzu verpflichtet seien. Für den Personalausweis, den britische Grenzbehörden für die Einreise als Dokument akzeptieren, gilt das jedoch nicht. Noch ist unklar, welchen Umfang die von Großbritannien geforderten Informationen haben und ob diese auch den biometrischen Teil der Ausweise umfassen. Denn diese dürfen auch nach dem Passgesetz bislang nicht ausgelesen werden. Angeblich habe die Bundesregierung wegen der angedrohten Landeverbote bei der britischen Regierung einen Aufschub erreicht. Das Auswärtige Amt habe „Signale erhalten, dass der britischen Regierung nicht an einer Eskalation gelegen ist“. In anderen Worten: Hier wird ein heikles Gesetz durchgepeitscht, weil Großbritannien auf EU-Ebene für eine Verschärfung der Überwachung sorgt und dabei Zeitvorgaben macht.

Europol-Datensammlung zu „Travellers“

Die EU-Polizeiagentur Europol hat im April einen „Focal Point Travellers“ eingerichtet, in dem „ausländische Kämpfer“ gespeichert werden. Der „Focal Point“ ist in der „Arbeitsdatei zu Analysezwecken“ (AWF) „Counter Terrorism“ angesiedelt und verarbeitet Informationen über die „Anwerbung“ verdächtiger Personen und ihre Reisebewegungen. Es handelt sich um eine umfangreiche Datensammlung, an der sich einzelne Mitgliedstaaten mit Zulieferungen und Abfragen be-

teiligen. Auch das Bundeskriminalamt (BKA) macht dabei mit. Außer den EU-Mitgliedstaaten nehmen Australien, Norwegen und die Schweiz am „Focal Point Travellers“ teil. Außer Serbien und Mazedonien beabsichtigten laut der Bundesregierung auch die Zoll- und Grenzbehörden der USA eine Teilnahme. Europol und die EU-Grenzagentur Frontex sollen noch dieses Jahr eine Vereinbarung über den Austausch personenbezogener Daten schließen. Diese könnten dann auch für den „Focal Point Travellers“ genutzt werden. Ein weiterer „Focal Point“ bei Europol lautet „islamistischer Terrorismus“, dürfte also teilweise deckungsgleich sein.

Interpol-Programm gegen „ausländische Kämpfer“

Die internationale Polizeiorganisation Interpol hat ein eigenes Programm zur Verfolgung „ausländischer Kämpfer“ gestartet, um die UN-Resolution 2178 vom September umzusetzen. Die Resolution unterstreicht die Rolle von Interpol hinsichtlich des „sicheren Kommunikationsnetzwerks“, der Nutzung seiner Datenbanken, seiner elektronischen Sammlung von gestohlenen Reisedokumenten und weiterer „Anstrengungen gegen Terrorismus“ („counter-terrorism efforts“). Die Organisation solle „nationale, regionale und internationale Maßnahmen“ ergreifen, darunter die Ausweitung von Benachrichtigungssystemen und die Verhinderung von Reisen bzw. Grenzübertritten. Das neue Interpol-Programm gegen „ausländische Kämpfer“ basiert auf einer engen Zusammenarbeit mit dem US-Interpol-Zentralbüro in Washington. Hierfür sei eine Partnerschaft mit dem Nationalen Sicherheitsrat der USA, dem US-Justizministerium und dem US-Heimatschutzministerium begonnen worden. Worin die Kooperation genau besteht, bleibt unklar.

Mehr Ausschreibungen über Interpol

Interpol bietet seinen 190 Mitgliedstaaten einen multilateralen Informationsaustausch an und betreibt dafür eine gesicherte Leitung. Die Organisation richtet auch Tagungen und Arbeitstreffen aus. Über Interpol werden Ausschreibungen verteilt (die sogenannten Buntecken), etwa zur Fahndung (rot), zur Beobachtung (blau) oder zur Warnung vor unliebsamem Verhalten (grün). Mit Stand vom 20. Oktober 2014 seien laut der Bundesregierung 820 „Fahndungsdurchgaben und Buntecken“ von 32 Mitgliedsländern zu „ausländischen Kämpfern“ veröffentlicht worden.

Verstärkte Zusammenarbeit von Europol und Interpol

Schon jetzt arbeiten die beiden Polizeiorganisationen in mehreren Projekten zusammen, seit 2001 besteht ein Abkommen zur operativen Zusammenarbeit. Das US-Militär kam bereits vor mehreren Jahren in Zusammenarbeit mit dem US-Justizministerium auf die Idee, Datentauschringe mit Europol und Interpol zu vermeintlich „identifizierten ausländischen Terroristen“ einzurichten[14]. Verarbeitet werden Personendaten, Fingerabdrücke aus Ausweisdokumenten, Telefonnummern, E-Mail-Adressen und sonstige Kontaktdaten. Interpol ist mit seiner

Abteilung „Counter-Terrorism, Public Safety & Maritime Security Directorate“ involviert. Laut einer Pressemitteilung von Interpol würden Informationen mit Behörden in mehr als 60 Staaten geteilt. Vermutlich ist hierfür eine „Fusion Task Force“ (bis 2002: „Interpol Fusion Centre“) zuständig, die von Interpol zum „Kampf gegen Terrorismus“ eingerichtet wurde. Auch das BKA ist mit einem „Fusion Contact Officer“ an Bord. Die „Fusion Task Force“ ist mit mit fast 300 nationalen Kontaktstellen in 145 Interpol-Mitgliedstaaten vernetzt. Die Zahl der MitarbeiterInnen soll erhöht werden, damit diese „an internationalen Treffen zur Thematik sogenannter ausländischer Kämpfer, etwa bei Europol, VN, OSZE, NATO und EU“ teilnehmen können.

Europol unterhält ebenfalls ein „Fusion Centre“, das mehr mit Interpol zu „ausländischen Kämpfern“ zusammenarbeiten soll. 2013 haben Europol und Interpol einen „Joint Annual Action Plan“ für die Jahre 2013 und 2014 verabschiedet, um die Qualität und Verfügbarkeit der Daten zu verbessern. Eine Ausdehnung der Zusammenarbeit auf weitere Bereiche ist geplant, etwa durch Assoziierung von Interpol zu weiteren „Focal Points“ bei Europol und einer „einsatzbezogenen Unterstützung“. Die Zusammenarbeit von Europol und Interpol könnte sich intensivieren, nachdem kürzlich der langjährige BKA-Vizepräsident Jürgen Stock offiziell in das Amt des Generalsekretärs von Interpol eingeführt wurde. Stock gilt als Experte für den internationalen Datentausch.

Vorgeschriebene Abfrage von Interpol-Datenbanken

Die internationale Polizeiorganisation unterhält eine Datenbank für gestohlene und verlorene Reisedokumente (SLTD-Datenbank), die aber noch nicht von allen Mitgliedstaaten genutzt wird. Laut Interpol seien 43 Millionen Einträge enthalten. Nach dem Verschwinden des malaysischen Flugzeugs MH370 und dem Bekanntwerden, dass zwei Personen mit als verlustig gemeldeten Pässen an Bord gelangt wären, hatte Interpol gefordert, dass grenzpolizeiliche Abfragen der SLTD-Datenbank verpflichtend werden würden. Damals ließ sich die Forderung nicht durchsetzen, zur Bekämpfung „ausländischer Kämpfer“ ging das plötzlich ganz schnell: Im Herbst 2013 wurde eine Arbeitsgruppe zur Ausgestaltung des Projekts gegründet, die drei Empfehlungen erarbeitet hat. Diese wurden auf dem Treffen der EU-Innenminister Anfang Oktober in „Schlussfolgerungen des Rates zur verstärkten Nutzung der Interpol-Datenbank für gestohlene und verlorene Reisedokumente“ durchgewunken und in einer Interpol-Resolution verabschiedet. Nun soll die Datenbank bei jeder Abfrage des Schengener Informationssystems gleichzeitig mitabgefragt werden. Auch die Internationale Zivilluftfahrt Organisation (ICAO) prüft, ob hierzu Empfehlungen verabschiedet werden könnten.

Abfrage von Interpol-Datenbank auch durch Private

Interpol beabsichtigt, dass unter dem Namen „I-Checkit“ auch Privatfirmen das SLTD-Register gestohlener oder verlorener Dokumente abfragen können, etwa

wenn ein Bankkonto eröffnet, ein Auto gemietet oder in ein Hotel eingecheckt wird. Hierzu hatte Interpol die Meldung lanciert[15], „ausländische Kämpfer" würden mittlerweile auch Kreuzfahrtschiffe nutzen, um unerkannt in die Türkei reisen zu können, allerdings keine Belege dafür präsentiert. Erste Tests von „I-Checkit" haben mit Fluglinien wie AirAsia und nicht näher benannten Hotels stattgefunden. Die Interpol-Generalversammlung beschloss die Fortführung der Tests und regte an, das Verfahren auf eine „große Bandbreite anderer Partner" auszudehnen. Qatar Airways kündigte an, als erste an „I-Checkit" teilzunehmen. Laut der Bundesregierung seien „zwei Verfahrensvarianten zur Umsetzung" vorgesehen: Entweder werde im Trefferfall eine Nachricht an die betroffenen nationalen Interpol-Zentralbüros und das private Unternehmen generiert. Das Unternehmen erhalte ein „grünes", „gelbes" oder „rotes Licht" als Rückmeldung. Das gelbe Licht zeige an, wenn eine Überprüfung nicht möglich war, etwa wenn ein Mitgliedsland nicht an „I-Checkit" teilnehme. In einer zweiten Variante erhielten nur die betroffenen nationalen Zentralbüros, nicht aber das private Unternehmen eine Mitteilung über Treffer. Auch „Mischvarianten" seien möglich. Die Ergebnisse der Pilotphase sollen auf der Generalversammlung 2015 vorgestellt und dort über den Fortgang des Projekts entschieden werden. Ein „Roll Out" ist für 2016 geplant. Die Bundesregierung stehe dem Vorhaben angeblich kritisch gegenüber und beteilige sich zunächst nicht.

Aufspüren und Bekämpfen von „Terrorismusfinanzierung"

Kriminalpolizeien wie das BKA unterhalten sogenannte „Financial Intelligence Units" zur Ausforschung verdächtiger Finanzströme und dem Aufspüren „terroristischer Netzwerke". Genutzt werden Vorratsdatenspeicherungen von Finanzdaten, die von Banken und Kreditinstituten geführt werden müssen. Im Falle der „ausländischen Kämpfer" sind vor allem Finanzströme in Syrien von Interesse. Laut dem früheren Bundesdatenschutzbeauftragten Peter Schaar[16] diene das Argument des Kampfs gegen den Terrorismus „als eine Art Türöffner" zu Kontodaten. Abfragen würden „oftmals ohne Begründung und ohne Nachricht an den Betroffenen" durchgeführt. Die nun angekündigten Verschärfungen im „Kampf gegen Geldwäsche" hinsichtlich einer „Terrorismusfinanzierung" könnten also zur weiteren Zunahme von Abfragen führen. Tatsächlich erklärte die Bundesregierung, es seien „Fälle bekannt geworden", in denen „Beschuldigte aus dem islamistisch-terroristischen Spektrum" Sozialhilfeleistungen bezogen hätten. Eine weitere Ausweitung von Abfragen auch bei Sozialbehörden ist also zu erwarten.

„Bekämpfung der Geldwäsche und der Terrorismusfinanzierung" innerhalb der Financial Action Task Force (FATF)

Die G7-Staaten hatten die weitreichenden Möglichkeiten von Finanzermittlungen erkannt und hierfür 1989 eine Financial Action Task Force on Money Laun-

dering (FATF) gegründet. Sie gehört zur Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und hat derzeit 36 Mitglieder. Unter anderem analysiert die FATF veränderte Methoden der Geldwäsche, Terrorismusfinanzierung oder anderer Kriminalitätsbereiche. Ihre „40 Empfehlungen" enthalten auch eine „proaktive Strafverfolgung". Wie die EU regt auch die FATF die Einrichtung neuer, übergreifender „nationaler Zentren" aus mehreren Behörden an. Sie sollten in jedem Mitgliedstaat als Kontaktstelle zur Entgegennahme, Analyse und Weitergabe von Meldungen über verdächtige Transaktionsmeldungen dienen. Im Oktober 2014 hat die FATF ein Papier zur Bekämpfung des „Islamischen Staat" veröffentlicht. Demnach sollten Staaten auch dann Ermittlungen zur „Terrorismusfinanzierung" vornehmen, wenn eine direkte Verbindung zu einem „terroristischen Akt" fehle. Auf „robuste Weise" sollten Sanktionen gegen Personen und Organisationen verhängt und die Betroffenen schnellstmöglich auf entsprechenden Listen geführt werden. Der „Islamische Staat" sollte am Zugang zu internationalen Finanzmärkten gehindert werden. Regierungen müssten hierfür Systeme errichten, um ankommende und abgehende Anweisungen zur Auszahlung von Geldbeträgen transparent zu machen. Würden deren InhaberInnen als verdächtig eingestuft, dürften Behörden die Anweisungen konfiszieren. Auch die Bundesregierung will die FATF-Empfehlungen umsetzen[17].

Bis Ende des Jahres sei beabsichtigt, einen Gesetzesentwurf zur „Strafbarkeit für das Waschen eigener Erträge durch Vortatbeteiligte" vorzulegen. Im Bereich der „Terrorismusfinanzierung" sollte ein Entwurf eines eigenständigen Straftatbestands der „Terrorismusfinanzierung" ausgearbeitet werden.

Stärkere Nutzung des „Programms zum Aufspüren der Finanzierung des Terrorismus"

Das zwischen der EU und den USA abgeschlossene „Programm zum Aufspüren der Finanzierung des Terrorismus" (TFTP) ist eher bekannt unter dem Begriff „SWIFT-Abkommen": Seit 2010 existiert der erneuerte Vertrag zum transatlantischen Datentausch von Finanzdaten des belgischen Finanzdienstleisters SWIFT. Das US-Finanzministerium erhält auf Anfrage Informationen über internationale Finanztransaktionen, Stammdaten, Post- oder Mailadressen der KontoinhaberInnen oder deren Telefonnummern. Damit können dann weitere Datensammlungen nach „Kreuztreffern" abgefragt werden.

GegnerInnen des EU-US-Abkommens hatten als Alternative die Errichtung eines gleichlautenden EU-Systems gefordert. Die EU-Kommission kommt zu dem Schluss, dass ein neues, europäisches System zur Analyse von Finanzdaten keinen Mehrwert habe. Stattdessen sollten europäische Strafverfolgungsbehörden ihre Abfragen (europäischer!) Finanzströme lieber weiterhin über die USA ausführen[18].

Maßnahmen gegen „terroristische Onlineaktivitäten“

Vor ihrer Oktober-Sitzung trafen sich die Innenminister der EU-Mitgliedsstaaten und die EU-Kommission mit den Internetkonzernen Twitter, Google, Microsoft und Facebook. Laut der Bundesregierung sei es um „internetbezogene Sicherheitsaufgaben im Kontext der Beziehungen zu Großunternehmen der Internet-Branche“ gegangen, auch „Verfahrensanforderungen“ seien erörtert worden. Außer „Möglichkeiten der Verhinderung der Verbreitung von Hinrichtungsbildern für Propagandazwecke“ sei auch die Nutzung von Accounts in sozialen Netzwerken durch „Terrororganisationen“ Thema gewesen. Inzwischen hat hierzu ein „Arbeitstreffen“ von Innenministerien aus Österreich, Deutschland, der Schweiz, Liechtenstein und Luxemburg stattgefunden. Laut der österreichischen Innenministerin Mikl-Leitner gehe es vor allem darum, dass „terroristische Inhalte möglichst rasch aus dem Internet genommen werden, um keinen Keim zu säen“.

In der gleichen Pressemitteilung ist davon die Rede, dass Mikl-Leitner hierzu das „Google Entwicklungszentrum Zürich“ besucht habe, das als der „größte Entwicklungsstandort der Firma außerhalb der USA“ beschrieben wird. Die Innenministerin habe sich dort angesehen, „an welchen Entwicklungen Google-Experten arbeiten, um verhetzende Inhalte zu erkennen“. Auch auf dem G6-Treffen europäischer Innenministerien war das Thema auf der Agenda. Mit den Ministerien aus den USA und Kanada wurde verabredet, einen „strukturierten Dialog mit den großen Netzbetreibern“ zu beginnen[19].

Diese sollten laut dem deutschen Innenminister Inhalte von sich aus sperren oder löschen („aus eigenem Interesse diese Quelle des digitalen Dschihad dadurch austrocknen, dass sie solche Inhalte selbst aus dem Netz entfernen“). Die Konzerne sind vom „eigenen Interesse“ offensichtlich nicht überzeugt, denn es handele sich laut dem Minister noch um einen „dringenden Appell“. Auch die Generalversammlung von Interpol hatte im November beschlossen, stärker gegen eine „terroristische Nutzung“ des Internets vorzugehen. Damit wird wohl der neue „Global Complex for Innovation“ (IGCI)[20] beauftragt, den Interpol derzeit in Singapur errichtet. Der Komplex soll ähnlich wie bei Europol neue, digitale Ermittlungstechniken entwickeln und bereitstellen. Das IGCI sollte ursprünglich noch dieses Jahr in Betrieb genommen werden, wird aber nach einer zunächst symbolischen Feier im Oktober erst im April seine Arbeit aufnehmen.

Nutzung des „Globalen Forums zur Bekämpfung des Terrorismus“

Auf Initiative der USA haben mehrere Staaten und supranationale Organisationen 2011 das „Global Counterterrorism Forum“ (GCTF) eingerichtet. Zu den Gründern gehört auch Deutschland, zur Eröffnung reisten Angehörige des Auswärtigen Amts und des Bundesinnenministeriums an. Ziel ist die Identifizierung dringender Maßnahmen zur Abwehr von „Terrorismus“ und „gewalttätigem Extremismus“. Das GCTF soll Lösungen erarbeiten und „Ressourcen“ zu ihrer Um-

setzung bereitstellen. Mittlerweile hat das GCTF in Abu Dhabi ein „Kompetenzzentrum zur Bekämpfung von gewalttätigem Extremismus“ ins Leben gerufen. Sein Zweck wird mit „Training, Dialog, Zusammenarbeit und Forschung“ angegeben. Unter Federführung der Niederlande und Marokkos wurde ein Arbeitsschwerpunkt „ausländische Kämpfer“ eingerichtet. Die Mitglieder des GCTF werden jetzt aufgerufen, die Zusammenarbeitsformen verstärkt zu nutzen. Über das GCTF kann auch mit anderen „Schlüsselländern“ zusammengearbeitet werden. Hierzu gehören Libyen, Algerien, Ägypten, Jordanien, Libanon, Marokko, Tunesien, die Türkei und der Irak.

Maßnahmen werden nicht zurückgenommen

Nur wenige der beschriebenen Maßnahmen werden von Bürgerrechtsgruppen überhaupt beachtet, vielfach findet eine kritische Behandlung lediglich in den Parlamenten statt. Eine Ausnahme bildet der Plan zum Aufbau einer EU-Fluggastdatensammlung, der nach heftiger Kritik durch das EU-Parlament 2012 zunächst auf Eis gelegt wurde.

Auf welche Weise die PNR-Vorratsdatenspeicherung trotzdem durch die Hintertür durchgedrückt wird, erklärte die EU-Abgeordnete Sophia in ’t Veld in der November-Sitzung des LIBE-Ausschusses. Bis vor anderthalb Jahren verfügte lediglich Großbritannien über ein PNR-System. Mittlerweile hat aber die EU-Kommission den Aufbau von 15 weiteren, nationalen Systemen finanziert. Nun wird behauptet, dass diese in einem Zentralsystem „harmonisiert“ werden müssten, die Einführung eines EU-PNR also unentbehrlich sei. Ein Land wie die Niederlande, das kein PNR-System beschaffen wolle, würde durch eine entsprechende EU-Richtlinie zur Einführung gezwungen.

Einmal eingerichtet dürfte jeder Widerstand zwecklos sein: Gewöhnlich werden Gesetzesverschärfungen, neue Kompetenzen von Polizeibehörden oder neue Datenbanken nicht mehr zurückgenommen. Vielmehr ist eine weitere Ausweitung zu erwarten.

Das Phänomen der „ausländischen Kämpfer“ soll also Maßnahmen begründen, die längst in der Pipeline sind, aber politisch zunächst nicht durchsetzbar waren. „Extremismus“, „Terrorismus“ oder „Radikalisierung“ sind Container-Begriffe und dadurch geeignet, sie jederzeit politisch neu zu definieren. Dann können sie gegen andere, unliebsame Bewegungen in Stellung gebracht werden.

Viele der Vorschläge sind technischer Natur und sollen digitale Analysefähigkeiten einführen oder verbessern. Ihr Nutzen ist aber meistens nicht belegt. Hinzu kommt, dass die wenigen Erfolge digitaler Bewegungen übergangen werden, wenn nun neue Vorratsdatensammlungen entstehen oder die Zweckbestimmung vorhandener Systeme ausgeweitet wird. Es ist also höchste Eile geboten, die feuchten Träume der Innenminister nicht ohne weiteres Realität werden zu lassen.

Anmerkungen

[1] http://dip21.bundestag.de/dip21/btd/18/024/1802429.pdf

[2] http://dipbt.bundestag.de/dip21/btd/18/027/1802725.pdf

[3] http://www.andrej-hunko.de/start/download/doc_download/520-massnahmen-der-polizeiorganisation-interpol-gegen-sogenannte-auslaendische-kaempfer

[4] https://www.cducsu.de/download/file/fid/42175

[5] http://www.un.org/depts/german/sr/sr_14/sr2178.pdf

[6] http://www.statewatch.org/news/2014/may/eu-council-coter-syrian-fighters-9280-14.pdf

[7] http://register.consilium.europa.eu/doc/srv?l=DE&f=ST%209956%202014%20INIT

[8] http://www.parlament.gv.at/PAKT/EU/XXV/EU/02/71/EU_27175/imfname_10470479.pdf

[9] http://www.parlament.gv.at/PAKT/EU/XXV/EU/04/19/EU_41912/index.shtml

[10] Die beschriebenen Maßnahmen beziehen sich lediglich auf die Zusammenarbeit der Strafverfolgungsbehörden. Zwar wird stets bekräftigt, auch die Geheimdienste müssten mehr kooperieren. Bekannt ist dazu aber wenig, etwa dass auf Ebene der Europäischen Union das Lagezentrum „Intelligence Analysis Centre" (EU INTCEN) stärker eingebunden werden müsste und hierzu auch mit „Drittstaaten" kooperiert werden sollte. Vermutlich wird aber auch die militärische geheimdienstliche Struktur des „EUMS INT Direktorat" mehr gefordert.

[11] Die beschriebenen Maßnahmen beziehen sich lediglich auf die Zusammenarbeit der Strafverfolgungsbehörden. Zwar wird stets bekräftigt, auch die Geheimdienste müssten mehr kooperieren. Bekannt ist dazu aber wenig, etwa dass auf Ebene der Europäischen Union das Lagezentrum „Intelligence Analysis Centre" (EU INTCEN) stärker eingebunden werden müsste und hierzu auch mit „Drittstaaten" kooperiert werden sollte. Vermutlich wird aber auch die militärische geheimdienstliche Struktur des „EUMS INT Direktorat" mehr gefordert.

[12] http://dipbt.bundestag.de/dip21/btd/18/029/1802972.pdf

[13] https://netzpolitik.org/2014/bundesregierung-will-gesetzesaenderung-um-ausweisdaten-auszulesen-und-sie-als-fluggastdaten-an-grossbritannien-zu-pushen/

[14] https://netzpolitik.org/2014/bundesregierung-bestaetigt-datentauschring-von-bka-europol-interpol-und-us-militaer-zu-identifizierten-auslaendischen-terroristen

[15] http://www.heise.de/tp/artikel/43/43272/1.html

[16] http://www.taz.de/!128251

[17] http://dipbt.bundestag.de/dip21/btd/18/028/1802888.pdf

[18] https://netzpolitik.org/2014/im-ernst-polizeien-der-eu-mitgliedstaaten-sollen-vorratsdaten-des-belgischen-finanzdienstleisters-swift-beim-us-finanzministerium-abfragen/

[19] http://www.neues-deutschland.de/artikel/951500.eu-will-islamisten-an-ihren-aussengrenze-abfangen.html

[20] https://netzpolitik.org/2014/neues-interpol-zentrum-gegen-weltweiten-cybercrime-verzoegert-sich-konferenz-mit-europol-wird-aber-nicht-abgeblasen

Matthias Monroy ist Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift Bürgerrechte & Polizei/CILIP. Er ist Mitarbeiter des MdB Andrej Hunko und publiziert in linken Zeitungen, Zeitschriften und Online-Medien, bei Telepolis, netzpolitik.org und in Freien Radios.

4 Algorithmen Allmächtig? Freiheit in den Zeiten der Statistik

von **Kai Biermann**

Was hat Statistik, was haben Big Data und Algorithmen mit Freiheit zu tun? Lassen Sie mich Ihnen dazu eine wahre Geschichte erzählen.

Target ist nach WalMart der zweitgrößte Discounteinzelhändler der USA. Kleidung, Möbel, Spielzeug, Zahnpasta – dort gibt es alles und das möglichst billig. Vor einiger Zeit kam ein wütender Mann in eine Target-Filiale außerhalb von Minneapolis und wollte den Filialleiter sprechen. Er wedelte vor dessen Nase mit Rabattgutscheinen herum und beschwerte sich: „Meine Tochter hat die hier in ihrer Post gefunden. Sie ist noch in der Highschool und Sie schicken ihr Rabattmarken für Babysachen und Kinderbetten? Wollen Sie sie etwa ermuntern, schwanger zu werden?"

Der Filialleiter schaute sich die Gutscheine an, sie waren eindeutig an die Tochter des Mannes adressiert und priesen unter anderem Schwangerschaftsmode und Wickelkommoden an. Er entschuldigte sich wortreich für das Missverständnis. Ein paar Tage später rief er bei dem Vater an, weil er noch einmal für den Ärger um Verzeihung bitten wollte. Zu seinem Erstaunen war der Vater reichlich beschämt und sagte: „Ich hatte ein längeres Gespräch mit meiner Tochter. Dabei musste ich feststellen, dass es Aktivitäten in meinem Haus gibt, von denen ich keine Ahnung hatte. Sie wird im August ein Kind bekommen. Und ich schulde Ihnen eine Entschuldigung."

Das Ganze – beschrieben in einem lesenswerten Text im Februar 2012 in der New York Times[1] – war kein Versehen von Target. Sondern es ist ein Beispiel dafür, wie viel Target über seine Kunden weiß und wie gut die Algorithmen des Unternehmens arbeiten. Es ist ein Beispiel für die Macht eines Systems, das wir mit dem Ausdruck Big Data bezeichnen. Big Data – also das Suchen mit statistischen Verfahren nach Mustern in großen Datenmengen – kann von unglaublichem Nutzen sein. Aber Big Data birgt auch eine gewaltige Gefahr: Mit Big Data könnten die Menschen das verlieren, was Menschsein ausmacht, ihre unbekannte Zukunft. Mit Big Data könnten sich die Menschen ihrer Freiheit berauben.

Menschen haben Gewohnheiten, sie trainieren sich bestimmte Verhaltensmuster an und behalten diese oft ein Leben lang bei. Denn Menschen sind faul, beziehungsweise sparsam mit ihrer Energie, und solche Muster ersparen dem Gehirn

Arbeit. Das bedeutet beispielsweise für Einzelhändler, dass es sehr schwer ist, neue Kunden zu gewinnen. Wenn sich jemand einmal daran gewöhnt hat, jeden Samstag bei dem gelben Netto mit dem Hund im Logo die Lebensmittel für eine ganze Woche zu kaufen, wird es Lidl oder Kaiser's kaum noch gelingen, diesen Menschen als Kunden zu gewinnen.

Doch es gibt Ausnahmen von dieser Regel, denn manchmal ändern sich Gewohnheiten. Zum Beispiel dann, wenn sich das Leben ändert. Eine neue Arbeit, ein Umzug, eine neue Beziehung – solche Lebensereignisse können dazu führen, dass Gewohntes aufgegeben wird und jemand offen für Neues ist. Die Warenhauskette Target nutzt diese Momente. Schwangerschaften sind ein solches Lebensereignis. Werdende Eltern brauchen Dinge, die sie nie zuvor gebraucht haben, eben Wickelkommoden oder Windeln. Sie haben somit keine dazu passenden Kaufgewohnheiten. Doch ist es aus Sicht des Verkäufers zu spät, den neuen Eltern entsprechende Werbung zu schicken, wenn das Kind schon auf der Welt ist. Sie haben die meisten Dinge dann schon gekauft und neue Gewohnheiten entwickelt. Target hat daher viel Mühe darauf verwendet, in seinen Kundendaten nach Verbindungen zwischen Schwangerschaften und Kaufgewohnheiten zu suchen.

Und an diesem Punkt lässt sich erkennen, wie Big Data funktioniert. Es geht um Ähnlichkeit, um den Vergleich eines gerade beobachteten Verhaltens mit bereits bekannten Verhaltensmustern. Der einzelne Mensch ist dabei egal. Wie er heißt, ist uninteressant. Warum er etwas tut, spielt keine Rolle. Es geht nur darum, mit Hilfe von Korrelationen, mit Hilfe von statistischen Zusammenhängen, sein Verhalten mit dem vieler anderer Menschen zu vergleichen. Es geht darum, die Schublade zu finden, in die er passt und ihn anschließend entsprechend dieser Schublade zu beurteilen. Bislang wurde ein solches Vorgehen mit dem Ausdruck „Vorurteil" bezeichnet und war gesellschaftlich geächtet. Mit Big Data aber kann es missbraucht werden, können Vorurteile zum Standard mutieren.

Target errechnet aus den Einkäufen seiner Kundinnen, ob diese schwanger sind. Das Unternehmen vergleicht dazu das Einkaufsmuster einer Kundin mit den Mustern, die es aus seinen Daten kennt und kann so mit hoher Wahrscheinlichkeit errechnen, wann genau das Baby auf die Welt kommen wird. Target ist nicht nur ziemlich gut darin, den Geburtstermin zu treffen, sie wissen auch, in welchem Abschnitt der Schwangerschaft die Eltern was kaufen. Warum das so ist, weiß das Unternehmen nicht. Es ist ihm auch egal. Dass es so ist, genügt – um zu wissen, wann welche Werbung eintreffen muss, um diesen bis dahin vielleicht noch unbewussten Kaufwunsch auszunutzen.

Alles, was Target dazu braucht, sind Daten. Das Unternehmen versucht, jeden Kunden, der in einen seiner Läden oder auf seine Website geht, eindeutig zu markieren. Jeder bekommt eine sogenannte Gast-ID, eine Nummer, unter der gespeichert wird, was dieser spezielle Kunde gekauft und getan hat. Was hat er angesehen, was bezahlt, was bewusst ignoriert? Hat er mit Kreditkarte bezahlt und mit

welcher? Hat er einen Rabattcoupon benutzt und woher kam der? Hat er sich beschwert und worüber? Auch Tageszeit und Wetter werden registriert. Alles wird gespeichert. Target erweitert diese Kundenprofile um jeden Datensatz, den der Konzern irgendwo kaufen oder bekommen kann. Alter, Familienstand, geschätztes Einkommen, Wohnort, Automarke, Jobs, Ausbildung, Interessen, politische Einstellungen – jede noch so kleine Information ist von Interesse.

Wenn Sie jetzt denken, solche Datensammlungen seien doch nur in den USA möglich, dann sollten Sie einen kurzen Moment lang darüber nachdenken, wie oft Sie bereits etwas bei Amazon bestellt haben. Oder bei Google. Oder bei Apple. Oder was Facebook über Sie weiß. Jeder dieser Konzerne sammelt genau wie Target alle Informationen über seine Kunden, die sich finden lassen. Und im Internet sind das eine Menge – beispielsweise dank Cookies und dank der Browserhistory, den Seiten also, die jemand zuvor im Netz besucht hat. Und auch in Deutschland kann man viele demographische Daten kaufen, samt der dazu gehörenden Namen und Adressen.

Target nun durchsucht diese Daten, um eine ganz spezielle Zielgruppe zu finden. Sie wollen Werbung an Frauen schicken, die im zweiten Drittel ihrer Schwangerschaft sind – denn ihre Daten zeigen, dass das der Zeitpunkt ist, an dem Eltern beginnen, Babyausstattung einzukaufen. Die einzelnen Informationen wirken harmlos und ohne Zusammenhang. In der Masse jedoch, als Big Data, zeigen sich darin Muster:

Schwangere kaufen größere Mengen unparfümierter Cremes als Nichtschwangere. Schwangere kaufen Nahrungsergänzungsmittel wie Kalzium, Magnesium oder Zink. Sie kaufen unparfümierte Seife, Wattebäusche, Händedesinfektionsmittel und Feuchttücher. Target – was übersetzt passenderweise „Ziel" bedeutet – hat in seinen Daten ungefähr 25 Produkte identifiziert, die zusammengenommen erlauben, Schwangeren-Profile und einen Schwangeren-Score zu errechnen. Denn da Schwangere einzelne dieser Produkte zu ganz bestimmten Zeitpunkten der Schwangerschaft zu kaufen scheinen, ist es dem Unternehmen sogar möglich, den Geburtstermin ziemlich genau zu berechnen. Und damit entsprechende Werbung zu verschicken, lange bevor der künftige Großvater weiß, dass er Enkel bekommt.

Warum erzähle ich all das? Weil flächendeckende Überwachung durch Geheimdienste nur eine Bedrohung für unsere Freiheit und unsere Bürgerrechte ist. Eine mindestens ebenso große geht von der Statistik aus und von den datensammelnden Institutionen, die statistische Vorhersagen dazu missbrauchen, Menschen zu beurteilen, ja sie zu verurteilen.Vorhersagen verringern Risiken, sie machen Dinge planbar, verhindern Schäden. Das spart Geld und Ressourcen. Aber es ist gleichzeitig gefährlich.

Wenn Target menschliche Gewohnheiten so zielsicher analysieren und vorhersagen kann, können andere das auch. Und sie tun es. Alle. Banken, Versicherungen,

Einzelhändler, Kommunikationsfirmen, Geheimdienste, Polizei – alle wollen genau das Gleiche können wie Target und wissen, ob jemand schwanger ist, bevor die werdenden Eltern das wissen. Sie wollen wissen, ob er seinen Kredit bezahlen kann. Oder ob er demnächst ein Auto kaufen will. Oder im kommenden Monat jemanden umbringen.

Aber damit beeinflussen sie das Verhalten der betroffenen Menschen, ohne dass diese es merken oder verhindern können. Sie nehmen ihnen die Freiheit, selbst zu entscheiden, was gut für sie ist. Sie machen sie zu Marionetten. Denn vielleicht hat derjenige zwar mit dem Gedanken gespielt, sich einen neuen Fernseher zu kaufen, aber eigentlich gar nicht das Geld dafür. Ohne gezielte Ansprache durch Werbung – ohne Überredung also, hätte er sich diesen vielleicht nie angeschafft.

Ein zweites Beispiel. Irgendwann bestellte ein Drogendealer bei Amazon eine digitale Feinwaage namens „American Weigh AWS 100". Ein anderer Dealer tat das gleiche. Und ein dritter und ein vierter. Es ist eine preiswerte und genau messende Waage. Amazon speicherte das. Genau wie die Dinge, die diese und andere Dealer anschließend auch noch kauften. Und nach einer Weile bekam, wer nach dieser Waage suchte, eine komplette Einkaufsliste zum Start einer Dealerkarriere angezeigt: ein Drogen-Test-Kit, kleine Plastiktüten mit aufgedruckten Hanfblättern, ein Mahlwerk, eine Maschine zum Füllen von Kapseln und die dazu gehörenden Gelatinekapseln, luftdicht verschließbare Behälter…

Bei Amazon entstehen solche Profile jeden Tag, sie wachsen in den Daten. Das weiß nicht nur Amazon, das wissen sicher auch staatliche Ermittler. Na und, könnten Sie sagen, das ist doch etwas Gutes, es trifft doch die Richtigen. Aber so funktionieren Profile und Wahrscheinlichkeiten nicht. Auch Apotheker bestellen Feinwaagen und Chemikalien. Es geht um Ähnlichkeit. Ihr Verhalten wird mit dem Verhalten der Zielgruppe verglichen und wenn es sich ähnelt, werden auch Sie zum Ziel, ob sie etwas damit zu tun haben oder nicht. Sie können es nicht verhindern, Sie können es nicht beeinflussen, ja Sie erfahren es nicht einmal.

Noch ein drittes Beispiel: Robert McDaniel lebt in Chicago in der Community Austin im Bezirk West Side, in einer Gegend, in der die Kriminalitätsrate hoch ist. Er ist in seiner Jugend ein paarmal verhaftet aber nie angeklagt worden. Nur einmal wurde er verurteilt, wegen einer Ordnungswidrigkeit. Als im Juli 2013 eine Polizistin vor der Tür des 22-Jährigen stand, war er leicht verwirrt. Sie war freundlich, aber eindeutig in ihrer Botschaft an McDaniel: Er solle besser schnell sein Leben ändern oder er müsse die Konsequenzen tragen. Barbara West, so der Name der Polizistin, gab ihm zu verstehen, dass sie viel über McDaniel wisse. Beispielsweise, dass sein bester Freund im vergangenen Jahr ermordet worden war. McDaniel drohe das gleiche Schicksal, wenn er nichts unternehme, sagte sie ihm. Außerdem werde er bei dem kleinsten Vergehen mit maximaler Härte bestraft werden – McDaniel war auf der sogenannten „Heat List"[2] gelandet.

West bezog ihre Informationen aus einer Datenbank der Polizei von Chicago. Die nutzt Mathematik, um vorherzusagen, wer in nächster Zeit Opfer oder Täter in einem Gewaltverbrechen wird und führt diese Namen in eben jener „Heat List". Ein Pilotprojekt, finanziert vom National Institute of Justice. Für die Liste werden viele Informationen gesammelt: Demografie, Einkommen, Hauspreise und natürlich Polizeiberichte. Doch geht es dabei nicht einfach um Wahrscheinlichkeiten. Die Polizei analysiert Netzwerke. Andrew Papachristos hat das Verfahren entwickelt. Er ist Professor für Soziologie an der Universität Yale. Er hat beobachtet, dass die Opfer von Gewaltverbrechen in der Region oft einen ähnlichen Hintergrund haben. Wenn man mit Leuten herumhängt, die ins Gefängnis gehen, die erschossen werden, so seine Theorie, so teilt man deren Haltungen und Verhaltensweisen und setzt sich also selbst dem Risiko aus, Gewalt zum Opfer zu fallen, auch wenn man gar nicht kriminell ist. Das Verhaltensprofil ist entscheidend. Auf Basis dieser Analyse führt die Polizei von Chicago 400 Menschen in ihrer „Heat List" und besucht sie wie McDaniel. Einerseits wird ihnen dabei gedroht, andererseits werden ihnen von der Stadt Angebote gemacht, ihnen bei der Jobsuche oder bei der Suche nach sozialen Angeboten zu helfen. Peitsche und Zuckerbrot – allein auf Basis von Statistik. Eine Art Sippenhaft, denn die Betreffenden müssen wie gesagt selbst gar nicht kriminell sein.

Und auch das gibt es in Deutschland. Wir nennen es nicht „Heat List", sondern „Gefährder". Das klingt nach Gefahr, nach bedrohlichen Leuten, und genau das soll es auch, um von der Tatsache abzulenken, dass es hier um Wahrscheinlichkeiten geht, nicht um Fakten. Denn damit sind Menschen gemeint, gegen die es keine Beweise gibt, keine Anklage, kein Urteil. Sie gelten allein deswegen als „Gefährder", weil ihr Verhalten dem Verhaltensprofil von jenen ähnelt, die später Terroristen wurden: zum Islam konvertiert, längere Zeit nach Pakistan oder Afghanistan gereist, mit Terroristen bekannt oder Geld gesammelt für Unterstützgruppen von Terroristen. Kriminelles getan haben müssen sie nichts. Trotzdem wird allein aufgrund von Verhaltensprofilen gegen sie vorgegangen, sie werden beobachtet, verfolgt, am Reisen gehindert.

Diese Art von „Gefahrenabwehr" ist inzwischen Standard in Deutschland. Alle Erweiterungen von Polizei- und Geheimdienstgesetzen der vergangenen zwanzig Jahre beschäftigen sich vor allem damit: kein Risiko eingehen. Die Polizei Hamburg hat seit 1995 mehr als 50 Mal ganze „Gefahrengebiete" in der Stadt ausgewiesen. Einziges Kriterium bei der Definition der Gefahr sind Verhaltensprofile, nicht Straftaten. Das bisher letzte, im Januar 2014, führte zu heftigen Protesten.

Und die Polizei von Nordrhein-Westfalen hat gerade angekündigt[3], die Software zu testen, mit der solche „Heat Lists" erstellt werden. Sie will so die Zahl der Einbrüche senken. Statistische Vorhersagen aufgrund von Ähnlichkeiten und Mustern haben beträchtliche Vorteile. Menschen können dank ihnen nicht nur künftige Risiken verstehen, sondern auch die zugrunde liegenden Faktoren versuchen

zu beeinflussen und so unter Umständen erreichen, dass die entsprechenden Probleme vielleicht nie eintreten. Damit lassen sich Gefahren verhindern, aber auch Warenkreisläufe effizienter machen. Es kann der Gesellschaft viel Geld und Leid ersparen.

Aber mit der Fähigkeit, die Zukunft vorherzusagen, geht auch etwas zutiefst Menschliches verloren: Zukunft wird so nicht mehr als offen begriffen, Schicksal nicht mehr als ungeschrieben. Es droht die Gefahr, dass jeder Mensch anhand der Vorhersage seines Verhaltens beurteilt wird und nicht mehr danach, was er wirklich tut. Noch bevor er oder sie handeln kann, sind er oder sie bereits schuldig gesprochen und verurteilt. Das erinnert manchen von Ihnen sicher an den Film „Minority Report", in dem eine „Pre-Crime"-Polizei Verbrecher festnimmt, bevor sie jemanden umbringen können. Das klingt erst einmal gut, es klingt wie ein Verbrechen ohne Opfer. Doch das stimmt nicht. Es gibt ein Opfer, es ist der- oder diejenige, der oder die festgenommen wird. Denn solche Vorhersagen aufgrund von Wahrscheinlichkeiten und Korrelationen sprechen dem Fast-Täter den freien Willen ab, sich im letzten Moment anders zu entscheiden. Sie entmündigen ihn und damit alle Menschen. Und das nicht aufgrund seines oder ihres eigenen Verhaltens. Sondern weil sein Verhalten so ähnlich aussieht wie das Verhalten von Menschen, die irgendwann zuvor die gleiche Tat begangen haben. Sieht so ähnlich aus… Es mag auf den ersten Blick wie eine gute Idee wirken, mit der Analyse vergangener Dinge auf die Zukunft zu schließen. Aber eigentlich ist es ein Schuldigsprechen aufgrund von Dingen, die andere Menschen in einer ähnlichen Lage getan haben und nicht aufgrund des individuellen Verhaltens.

Das ist nicht fair.

Es verweigert den Betroffenen die Freiheit, selbst zu bestimmen, wohin ihr Weg sie führen soll. Es verhindert unter Umständen Risikobereitschaft und Neugier. Menschen können nicht mehr unbeschwert nach vorn blicken, nicht mehr ausprobieren, sich nicht mehr spontan anders entscheiden. Seit dem Feudalismus war diese ureigene Freiheit des Menschen, selbstbestimmt zu agieren, nicht mehr so gefährdet wie heute. Der Wille, immer genauere Vorhersagen zu treffen, immer effizienter zu sein, immer mehr planen zu können, führt dazu, dass immer mehr Daten gesammelt werden.

So entsteht Schritt für Schritt eine totale Überwachung aller Lebensbereiche.

Um das zu verhindern, braucht es neue Gesetze. So wie einst die Meinungs- und Pressefreiheit in Verfassungen verankert wurde, muss nun festgeschrieben werden, dass wir unabhängig von Vorhersagen und Vergleichen sein müssen.

Es braucht Transparenz und Aufklärung. Jedem muss klar sein und klar werden können, was Wahrscheinlichkeiten sind, wie Profile entstehen, wie Algorithmen wirken und welche Aussagen damit über einen Menschen und sein Verhalten möglich sind.

Es braucht Kontrolle und Grenzen. Datenspeicherung lässt sich nicht mehr verhindern, wenn jedes Gerät Daten sammelt. Das Verknüpfen von Daten, das Bilden von Profilen aber kann kontrolliert werden.

Es braucht mehr Macht für den Einzelnen, und weniger Macht für die Staaten und Konzerne. Recht und Technik müssen jedem Nutzer die Möglichkeit geben, zu erkennen, was andere über ihn erfahren können und selbst zu bestimmen, ob sie das auch erfahren sollen. Ohne solche Regeln wird es bald keine Freiheit mehr geben, sondern nur noch Sklaven der Statistik.

Dieser Beitrag erschien zuerst am 2. Juli 2014 als Vortrag auf der Tagung „Algorithmen Allmächtig?" in Erfurt sowie auf Kai Biermanns Blog www.tagebau.com.

Anmerkungen

[1] http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[2] http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list

[3] http://www.heise.de/newsticker/meldung/Rheinischer-Minority-Report-Polizei-NRW-will-mit-Predictive-Policing-Einbrueche-aufklaeren-2243936.html

Kai Biermann hat Psychologie studiert und unter anderem für die „Brigitte", die „Berliner Zeitung", „Das Magazin" und die „taz" geschrieben. Seit Mai 2007 ist Biermann bei ZEIT ONLINE, anfangs als Hauptstadtkorrespondent, später für die Themen Internet, Datenschutz und Netzpolitik. Seit Anfang 2014 ist er Mitglied des Teams Investigativ/Daten.

5 Metadaten: Wie dein unschuldiges Smartphone fast dein ganzes Leben an den Geheimdienst übermittelt

von **Dimitri Tokmetzis**

Geheimdienste sammeln Metadaten über die Kommunikation aller Bürger. Die Politiker wollen uns glauben machen, dass diese Daten nicht allzu viel aussagen. Ein Niederländer hat das überprüft und das Gegenteil demonstriert: Metadaten verraten viel mehr über dein Leben, als du denkst.

Ton Siedsma ist nervös. Er traf die Entscheidung vor Wochen, aber verschiebt sie doch immer weiter. Es ist der 11. November, ein kalter Herbstabend. Um zehn nach acht (20:10:48 Uhr um genau zu sein), während er auf dem Weg nach Hause den Elst-Bahnhof passiert, aktiviert er die App. Sie wird alle Metadaten seines Telefons in der kommenden Woche speichern. Metadaten sind nicht der tatsächliche Inhalt der Kommunikation, sondern die Daten über die Kommunikation; etwa die Nummern, die er anruft oder antextet, und wo sein Handy sich zu einem bestimmten Zeitpunkt befindet. Wem er E-Mails schreibt, die Betreffzeilen der E-Mails und die Webseiten, die er besucht.

Ton wird nichts Außergewöhnliches tun. Er wird einfach sein normales Leben führen. An Wochentagen bedeutet das, Radfahren von seinem Haus in Nijmegen zum Bahnhof und mit dem Zug nach Amsterdam. Am Samstag wird er sein Auto nach Den Bosch fahren und die Nacht in der Nähe von Zuiderpark verbringen, um am nächsten Tag mit den öffentlichen Verkehrsmitteln wieder nach Nijmegen zurückzufahren. Im Verlauf des Tages wird er in einem Café namens St. Anna etwas trinken gehen.

Nach genau einer Woche, am Montag, den 18. November, beendet er das Experiment und wird danach erzählen, dass er sich dabei befreit fühlte. Es gibt eine einfache Erklärung für seine Nervosität: Was er tun wird, wo er sich aufhalten wird und mit wem er in Kontakt ist, werden Zehntausende von Menschen sehen. Heute, du und ich, und alle anderen Leserinnen und Leser dieses Artikels.

In den vergangenen Monaten ist klar geworden, dass Geheimdienste, angeführt von der National Security Agency (NSA), enorme Mengen an Metadaten sammeln. Dazu gehört die Speicherung von E-Mail-Verkehrsdaten und den Standortdaten von Handys. Von Anfang an haben Politiker und Geheimdienste diese Überwachung dadurch verteidigt, dass der Inhalt der Kommunikation nicht überwacht wird, und dabei betont, dass die Dienste nur an Metadaten interes-

siert sind. Laut Präsident Obama, der NSA sowie dem niederländischen Innenminister Ronald Plasterk und dem niederländischen Geheimdienst „Allgemeiner Auskunfts- und Sicherheitsdienst“ (AIVD) richtet das kaum Schaden an. Erst vor kurzem beschrieb AIVD das Abhören von Metadaten auf seiner Webseite als „geringfügige Verletzung der Privatsphäre“.

Aber ist das der Fall? Sicher nicht, wie Ton Siedsmas Experiment zeigt. Metadaten – auch deine Metadaten – verraten mehr, als du denkst, und viel mehr, als die Behörden dich glauben machen wollen.

Eine Woche sagt genug

Ich übergab Tons Metadaten dem iMinds Forschungsteam der Universität Gent und Mike Moolenaar, Inhaber von „Risk and Security Experts“. Ich machte auch meine eigene Analyse. Aus den Metadaten einer Woche konnten wir 15.000 Datensätze mit einem Zeitstempel versehen. Jedes Mal, wenn Tons Telefon eine Verbindung mit einem Funkturm herstellte und jedes Mal, wenn er eine E-Mail schrieb oder eine Website besuchte, konnten wir sehen, wann dies geschah und wo er in diesem Moment war, bis auf wenige Meter genau. Wir waren in der Lage, basierend auf seinem Telefon- und E-Mail-Verkehr sein soziales Netzwerk zu erkennen. Über seine Browser-Daten konnten wir auch die Websites, die er besuchte, und seine Suchanfragen sehen. Und wir konnten das Thema, den Absender und Empfänger jeder seiner E-Mails sehen.

Also, was haben wir über Ton herausgefunden?

Folgendes konnten wir aus nur einer Woche an Metadaten über Ton Siedsmas Leben herausfinden: Ton ist ein Jungakademiker in seinen frühen Zwanzigern. Er empfängt E-Mails über Studentenwohnungen und Teilzeitstellen, das kann aus den Betreffzeilen und den Versenderdaten abgeleitet werden. Er arbeitet viel, zum Teil weil er weit mit dem Zug pendeln muss. Er kommt meist erst nach acht Uhr abends nach Hause. Dort angekommen, arbeitet er oft bis spät am Abend weiter.

Seine Freundin heißt Merel. Man kann nicht sicher sagen, ob die beiden zusammenwohnen. Sie schicken sich gegenseitig im Durchschnitt hundert WhatsApp-Nachrichten pro Tag, vor allem, wenn Ton nicht zu Hause ist. Bevor er in den Zug am Amsterdamer Hauptbahnhof steigt, ruft Merel ihn an. Ton hat eine Schwester, die Annemieke heißt. Sie ist noch Studentin: In einer ihrer E-Mails geht es, laut der Betreffzeile, um ihre Abschlussarbeit. Er hat dieses Jahr Sinterklaas (Nikolaus) gefeiert und loste die Vergabe der Geschenke aus. Ton liest gerne Sportnachrichten auf nu.nl, nrc.nl und vk.nl. Sein Hauptinteresse ist Radfahren, er fährt auch selbst gerne Rad. Er liest auch skandinavische Krimis, oder zumindest sucht er bei Google und Yahoo danach. Seine weiteren Interessen sind Philosophie und Religion.

Wir vermuten, dass Ton Christ ist. Er sucht nach Informationen über die Religionsexpertin Karen Armstrong, das Thomas-Evangelium, das „Messias-Buch des

Mittelalters“ und Symbolik in Kirchen und Kathedralen. Er bezieht eine Menge Informationen aus der Wikipedia.

Ton hat auch eine weniger tiefgründige Seite. Er schaut YouTube-Videos wie „Jerry Seinfeld: Sweatpants“ und Rick Astleys „Never Gonna Give You Up“. Er schaut auch ein Video von Roy Donders, einem niederländischen Reality-TV-Star. Im Internet liest er über „Katzen in Strumpfhosen“, „Disney-Prinzessinnen mit Bärten“ und „Gitarren durch Hunde ersetzt“. Er sucht auch nach einem „Snuggie“, dabei sticht ihm besonders eine gewisse „Batman Decke mit Ärmeln“ ins Auge. Oh, und er sucht intensiv nach einem guten Headset (wenn möglich mit Bluetooth).

Wenn wir Tons Profil aus einer kommerziellen Perspektive betrachteten, würden wir ihn mit Online-Angeboten bombardieren. Er ist für eine große Anzahl von Newslettern von Unternehmen wie Groupon, WE Fashion und verschiedenen Computergeschäften angemeldet. Er betreibt scheinbar eine Menge Online-Shopping und sieht keine Notwendigkeit, sich von den Newslettern abzumelden. Das könnte ein Hinweis dafür sein, dass er Online-Angeboten gegenüber offen ist.

Er hält seine E-Mail-Kommunikation recht gut getrennt, mit drei verschiedenen E-Mail-Konten. Er empfängt alle Werbeangebote auf seinem Hotmail-Konto, über das er auch mit einer Reihe von Bekannten kommuniziert, obwohl er darüber kaum Nachrichten selbst sendet. Er hat ein zweites persönliches E-Mail-Konto, das er für Arbeit und Korrespondenz mit engeren Freunden verwendet. Er verwendet dieses Konto wesentlich aktiver. Außerdem hat er noch ein weiteres E-Mail-Konto für die Arbeit.

Ton weiß eine Menge über Technologie. Er ist an IT, Informationssicherheit, Datenschutz und Freiheit im Internet interessiert. Er sendet regelmäßig Nachrichten mit der Verschlüsselungssoftware PGP. Er sucht auch nach Datenbank-Software (SQLite). Er ist regelmäßig auf Tech-Foren und sucht Informationen über Datenerfassung und -verarbeitung. Er bleibt auch bei Nachrichten über Hacking und aufgeflogene Kinderpornoringe auf dem Laufenden.

Wir vermuten auch, dass er mit der niederländischen „Grün-Linken“ Partei sympathisiert. Durch seine Arbeit (dazu später mehr) ist er in regelmäßigem Kontakt mit politischen Parteien. Die Grüne Linke ist die einzige Partei, von der er E-Mails über sein Hotmail-Konto empfängt. Er hat dieses Konto schon länger als sein Arbeitskonto. Ein Tag im Leben des Ton Siedsma: Dienstag 12. November 2013. An diesem Tag nimmt er einen anderen Weg nach Hause, von Amsterdam nach Nijmegen, als seine übliche Route über Utrecht. Er erhält einen Anruf von Hilversum und geht auf seinem Heimweg am Mediapark vorbei.

Was arbeitet Ton?

Basierend auf den Daten ist es ziemlich klar, dass Ton als Anwalt für die digitale Bürgerrechtsorganisation Bits of Freedom arbeitet. Er beschäftigt sich hauptsäch-

lich mit internationalen Handelsabkommen und hält mit dem Außenministerium und ein paar Mitgliedern des Parlaments zu diesem Thema Kontakt. Er verfolgt die Entscheidungsprozesse der Europäischen Union sehr genau. Er interessiert sich auch für die Ermittlungsmethoden von Polizei und Geheimdiensten. Das erklärt auch sein Interesse an Nachrichten über Hacking und enttarnte Kinderpornoringe.

Während der analysierten Woche nimmt Ton aktiv an einer E-Mail-Diskussion mit Kollegen über das Thema „Van Delden muss gehen" teil. Die E-Mails beziehen sich auf Bert van Delden, den Vorsitzenden des „Intelligence and Security Services Review Committee" (CTIVD), das ist das Kontrollgremium für die Geheimdienste AIVD [Inlands- sowie Auslandsgeheimdienst, Anm. d. Red.] und MIVD, dem Militärgeheimdienst. Ot van Daalen, ein Kollege, hat während der Woche daran gearbeitet, eine Strategie für den „Freedom Act" zu entwerfen, was offenbar ein Projekt von Bits of Freedom ist.

Am Donnerstag sendet Ton eine Nachricht an alle Mitarbeiter mit dem Titel „Wir sind durch!". Es gibt offenbar einen Grund zur Erleichterung. Ton guckt sich auch eine wissenschaftliche Arbeit über unsichtbare SMS an und er beschließt, dass er zu einer Podiumsdiskussion der Jungen Demokraten gehen wird. Eine Reihe von Nachrichten drehen sich um die Planung einer Leistungsüberprüfung, die wahrscheinlich von Hans, dem Direktor von Bits of Freedom, durchgeführt wird.

Ton aktualisiert ein paar Dateien für sich selbst auf einem geschützten Teil der Website von Bits of Freedom. Wir können die Namen der Dateien in den URLs erkennen. Sie beschäftigen sich mit internationalen Handelsabkommen, dem niederländischen Parlament, WCIII (Computerkriminalitätsgesetz III) und Gesetzgebung. Ton aktualisiert auch die Website. Es ist einfach für uns, zu sehen, welche Blog-Artikel er überarbeitet.

In seiner Freizeit macht Ton anscheinend nicht allzu viel. Er sendet und empfängt weiter bis spät am Abend Arbeits-E-Mails. Ton besucht auch eine Menge Nachrichten-Seiten und textet mit uns unbekannten Personen. Normalerweise geht er um Mitternacht ins Bett.

Mit wem interagiert Ton?

Ton Siedsmas soziales Netzwerk – basierend auf seinem E-Mail-Verhalten – zeigt verschiedene Cluster. Durch eine soziale Netzwerkanalyse von Tons E-Mail-Verkehr ist es uns möglich, verschiedene Gruppen, denen er angehört, zu unterscheiden. Diese Cluster werden von seinen drei E-Mail-Konten strukturiert. Es kann sein, dass die Gruppen ein wenig anders aussähen, wenn wir zusätzlich die Metadaten seines Telefons verwenden würden. Allerdings haben wir vereinbart, keine zusätzliche Untersuchungen durchzuführen, bei denen wir aktiv versuchen, die Identität von Benutzern einer bestimmten Telefonnummer aufzudecken, damit die Privatsphäre der Menschen in Tons Netzwerk geschützt bleibt.

Über sein Hotmail-Konto kommuniziert Ton mit Freunden und Bekannten. Thomas, Thijs und Jaap steuern, innerhalb einer größeren Gruppe von Freunden, am meisten bei. Beurteilt anhand der E-Mail-Adressen, besteht diese Gruppe nur aus Männern. Es gibt auch Kommunikation mit einer separaten Gruppe, die von jemandem namens Bert geleitet wird. Der Hintergrund dieser Gruppe ist das einzige, was von Ton zensiert wurde. Er sagt, das sei einfach eine persönliche Angelegenheit.

Wir können eine weitere, kleinere Gruppe von Freunden, nämlich Ton, Huru, Tvanel und Henry ausmachen. Wir denken, dass sie Freunde sind, weil sie sich alle an der E-Mail-Diskussion beteiligen, d. h. sie kennen einander. Außerdem sendet eine Reihe von ihnen auch E-Mails an ton@sieds.com, Tons Adresse für Freunde und Familie.

Schließlich gibt es auch Tons Arbeits-Cluster. Hier sehen wir, dass seine Hauptkontakte Rejo, Hans und Tim sind. Tim und Janneke sind die Einzigen, die auch in seiner persönlichen E-Mail-Korrespondenz auftauchen. Die Anzahl der E-Mails, die zwischen ihm und seinen sechs Kollegen verschickt werden, ist auffallend groß. Es gibt offenbar einen Hang zum „CC-Setzen" in E-Mails bei Bits of Freedom. Es ist selten, dass Ton eine E-Mail an nur einen Kollegen sendet, aber wenn, dann ist es meistens entweder Rejo oder Tim. Viele E-Mails werden an die Gruppenadresse für alle Mitarbeiter gesendet.

Ton hat relativ wenig Kontakt mit Externen. Während der Woche tauschte er nötige E-Mails zur Terminvereinbarung mit dem Assistenten von Foort van Oosten, einem Abgeordneten der Volkspartei für Freiheit und Demokratie (VVD), und mit einem Journalisten namens Bart aus. Er kommuniziert auch viel mit Anbietern von Anti-Viren-Software. Auf Basis der Metadaten folgert Sicherheitsexperte Mike Moolenaar, dass Ton „eine gute Informationsposition innerhalb von Bits of Freedom inne hat." Er scheint eine gute Übersicht zu haben über alles, was passiert – eine wichtige Tatsache, wenn man dieses Netzwerk aus geheimdienstlicher Perspektive betrachtet.

Aber das ist noch nicht alles. Die Analysten von iMinds aus Belgien verglichen Tons Daten mit einer Datei geleakter Passwörter. Anfang November gab Adobe (das Unternehmen hinter dem Acrobat PDF-Reader, Photoshop und dem Flash Player) bekannt, dass eine Datei mit 150 Millionen Benutzernamen und Passwörtern gehackt wurde. Die Passwörter waren verschlüsselt, die Passwort-Vergessen-Hinweise jedoch nicht. Die Analysten konnten sehen, dass einige Nutzer das gleiche Passwort wie Ton hatten, und ihre Passworthinweise waren „Punk-Metall", „Astrolux" und „Another Day in Paradise". „Das führte uns schnell zu Ton Siedsmas Lieblingsband, Strung Out, und dem Kennwort strungout", schreiben die Analysten.

Mit diesem Passwort waren sie in der Lage, auf Tons Twitter-, Google- und Amazon-Konten zuzugreifen. Die Analysten zeigten uns einen Screenshot der Di-

rektnachrichten auf Twitter, die normalerweise geschützt sind, was bedeutet, dass sie sehen konnten, mit wem Ton vertraulich kommunizierte. Sie zeigten uns auch ein paar Einstellungen seines Google-Kontos. Und sie konnten Produkte über Tons Amazon-Konto bestellen – was sie allerdings nicht getan haben. Die Analysten wollten nur zeigen, wie einfach es ist, schon mit wenigen Informationen auf hochsensible Daten zuzugreifen.

Was sie und ich für diesen Artikel getan haben, ist Kinderkram im Vergleich zu dem, was Geheimdienste tun könnten. Wir konzentrierten uns vor allem auf die Metadaten, die wir mit gängiger Software analysierten. Wir verzichteten auf zusätzliche Recherchen, mit Ausnahme des geleakten Datensatzes von Adobe.

Außerdem war dieses Experiment auf eine Woche beschränkt. Einem Geheimdienst stehen Metadaten über viel mehr Menschen, über einen viel längeren Zeitraum und dazu viel ausgefeiltere Analyse-Tools zur Verfügung. Internetanbieter und Telekommunikationsunternehmen sind in den Niederlanden gesetzlich verpflichtet, Metadaten für mindestens sechs Monate zu speichern. Polizei und Geheimdienste haben keine Schwierigkeiten, diese Art von Daten anzufordern und zu erhalten.

Also das nächste Mal, wenn du einen Minister, Sicherheitsexperten oder Informationsbeauftragten sagen hörst: „Oh, aber das sind nur Metadaten," denke an Ton Siedsma – den Typen, über den du so viel weißt, weil er nur eine Woche an Metadaten mit uns geteilt hat.

Dieser Beitrag erschien zuerst auf decorrespondent.nl.

Dimitri Tokmetzis ist ein niederländischer Journalist, der sich speziell mit Daten beschäftigt, die man durch Informationsfreiheitsgesetze erhalten kann. Seine Schwerpunktthemen sind Datenschutz, Geldströme und die Analyse sozialer Netzwerke.

6 Die NSA-Station im 22. Wiener Gemeindebezirk

von **Erich Moechel**

Wie eine Fotoserie zeigt, befindet sich der in den Snowden-Dokumenten erwähnte „Vienna Annex“ in den Dachgeschoßen des IZD-Towers neben der UNO-City.

Auch wenn die Nachrichtenlage seit Beginn der NSA-Enthüllungen in Bezug auf Österreich noch immer dürftig ist, lassen sich nun drei der bisherigen vier Erwähnungen Österreichs zweifelsfrei zuordnen. Der in einem Dokument erwähnte „Vienna Annex“ zur NSA-Station in der US-Botschaft befindet sich in den obersten drei Geschoßen des IZD-Towers im 22. Wiener Gemeindebezirk. Das geht aus einer aktuellen Fotoserie, die ORF.at zugespielt wurde, klar hervor.

Seit der Fertigstellung des Towers Ende 2001 residiert dort die US-Vertretung bei den Vereinten Nationen. Auf dem Dach befindet sich in einer Höhe von etwa 130 Metern derselbe Aufbau wie auf dem Dach der US-Botschaft im 9. Wiener Gemeindebezirk. In beiden Fällen hat das als „Wartungsaufbau“ getarnte Häuschen eine Grundfläche von etwa 15 Quadratmetern. Vom Boden aus ist es praktisch nicht zu erkennen, da es etwas versetzt hinter dem charakteristischen Vorsprung der obersten Geschoße des IZD-Towers steht. Das Häuschen ist direkt auf die Gebäude der UNO-City ausgerichtet.

Abbildung 3: Nomen Nescio / CC BY-SA 2.0 AT

Dieser Bereich ist durch massive Stahlgitter vom Rest des Dachs abgetrennt und wird durch etwa zehn Kameras lückenlos überwacht. Er ist nur über eine stählerne Treppe zu erreichen, die sich im Vorsprung befindet. In der „Bau- und Ausstat-

tungsbeschreibung“ des IZD-Towers sind zwar zwei Materiallifte erwähnt, die bis zum Dachgeschoß reichen sollen, auf den Fotos ist jedoch deutlich zu sehen, dass keiner der Lifte auf diese abgetrennte Dachhälfte führt.

Abbildung 4: Die kleine Schüssel rechts im Bild ist eine gewöhnliche Sat-TV-Schüssel. Sogar daraus lässt sich eine Schlussfolgerung ziehen, nämlich dass die gesamte Annex-Station nicht an das UPC-Kabel-TV angeschlossen ist, das im IZD-Tower zur Verfügung steht – Nomen Nescio / CC BY-SA 2.0 AT

Diese Beschreibung, die längst von der Website des IZD-Towers verschwunden, aber in Archiven wie der „Waybackmachine“ noch aufzufinden ist, enthält auch Hinweise auf die Anbindung des Towers. Die vertikale Verkabelung sei mit Lichtwellenleitern erfolgt, heißt es in der Beschreibung, die mit Juli 2002 datiert ist. Der ab 1998 errichtete IZD-Tower war also von Anbeginn mit Glasfaser bis knapp unter das Dach verkabelt.

Abbildung 5: Nomen Nescio / CC BY-SA 2.0 AT

Was sonst auf dem Dach ist

Das Häuschen auf dem Dach verfügt über eine Klimaanlage, an den Schmalseiten links und rechts sind Zufuhr und Abluft zu sehen. Gegen Starkwinde ist das

Häuschen nur in eine Richtung abgeschirmt, anonsten ist es in dieser exponierten Lage Wind und Wetter ausgesetzt und praktisch überhaupt nicht gegen Sonneneinstrahlung abgeschattet. Daher muss es relativ solide gebaut und natürlich auch klimatisiert sein. Denn klar ist, dass sich darunter kleindimensionierte Antennen und die dazugehörige Elektronik verbirgt (mehr dazu weiter unten).

Es ist noch eine weitere Antenne im von der US-Vertretung kontrollierten Dachbereich. Bei dem Gebilde über dem Aufbau mit der Klimaanlage handelt es sich um eine Antenne, die einerseits zwar annähernd Rundstrahlcharakteristik hat, aber einen wesentlich höheren Verstärkungsgrad als herkömmliche Rundstrahler aufweist.

Abbildung 6: Der Rundstrahler ist im Bild links oben, baugleiche Antennen sind auch auf den Dächern anderer US-Vertretungen zu finden. Ganz rechts steht ein Mobilfunkmast – Nomen Nescio / CC BY-SA 2.0 AT

Rundum strahlende Richtantenne

Die vier übereinander gestockten vertikalen Schleifendipole sind für sich jeweils Richtantennen, die aber gegeneinander so versetzt sind, dass sich die vier Abstrahlbereiche so ergänzen, dass sie in alle Richtungen gleich gut funktionieren. Mit hoher Sicherheit dient diese Antenne nicht Abhörzwecken, sondern der eigenen verschlüsselten Kommunikation mit mobilen Geräten.

Der Frequenzbereich irgendwo bei 400 MHz ist gerade für den Einsatz in urbanen Räumen sehr gut geeignet, denn die Funkwellen in diesem Bereich dringen zum einen noch ausreichend tief in Gebäude ein. Zum anderen werden die Wellen vor allem der am Boden operierenden Mobilgeräte an glatten Hausfassaden reflektiert, gerade verspiegelte Stahlbetongebäude sind nachgerade ideale Reflektoren.

Vom Boden erreicht man damit den Rundumverteiler auf dem Tower, auch wenn kein direkter Sichtkontakt besteht.

Wohin Sichtverbindung besteht

Diese Antenne dient klarerweise der Kommunikation von Fahrzeugen, Personenschützern und anderem, der Botschaft zugeordnetem Personal im Großraum Wien. Vom Dach des IZD-Towers wiederum ist in etwa freie Sicht sowohl auf die US-Botschaft in Wien 1090 gegeben, in Richtung der sogenannten „NSA-Villa" in Pötzleinsdorf (18. Bezirk) ist die Funklage nachgerade ideal. Von ihrer jeweiligen Lage her bestehen zwischen diesen drei „Points of Presence" also sehr gute Funkverhältnisse.

Abbildung 7: Dieses Diagramm stammt aus einem Programm zur Antennensimulation unter Einbeziehung der topografischen Gegebenheiten. Der Standort ist die „NSA-Villa" in Wien, Pötzleinsdorfer Straße 126, der grüne Bereich zeigt an, welche Bereiche Wiens von den Antennen dort abgedeckt werden können – Radio Flux

Die „NSA-Villa" in Pötzleinsdorf

Im Antennenwald auf dem Dach der „NSA-Villa" wiederum finden sich fast nur Yagi-Richtantennen für etwa eben diesen Frequenzbereich. Auch bei diesen Antennenformen lassen sich nämlich schon aus der Länge der einzelnen Antennenelemente Rückschlüsse auf die Frequenzen ziehen. Eine Anzahl davon ist auf verschiedene Standorte im Stadtgebiet darunter gerichtet, doch auch hier wird mit ziemlicher Sicherheit nichts abgehört. Vielmehr dürften hier Außenstellen der US-Botschaft angebunden sein sowie Bereiche ausgeleuchtet werden, die vom Rundstrahler auf dem IZD-Tower nicht erreicht werden können.

Hauptfunktion der „NSA-Villa" muss also die einer Relaisstation für die interne Kommunikation der über die Stadt verstreuten Außenstellen sein. Was darüber hinaus dafür spricht, dass es sich in erster Linie um einen Verteiler handelt, sind zwei mittelgroße Parabolspiegel, die am Rande dieses Geländes in 1180 Wien zu sehen sind.

Abbildung 8: Auf diesem Bild ist nur ein Teil des Antennenwalds auf dem Dach der „NSA-Villa“ zu sehen – APA

Auch hier wird mit ziemlicher Sicherheit nichts abgehört, denn ein, zwei derartige Spiegel gehören wie ehedem Kurzwellensendeanlagen zur Grundausstattung jeder diplomatischen Vertretung und nicht nur von solchen der USA. Darüber lassen sich Direktverbindungen in das eigene Land schalten, ohne dass man dabei auf Netzwerke im Gastland angewiesen ist. Da sich weder auf der Botschaft noch dem IZD-Tower derartige Schüsseln finden, spricht auch das für die primäre Funktion der „NSA-Villa“ als Relaisstation.

Was in den „Wartungshäuschen“ sein dürfte

Die eigentlich interessanten Antennen sind dort hinter Scheinfassaden verborgen, die aus einem ähnlichen strahlungsdurchlässigen Material – wahrscheinlich Glasfasermatten – bestehen, wie die Wände der „Wartungshäuschen“. Was sich hinter allen verbirgt sind kleindimensionierte Antennen, nach übereinstimmender Ansicht einer ganzen Reihe von Fachleuten muss es sich dabei an allen drei Standorten in erster Linie um passives Equipment zur Überwachung der Mobilfunknetze handeln.

Sogenannte IMSI-Catcher greifen in den Mobilfunk ein, indem sie durch Aussendung von Signalen eine legitime Mobilfunkstation für ihre Umgebung simulieren und alle Handys in der näheren Umgebung auf sich ziehen. Als permanente Anlage zur Überwachung sind IMSI-Catcher schon deshalb weniger geeignet, weil sie zwar nicht ganz einfach, aber mit geeigneten Messgeräten dennoch zu entdecken sind.

Was noch gegen „IMSI-Catcher“ spricht

Ein Dauereinsatz solcher Geräte würde in den betroffenen Funkzellen unweigerlich zu einer überdurchschnittlichen Rate von Gesprächsabbrüchen führen. Bei einem hohen Aufkommen von Telefonaten in der Umgebung wird ein solches,

eher klein dimensioniertes Überwachungsgerät nämlich überlastet und kann einzelne Gespräche nicht mehr vermitteln. Genau derselbe Effekt tritt bei ganz normalen Mobilfunkstationen auf, die durch zuviele Telefonate auf einmal überlastet werden.

Deshalb werden alle Mobilfunkstationen von den Netzbetreibern auf Abbrüche überwacht und zwar nicht um nach illegalen Aktivitäten dort zu fahnden, sondern um zu erfahren, welche der Basisstationen aufgerüstet werden müssen. Passive Überwachung bietet zwar weniger „Features" für die Überwachung als der Einsatz von IMSI-Catchern, ist aber nicht zu entdecken, da eben nichts gesendet, sondern nur empfangen wird.

GSM in den Bereichen 900 und 1.800 MHz ist seit Jahren bereits mit einfachen Mitteln passiv abzuhören, denn die Verschlüsselung der Gespräche lässt sich nur wenig zeitversetzt mit relativ geringem Aufwand knacken. Bei Mobiltelefonie im Bereich 2.600 MHz (UMTS) ist diese in den 90er Jahren absichtlich gesetzte Lücke in den GSM-Protokollen zwar geschlossen. Es ist aber davon auszugehen, dass wenigstens die NSA und andere führende Geheimdienste Wege gefunden haben, auch diese Protokolle zu knacken.

Abbildung 9: Auf der Anzeige im Erdgeschoß des IZD-Towers taucht die US-Vertretung in den obersten Stockwerken gar nicht auf – Nomen Nescio / CC BY-SA 2.0 AT

Daten-Exfiltration aus der UNO-City

Anders als bei den anderen beiden Standorten gibt es vom Dach des IZD-Towers noch eine Möglichkeit, die diesen Standort einzigartig macht. Aufgrund der räumlichen Nähe zu den Gebäuden der Vereinten Nationen – sie sind gerade einmal um die 100 Meter Luftlinie entfernt – ist der Dachbereich des Towers ein nachgerade idealer Ort, um Daten aus der UNO-City zu „exfiltrieren". Dieser Begriff bezeichnet den verdeckten Abtransport abgefangener Daten an den Ort ihrer Verarbeitung. In diesem Fall können es zum Beispiel Audio- und Videodaten aus verwanzten Räumlichkeiten in der UNO-City sein.

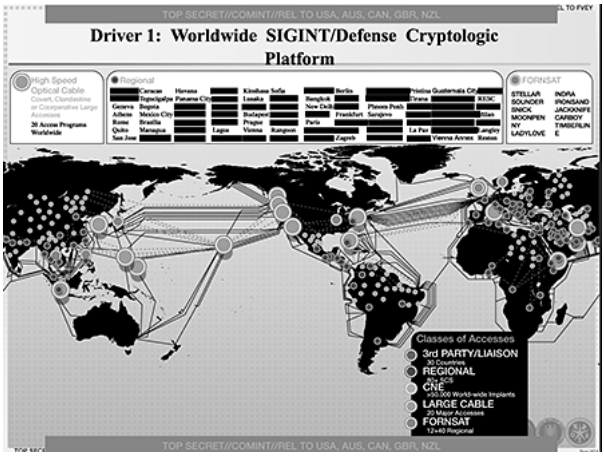

Abbildung 10: Im Kopf dieser NSA-Folie werden die „Vienna Station" und der „Vienna Annex" explizit angeführt. Eines der Akronyme, die rechts unter „FORNSAT" gelistet sind, muss für die Königswarte stehen. Unter „FORNSAT" sind Sat-Spionagestationen zu verstehen, die nicht von der NSA selbst betrieben werden.

Im Zuge dieser Recherche kam auch zutage, dass es vor allem in den oberen Stockwerken des IZD-Towers, aber auch in der Umgebung zu regelmäßigen und teils massiven, breitbandigen Funkstörungen gekommen ist, sodass Mobilfunknetze oft über Stunden nicht erreichbar waren. Die Herkunft der Störungen ist zwar nicht bekannt, rein technisch ist es aber weniger wahrscheinlich, dass sie aus den obersten Stockwerken des Turmes kamen, denn die sind durch die Stahlbetondecken nach unten gegen Strahlung isoliert. Wahrscheinlicher ist, dass diese Störsignale von außen kamen und eben nicht von der US-Seite stammen dürften.

Die Geplänkel der Dienste

Was hier nämlich für eine breitere Öffentlichkeit in Ansätzen aufgearbeitet wurde, ist den Geheimdiensten von Drittstaaten wie Russland oder China längst und auch in technischen Details bekannt. Nach dem Muster der laufenden, gegenseitigen Hackangriffe durch staatliche Stellen im Internet wird auch das Funkspektrum weltweit regelmäßig für technische Geplänkel zwischen nicht-befreundeten Geheimdiensten missbraucht.

Die US-Vertretung bei der UNO verfügt so zwar über einen hervorragenden Funkstandort, der allerdings auch einen Nachteil mit sich bringt. Ebenso einzigartig wie seine Lage ist auch die Exponiertheit dieses Standorts, der in den obersten Stockwerken des IZD-Towers wie auf dem Präsentierteller für Störangriffe von allen Seiten liegt.

Abbildung 11: Die Sat-Spionagestation Königswarte ist der Grund, warum Österreich als „approved SIGINT"-Partner der NSA gelistet ist.

Offene Fragen

Drei der Erwähnungen Österreichs in den bisher veröffentlichten Dokumenten können zwar nun zugeordnet werden. Die vierte bleibt jedoch weiterhin offen und kann beim derzeitigen Stand der Informationen nicht beantwortet werden. Die laut dem NSA-Veteranen und Whistleblower Bill Binney mithin wichtigste Information auf der oben abgebildeten Folie mit dem Titel „Worldwide SIGINT/Defense Cryptogic Platform" ist im schwarzen Kästchen unten rechts zu finden.

Unter „CNE" ist da vermerkt, dass der NSA „weltweit 50.000+ Implants" zur Verfügung stehen. CNE steht für „Computer Network Exploitation" und „Implants" sind verdeckte Zugriffsmöglichkeiten der NSA auf die zentralen Router großer Netzwerkbetreiber. Sowohl der Hack der Router bei der Belgacom wie auch die erst in der vergangenen Woche bekannt gewordenen Enthüllungen des Spiegel über die Infiltration der Router deutscher Sat-Internetanbieter durch das GCHQ fallen in diese Kategorie.

In direktem Zusammenhang damit steht nämlich die vierte Erwähnung Österreichs in den geleakten Dokumenten als sogenannter „Tier B"-Partner der NSA. Laut einem der weltweit besten Kenner der Materie, dem Echelon-Aufdecker Duncan Campbell, bezieht sich der Status Österreichs als „Tier-B"-Partner weder auf die Königswarte noch auf die „Wartungshäuschen" auf den Dächern, sondern ausschließlich auf „Computer Network Operations".

Die Annahme liegt also nahe, dass es im Heeresnachrichtenamt Personen geben könnte, die mehr darüber wissen als etwa die Techniker der A1-Telekom, die ihr Netz seit einem Jahr auf solche „Implants“ durchsucht haben, was bis jetzt wenigstens offiziell ohne Ergebnis geblieben ist.

Dieser Beitrag erschien zuerst am 22. September 2014 auf fm4.orf.at, Veröffentlichung mit freundlicher Genehmigung von ORF.at

Anmerkungen

[1] http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[2] http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list

[3] http://www.heise.de/newsticker/meldung/Rheinischer-Minority-Report-Polizei-NRW-will-mit-Predictive-Policing-Einbrueche-aufklaeren-2243936.html

Erich Moechel ist ehemaliger Redakteur der Futurezone, der früheren IT-News Website des ORF, und schreibt derzeit für fm4. Aufsehen erregten seine Recherchen zu den Enfopol-Papieren, die zu weiteren Berichten über die europäischen Normierungsanstrengungen in Sachen Telekommunikationsüberwachung führten. Er ist Mitglied im Board of Advisors von Privacy International und Mitbegründer der Big Brother Awards in Österreich sowie der Quintessenz.

7 Warum protestiert eigentlich niemand?

von **Anne Roth**

Beim Jahresrückblick des Chaos Computer Clubs (CCC) während des 30C3-Kongresses Ende Dezember in Hamburg berichtete Constanze Kurz: „Es gibt eigentlich kein Interview, was wir seit diesen Monaten geführt haben, das nicht auch die Frage enthält: 'Wie erklären Sie sich denn, dass sich niemand empört?'. Und nach dem Wahlergebnis: 'Wie erklären Sie sich denn dieses hohe Wahlergebnis für Merkel?'"

Constanze Kurz gehört zum Presseteam des CCC. Die Frage, die sie wieder und wieder beantworten soll, lautet, warum es keine größeren Proteste gegen die Durchleuchtung aller Kommunikation durch die Geheimdienste gebe, die die Leaks von Edward Snowden seit Juni vergangenen Jahres ans Licht bringen würden.

Es hat wenig Protest gegeben, das stimmt. Was nicht stimmt, ist, dass sich die meisten nichts daraus machen, dass die Regierungen, die sich gern selbst als gutes Beispiel für Demokratie und Rechtsstaatlichkeit präsentieren, offensichtlich lügen. Und zwar nicht nur andere Regierungen belügen, sondern die jeweils eigene Bevölkerung.

Genauso wenig stimmt, das sich die meisten nichts daraus machen, dass ihre vermeintlich private Kommunikation gerastert und gespeichert wird. Ich habe jahrelang wie Don Quijote gegen die Windmühlen gekämpft bei dem Versuch, Menschen dazu zu bewegen, kein Googlemail zu benutzen oder ihre Mails sogar zu verschlüsseln.

Textbausteine, die ich im Schlaf aufsagen konnte, sind plötzlich überflüssig geworden. Stattdessen werde ich jetzt gefragt, welche Mailprovider denn sicher seien. Wenn ich wollte (und die Zeit hätte) würde ich den ganzen Tag nichts anderes machen, als zu erklären, was Metadaten sind oder was als Alternative zu Skype benutzt werden kann. Woher kommt also die Erzählung, niemand interessiere sich für das, was wir seit Juni wissen?

Irgendwann hat eine Gewöhnung eingesetzt an Artikel mit vielen Ausrufezeichen, die über neue Enthüllungen berichten. Eine Ausnahme war Merkels Handy, aber als im Oktober bekannt wurde, dass sogar! das! Handy! der! Kanzlerin! . . . , verschwammen die einzelnen Skandale schon zu einer trüben Brühe. Merkels Handy und die seltsamen Aufbauten auf den Botschaften am Brandenburger

Tor lösten Begeisterung und ein bisschen Gruseln in den Redaktionen und sonst Schadenfreude aus. Es hatte keinen Aufstand gegeben. Es gibt Gründe für den fehlenden Aufstand.

Grund Nummer eins

Ein Grund ist das Ohnmachtsgefühl, das viele angesichts des Ausmaßes an purer, von demokratischen Grundideen ungetrübter Herrschaftsausübung verspürten. Die Bundesregierung hatte dazu maßgeblich beigetragen, als sie deutlich machte, dass ihre Loyalität der US-Regierung und nicht der Bevölkerung in Deutschland galt.

Auf die Straße gehen, wenn ein Apparat aus mehreren Regierungen und unkontrollierten Geheimdiensten auf der anderen Seite steht? Wenn die Bundesregierung, nachdem von ihrer Souveränität nur noch Fetzen übrig sind, unterwürfig nach Washington reist und darum bittet, das Vertrauen wiederherstellen zu dürfen? Um das Gefühl auszulösen, dass dagegen etwas auszurichten sei, wäre eine große Bewegung nötig gewesen.

In Deutschland gab es eine Bewegung, die sich gegen ACTA, gegen die Vorratsdatenspeicherung und für viele andere Netzthemen eingesetzt hat, auch auf der Straße. Sie war nicht klein. Die „Freiheit-statt-Angst"-Demonstrationen in Berlin sind international legendär. Von der Bewegung war nichts zu sehen.

Irgendwann im Spätsommer, nach der Bundestagswahl, haben sich einige an der Idee versucht, die gesamte Netzpolitik sei tot. Das ist Quatsch. Politikbereiche lösen sich nicht eben in Luft auf, aber die Frage stand schon deutlich im Raum, warum der NSA/GCHQ/BND-Skandal die Wahl nicht so beeinflusst hat, wie es vier Jahre zuvor die Internetsperren und „Zensursula" getan hatten.

Grund Nummer zwei

Die Bewegung war zum denkbar unpassendsten Zeitpunkt in der Versenkung verschwunden. Eine Ursache ist, dass offenbar viele das Verfassen von Online-Petitionen und Offenen Briefen mit effektivem Protest verwechseln. Sie sind nicht falsch, und es schadet wahrscheinlich auch nicht, Forderungen durch entweder viele Klicks oder bekannte Namen Nachdruck zu verleihen.

Aber, wie mein Kollege Kaustubh Srikanth ebenfalls beim CCC-Kongress in Hamburg sagte: „Change doesn't happen unless a bunch of people go in the streets and protest" (Es gibt solange keine Veränderung, bis ein Haufen Leute auf die Straße geht und protestiert). Er sprach über Überwachung in Indien und darüber, wie sich „die größte Demokratie der Erde" ungestört in einen Überwachungsstaat verwandelt: u. a. weil es keine Bewegung und keinen Protest auf der Straße dagegen gibt. Es ist zu befürchten, dass sich die aktuelle deutsche Regierung davon ein paar Details abgucken wird.

Und so gibt es inzwischen eine endlose Zahl von Resolutionen, 10-, 12- oder 13-Punkte-Papieren, Offenen Briefen und Appellen, die Regierungen oder interna-

tionalen Institutionen empört überreicht wurden, zu denen Unterschriften gesammelt werden und die bei Facebook geteilt werden.

Grund Nummer drei

Schriftsteller_innen, Richter_innen, Wissenschaftler_innen: alle haben ihre Bedenken wohlbegründet vorgetragen. Gute Texte, wirklich. Aber es ist ein Riesenmissverständnis, zu erwarten, dass das allein irgendetwas ändert. Stattdessen steckt viel Arbeit und diplomatische Verhandlung in den Texten. Ein Teil dieser Energie hat anderswo gefehlt. Die Energie, die in politischer Motivation steckt, lässt sich nicht einfach von hier nach da verschieben, insofern lässt sich den Initiator_innen der Appelle nicht vorhalten, sie hätten besser was anderes gemacht. Aber sie müssen sich schon fragen lassen, welches Bedürfnis sie mit der zigsten Petition befriedigt haben.

Es kommt vor, dass sich Protest spontan entlädt, aber in der Regel ist für Proteste in einer Größenordnung, die von Medien und damit Regierungen als relevant anerkannt wird, eine Infrastruktur nötig, für die Menschen, Erfahrung, Bereitschaft, Zeit und Geld gebraucht werden. Die gab es, aber just im letzten Jahr hatten sich die Beteiligten der vorigen Jahre frühzeitig – vor den Snowden-Leaks – in Konkurrenzen und Privatfehden verstrickt. Und weil die Bedeutung der inzwischen traditionellen Demo nach dem Sommer bis zum Juni nicht absehbar war (auch kein Thema wie „Zensursula“ in Sicht), war das einst große Bündnis ziemlich ausgedünnt, als klar wurde, dass das Thema größer war als alle anderen (Netzthemen) vorher.

Grund Nummer vier

Manche waren mit sich oder anderen Themen beschäftigt, andere hatten eine Partei gegründet. Viele von denen, die vor Jahren „die Netzaktivist_innen“ waren, sind inzwischen bei den Piraten und rund um die Uhr mit Geschäftsordnungsanträgen, Listenparteitagen oder Flügelkämpfen beschäftigt. Dazu war Wahlkampf, und es sah nicht so gut aus für die Piraten. Sicher haben auch Piraten mobilisiert und waren an zahlreichen kleineren Protestaktionen beteiligt – aber eben mit orangenen Fahnen und Flugblättern, und wurden damit von Medien wie allen anderen vor allem als wahlkämpfend wahrgenommen. Spürbarer Teil der Netzpolitik-Bewegung, die sich für ein Thema engagiert, waren sie damit nicht mehr.

Und schließlich, nicht zu unterschätzen, die Fähigkeit von Angela Merkel, Themen schweigend auszusitzen, bis sich alle in das scheinbar Unvermeidbare fügen und sich mit dem Verhandeln von Sachzwängen und Nebensätzen beschäftigen.

Das Gute: es ist nicht zu spät. Wir haben schließlich nichts mehr zu verlieren.

Dieser Beitrag erschien zuerst am 15. Januar 2014 in der Bewegungskolumne des Neuen Deutschland.

Anne Roth ist Bloggerin, Netz- und Medienaktivistin, Politologin. Sie war Journalistin, Online-Redakteurin, Übersetzerin und als Researcher beim Tactical Technology Collective, wo sie das Projekt „Me and My Shadow“ betreute. Zur Zeit arbeitet Sie hauptberuflich als Referentin der Fraktion DIE LINKE im NSA-Untersuchungsausschuss im Bundestag. Sie spricht regelmäßig über die Themen Überwachung, Schutz der Privatsphäre und generell innenpolitische Aspekte der Netzpolitik.

8 Der NSA-Skandal und die globale Gegenwehr

von **Ben Hayes** und **Eric Töpfer**

Mehr als ein Jahr nach Beginn der von Edward Snowden angestoßenen Enthüllungen über die massenhafte Überwachung durch westliche Geheimdienste ist die Bilanz ernüchternd. Im Schatten des neuen Paradigmas Cybersicherheit und angesichts der dramatischen Konflikte an den Rändern Europas schwindet die Hoffnung auf Reformen und eine Beschneidung der unkontrollierten Macht der Dienste. Mut machen allein die Entwicklungen rund um Verschlüsselung und Selbstdatenschutz sowie das international wachsende Bekenntnis zum Menschenrecht auf Privatsphäre.

Wenn uns jemand etwas über die gegenwärtigen Herrschaftsverhältnisse gelehrt hat, war es Edward Snowden. Er enthüllte, dass einige westliche Regierungen bereit und durch ihre Überwachungstechnologien auch in der Lage sind, auf fast jede Lebensäußerung zuzugreifen, die ihre BürgerInnen online, über Festnetz- oder Mobiltelefon tätigen – und dies ohne ernstzunehmende Kontrolle und für deutlich mehr als den angeblich ausschließlichen Zweck der Terrorbekämpfung. In einer nicht abreißenden Serie von Veröffentlichungen klassifizierter Dokumente über eine Vielzahl geheimer Überwachungsprogramme wurde das ungeheure Ausmaß der Datensammlungen und Auswertungen durch die National Security Agency (NSA) und ihre Partnerdienste sichtbar. Dass dabei auch die deutschen Dienste und insbesondere der Bundesnachrichtendienst eine wichtige Rolle spielen, lag als Verdacht von Anfang an in der Luft, wurde aber durch die Deutschland-Akte des Spiegels und die Arbeit des NSA-Untersuchungsausschusses 2014 immer klarer.

Die Intelligence Community beschaffe Informationen, wo sie nur könne und mit allen erdenklichen Mitteln, hatte Snowden von Anfang an erklärt. Die von ihm enthüllten Unterlagen zeigen, dass dabei komplette Kommunikationsnetzwerke und ganze Länder überwacht werden – zum einen „rechtmäßig" aufgrund richterlicher Anordnungen, die beim Zugriff auf die Daten jedoch unbegrenztes Ermessen bieten, zum anderen durch „freiwillige" Zusammenarbeit der Diensteanbieter mit den Geheimdiensten oder gar durch staatlich betriebenes Hacking direkt in den Glasfasernetzen und Datenzentren. Zudem hat die NSA Hintertüren in Apps und Software von einigen der weltgrößten IT-Firmen eingebaut und

Schadsoftware eingesetzt, um Daten aus privaten, Firmen- und Regierungsnetzen zu stehlen. Sie habe weltweit über 50.000 Computernetzwerke infiziert, heißt es in einem der Dokumente.

Die Massenüberwachung ist heute nicht länger die Domäne totalitärer Regime. Es braucht dafür auch nicht mehr eine Stasi, die Akten über ganze Bevölkerungen anlegt. An vorderster Front der Informationssammlung steht heute eine private Infrastruktur. Die Revolution der Informations- und Kommunikationstechnologien transformiert unsere Beziehungen: Je mehr diese online gehen – unsere Interaktion mit FreundInnen in Sozialen Netzwerken, mit Banken via e-Commerce, mit e-Government und politischen Kampagnen – desto mehr Informationen werden über uns aufgezeichnet, gespeichert und ausgewertet.

In der digitalen Welt verraten wir unsere Gedanken, Interessen, Gewohnheiten und Charakterzüge und werden zunehmend berechenbar. Je mehr Dinge, die wir besitzen, mit der digitalen Welt verbunden sind, und je mehr Online-Dienste wir nutzen, desto sensibler und umfassender sind die Informationen, die wir hinterlassen – wo wir waren, was wir getan haben und mit wem. Es geht um personenbezogene Daten (Informationen, die uns identifizieren), Inhaltsdaten (was wir schreiben und sagen) und „Metadaten" (Daten über Daten, wie Verkehrs- und Standortdaten zu Anrufen und Internetverbindungen). Zahlreiche digitale Innovationen basieren auf dem Sammeln und der Analyse dieser Informationen, von den Karten auf unseren Smartphones bis hin zu den diversen Apps, durch die Informationen und Gegenwartskultur verbreitet und konsumiert werden. Die Notwendigkeit, uns vor Geheimdiensten und Sicherheitsagenturen zu schützen, ist also nur ein Teil des Problems. Schützen müssen wir uns auch vor jenen Firmen, deren Profit abhängt vom Zugang zu (und der Monetarisierung von) so vielen unserer persönlichen Informationen wie möglich.

Hinzu kommt ein drittes Problem: Big Data – weniger ein Konzept, als der Marketingslogan einer neuen Industrie: Haben Sie einen großen Datensatz? Wir helfen Ihnen, Ihre Kunden zu verstehen, Ihre Angestellten, Netzwerke, Risiken, und Chancen! Hier wird die „dunkle Seite" der Informations- und Kommunikationstechnologien offensichtlich, in Naomi Kleins Worten: die „Verschmelzung von Shopping Mall und Geheimgefängnis". Die gleichen Algorithmen, die Facebook nutzt, um unsere Interessen und Sehnsüchte zu verstehen, dienen Regierungen und privaten Sicherheitsfirmen, um zu kalkulieren, ob wir heute oder in der Zukunft ein Risiko darstellen. Dieser Dual-Use-Charakter der Technologien macht es so schwierig, sie zu regulieren.

Silicon Valley gegen die Five Eyes?

Die von Edward Snowden enthüllte Überwachung zu problematisieren, ist relativ einfach: Geheimdienste laufen Amok in einer unsicheren digitalen Infrastruktur und nutzen dabei die unkontrollierte Macht, die sie aus dem analogen Zeitalter

übernommen haben. Viel schwieriger sind dagegen, sinnvolle Reformen und tatsächliche Problemlösungen durchzusetzen. Und das nicht nur, weil die Interessen, die den Status Quo stützen, so mächtig sind, sondern auch weil transnationale Überwachungsnetzwerke kaum durch nationale Rechtssysteme zu begrenzen sind. Zusätzlich verschärft werden die Probleme durch fundamentale Veränderungen im Verhältnis von Bevölkerung, Staaten und Konzernen. Im Dezember 2013 forderten acht der erfolgreichsten US-Technologiefirmen – AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter und Yahoo! – einen „grundlegenden Wandel" der Überwachung durch ihre Regierung. Im März 2014 beschwerte sich Facebook-Chef Mark Zuckerberg persönlich bei US-Präsident Obama, nachdem bekannt geworden war, dass die NSA als Facebook-Server getarnte Rechner für Angriffe auf Zielcomputer genutzt hatte. Kurze Zeit später kündigte Google an, künftig den Gmail-Verkehr zwischen seinen Datenzentren zu verschlüsseln, um Schnüffeleien bei der Übertragung auszuschließen. Yahoo erschreckte die britische Innenministerin Theresa May mit der Meldung, seine Europa-Zentrale von London ins irische Dublin zu verlegen, um sich und die Daten seiner KundInnen vor dem Zugriff britischer Dienste in Sicherheit zu bringen. Im Sommer meldeten Google und Yahoo dann, dass sie daran arbeiteten, demnächst auch eine optionale Ende-zu-Ende-Verschlüsselung für die 700 Millionen NutzerInnen ihrer E-Mail-Dienste anzubieten; im November folgte Kurznachrichten-Marktführer WhatsApp mit einem ähnlichen Versprechen. Und auch Apple gibt vor, sein Herz für Privacy by Design entdeckt zu haben – sollen doch mit dem neuen iOS 8 Kurznachrichten verschlüsselt auf den Endgeräten gespeichert werden.

Der Versuch, Vertrauen zurückzugewinnen

Zudem gehen die Unternehmen in die Transparenzoffensive: Seit Juli 2013 benachrichtigt Yahoo seinen NutzerInnen, wenn es Anfragen der Strafverfolgungsbehörden gibt. Untersagt bleibt solche Offenheit aber für den Datenzugriff auf Grundlage der berüchtigten National Security Letters oder des Foreign Intelligence Surveillance Act. Gemeinsam versuchen sich die Firmen daher gegen solche Maulkörbe zu wehren. Nur einen guten Monat nach Beginn der Snowden-Enthüllungen forderte eine Allianz von 63 US-amerikanischen Unternehmen und zivilgesellschaftlichen Organisationen von Präsident Obama, regelmäßig und umfassend über die Zahl der Anfragen nach Bestands-, Inhalts- und Verbindungsdaten berichten zu dürfen. Im Mai 2014 legte selbst die Deutsche Telekom erstmals einen „Jahresbericht – Auskunft an Sicherheitsbehörden" vor, nachdem nur Stunden zuvor der kleine Wettbewerber Posteo mit seinen Zahlen an die Öffentlichkeit gegangen war.

Im Kampf um KundInnenvertrauen und Marktanteile, so scheint es, werden technischer Datenschutz und Transparenzgebahren zunehmend als Wettbewerbsvorteil wahrgenommen. Man mag angesichts der Dominanz proprietärer Lösungen und den gewinnorientierten Motiven der Unternehmen seine Zweifel haben, dass

diese sich wirklich selbst aussperren und es nicht doch irgendwelche Schlüssel zu Hintertüren gibt, deren Herausgabe die Behörden bei Bedarf erzwingen können. Dennoch: Polizei, Strafverfolger und Geheimdienstler sind wütend und schlagen Alarm. Ein neuer Wettlauf um den technischen Zugang zu Inhaltsdaten ist eröffnet.

Es bleibt abzuwarten, welche neuen Geschäftsmodelle sich entwickeln, wenn die Diensteanbieter sich durch Verschlüsselung das maschinelle Mitlesen der Kommunikationsinhalte tatsächlich unmöglich machen. Wird das Produkt wieder zum zahlenden Kunden? Wird Digital Divide künftig weniger den ungleichen Zugang zum Internet meinen, sondern Umschreibung für ein ungleiches Maß an Privatsphäre sein? Oder reichen den Firmen und der von ihnen bedienten Marketingindustrie die aussagekräftigen Verbindungsdaten und diversen anderen Informationen, die sie über uns sammeln, für ihre Zwecke?

Bislang jedenfalls haben die meisten von ihnen schärfstens jeden Versuch bekämpft, den Individuen mehr Kontrolle über die Daten zu geben, aus denen sie ihre Profite ziehen. Nach Angaben von Forbes hätten die großen US-amerikanischen Internet-Unternehmen im Jahr 2013 über 35 Mio. US-Dollar in Lobbyaktivitäten investiert. Zweifellos sind diese Unternehmen echte Gegner der von der NSA betriebenen Schleppnetzüberwachung und gigantischen Datenspeicherung, weil beides eine tatsächliche Gefahr für ihre Profite darstellt. Aber während die Top-Manager im Namen der Integrität des Internets mehr Transparenz und Kontrolle der Überwachung fordern, sollten wir uns fragen, was sie sonst noch alles von unseren Gesetzgebern fordern und bekommen.

Zudem werden die Beziehungen zwischen Staat und Internetwirtschaft enger, wenn es um die Überwachung und Zensur „radikaler" und „extremistischer" Propaganda auf Websites, Blogs und in Sozialen Medien geht. In Großbritannien scannt eine Counter Terrorism Internet Referral Unit (CTIRU) bereits seit 2010 das Netz, führt Listen mit Filtern und hat allein seit Ende 2013 die Löschung von 34.000 „terroristischen" Inhalten durch Intervention bei Service Providern erreicht. Auch auf EU-Ebene arbeitet die Kommission seit der Neuauflage ihrer De-Radikalisierungsstrategie im Januar 2014 auf eine engere Zusammenarbeit mit Internetfirmen hin.

Europa gegen die USA?

Die EU-Regierungen haben zwar in einer gemeinsamen Erklärung ihren Partner auf der anderen Seite des Atlantiks kritisiert, aber keine Sanktionen angedroht. Während die britische Regierung jegliche Kritik an GCHQ als versponnen denunzierte und eine Hexenjagd gegen den Guardian betrieb, haben die kontinentaleuropäischen Regierungen zwar die Aktivitäten der USA und Großbritanniens lauthals kritisiert, bemühen sich aber zugleich, das Treiben ihrer eigenen Geheimdienstapparate nicht zum Thema der Debatte werden zu lassen. Das Ver-

handlungsteam, das Bundeskanzlerin Angela Merkel nach Washington schickte, schien eher bemüht, Deutschlands Beitritt zur Five-Eyes-Allianz aus NSA, GCHQ und den Diensten Kanadas, Australiens und Neuseelands zu erreichen. Zudem blockierte die Bundesregierung gemeinsam mit Großbritannien die EU-Datenschutzreform. Auch die französische Regierung nannte die NSA-Praktiken absolut inakzeptabel, erweiterte aber kurz darauf mit dem Verteidigungsgesetz 2014-2019 die Befugnisse ihrer Geheimdienste zur Telekommunikationsüberwachung und zum Zugriff auf Standort- und andere Verkehrsdaten – ohne richterliche Kontrolle.

Die EU-Kommission, machtlos in allen Fragen, die die nationale Sicherheit der Mitgliedstaaten betreffen, äußerte sich zwar sehr deutlich zur NSA-Überwachung, beschränkte sich aber praktisch darauf, mit erhobenem Finger in Richtung Silicon Valley zu zeigen – reichlich selbstgerecht angesichts der problematischen Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten, die der Europäische Gerichtshof im April 2014 aus gutem Grund kippte. Im März 2014 schloss das Europäische Parlament eine Untersuchung zur Überwachungspraxis der NSA und ihrer europäischen Partner ab, aber weil es keine ZeugInnenaussagen erzwingen kann, musste es sich mit der Befragung von JournalistInnen, CampaignerInnen und unabhängigen ExpertInnen begnügen. Seine unverbindlichen Empfehlungen beinhalten u. a., verschiedene Abkommen zum Datenaustausch mit den USA auszusetzen, solange nicht wechselseitig Privatsphäre und Datenschutz respektiert werden. Die Aufgabe, auch Perspektiven für Reformen im eigenen europäischen Haus zu entwickeln, wurde vorerst an die EU-Grundrechteagentur delegiert. Die Reaktionen in den Mitgliedstaaten auf ihren für 2015 angekündigten Bericht dürften jedoch verhalten sein, und aus Brüssel ist nach dem Rechtsruck bei den Wahlen zum Europaparlament wenig Initiative zu erwarten.

Mit Ausnahme Deutschlands scheint eine parlamentarische Aufarbeitung der Enthüllungen in den Ländern der EU auszubleiben, und welche Ergebnisse der NSA-Untersuchungsausschuss des Bundestages angesichts der hartnäckigen Blockaden der Bundesregierungen und vor dem Hintergrund der aktuellen Machtverhältnisse zeitigen wird, bleibt abzuwarten. So liegen vielfältige Hoffnungen – mal wieder – bei den Gerichten: Hat sich hierzulande eine Verfassungsbeschwerde gegen die BND-Überwachung leider vorzeitig erledigt, sind doch in Großbritannien und vor dem Europäischen Gerichtshof für Menschenrechte verschiedene Klagen gegen das Treiben des GCHQ anhängig. Auch wenn bei dem aktuellen politischen Klima auf der zunehmend von Kontinentaleuropa wegdriftenden Insel nicht zu erwarten ist, dass kritische Worte aus Straßburgs die Regierung in London beeindrucken, so könnte eine menschenrechtlich begründete Absage an den unregulierten Ringtausch von Geheimdienstinformationen zumindest auf dem Festland neue Argumente für Reformen liefern.

In den USA sah es eine Zeit lang so aus, als ob sie den EU-Staaten bei den Reformüberlegungen, die ihre BürgerInnen vor geheimdienstlichem Übermaß schützen sollen, um Längen voraus wären. Im Dezember 2013 urteilte ein Bundesrichter, dass das massenhafte Sammeln von Telefonverbindungsdaten gegen die Verfassung verstoße; diese Praxis sei „wahllos", „willkürlich" und „fast orwellianisch". Die Entscheidung ist zwar nicht rechtskräftig, fand aber Widerhall in den Empfehlungen einer von Präsident Obama eingesetzten „Review Group on Intelligence and Communication Technologies", deren 46 Empfehlungen eine deutliche Beschränkung der NSA-Vollmachten bedeutet hätten. Allerdings folgte Obama den Empfehlungen seiner Kommission bestenfalls halbherzig, als er am 17. Januar 2014 seine Presidential Policy Directive/PPD 28 zur Reform der Signal Intelligence Activities bekannt gab. Versuche, weitergehende Reformen gesetzlich abzusichern, scheiterten schließlich im November 2014, als die neu erstarkten Republikaner den zuvor im parteiübergreifenden Konsens ausgehandelten Entwurf für einen USA Freedom Act im Senat durchfallen ließen. Dass das nach Parteiproporz besetzte Privacy and Civil Liberties Oversight Board (PCLOB), zuständig für die Kontrolle exekutiver Maßnahmen zur Terrorismusbekämpfung, im Laufe des Jahres in mehreren Berichten deutliche Kritik an der uferlosen Überwachung geäußert hatte, wurde ignoriert.

Trotz aller transatlantischen Dissonanzen haben insbesondere der Konflikt in der Ukraine und die Ausrufung des Kalifats durch den Islamischen Staat (IS) im Irak und Syrien die Reihen wieder weitgehend geschlossen. Die UN-Sicherheitsratsresolution 2178 (2014) gegen die „ausländischen Kämpfer" betonte ausdrücklich die Bedeutung der Internetüberwachung und die Notwendigkeit des internationalen Informationsaustausches. Und es war der Verweis auf den IS, der als Begründung für die Ablehnung des Freedom Act herhalten musste.

Völkerrecht gegen (trans-)nationale Sicherheit

Ob wir in einer Welt leben, in der die NSA und ihre Verbündeten gegen das Internet und seine Geheimnisse unternehmen können, was immer sie wollen, wird sich letztlich an der Frage entscheiden, wie viel Respekt wir für den Rechtsstaat und die universellen Menschenrechte haben, insbesondere für das Recht auf Privatsphäre – ein Recht, von dem viele andere Rechte abhängen.

Im Rahmen nationaler Verfassungen, die das Recht auf Privatsphäre garantieren, sind den Überwachungsbefugnissen im Inland vergleichsweise klare Grenzen gezogen. Das weitaus größere Problem ist, dass BürgerInnen anderer Länder in der Regel nicht die gleichen Rechte genießen. Das ist entscheidend aus zwei Gründen: Zum einen wird elektronische Kommunikation häufig über fremde Territorien geleitet, insbesondere über die USA. Wer keine US-Bürgerin oder US-Bürger ist, dem nützt es nichts, dass die Verfassung ihres und seines Heimatlandes das Recht auf Privatsphäre formuliert. Zum anderen sind zwar die USA der Protago-

nist der Snowden-Dokumente, aber sie stehen nur im Zentrum der Five Eyes, jenes immer noch sehr verschwiegenen und fast völlig unregulierten transnationalen Netzwerks von Geheimdiensten mit globaler Reichweite.

Obamas bereits zitierte Kommission als auch das PCLOB haben zwar empfohlen, die Überwachung von Nicht-US-BürgerInnen stärker zu überprüfen. Einen gerichtlichen Rechtsschutz schlossen sie jedoch praktisch aus. AusländerInnen werden auch nichts vom Kommissionsvorschlag einer Minimierung der Überwachung von US-BürgerInnen haben. Es ist kaum anzunehmen, dass dieses Konzept die europäischen Kritiker zufriedenstellen oder Brasilien besänftigen wird. Das Land fordert von allen ausländischen Anbietern, die in Brasilien Telekommunikationsdienstleistungen erbringen, auch ihre Server dort zu hosten, sodass sie brasilianischem Recht unterlägen. Inzwischen denken auch andere Regierungen in diese Richtung. Nicht nur Privatfirmen warnen deshalb vor einer Balkanisierung des Internets, die existierende Standards und Normen zerpflücken werde.

Nachdem der „Sommer Snowdens" die Macht der NSA und der großen Technologiekonzerne demonstriert hat, wird nun auch die Schwäche des Völkerrechts deutlich. Menschenrechtsverträge und deren juristische Interpretation lassen wenig Zweifel daran, dass die Five Eyes und andere gegen die Buchstaben und den Geist des Völkerrechts verstoßen. Ignoriert wurden nicht nur Menschenrechtsstandards, sondern auch in Jahrzehnten gewachsene Systeme zur gegenseitigen Rechtshilfe.

FürsprecherInnen von Global Governance rufen wehmütig nach internationalen Abkommen, die Massenüberwachung beschränken und individuelle Rechte auf Privatsphäre und ein faires Verfahren stärken. Gegenwärtig ist jedoch unvorstellbar, dass Staaten irgendeinen völkerrechtlichen Vertrag akzeptieren, der ihre Befugnisse im Bereich nationaler Sicherheit beschränkt. Auch die Big-Data-Firmen werden sich jedem Versuch widersetzen, auf internationaler Ebene ein Recht auf Datenschutz explizit zu kodifizieren. Bei allem Gerede über eine Reform der Überwachung ist auffällig, dass Silicon Valley individuelle Rechte – digital oder analog – mit keiner Silbe erwähnt.

Gleichwohl wächst der Kreis der BefürworterInnen einer solchen Kodifizierung. Im November 2013 verabschiedete die UN-Generalversammlung eine Resolution zum „Recht auf Privatsphäre im digitalen Zeitalter", die allerdings nur für die UN-Hochkommissarin für Menschenrechte bindend ist. Auftragsgemäß legte sie Ende Juni 2014 einen Bericht zum Thema vor, der in seiner deutlichen Absage an unverhältnismäßige und willkürliche geheimdienstliche Massenüberwachung kaum zu überbieten ist. Bereits im März musste sich die US-Regierung vor dem UN-Menschenrechtsausschuss im Berichtsverfahren zur Umsetzung des Internationalen Paktes für bürgerliche und politische Rechte (Zivilpakt) ähnlich deutliche Kritik gefallen lassen. Im September sekundierte Ben Emmerson, UN-Sonderberichterstatter für die Achtung der Menschenrechte in der Terro-

rismusbekämpfung und selbst US-Amerikaner, als er feststellte, dass die aufgedeckten Programme „eine direkte und andauernde Verletzung etablierter Völkerrechtsnormen" darstellten. All dies lässt Washington jedoch bislang mit dem Verweis auf konkurrierende Rechtsauffassungen an sich abperlen. Ob nun Anregungen aufgenommen werden, ein internationales Datenschutzabkommen auszuhandeln, oder ob – wie von der American Civil Liberties Union vorgeschlagen – nur der UN-Menschenrechtsausschuss eine zeitgemäße Interpretation von Art. 17 (Recht auf Privatsphäre) des Zivilpaketes erarbeiten wird, muss sich zeigen. Doch selbst wenn die politischen Widerstände gemeistert werden könnten, dürfte es bis zur Aushandlung solcher Initiativen Jahre dauern, und auch dann kann ihre Durchsetzung nicht erzwungen werden. Somit bleiben kurzfristig nationale Maßnahmen zur Eindämmung der geheimdienstlichen Massenüberwachung der einzig sinnvolle Weg zur Reform. Indes kann eine kritische internationale Diskussion ein hilfreicher Referenzpunkt hierfür sein.

Nadeln und Heuhaufen

Die alte Debatte um das Verhältnis von Freiheit und Sicherheit scheint also neu eröffnet. Allerdings bedeutet nationale Sicherheit heute nicht mehr arbeitsintensive Aktenhaltung wie zu Zeiten des Kalten Krieges, sondern Big-Data-Banken und rechenintensive Weiterverarbeitung. Die Schwierigkeit, diesem neuen, durch transnationale, präventive Massenüberwachung geprägten Modell von Sicherheit Respekt für die traditionellen Vorstellungen von Rechtsstaatlichkeit und Verhältnismäßigkeit beizubringen, liegt darin, dass die allermeisten der neuen Methoden die Antithese zu den überkommenen Normen darstellen.

Die Geheimdienstchefs rechtfertigen ihre Programme zur Massenüberwachung mit dem Mantra: „Wir brauchen den Heuhaufen, um die Nadel zu finden." Kritik an den Überwachungsprogrammen wird als Gefahr für die nationale Sicherheit denunziert. Verschleiert wird damit, dass Polizei und Geheimdienste bereits seit langem teils anlassbezogen, teils generell Zugriff auf den Heuhaufen hatten. Snowdens Enthüllungen zeigen nun, dass die NSA und ihre Partner einen gewaltigen Heuhaufen aus so vielen Daten wie irgend möglich auftürmten, der es ihnen erlaubte, beliebig zurückzuverfolgen, was ihre BürgerInnen zu irgendeinem Zeitpunkt in der Vergangenheit getan haben.

Notwendige Schritte

Der erste Lackmustest für die Reform der Überwachung wäre daher die Absage an die massenhafte Datensammlung durch die Geheimdienste – eine ungeheure Aufgabe angesichts der Kultur der Überwachung, die den Berufsalltag Hunderttausender staatlicher Sicherheitsbeamter und ihrer Auftragnehmer prägt und angesichts der Infrastruktur, die nicht nur die NSA hierfür geschaffen hat.

Der zweite Lackmustest besteht darin, so weit wie möglich zu verhindern, dass große Vorratsdatensammlungen entstehen, zu denen sich staatliche Agenturen

grundlos und unkontrolliert Zugriff verschaffen können. Das Problem stellt sich nicht nur bei den Verkehrsdaten der Telekommunikation, sondern auch bei Gesundheitsdaten, bei Reisen (Fluggastdaten) usw. Wenn wir die Unschuldsvermutung und das Recht auf Privatsphäre in Zeiten von Big Data retten wollen, dann benötigen wir zwingend Brandmauern, die Profiling und Rasterfahndungen verhindern, deren Zweck darin besteht, Verdachtsmomente gegenüber Unschuldigen zu generieren.

Drittens ist zu definieren, unter welchen Bedingungen Geheimdienste Zugang zu Daten anderer Behörden oder privater Firmen haben dürfen, um ihre Aufgaben zu erfüllen. Dafür braucht es zum einen mehr Transparenz darüber, wer, wie und warum in den Heuhaufen stochert. Zum anderen braucht es eine deutlich klarere Trennung zwischen Fragen nationaler Sicherheit und dem Sammeln von Informationen für Zwecke der Strafverfolgung. Im Kern geht es dabei um die Entscheidung, ob die Terrorismusbekämpfung Sache von Militär und Geheimdiensten oder rechtsstaatliche Polizeiarbeit ist.

Viertens schließlich müssen die auf Kuschelkurs bedachten, parlamentarischen Gremien zur Geheimdienstaufsicht durch eine ernsthafte demokratische Kontrolle ersetzt werden.

Der tiefe Staat

Rechenschaftspflichten und eine bessere Aufsicht über die Geheimdienste, so lautet eine der beliebtesten Forderungen in der Zeit nach Snowden. Das ist eine Herkulesaufgabe, denn, wie ein ehemaliger britischer Richter zurecht erklärte:

> Der Sicherheitsapparat ist heutzutage in vielen Demokratien in der Lage, derart stark Einfluss auf die anderen Staatsorgane auszuüben, dass er quasi autonom ist: Er sorgt für eine Gesetzgebung, die seine Interessen über die Individualrechte stellt, dominiert exekutive Entscheidungsprozesse, sperrt seine Gegner aus gerichtlichen Verfahren aus und operiert nahezu jenseits öffentlicher Kontrolle.

Es wäre naiv zu glauben, dass Forderungen nach mehr Kontrolle wie selbstverständlich Erfolg haben, wo doch bereits seit einem Jahrzehnt gegen massive Widerstände versucht wird, die USA und ihre Verbündeten für Verschleppung, Geheimgefängnisse, Folter und Kriegsverbrechen im „Krieg gegen den Terror" zur Verantwortung zu ziehen. Versuche, Gerechtigkeit wiederherzustellen, sind trotz vieler Untersuchungen in Europa und Nordamerika immer wieder gescheitert. Standardmäßig haben die Regierungen die Aktionen ihrer Dienste verteidigt, ignoriert oder entschuldigt. Warum? Weil ihre Geheimdienste eng einbezogen sind in alles Militärische und in einen Großteil ihrer Außen- und Wirtschaftspolitik. Geopolitisch betrachtet stehen Überwachungskapazitäten – oder Lagebildeinschätzung – im Zentrum jeglicher Machtprojektion. Hinzu kommt,

dass die Exekutiven und ihre geheimen Dienste sich mit der transnationalen Zusammenarbeit noch stärker der nationalstaatlich gefesselten legislativen Kontrolle entziehen. Dass die Bundesregierung dem NSA-Untersuchungsausschuss des Bundestages mit dem Verweis auf Quellenschutz und Zusagen gegenüber ausländischen Partnerdiensten massiv Informationen vorenthält, ist für diese Umkehr der Machtverhältnisse nur exemplarisch.

Die Rufe nach Reformen und Kontrolle stehen vor einem weiteren grundlegenden Problem: Der Aufbau von Kontrollmechanismen für Überwachungsagenturen, die im Geheimen arbeiten, um präventiv Gefahren durch bekannte und unbekannte Feinde zu begegnen, ist eine widersprüchliche Übung. Zu Ende gedacht kann die Forderung, Überwachung auf das Erforderliche und Verhältnismäßige zu reduzieren und angemessener demokratischer und gerichtlicher Kontrolle zu unterwerfen, nur bedeuten, das Mandat und die Vollmachten der Geheimdienste radikal zu beschränken, die Aufgabe der Terrorismusbekämpfung auf die Polizei zu übertragen und dabei deren weit ins Vorfeld von Straftaten und konkreten Gefahren expandierte Eingriffsbefugnisse deutlich zu beschneiden. Eine solche Konsequenz kommt jedoch in Zeiten massiver globaler Verunsicherung einer Blasphemie gleich und ihre politisch-praktische Umsetzung der Quadratur des Kreises.

Gute Geschäfte

Überwachung findet nicht im luftleeren Raum statt. Die Sicherheitsapparate haben insbesondere seit dem 11. September 2001 eine atemberaubende Entwicklung genommen, deren Auswirkungen auf „verdächtige Gemeinschaften" wir genauso wenig ignorieren dürfen wie ihre Strategien gegen „Radikalisierung" und „inländischen Extremismus". Weltweit sind sozialer Protest und ziviler Ungehorsam unter Druck wie nie zuvor. Der Kampf gegen unkontrollierte Überwachung steht somit im Zentrum der Kämpfe um soziale Gerechtigkeit.

Während der Neoliberalismus ständig mehr öffentliche Dienstleistungen zusammenstreicht, können die Hohepriester des Sicherheitsstaates ungezählte Milliarden von Euro ausgeben für Armeen von Auftragsdienstleistern und für Ausrüstung nach dem Vorbild von Hollywood-Ausstattern.

Was immer für den Sicherheitsstaat gut ist, ist auch gut fürs Geschäft. Der stark auf Massenüberwachung ausgerichtete „Heimatschutz" ist bereits heute ein Milliarden-Geschäft. Die Grenzen zwischen Militär, nationaler Sicherheit und öffentlicher Ordnung verschwimmen und es besteht ein geradezu manisches Interesse an neuen technischen Möglichkeiten: von Drohnen über „weniger tödliche" Waffen und Technologien zur Kontrolle von Menschenmengen oder zur militarisierten Grenzkontrolle bis hin zu neuen Anwendungen für Massenüberwachung. Der neue Kaiser trägt Designerkleider und eine Designerrüstung.

Wir müssen davon ausgehen, dass die einflussreiche Überwachungsindustrie versuchen wird, jede Sicherheitslücke zu füllen, die sich durch die demokratische Kontrolle der Staatsmacht ergibt. Wenn wir es ernst meinen mit der Begrenzung der Überwachung, müssen wir die Staatsmacht gleichermaßen einhegen wie die des Privatsektors.

Dieser Beitrag ist eine übersetzte und aktualisierte Fassung von Ben Hayes Beitrag „State of Surveillance. The NSA Files and the Global Fightback", der im Frühjahr 2014 in der Textsammlung „State of Power 2014" des Transnational Institute in Amsterdam erschienen ist.

Ben Hayes erforscht und analysiert komplexe internationale Sicherheitsthematiken, insbesondere zu Terrorismusbekämpfung, Überwachung und Migrationskontrolle. Er arbeitet unter anderem mit dem Transnational Institute und als Projektleiter bei Statewatch.

Eric Töpfer ist wissenschaftlicher Mitarbeiter beim Deutschen Institut für Menschenrechte in Berlin. Er hat Politikwissenschaft studiert und forschte zu den Themen Informationstechnik und Gesellschaft, Überwachungs- und Polizeistudien, Friedens- und Konfliktforschung und dem Wandel von Stadt, Staatlichkeit und sozialer Kontrolle.

9 Immunität für Snowden? Warum wir die Rechte von Whistleblowern stärken sollten

von **Jochai Benkler**

Insider veröffentlichen Missstände in staatlichen oder privaten Institutionen – das nennt man Whistleblowing und hat eine lange Geschichte. Die NSA-Enthüllungen durch Edward Snowden bilden nur die Spitze des Eisberges und lösen eine Grundsatzdebatte aus: Könnte eine rückwirkende Immunität für Snowden zukünftigen Whistleblowern die nötige Rechtssicherheit geben und ihre gesellschaftliche Rolle stärken? Juraprofessor und Netz-Experte Yochai Benkler über die heikle Rolle des Whistleblowers.

1970 enthüllte Christopher Pyle in einem öffentlichen Schreiben, dass die U.S. Army ein innerstaatliches Überwachungsprogramm betrieb, das auf Kriegsgegner und Bürgerrechtsaktivisten ausgerichtet war. Seine Enthüllung inspirierte eine Vielzahl von Whistleblowern. Bekanntestes Beispiel dürften wohl Daniel Ellsbergs Pentagon Papers sein. Diese Enthüllungen, wie der berühmt-berüchtigte Missbrauch des FBI in COINTELPRO-Operationen und der Watergate-Skandal, lehrten die US-Amerikaner, dass das National Security System tiefgehende verfassungsschädliche Wendungen nehmen kann. Also gründeten sie die Stiftung für politische Bereitschaft, welche 1978 schließlich zum Gesetz zum Abhören in der Auslandsaufklärung (FISA) führte. Und obgleich Ellsberg und sein Mitarbeiter Anthony Russo strafrechtlich verfolgt wurden, ließ man die Anklage gegen sie fallen. Diese Ereignisse halfen, die Funktion des Whistleblowings zu festigen. Die Leaker der 1970er Jahre wurden zu Helden, die das Scheitern des Systems entlarvten. Und diejenigen, die halfen Missstände zu bereinigen, wurden vom Staat nicht bestraft.

Lange Geschichte der Leaks

Über ein viertel Jahrhundert verbreiteten sich Leaks weiterhin, wenn auch nicht mit der Transparenz, die typisch für den Beginn der 1970er war. Diese Leaks waren wie Wasser auf den Mühlen der nationalen Presse: Gerüchte und Verrat, Versuchsballons und glorifizierte Kriegsgeschichten von Insidern. Nur die Veröffentlichung von Satellitenbildern eines sowjetischen Flugzeugträgers durch die Jane's Information Group wurde jemals strafrechtlich verfolgt. Derartige Leaks an die Presse nicht zu bestrafen, wurde in solchem Maße zur Norm, dass Senator Daniel Patrick Moynihan Präsident Bill Clinton davon überzeugen konnte, selbst diese Straftat zu begnadigen.

Als Jesselyn Radack 2002 ans Licht brachte, dass die Verfolgung des „amerikanischen Taliban" John Walker Lindh etliche Grundrechte verletzte, brach eine neue Welle von Whistleblowern und Leaks bezüglich öffentlicher Transparenz hervor. Thomas Tamm und Russ Tice enthüllten zusammen die unrechtmäßige Abhöraktion der Bush-Regierung und leiteten die Informationen an die New York Times weiter. AT&T-Mitarbeiter Mark Klein deckte die Mitschuld seiner Firma an illegaler Telefonüberwachung auf; und William Binney, Thomas Drake und andere stellten intern – in Drakes Fall sogar öffentlich – frühe Aspekte des NSA-Überwachungsnetzes infrage.

Chelsea Manning gab eine bedeutende Anzahl von Dokumenten an WikiLeaks weiter, getrieben durch das, was sie als gefühllose Gleichgültigkeit gegenüber Zivilopfern und stille Mitschuld der amerikanischen Streitkräfte während von der Regierung geduldeten Folterungen im Irak erachtete. Als am entscheidendsten gelten aber die Enthüllungen Edward Snowdens, die zur Einführung zahlreicher Gesetzesentwürfe im US-Kongress führten, etwa zu einem richterlichen Beschluss und zwei unabhängigen Berichten der Exekutive, die weitreichende Reformen von Überwachungsprogrammen forderten.

Wie im Falle der Leaks der Vietnam-Ära war die Welle an Leaks bezüglich staatlicher Transparenz der letzten Jahre das Ergebnis der permanenten Überschreitung von verfassungsrechtlichen Grenzen in Ausnahmezuständen durch nationale Sicherheitsbehörden. Als Reaktion auf den Schock vom 11. September antwortete das National Security System so gut es konnte. Einige Reaktionen waren wohlüberlegt und notwendig. Andere waren gravierende Fehler gefolgt von aggressiven Verschleierungstaktiken.

NSA-Überwachungsapparat überschreitet Autorität

Die Armee ordnete zunächst Ermittlungen aufgrund der Beschuldigungen von Folter durch Angehörige des Militärs an und zwang später den General, der pflichtbewusst die von ihm entdeckten „sadistischen, offenkundigen und schamlosen systematischen illegalen Misshandlungen" meldete, aus der Armee auszutreten. Die CIA begegnete Folterung mit Vergeltung, war damit nicht ehrlich zu Regierung und Kongress und ging in dem Versuch, ihre Spuren zu verwischen, sogar so weit, die Aufsichtsbehörde des Senats auszuspionieren. Die NSA hat einen Überwachungsapparat erschaffen, der seine gesetzliche und verfassungsrechtliche Autorität bei Weitem überschritten hat und während man diesen Apparat „zurechtbiegen" wollte, zwang man Teile der Judikative und des Kongresses, eine Fassade zu errichten, die die Handlungen der NSA als zulässig erscheinen lassen sollte. Aus diesem Blickwinkel kann der Krieg gegen Whistleblower durch Präsident Obama und seinen Generalstaatsanwalt nicht länger als einfache Reaktion auf zunehmende Leaks im Allgemeinen gesehen werden. Stattdessen spiegelt dies ein zunehmend in Bedrängnis geratendes nationales Sicherheitssystem

wider, welches tiefer und tiefer in kaum noch zu vertretende oder unhaltbare verfassungsrechtliche Auswege gerät und aggressive kriminelle Strafverfolgung auch noch intensiviert, um sich vor dem zu schützen, was dieses missbrauchende System beenden könnte: das Gewissen des Einzelnen.

Eines ist klar: Ohne die Männer und Frauen mit diesem Gewissen, die in den letzten zwölf Jahren in Erscheinung getreten sind, um Aspekte des Missbrauchs zu enthüllen, hätte sich das System fortwährend selbst aufgerieben.

Die wichtigste Lektion, die wir aus den Snowden-Enthülllungen mitnehmen, ist, dass selbst gut durchdachte und gut gemeinte Systeme der Gewaltenteilung mit der Zeit zerrüttet und untergraben werden können. Egal, wie perfekt das Regelwerk oder das institutionelle oder organisatorische System zu Beginn war, es kann so nicht im Angesicht von Zeit, Veränderung und Druck durch neue Notfälle bestehen. Das FISA-System, welches in den 70er Jahren entstand, funktionierte ziemlich gut in den späteren Stadien des Kalten Krieges, als es mit der Art von Bedrohungen und technischer Umgebung rang, für die es gemacht wurde. Aber, so sagte Binney, das alles änderte sich nach dem 11. September 2001.

Das Versagen großer Systeme

Die Dringlichkeit, andere Attacken dieser Art in Zukunft verhindern zu müssen, setzte auch die bisher bekannten Regeln außer Kraft. Zum einen als Antwort auf heldenhafte Bemühungen einiger Insider, die die Regelwerke verändern wollten; und hauptsächlich aufgrund der öffentlichen Exposition des unerlaubten Abhörprogramms, wurden Elemente des richterlichen Aufsichtssystems ab 2006 wieder eingeführt. Der Kongress durchlief das FISA-Anpassungsgesetz in 2008. Doch da die Praktiken, die sich entwickelt hatten, so komplex und vielfältig waren, wurde klar, dass das neue Aufsichtssystem deren Kontrolle absolut nicht gerecht werden konnte.

Das Versagen des FISA-Systems, ob alt oder neu, ist nicht singulär. Alle großen Systeme leiden unter dieser Art des Versagens, wenn sie älter werden und neue Bedingungen die alten Praktiken infrage stellen und wenn die einst geliebten Grundprinzipien für diese Prozesse in der Eintönigkeit des Alltags der Bürokratie verloren gehen. Die Demokraten in den USA mögen sich bevorzugt auf General Motors oder Lehman Brothers konzentrieren. Die Republikaner hingegen werden die Obamacare-Website oder das US-Bundesministerium für Gesundheit und Human Services hervorheben. Worauf sich alle einigen können, wenn es um das Versagen öffentlicher Behörden geht, ist Katrinagate[1].

Begrenzter Schutz für Whistleblower

Whistleblowing ist ein wichtiger Grundpfeiler des US-Rechts, wenn es um das Aufdecken von Fehlentwicklungen, Inkompetenzen oder Gesetzesübertretungen in großen Organisationen und Behörden geht. Ob bei Verstößen gegen die Sicherheit am Arbeitsplatz, bei Betrug innerhalb der staatlichen Krankenversicherung

oder bei Anti-Korruptionskampagnen auf der ganzen Welt: Wir beschützen und belohnen diejenigen, die den internen Abläufen folgen und diejenigen, die den Missbrauch der Öffentlichkeit bekannt machen. Interne Überprüfungen und Begutachtungsprozesse sind wichtig, müssen jedoch durch Insiderwissen gestärkt werden.

Wenn es um die nationale Sicherheit geht, verhält es sich jedoch anders. Hier gibt es nur begrenzten Schutz für interne Whistleblower und gar keinen für die, die mit ihrem Wissen zur Presse gehen. Verfechter dieser Methode behaupten, dass das riskante Wesen der nationalen Sicherheit absolute Geheimhaltung rechtfertige. Aber eben dieses riskante Wesen bedeutet auch, dass Fehler verheerende Auswirkungen haben können, während die von den nationalen Sicherheitssystemen geforderte Geheimhaltung diese mit höherer Wahrscheinlichkeit in fehlerhaften Muster steckenbleiben lässt.

Geheimhaltung verhindert viele Mechanismen, die von anderen Systeme genutzt werden, um eben solche fehlerhaften Dynamiken zu korrigieren. Im öffentlichen Sektor ermöglichen informierte und interessierte Außenstehende eine starke Kontrolle der Judikative, Legislative oder Exekutive. Im privaten Sektor verlassen sich sowohl der Aktienmarkt als auch Regulatoren auf öffentliche Informationen und Offenlegungspflicht, um Fehler, Inkompetenz und gesetzeswidriges Verhalten zu bestrafen. Von defekten Produkten bis hin zur schlechten Geschäftsentscheidung ist Informationsfluss die entscheidende Zutat für Verbesserungen.

Die internen und externen Informationsspeicher, die die nationale Sicherheit verkörpern, und die Geheimhaltung der Behörden verhindern all diese Standardprozeduren, die wir nutzen, um Fehlerquellen anderer großer Organisationen auszugleichen. Die Komplexität und Ungewissheit der Bedrohungen, denen das nationale Sicherheitssystem entgegentritt, verschlimmern diese Schwierigkeiten, sodass selbst Insider – über Außenstehende wollen wir hier gar nicht reden – mit der Entscheidung ringen, ob ein System funktioniert oder vom rechten Weg abgekommen ist.

Da es für Außenstehende praktisch unmöglich ist, dieses System zu überprüfen, erweist sich Insider-Whistleblower zu schützen als besonders heikel. Das Hauptziel der FISA-Reform war die Erzeugung eines „Insiders-Outsiders"-Systems. Ausgewählte Mitglieder des Kongresses (der Geheimdienstausschuss) und ein paar Richter (der FISA-Gerichtshof) sollten dies gewährleisten.

Ein Überwachungsschauspiel

Aber der Fall des NSA-Überwachungsnetzes zeigte, dass die Wachhunde von Geheimhaltung und einem Ungleichgewicht der Ressourcen behindert wurden, was es für sie unmöglich machte, als echter Schutz gegen Missbrauch zu agieren. Das Ergebnis war ein „Aufsichtstheater": ein Überwachungsschauspiel, das dazu diente, Kritiker zu beschwichtigen und öffentliche Forderungen nach Reformen

zu entschärfen. Einzig und allein die wiederholten gewissenhaften Enthüllungen von Insidern gingen mit den Grenzen von Überwachung an die Öffentlichkeit.

Reformen, die versuchen die funktionierenden Aspekte des Systems zu erneuern, dabei aber die ernste Schalterrolle der eigenmächtig handelnden Whistleblower ignorieren, sind zum Scheitern verurteilt. Leaks und Leaker zu respektieren, ist keine Beleidigung des Patriotismus der Mitarbeiter des nationalen Sicherheitssystems, des Kongresses oder von den Justizbeamten, welche das Insider-Kontrollsystem bilden. Es ist ein Zugeständnis, dass es praktisch unmöglich ist, ein rein unabhängiges Überwachungsregime zu erschaffen.

Ob jemand ein Gewissen hat, auf das er oder sie hört, hängt überhaupt nicht damit zusammen, ob ein System an sich funktioniert oder nicht. Das Gewissen entsteht nicht durch eine bestimmte Position, Ausbildung oder Aufsichtsrolle. Es hat seinen Ursprung in den unterschiedlichen Arten, wie wir aufwachsen. Es formt sich durch unsere Erfahrungen und wird ausgelöst durch verschiedene Zwänge, denen wir unterliegen. Das Gewissen kann jeden bewegen, vom absolut loyalen technischen Insider wie Binney bis zum in den Ruhestand gegangenen Mitarbeiter einer Telefongesellschaft wie Klein. Es funktioniert also wie eine Zufallsinspektion. Dieser Mangel an Vorhersehbarkeit macht eigenmächtige Leaks in Bezug auf Transparenz so brisant.

Gesetzliche Vorgänge für Whistleblowing zu verbessern, ist daher zwar wichtig, aber nicht ausreichend. Eine weniger unterwürfige Version des aktuellen Systems für nationale Sicherheitsmitarbeiter – ausgeweitet auf die Einbeziehung von Arbeitnehmern – würde Lohnerhöhungen dienlich sein und Rückstände oder schlechtes Management auflösen.

Immunität als Sicherheit für Insider

Und das ist der Grund, warum Immunität für Edward Snowden so entscheidend ist. Im Prinzip sollte es eine Verteidigung für staatliche Transparenz im Strafrecht geben, ähnlich der zur Notwehr und Verteidigung von anderen. Ich habe darüber geschrieben, warum wir solch eine Verteidigung benötigen und wie wir diese gestalten sollten. Aber der Kongress sollte auch eine simple, direkte Intervention einführen: Snowden rückwirkend Immunität zu gewähren, sollte auf den NSA-Reform-Gesetzesentwurf kommen, welcher im Moment im Regierungsviertel diskutiert wird.

Rückwirkende Immunität würde schlicht und einfach die Immunität widerspiegeln, die in den FISA-Gesetzesänderungen von 2008 garantiert wurde. Diese Abänderung bezog sich auf Telefongesellschaften, die das Gesetz durch die Zusammenarbeit mit illegaler Überwachung verletzt haben. Das Weiße Haus wollte diese Immunität durch das neue Reformgesetz auch auf andere Firmen, die ebenfalls private Daten weitergaben, ausweiten.

Rückwirkende Immunität würde eher eine rechtsstaatliche Kultur erschaffen als eine dauerhaft rechtliche Lösung. Unsere (verschwommenen) Erinnerungen der 1970er Jahre lehren uns, dass diese Leaker, die wesentliches Fehlverhalten aufdeckten, Helden waren und dass Respekt, nicht Gefängnis, deren Lohn sein sollte. Das ist die Lektion, die Immunität für Snowden untermauern würde. Es wird Leaken weder zu einer ungefährlichen Angelegenheit machen, noch wird es die Furcht vor Auswirkungen wie Chelsea Mannings 35-jährigem Gefängnisurteil auslöschen.

Aber diese Immunität wäre ein überzeugendes Statement für Insider. Sie könnten dazu bewegt werden, wenn das System weit genug vom Kurs abweicht und öffentliche Enthüllungen von ehrlichem Nutzen sind, auf ihr Gewissen zu hören und das Richtige zu tun. Selbst wenn der Leak illegal ist, die Öffentlichkeit wird Whistleblower, die bedeutende Missstände aufzeigen, unterstützen, und die Whistleblower werden nicht gezwungen, ihr Leben im Gefängnis oder Exil zu verbringen, während die, deren Verbrechen sie aufgedeckt haben, nicht belangt werden.

Dieser Beitrag erschien zuerst am 16. Oktober 2014 auf http://berlinergazette.de.

Anmerkungen

[1] Anm. d. Redaktion: Versäumnisse im Katastrophenmanagement nach dem Hurrikan Katrina im August 2005

Jochai Benkler ist Juraprofessor und Autor. 1996 bis 2003 forschte er an der New York University School of Law, bis 2007 an der Yale Law School. Er unterrichtet seitdem an der Harvard Law School und veröffentlichte mehrere Bücher und Aufsätze, darunter "The Wealth of Networks" (2006) und "Coase's Penguin" (2002).

10 Hack Back! Ein Do-it-yourself-Guide für alle, die keine Geduld haben, auf Whistleblower zu warten

von **@GammaGroupPR**

1. Einführung

Ich schreibe das nicht, um anzugeben, was für ein cooler Hacker ich bin und welche krassen Fähigkeiten ich eingesetzt habe, um Gamma bloßzustellen. Ich schreibe das, um Hacken zu entmystifizieren und um zu zeigen, wie einfach es ist. Und hoffentlich, um dich zu informieren und zu inspirieren, raus zu gehen und zu hacken.

Wenn du keine Erfahrung mit Programmieren oder Hacken hast, wird dir einiges in diesem Text wie eine Fremdsprache vorkommen. Schau dir den Abschnitt über Quellen und Materialien am Ende an, der hilft dir loszulegen. Und glaube mir, sobald du die Grundlagen gelernt hast, wird dir klar werden, dass es wirklich einfacher ist, als eine Informationsfreiheitsanfrage zu stellen.

2. Sicher bleiben

Das hier ist illegal, also musst du ein paar grundlegende Vorsichtsmaßnahmen treffen:

1. Lege dir eine versteckte, verschlüsselte Partition mit Truecrypt 7.1a an.
2. Installiere Whonix in der verschlüsselten Partition.
3. (Optional) Wahrscheinlich dürfte es ausreichen, mit Whonix alles über Tor laufen zu lassen. Besser ist es jedoch, keine Internetverbindung zu verwenden, die mit deinem Namen und deiner Adresse verknüpft ist. Eine Antenne, Aircrack und Reaver können hier nützlich sein.

Solange du deinen gesunden Menschenverstand benutzt – das heißt, nie etwas mit Hacking-Bezug außerhalb von Whonix machst, nie deine normale Computernutzung innerhalb von Whonix erledigst, keine Informationen über dein echtes Leben im Gespräch mit anderen HackerInnen erwähnst und nie mit deinen illegalen Hacker-Taten bei FreundInnen im echten Leben prahlst – dann kannst du so ziemlich alles tun, was du willst, ohne Angst zu haben.

HINWEIS: Ich empfehle, NICHT direkt über Tor zu hacken. Tor ist brauchbar für Dinge wie etwa im Internet zu surfen. Wenn es aber um die Verwendung

von Hacking-Tools wie nmap, sqlmap und nikto geht, die Tausende von Anfragen machen, laufen die nur sehr langsam über Tor. Außerdem wirst du eine öffentliche IP-Adresse wollen, um „connect back shells“ zu empfangen. Ich empfehle, über Server zu hacken, die du selbst gehackt hast oder über einen Virtual Private Server (VPS), den du mit Bitcoin bezahlt hast, zu hacken. So läuft nur die Textschnittstelle, die geringe Bandbreite braucht, zwischen dir und dem Server über Tor. Alle Befehle, die du ausführst, laufen über eine schöne, schnelle Verbindung zu deinem Ziel.

3. Das Ziel erkunden

Im Grunde benutze ich nur immer wieder fierce, Whois-Abfragen von IP-Adressen und Domain-Namen sowie Reverse-Whois-Abfragen, um alle IP-Adressbereiche und Domain-Namen zu finden, die mit einer Organisation verbunden sind.

Zum Beispiel Blackwater: Wir fangen an und wissen, dass ihre Homepage unter academi.com zu finden ist. Lassen wir „fierce.pl -DNS academi.com“ laufen, finden wir diese Subdomains:

```
67.238.84.228 email.academi.com 67.238.84.242 extranet.academi.com
67.238.84.240 mail.academi.com 67.238.84.230 secure.academi.com
67.238.84.227 vault.academi.com 54.243.51.249 www.academi.com
```

Jetzt machst du Whois-Abfragen und findest heraus, dass die Homepage von www.academi.com von Amazon Web Service gehostet wird, während die anderen IPs im folgenden Bereich liegen:

```
NetRange: 67.238.84.224 – 67.238.84.255 CIDR: 67.238.84.224/27 CustName:
Blackwater USA Adresse: 850 Puddin Ridge Rd
```

Eine Whois-Abfrage von academi.com verrät auch, dass sie unter der gleichen Adresse registriert ist, also verwendest du das als String (Zeichenfolge) für die Reverse-Whois-Suche. Soweit ich weiß, kosten alle tatsächlichen Reverse-Whois-Suchdienste Geld, also schummle ich einfach mit Google:

```
"‘850 Puddin Ridge Rd"’ inurl:ip-address-lookup "‘850 Puddin Ridge Rd"’
inurl:domaintools
```

Jetzt lässt du „fierce.pl -range“ über die IP-Bereiche laufen, um DNS-Namen nachzuschlagen und „fierce.pl -dns“ über die Domain-Namen, um Subdomains und IP-Adressen zu finden. Mache weitere Whois-Abfragen und wiederhole den Vorgang, bis du alles gefunden hast.

Google die Organisation auch einfach und stöbere auf ihrer Webseite herum. Beispielsweise findest du auf academi.com Links zu einem Karriere-Portal, einem Online-Shop, und einer Mitarbeiter-Infoseite, damit haben wir jetzt einige weitere:

```
54.236.143.203 careers.academi.com 67.132.195.12 academiproshop.com
67.238.84.236 te.academi.com 67.238.84.238 property.academi.com
67.238.84.241 teams.academi.com
```

Wenn du die Anfragen von Whois und anderen wiederholst, stellst du fest, dass academiproshop.com scheinbar nicht von Blackwater gehostet oder gewartet wird, sodass du es von der Liste der interessanten IPs/Domains streichen kannst.

Im Falle von FinFisher war es einfach eine Whois-Abfrage von finfisher.com, die mich zur ungeschützten Seite finsupport.finfisher.com geführt hat, weil sie auf denselben Namen „FinFisher GmbH" registriert war. Googelt man nach „FinFisher GmbH" inurl:domaintools, findet man gamma-international.de, was wiederum zu finsupport.finfisher.com weiterleitet.

Jetzt hast du eine grobe Idee, wie ich ein Ziel auskundschafte.

Das ist tatsächlich einer der wichtigsten Teile, denn je größer die Angriffsfläche ist, die du aufdeckst, desto leichter wird es sein, irgendwo darin ein Loch zu finden.

4. Scannen & Ausnutzen

Scanne alle IP-Bereiche, die du gefunden hast, mit nmap, um alle laufenden Dienste zu finden. Neben einem Standard-Port-Scan wird unterschätzt, nach SNMP zu scannen.

Jetzt, für jeden laufenden Service, den du findest:

Legt er etwas offen, was er nicht sollte? Manchmal lassen Unternehmen Dienste laufen, die keine Authentifizierung erfordern und gehen davon aus, dass es sicher ist, weil die URL oder IP, um darauf zuzugreifen, nicht öffentlich ist. Vielleicht hat fierce eine git-Subdomain gefunden und du kannst auf git.companyname.come/gitweb/ gehen und den Quellcode suchen.

Ist er schrecklich falsch konfiguriert? Vielleicht haben sie einen FTP-Server, der einen anonymen Lese- oder Schreib-Zugang zu einem wichtigen Verzeichnis erlaubt. Vielleicht haben sie einen Datenbank-Server mit einem leeren Admin-Passwort (lol Stratfor). Vielleicht verwenden ihre eingebundenen Geräte (VOIP-Boxen, IP-Kameras, Router, etc.) das Standardpasswort des Herstellers.

Läuft er mit einer alten Softwareversion, die für einen öffentlichen „Exploit" anfällig ist? Webserver verdienen eine eigene Kategorie. Für alle Webserver, darunter auch solche, die nmap oft auf Nicht-Standard-Ports findet, tue ich in der Regel Folgendes:

1. Klicke im Browser durch. Besonders auf Subdomains, die Fierce findet, die nicht für die Öffentlichkeit bestimmt sind, wie test.company.com oder dev.company.com, findet man oft interessante Sachen einfach nur beim Surfen.

2. Verwende nikto. Es wird Dinge wie webserver/.svn/, webserver/backup/, webserver/phpinfo.php und ein paar Tausend andere verbreitete Fehler und Fehlkonfigurationen überprüfen.
3. Finde heraus, welche Software auf der Webseite verwendet wird. WhatWeb ist nützlich.
4. Je nachdem mit welcher Software die Webseite läuft, verwende spezifischere Werkzeuge wie wpscan, CMS-Explorer, und Joomscan. Probiere das zunächst auf allen Diensten, um zu sehen, ob irgendeine Fehlkonfiguration, öffentlich bekannte Sicherheitslücke oder eine andere einfache Zugangsmöglichkeit besteht. Wenn nicht, wird es Zeit, eine neue Sicherheitslücke zu finden:
5. Kundenspezifisch programmierte Web-Apps sind ein fruchtbarerer Boden für Fehler als große, weit verbreitete Projekte, also versuche es dort zuerst. Ich benutze ZAP und einige Kombinationen seiner automatisierten Tests, zusammen mit händischem Herumstochern mit Hilfe des „Intercepting Proxy".
6. Besorg dir eine Kopie für die nicht-kundenspezifische Software, die sie verwenden. Wenn es freie Software ist, kannst du sie einfach herunterladen. Wenn sie proprietär ist, kannst du sie in der Regel raubkopieren. Wenn sie proprietär und so obskur ist, dass man sie nicht raubkopieren kann, kannst du sie kaufen (lame) oder über Google eine andere Webseite finden, die die gleiche Software verwendet und leichter zu hacken ist, und von dort eine Kopie ziehen.

Für finsupport.finfisher.com war es folgender Prozess:

- Nikto im Hintergrund laufen lassen.
- Die Webseite aufrufen. Nach einer Login-Seite schauen. Schnell mit sqli das Login-Formular checken.
- Nachschauen, ob WhatWeb weiß, auf welcher Software die Webseite läuft.
- WhatWeb kennt sie nicht, also will ich als Nächstes die Frage beantworten, ob es eine eigene Webseite von Gamma ist, oder ob es andere Webseiten mit der gleichen Software gibt.
- Ich schaue in den Quelltext der Seite und finde eine URL, nach der ich suchen kann (index.php ist nicht wirklich einzigartig für diese Software). Ich nehme Scripts/scripts.js.php und google: allinurl:"Scripts/scripts.js.php"
- Ich finde eine Handvoll anderer Seiten mit der gleichen Software, die alle von der gleichen kleinen Webdesign-Firma programmiert wurden. Es sieht aus, als wäre jede Webseite individuell programmiert, aber sie bestehen zu großen Teilen aus dem gleichen Quelltext. Also hacke ich ein paar davon, um Code von der Webdesign-Firma zu sammeln.

An dieser Stelle kann ich die Berichte der Journalisten vor mir sehen, die aufbauschend schreiben: „In einem raffinierten, mehrstufigen Angriff kompromittierten die Hacker erst eine Webdesign-Firma, um vertrauliche Daten zu erlangen, die ihnen dann beim Angriff auf die Gamma Group behilflich waren."

Aber es ist wirklich ziemlich einfach und fast auf Autopilot durchzuführen, sobald du den Dreh raus hast. Es dauerte nur ein paar Minuten, um „Scripts/scripts.js.php" zu googlen und die anderen Webseiten zu finden und festzustellen, dass sie alle für SQL-Injection anfällig sind, beim ersten URL-Parameter, den ich versuchte. Und zu realisieren, dass sie alle mit Apache ModSecurity laufen, weshalb ich sqlmap mit der Option „–tamper='Sabotage/modsecurityversioned.py" verwenden muss. Um die Admin-Login-Daten zu erlangen, mich einzuloggen, eine PHP-Shell hochzuladen (die Überprüfung für zulässige Dateinamenserweiterungen wurde auf Client-Seite in Javascript gemacht) und den Quellcode der Webseite herunterzuladen.

Bei einem Blick in den Quellcode stellte ich fest, dass sie es auch „verdammt anfällige Web App v2" hätten nennen können. Es hat SQL-Injection, Local File Inclusion, die Datei-Upload-Überprüfung wird vom Client in JavaScript gemacht, und wenn du nicht authentifiziert bist, schickt dich die Admin-Seite einfach wieder auf die Login-Seite mit einem Location-Header, den man mit einem „Intercepting Proxy" einfach herausfiltern kann und der Zugang funktioniert bestens.

Zurück auf der finsupport Seite antwortet die Admin-Seite /BackOffice/ mit „403 Forbidden" und ich habe einige Probleme mit der Local File Inclusion, also wechsle ich zu SQL-Injection (es ist schön, ein Dutzend Optionen zur Auswahl zu haben). Die anderen Webseiten der Webdesigner hatten alle eine print.php, in die man eigene Datenbankbefehle einschleusen konnte, also stellte ich einige schnelle Anfragen an:

```
https://finsupport.finfisher.com/GGI/Home/print.php?id=1 AND 1=1
https://finsupport.finfisher.com/GGI/Home/print.php?id=1 AND 2=1
```

Die zeigten, dass auch finsupport diese print.php hat und diese anfällig ist. Und es hat Adminrechte in der Datenbank! Für MySQL bedeutet das, du kannst Dateien lesen und schreiben. Es stellte sich heraus, dass die Seite magicquotes aktiviert hat, sodass ich „INTO OUTFILE" nicht verwenden konnte, um Dateien zu schreiben. Aber ich konnte ein kurzes Skript verwenden, das

- „sqlmap –file-read" verwendet, um den PHP-Quelltext für eine URL zu bekommen
- eine normale Web-Anfrage stellt, um das HTML zu bekommen
- Dateien findet, die im PHP-Quelltext enthalten oder erforderlich sind
- PHP-Dateien findet, die im HTML verlinkt sind

..., um rekursiv den Quelltext der gesamten Webseite herunterzuladen. Beim Durchschauen des Quelltexts sehe ich, dass Kunden an ihre Support-Tickets eine Datei anhängen können und es gibt keine Überprüfung der Dateierweiterung. Also suche ich mir einen Benutzernamen und Kennwort aus der Kundendatenbank, erstelle eine Support-Anfrage mit einer angehängten PHP-Shell und ich bin drin!

5. Rechte ausweiten (oder dabei versagen)

```
 _____________
}
< got r00t? >
-------
       \    ^__^
        \   (oo)\_______
            (__)\       )\/\
                ||--w |
                ||     ||
            ^^^^^^^^^^^^^^^^
```

Auf über 50 Prozent der Linux-Server da draußen kann man mit zwei einfachen Skripts – Linux_Exploit_Suggester, und unix-privesc-check – „root" erlangen, also Admin-Rechte.

Auf finsupport lief die aktuellste Version von Debian ohne lokale Root-Exploits, aber unix-privesc-check ergab:

```
WARNUNG: /etc/cron.hourly/mgmtlicensestatus wird von cron als root
ausgeführt. Der Benutzer www-data kann in
/etc/cron.hourly/mgmtlicensestatus schreiben WARNUNG:
/etc/cron.hourly/webalizer wird von cron als root ausgeführt. Der
Benutzer www-data kann in /etc/cron.hourly/webalizer schreiben
```

Also füge ich in /etc/cron.hourly/webalizer hinzu:

```
chown root:root /path/to/my\_setuid\_shell chmod 04755
/path/to/my\_setuid\_shell
```

Warte eine Stunde und - nichts. Es stellt sich heraus, dass obwohl der cron-Prozess läuft, scheinbar keine echten cron-Jobs ausgeführt werden. Im Webalizer-Verzeichnis zeigt sich, dass die Statistik seit letztem Monat nicht aktualisiert wurde. Offenbar wird cron nach einer Änderung der Zeitzone manchmal zur falschen Zeit oder manchmal gar nicht ausgeführt und muss nach Änderung der Zeitzone neu gestartet werden. ls -l /etc/localtime zeigt, die Zeitzone wurde am 6. Juni aktualisiert, zur gleichen Zeit hat Webalizer die Aufzeichnung der Statistiken gestoppt, also ist das wahrscheinlich das Problem. Jedenfalls ist das Einzige, was dieser Server macht, die Webseite auszuliefern, sodass ich bereits Zugang zu allem Interessanten darauf habe. Root würde nicht viel Neues bringen, also schaue ich mir den Rest des Netzwerks an.

6. Weiter umschauen

Der nächste Schritt ist, dich um das lokale Netzwerk der gehackten Box herum umzusehen. Das ist so ziemlich das Gleiche wie der erste „Scannen & Ausnutzen"-Schritt, außer dass hinter der Firewall viel mehr interessante Dienste offenliegen. Ein Tarball, der eine statisch gelinkte Kopie von nmap und all seinen Skripten enthält, die du hochladen und auf jeder Box laufen lassen kannst, ist dafür sehr praktisch. Die verschiedenen nfs-*- und insbesondere smb-*-Skripte, die nmap hat, werden extrem hilfreich sein.

Die einzige interessante Sache, die ich aus dem lokalem Netzwerk von finsupport ziehen konnte, war ein weiterer Webserver mit einem Ordner namens „qateam", der ihre mobile Malware enthielt.

7. Spaß haben

Sobald du im Netzwerk bist, beginnt der eigentliche Spaß. Verwende einfach deine Fantasie. Ich habe diese Artikel zwar als Anleitung für Möchtegern-Whistleblower bezeichnet, aber es gibt keinen Grund, dich auf das Leaken von Dokumenten zu beschränken. Mein ursprünglicher Plan war folgender:

- Gamma hacken, um eine Kopie der FinSpy-Server-Software bekommen.
- Schwachstellen in FinSpy-Server finden.
- Im Internet nach allen FinSpy command-and-control Servern (C&C) suchen und sie hacken.
- Die Gruppen, die sie betreiben, identifizieren.
- Die C&C-Server dazu verwenden, ein Programm auf alle Ziele hochzuladen und auszuführen, das ihnen sagt, von wem sie ausspioniert wurden.
- Die C&C-Server verwenden, um FinFisher auf allen Zielen zu deinstallieren.
- Die ehemaligen C&C-Server zu einem Botnetz verbinden, um Gamma Group zu DDoSen.

Erst als es mir nicht gelang, Gamma vollständig zu hacken, ich dafür einige interessante Dokumente aber keine Kopie der FinSpy-Server-Software hatte, musste ich ich mit dem weit weniger lustigen Backup-Plan anfreunden, ihr Zeug zu leaken und mich auf Twitter über sie lustig zu machen.

Richtet eure GPUs auf FinSpy-PC+Mobile-2012-07-12-Final.zip und crackt das Passwort, damit ich endlich mit Schritt 2 weitermachen kann!

8. Andere Methoden

Die allgemeine Methode, die ich oben beschrieben habe – also durchsuchen, Schwachstellen finden und diese ausnutzen – ist nur eine Möglichkeit zu hacken und wahrscheinlich eher für Menschen mit Programmierkenntnissen geeignet.

Es gibt nicht den einen richtigen Weg und jede Methode, die funktioniert, ist so gut wie jede andere. Diese anderen Wege will ich, ohne dabei ins Detail zu gehen, noch erwähnen:

1. Exploits in Web-Browsern, Java, Flash oder Microsoft Office in überzeugenden E-Mails an Mitarbeiter schicken, die sie dazu bewegen, den Link oder den Anhang zu öffnen. Oder eine Webseite hacken, die von den Mitarbeitern häufig besucht wird und den Browser/Java/Flash-Exploit dort einbauen.

Diese Methode wird von den meisten Regierungs-Hackergruppen verwendet, aber du musst keine Regierung mit Millionenbudgets für 0-Day-Forschung und FinSploit- oder VUPEN-Abonnements sein, um das durchzuziehen. Man bekommt ein qualitativ hochwertiges Exploit-Kit aus Russland für ein paar Tausender und für viel weniger kann man Zugang zu einem mieten. Es gibt auch Metasploit browser autopwn, aber wahrscheinlich hast du mehr Glück ohne Exploits und mit einer gefälschten Flash-Update-Nachricht.

2. Die Ausnutzung der Tatsache, dass die Menschen zu 95 Prozent nett, vertrauensvoll und hilfsbereit sind.

Die Informationssicherheits-Industrie hat dazu einen Begriff erfunden, um das wie eine Wissenschaft klingen zu lassen: „Social Engineering“. Das ist wahrscheinlich der beste Weg, wenn du nicht allzu viel über Computer weißt und es ist wirklich alles, was man braucht, um ein erfolgreicher Hacker zu sein.

Links

- https://www.pentesterlab.com/exercises/
- http://overthewire.org/wargames/
- http://www.hackthissite.org/
- http://smashthestack.org/
- http://www.win.tue.nl/~aeb/linux/hh/hh.html
- http://www.phrack.com/
- http://pen-testing.sans.org/blog/2012/04/26/got-meterpreter-pivot
- http://www.offensive-security.com/metasploit-unleashed/PSExec_Pass_The_Hash
- https://securusglobal.com/community/2013/12/20/dumping-windows-credentials/
- https://www.netspi.com/blog/entryid/140/resources-for-aspiring-penetration-testers (Alle seine anderen Blog-Beiträge sind auch großartig)
- https://www.corelan.be/ (Starte beim Exploit-Writing-Tutorial Teil 1)

- http://websec.wordpress.com/2010/02/22/exploiting-php-file-inclusion-overview/
- http://www.dest-unreach.org/socat/

Bücher

- The Web Application Hacker's Handbook
- Hacking: The Art of Exploitation
- The Database Hacker's Handbook
- The Art of Software Security Assessment
- A Bug Hunter's Diary
- Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier
- TCP/IP Illustrated

Abgesehen von Hacker-spezifischen Dingen hilft fast alles, was für einen Systemadministrator sinnvoll ist, um ein Netzwerk einzurichten und zu verwalten, auch dabei, es zu erkunden. Das umfasst unter anderem die Vertrautheit mit der Windows-Kommandozeile und der UNIX-Shell, grundlegende Scripting-Fähigkeiten, Kenntnisse von LDAP, Kerberos, Active Directory, Netzwerken usw.

10. Outro

Du wirst feststellen, dass einiges hier genauso klingt wie das, was Gamma macht. Hacken ist ein Werkzeug. Es ist nicht der Verkauf von Hacking-Tools, der Gamma böse macht. Es ist der Fakt, auf wen Gammas Kunden es abgesehen haben und zu welchem Zweck sie die Tools einsetzen, der sie böse macht. Das heißt nicht, dass Werkzeuge automatisch neutral sind. Hacken ist ein offensives Werkzeug. Genauso wie Guerilla-Kriegsführung es schwieriger macht, ein Land zu besetzen: Immer, wenn Angriff billiger ist als Verteidigung, ist es schwieriger, illegitime Autorität und Ungleichheit aufrecht zu halten. Deswegen habe ich diesen Artikel geschrieben, um Hacken ein Stück einfacher und zugänglicher zu machen. Und ich wollte zeigen, dass der Hack der Gamma Group wirklich nichts Besonderes war – es war nur eine normale SQL-Injection – und dass du die Möglichkeit hast, rauszugehen und ähnliche Aktionen zu starten.

Solidarität mit allen in Gaza, israelischen Kriegsdienstverweigerern, Chelsea Manning, Jeremy Hammond, Peter Sunde, anakata und allen anderen inhaftierten Hackern, Dissidenten und Verbrechern!

Dieser Beitrag wurde zuerst auf Pastebin veröffentlicht.

@GammaGroupPR ist ein Pseudonym des Hackers von Gamma FinFisher.

11 Nehmt euch die Kontrolle über eure privaten Daten zurück!

von **Hannes Mehnert**

Enthüllungen von Whistleblowern belegen, dass Ermittlungsbehörden Zugriff auf persönliche Daten wie Adressbücher, Freundeslisten und Kommunikationsmetadaten haben und diese großflächig auswerten. Viele Menschen vertrauen diese Daten großen Konzernen wie Apple, Facebook, Google oder Microsoft an[1]. Die Services dieser Konzerne kosten meist kein Geld, allerdings räumen sich die Konzerne verschiedenste Rechte an den gespeicherten Daten ein. Die Konzerne analysieren diese Daten akribisch für personalisierte Werbung, Empfehlungssysteme, etc.

Aber vor allem haben die Menschen keine Kontrolle mehr über ihre Daten – die Konzerne haben ihren Sitz meist in den Vereinigten Staaten von Amerika und arbeiten dort mit den Ermittlungsbehörden zusammen (freiwillig oder unfreiwillig per FISA-Urteil). Oft ist lediglich die Verbindung zwischen Endgerät und Server verschlüsselt, aber die Daten befinden sich auf dem Server im Klartext.

Das Benutzen dieser Services ist bequem, viel einfacher und weniger zeitaufwendig als einen eigenen Service aufzusetzen, bei dem mensch sich auch noch fortlaufend um die Administration kümmern muss. 2014 gab es diverse Schwachstellen in offener Software (Heartbleed, Shellshock, ...), sodass die Leute, die eigene Services betreiben, immer wieder Wochenenden mit Softwareupdates verbringen mussten.

Ich werde das Forschungsprojekt Nymote[2] der University of Cambridge vorstellen. In diesem wollen wir Menschen (auch Nicht-ExpertInnen) ermöglichen, die Kontrolle über ihre persönlichen Daten wieder zu erlangen. Die Grundlage dafür stellt Mirage OS[3] dar, ein von Grund auf neu entwickeltes modulares Betriebssystem. Jedes sogenannte Unikernel beinhaltet nur die Funktionalität, die es wirklich braucht; so wird zum einen der Code kleiner, zum anderen das System einfacher zu konfigurieren und zu warten. Mirage OS wird in der funktionalen Programmiersprache OCaml entwickelt, dadurch werden einige Fehlerklassen vermieden, die oft zu Sicherheitsproblemen führen.

Motivation

Kaum ein Mensch in der westlichen Welt lebt heutzutage ohne einen Computer, den er zum kommunizieren via Internet benutzt. Leider sind einige ursprüngliche Eigenschaften des Internets – wie dezentrale Datenspeicherung und jedeR ist Service-nehmerIn und Service-anbieterIn – auf der Strecke geblieben. Einige Ursachen dafür, dass viele Menschen nur Service-Nehmende sind, sind die Konfigurations- und Administrations-Komplexität von Services und Bequemlichkeit.

Das Grundrecht auf digitale Intimsphäre soll persönliche Daten, die in Computern gespeichert sind, schützen. Dieses gilt allerdings nur auf deutschem Bo-

den. Besonders junge Menschen erleben einen Großteil ihrer Privatsphäre online – statt Tagebücher schreiben sie anonym Blogs, statt Telefonketten werden Aufrufe via Twitter oder Facebook verbreitet. Die Ansage, Privates mit FreundInnen im Wald zu besprechen ist realitätsfern, da FreundInnen möglicherweise gerade auf der anderen Seite der Welt leben. Ich kenne einige Leute in Neuseeland besser als meine direkten NachbarInnen in Berlin.

In der Praxis sind verschiedene Entitäten an der Kommunikation beteiligt – um konkret zu werden, betrachten wir das föderale und asynchrone E-Mail-System: Anna will Arthur eine Nachricht schicken. Nehmen wir an, Anna hat ein Postfach bei Gmail, Arthur ist bei Yahoo. Somit sendet Anna die Nachricht an Gmail, Gmail leitet sie an Yahoo weiter, und Arthur ruft sie vom Yahoo-Server ab. Wenn die Nachricht von Anna an Arthur verschlüsselt ist (beispielsweise mit OpenPGP), ist der Inhalt nur für Anna und Arthur lesbar. Allen Beteiligten, Yahoo, Gmail, Anna und Arthur, liegen die sogenannten Metadaten der Kommunikation vor: Anna und Arthur haben kommuniziert, der genaue Zeitpunkt, möglicherweise auch noch wo sich Anna und Arthur gerade befinden.

Wenn wir die Entitäten, bei denen Daten anfallen, vermindern, müssen wir weniger Entitäten vertrauen. Das wichtigste Credo der OpSec (Operations Security) ist „need to know“: jede Entität bekommt nur die Informationen, die sie zwingend benötigt, um ihre Aufgabe zu erfüllen. Wenn also Anna und Arthur ihre eigenen Mailserver betreiben, sind Gmail und Yahoo außen vor und wir müssen ihnen nicht vertrauen. Ein weiteres Argument dafür, dass jedeR einen eigenen Mailserver betreiben sollte, ist, dass das Abschalten von Lavabit hunderte Menschen betraf, nicht nur Edward Snowden.

Zurück zum Anfang: Warum verwalten Menschen nicht ihre eigene Services? Die Komplexität ist hoch: Zum einen setzt es Wissen voraus bezüglich des verwendeten Betriebssystems (was ist ein Dateisystem, was sind BenutzerInnenrechte, etc.), sowie bezüglich der eingesetzten Software – wo muss da welches TLS-Zertifikat konfiguriert werden und welche Rechte braucht dieses? Und weiter – wer kümmert sich um zeitnahe Softwareupdates und was, wenn das mal schiefgeht?

Im Jahre 2014 gab es diverse Schwachstellen in offenen Implementierungen von Sicherheitsprotokollen – angefangen mit goto fail von Apple, Heartbleed in OpenSSL, etc. (Quell)offene Software bedeutet nicht zwingend, dass diese sicher ist oder dass irgendwer diese auf Schwachstellen durchschaut. Offene Software ist aber eine zwingende Voraussetzung, um qualifizierte Aussagen über Sicherheit treffen zu können. Im Gegensatz zu anderer kritischer Infrastruktur (Straßen, Wasser- und Stromleitungen, etc.) werden kritische Softwarekomponenten nicht gefördert[4].

Utopie

Ich möchte in einer Welt leben, in der Menschen in der Lage sind, Kontrolle über ihre Daten zu haben. In einer Welt, in der keine großen Konzerne durch das kostenlose Anbieten von Services an die sozialen Netzwerke von Individuen kommen. Eine Welt, in der das Teilen von Ressourcen (Speicherplatz, Netzanbindung) nicht denen vorbehalten ist, die eine Ausbildung in UNIX-Systemadministration abgeschlossen haben (um remote access zu konfigurieren und zu benutzen). Eine Welt, in der mensch sich nicht durch Berge von Werbung klicken muss (die alle fleißig Daten sammeln), nur um die Urlaubsbilder von FreundInnen herunterzuladen. Um diese Utopie zu realisieren, brauchen wir radikale Ansätze. Es ist nicht mit ein paar Zeilen Shell-Skript oder PHP getan. Die inhärente Komplexität beim Betreiben von Services heutzutage müssen wir massiv vereinfachen.

In dieser Welt können dann endlich Menschen frei über alles kommunizieren, ohne sich fürchten zu müssen, dass dieses mitgelesen und ausgewertet wird. Eine freie Welt ist nur mit freier Kommunikation möglich und wenn Menschen direkte Kontrolle über ihre Daten haben.

Der Weg ins Paradies

Statt mit herkömmlichen universellen Betriebssystemen Services zu betreiben, entwickeln wir sogenannte Unikernel: Dies sind spezialisierte Betriebssysteme, die exakt auf den zu betreibenden Service zugeschnitten sind. Die Komplexität des UNIX-Kernels, von Sockets, Prozessen, Programmiersprachenumgebung, Threading, tatsächlicher Applikation und Konfiguration im Dateisystem wird in Mirage OS auf ein Unikernel reduziert. Ein Unikernel ist eine Applikation, die wahlweise als Xen-Gastbetriebssystem (ohne UNIX-Kernel oder libc) oder direkt auf UNIX ausgeführt werden kann. Die Konfiguration findet in einer domänenspezifischen Sprache statt und wird direkt zur Kompilierzeit ausgewertet (und kann für Optimierungen benutzt werden).

Mirage OS ist ein Betriebssystem, das zur Zeit vor allem an der University of Cambridge entwickelt wird. Es steht unter einer BSD/MIT/ISC-Lizenz. Es ist in der modularen und funktionalen Programmiersprache OCaml implementiert. Module in OCaml sind eigenständige Entitäten, und auch auf deren Ebene kann programmiert werden. OCaml ist stark typisiert und hat ein ausdrucksstarkes Typsystem – viele Fehler werden schon zur Kompilierzeit erkannt. OCaml benutzt automatische Speicherverwaltung – ganze Fehlerklassen wie Buffer Overflows werden so vermieden. Seiteneffekte wie Kommunikation mit dem Netzwerk, Fehlerbehandlung, etc. werden (nach Konvention) explizit gekapselt: Es ist viel einfacher, ein Programm zu verstehen, da kein anderes Programmfragment Speicher verändert.

Wir werden Mirage OS in die heutige Service-Welt integrieren, indem wir die locker spezifizierten Netzwerkprotokolle implementieren, damit Mirage OS mit

den anderen Services kommunizieren kann. Um nicht direkt mit der Programmierung von Gerätetreibern anfangen zu müssen, benutzen wir Xen als Virtualisierungsplattform und haben die virtuellen Netzwerk- und Konsolentreiber implementiert.

Als Bibliotheken haben wir schon einen TCP/IP-Stack, DNS, HTTP, TLS, XMPP, IMAP und vieles mehr. Die Unterstützung von IPv6 ist in Sicht und wird voraussichtlich noch 2014 integriert. Zum Verwalten von Daten haben wir eine persistente Datenspeicherung implementiert, ähnlich dem Versionsverwaltungssystem git. Es basiert auf einem Graphen, der immer nur erweitert wird (kein veränderbarer Zustand!) – ältere Versionen sind immer verfügbar! – und einer Notiz, welches der aktuelle Graph ist.

Als Zielplattform dient momentan ein kleines (50 Euro) ARM-Board (Cubieboard 2). Unsere Idee ist, dass mensch sich sowas zuhause an die Internetverbindung anschließt und dort die privaten Daten, wie E-Mail, Adressbuch und Kalender, lagert. Auch an einer verschlüsselten und vertrauenswürdigen Vernetzung dieser Systeme untereinander (wenn sich Annas Telefonnummer ändert, soll diese sich auch in den Adressbüchern von Annas Freunden ändern) wird aktuell geforscht – zuerst mithilfe von DNS, DNScurve und DNSSec, wobei DNS hier eine zentrale hierarchische Komponente darstellt, die wir hoffentlich durch verteilte Hashtabellen ersetzen werden.

Auf dem Weg zu diesen Unikernels haben wir viele Protokolle implementiert. Und natürlich machen auch wir Fehler. Von daher erforschen wir auch das automatisierte Erstellen von Tests, bei denen wir dann verschiedene Implementierungen des gleichen Protokolls miteinander testen. So etwas gibt es bei vielen Protokollen nicht – TCP/IP hat keine solche Testsuite, TLS auch nicht – obgleich es das meist verwendete Sicherheitsprotokoll im Internet ist und es schon seit 15 Jahren existiert. Durch unsere Implementierung ohne Seiteneffekte wollen wir gültige und fehlerhafte Sequenzen von Eingaben und erwarteten Ausgaben erzeugen, die den Zustandgraphen ablaufen und teils zufällige Pakete erzeugen. So wollen wir das Vertrauen in unsere Protokollimplementierungen erhöhen und die Qualität anderer steigern, indem wir die gefundenen Unstimmigkeiten den EntwicklerInnen melden.

Welchen Komponenten muss für Mirage vertraut werden? Angefangen bei der Hardware (CPU, Netzwerkkarten, etc.), die wir nicht selbst entwickeln (aus Zeit- und Interessensgründen), über den OCaml-Compiler und der OCaml-Laufzeitumgebung, die in C geschrieben ist (somit muss auch dem C-Compiler vertraut werden). Auch dem Xen-Hypervisor und Linux-Netzwerkkartentreibern, die wir benutzen und virtualisiert an die Unikernels durchreichen, muss vertraut werden.

Agenda: An die Keyboards

Was immer noch zu tun ist, sind verschiedenste Protokolle zu implementieren und Interoperabilität mit bestehenden Implementierungen und Geräten auszuprobieren. Auch Menschen, die Code lesen, um Unklarheiten oder mögliche Schwachstellen aufzudecken, sind gern gesehen.

Das Ausprobieren bestehender Projekte und deren Installationsanleitungen[5] ist immer gut. Es finden sich sicherlich Probleme und Unzulänglichkeiten, sowohl in der Software als auch in den Anleitungen.

Es ist auch jetzt an der Zeit, Projekte wie ein Weblog oder ein Wiki anzufangen. Sowohl die Mailingliste mirageos-devel@lists.xenproject.org als auch der IRC-Channel #mirage auf irc.freenode.net sind offen und hilfreich.

Da wir an Services in einer einzigen Programmiersprache denken, ist allerdings das Lernen von OCaml eine Voraussetzung[6]. Aber Diversität von Programmiersprachen, die einE EntwicklerIn beherrscht, ist nie verkehrt.

Also: An die Tasten! Eine andere Welt ist möglich! Nimm dir die Kontrolle über deine Daten zurück!

Anmerkungen

[1] https://code.nadir.org/nhome//news/Pl ProzentC3 ProzentB6tzlich_plappern_Anna_und_Arthur.html

[2] http://nymote.org

[3] http://openmirage.org; *Unikernels: Rise of the Virtual Library Operating System*. https://queue.acm.org/detail.cfm?id=2566628

[4] Die angedachten 1,6 Millionen sind da ein Tropfen auf den heißen Stein. https://twitter.com/Senficon/status/524894994336055296

[5] *OCaml-TLS Workshop-Paper*. http://itu.dk/~hame/tls-ocaml2014.pdf; *Blogbeitrag*. http://openmirage.org/blog/introducing-ocaml-tls; *Code*. https://github.com/mirleft/; *OTR-Code*. https://github.com/hannesm/ocaml-otr

[6] *Beginner's guide to OCaml beginner's guides*. http://blog.nullspace.io/beginners-guide-to-ocaml-beginners-guides.html; *Awesome OCaml*. https://github.com/rizo/awesome-ocaml

Hannes Mehnert arbeitet in verschiedenen Bereichen der Programmiersprachenforschung: von Compileroptimierungen in Dylan über einen TCP/IP-Stack inklusive einer Domain-Specific Language für Binärprotokolle bis hin zu einer Erweiterung des Editors Emacs zur interaktiven Entwicklung von Idris-Code. In seiner Dissertation forschte er an Korrektheitsbeweisen von Java Code. In seiner Freizeit ist er nicht nur Hacker sondern auch leidenschaftlicher Barista; benutzt am liebsten das Betriebssystem FreeBSD, fährt und repariert gern sein Liegerad, und schrieb 2013 auch mit an dem Curry-Buch (O'Reilly) über funktionale Programmierung in JavaScript.

12 Vor Windows 8 wird gewarnt

von **Rüdiger Weis**

Bei der Einführung von Windows 8 versucht Microsoft ein weiteres Mal eine von Microsoft kontrollierte Umgestaltung der PC-Welt. Mittels Secure Boot und Trusted Computing verlieren die Besitzer sehr weitgehend die Kontrolle über die vormals persönlichen Computer. Was für den Privatanwender eine kartellrechtlich problematische Einschränkung darstellt, ist für die Industrie insbesondere im Zusammenhang von eingebetteten Systemen (*Industrie 4.0*) völlig unakzeptabel. Während innerhalb der Bundesregierung noch diskutiert wird, in wie weit vor Windows 8 gewarnt wird, verbot die Volksrepublik China kurzerhand den Einsatz von Windows 8 auf staatlichen Computern. Abhilfe kann nur durch eine alternative Vertrauensinfrastruktur und quelltextoffene Realisierung in Hardware und Software geleistet werden. Hier sind insbesondere auch staatliche Stellen in einer unmittelbaren Bringschuld.

Der von vielen schon leichtfertigerweise für abgewehrt gehaltene Angriff der Computer-Industrie auf die Kontrolle bisher persönlicher Computer muss seit der Einführung von Windows 8 neu bewertet werden. Microsoft versucht den Nutzern eine neue, von Microsoft kontrollierte Sicherheitsarchitektur aufzuzwingen. Hierbei soll ein Trusted Computing Modul (TPM) in die persönlichen Computer und Mobilgeräte eingebaut werden. Dieses enthält einen Schlüssel, auf den der Besitzer des Computers keinen Zugriffs hat.

Zusammen mit den nun von Microsoft implementierten Verfahren innerhalb von Windows 8 (insbesondere Secure Boot) wird dem Nutzer weitgehend die Kontrolle über seine eigene Hardware und Software entzogen.

Ähnlich analysierte das Bundesamt für die Sicherheit in der Informationstechnik in einer „Stellungnahme des BSI zur aktuellen Berichterstattung zu MS Windows 8 und TPM“:

> Aus Sicht des BSI geht der Einsatz von Windows 8 in Kombination mit einem TPM 2.0 mit einem Verlust an Kontrolle über das verwendete Betriebssystem und die eingesetzte Hardware einher. Daraus ergeben sich für die Anwender, speziell auch für die Bundesverwaltung und kritische Infrastrukturen, neue Risiken.[1].

Es erinnert fatal an eine elektronische Fußfessel. So kann beispielsweise über das Netz angefragt werden, ob nur genehmigte Software läuft. Das Ende der persön-

lichen Computer und Smartphones. Es klingt wie aus einem Traum für außer Kontrolle geratene Geheimdienste und repressive Staaten.

Kryptographische Probleme im Trusted-Computing-Standard

Erschreckenderweise muss festgestellt werden, dass weiterhin die wissenschaftlichen unstrittigen Kritikpunkte an der Algorithmenauswahl (insbesondere die Weiterverwendung der gebrochenen Hashfunktion SHA1) und der unzureichenden Schlüssellänge (2048 bit RSA) auch in den neueren Standardaausarbeitungen weitgehend ignoriert wurden.

Unzureichende Schlüssellängen

Der TC-Standard verwendet eine Schlüssellänge von 2048 bit für die RSA-Verfahren. Angesichts der Wichtigkeit dieser Schlüssel und der oft langen Verwendungszeiten insbesondere im Bereiche kritischer Infrastrukturen, ist diese Entscheidung nicht nachvollziehbar.

Beispielsweise empfiehlt das BSI mindestens 3072 bit selbst für mittelfristige Sicherheit.

Gebrochene Hashfunktionen

Wirklich düster sieht die Lage bei Hashfunktionen aus. Hashfunktionen sind wichtige Bausteine von kryptographischen Systemen, denen bisher relativ geringe Aufmerksamkeit gewidmet wurden. Dies ist auch deshalb überraschend, da Schwächen von Hashfunktionen beispielsweise für das Fälschen von Zertifikaten ausgenutzt werden können, selbst wenn die eigentliche Signaturfunktion sicher ist.

Gegen Hashfunktionen gab es in der öffentlichen Forschung einige dramatische Durchbrüche. Fast alle in Anwendung befindlichen Hashfunktionen stammen von Ron Rivests MD4-Hashfunktion ab. Gegen MD4 gab es schon früh Sicherheitsbedenken, MD5 und SHA1 ergänzten Operationen zur Erhöhung der Sicherheit. MD4 ist inzwischen mit Bleistift und Papier brechbar. MD5 und SHA1 sind ebenfalls schon mit überschaubarem Aufwand praxisrelevant angreifbar.

Eine Analyse von stuxnet ergab, dass die NSA wohl über Techniken zum Angriff auf die MD4-basierte Hashfunktionen-Familie verfügt, die in der öffentlichen Forschung bisher so nicht bekannt waren.

Auch das inzwischen angewendete und bisher noch nicht gebrochene SHA2-Verfahren stammt aus dem Hause der NSA und ist ähnlich konstruiert. Das neue Hashverfahren SHA3 wurde in einem offenen, transparenten Wettbewerb ausgewählt und ist bewusst völlig anders konstruiert.

Trotz zahlreicher Einwände unter anderem von DIN- Arbeitsgruppen erlauben auch neuere Versionen des Trusted Computing Standards selbst die Verwendung des gebrochenen SHA1.

Kryptographen warnen vor Trusted Computing Architektur

Whitfield Diffie, einer der Entdecker der Public-Key-Kryptographie, zeigte sich besorgt über die dominierende Stellung von Microsoft und forderte, dass die Benutzer die vollständige Kontrolle über die Schlüssel des eigenen Computers behalten sollten:

> The Microsoft approach) lends itself to market domination, lock out, and not really owning your own computer.
>
> To risk sloganeering, I say you need to hold the keys to your own computer.

Auch Ron Rivest mahnte eindringlich, die möglichen Konsequenzen gründlich abzuwägen:

> We should be watching this to make sure there are the proper levels of support we really do want.
>
> We need to understand the full implications of this architecture. This stuff may slip quietly on to people's desktops, but I suspect it will be more a case of a lot of debate.

„Sabotageakte Dritter"

Wenn Wirtschaft und Behörden mittels Windows und Trusted Computing eine Sicherheitsinfrastruktur aufbauen, können die US-Behörden im Zweifelsfall die völlige Kontrolle übernehmen.

> Darüber hinaus können die neu eingesetzten Mechanismen auch für Sabotageakte Dritter genutzt werden. Diesen Risiken muss begegnet werden., BSI, August 2013

Angesichts der Tatsache, dass wiederholt Druck auf Hersteller ausgeübt wurde, Hintertüren einzubauen, wirkt die Idee, dass ein Schlüssel vom Benutzer nicht ersetzt werden kann, sehr bedrohlich. Besonders brisant ist, dass die geheimen Schlüssel während des Herstellungsprozesses außerhalb des Chips erzeugt und danach in den Chip übertragen werden. Hier ist es trivial, eine Kopie aller Schlüssel herzustellen. Es ist nicht auszuschließen, dass entsprechende Rechtsvorschriften bestehen und über diese nicht berichtet werden darf.

Das andere realistische Szenario, dass der TPM-Hersteller nicht in der Reichweite der NSA, sondern beispielsweise in der Volksrepublik China sitzt, kann nicht wirklich beruhigen.

Da neben den Überwachungsmöglichkeiten auch die Wahlmöglichkeiten der Nutzer eingeschränkt werden, stellen sich natürlich kartell- und verbraucherrechtliche Fragen. Unter anderem die Tatsache, dass Microsoft die übliche Praxis verlassen hat und den Überwachungschip bei den modernen ARM-Systemen automatisch einschaltet und nicht mehr ausschalten lässt, verstößt unter anderem gegen das Eckpunktepapier des Bundesinnenministeriums zur vertrauenswürdigen Technikgestaltung.

Secure Boot Probleme für Linux

Nachdem die Einführung einer Microsoft-kontrollierten Sicherheitsinfrastruktur durch politischen Widerstand lange aufgehalten werden konnte, hat Microsoft ein weiteres Mal in Geheimverhandlungen Fakten geschaffen. In den Hardwareanforderungen für Windows 8 wird Secure Boot verpflichtend vorausgesetzt. Alternative Betriebssysteme können in der Praxis bisher nur mit technisch und rechtlich nicht unproblematischen Notkonstruktionen gestartet werden.

Microsoft kann und hat auch ohne nachvollziehbare Begründung konkurrierende Bootloader deaktiviert. Ein Szenario, dass Microsoft (möglicherweise durch US-Regierungsdruck) die Berechtigung, die von Microsoft unterschriebenen Bootloader für Linux-Distributionen zurückzieht, will man sich insbesondere für sicherheitskritische Systeme oder eingebettete Systeme nicht wirklich vorstellen.

> Insbesondere können auf einer Hardware, die mit einem TPM 2.0 betrieben wird, mit Windows 8 durch unbeabsichtigte Fehler des Hardware- oder Betriebssystemherstellers, aber auch des Eigentümers des IT-Systems Fehlerzustände entstehen, die einen weiteren Betrieb des Systems verhindern. Dies kann soweit führen, dass im Fehlerfall neben dem Betriebssystem auch die eingesetzte Hardware dauerhaft nicht mehr einsetzbar ist. Eine solche Situation wäre weder für die Bundesverwaltung noch für andere Anwender akzeptabel., BSI, August 2013, a.a.O..
>
> Während deutsche Behörden darüber diskutieren, wie sehr vor Windows 8 gewarnt werden sollte, *verbot die Volksrepublik China Windows 8 auf staatlichen Computern*.

Alternative Vertrauensanker

Es erscheint zwingend notwendig, Alternativen zum Vertrauensanker von Microsoft zur Verfügung zu stellen. Aus technischen Gründen ist dies sogar deswegen notwendig, weil Microsoft mit einer Schlüssellänge von 2048 bit arbeitet, welche vom BSI nicht für langfristige Sicherheit empfohlen wird.

> Für den staatlichen Bereich könnte beispielsweise die Bundesnetzagentur eine führende Position einnehmen. Hier sind im Zusammenhang mit dem Signaturgesetz schon erhebliche Vorarbeiten vorgenommen worden.
>
> Für nichtstaatliche Bereiche erscheint eine gemeinnützige Stiftung außerhalb der USA die bessere Lösung. Ähnliche Diskussionen werden bereits zu ICANN und DNSSEC Rootzonenschlüssel geführt.

Die Kryptographieforschung hat Lösungen für feingranulare Sicherheitspolitiken mit mathematisch beweisbaren Sicherheitseigenschaften entwickelt. Beispielsweise können Vertrauensbeziehungen durch mehre mögliche Stellen dezentralisiert werden oder eine Zusammenarbeit von mehren Instanzen erforderlich gemacht werden.

Hintertüren in Closed Source Soft- und Hardware

> Remember this: The math is good, but math has no agency. Code has agency, and the code has been subverted, Bruce Schneier, 5. September 2013

Es gibt ein eigenes Teilgebiet der Kryptographie namens *Kleptographie*, welches sich unter anderem mit dem sicheren Stehlen von Geheiminformationen durch Manipulation von Software und Hardware beschäftigt. Ohne Einsicht in den Source-Code und das Hardware-Design ist der Angegriffene beweisbar hilflos.

> Nach Snowden ist dollargenau bekannt, dass die Geheimdienste über einen Milliarden-Etat verfügen, um die Sicherheit von kommerzieller Software und Geräten mit Hintertüren zu versehen. Lesbarer Quellcode und aufmerksame Entwickler bieten hiergegen Sicherheit.

Lesbarer Quellcode

Während über die Notwendigkeit der ausschließlichen Verwendung von Open-Source-Programmen für sicherheitskritische Bereiche noch kontrovers diskutiert wird, ist die schwächere „Lesbarer Quellcode“-Forderung innerhalb der Wissenschaftsgemeinde unumstritten. Ohne die Möglichkeit, den Quellcode zu überprüfen, ist es faktisch unmöglich, Hintertüren zu entdecken.

Lesbarer Quellcode bedeutet nicht zwangsläufig die Verwendung einer offenen Lizenz. Auch veröffentlichter Quellcode kann unter kommerzielle Lizenzen gestellt werden, die die Verwendung und Weitergabe nahezu beliebig einschränken können. Dies ist seit Langem gängige Praxis, wie die Beispiele PGP und CryptoPhone zeigen.

Shared Code Probleme

Shared-Code-Initiativen für Windows, die beispielsweise Microsoft mit verschiedenen Regierungen vereinbart hat, bieten geringeren Schutz, da nicht die gesamte kryptographische Forschungsgemeinde an der Sicherheitsanalyse teilnehmen kann.

> Die freie Forschung arbeitet besser als ihre Gegenspieler im Verborgenen und tut dies in der Regel kostenlos für (akademischen) Ruhm und Ehre.
>
> Ein exklusiver Quellcode-Zugang für Regierungen ist problematisch, da viele Dienste diesen Wissensvorsprung für Angriffe missbrauchen.

Open Source schließt Sicherheitslücken schneller

Open-Source-Programme bieten den wichtigen Vorteil, dass beim Schließen von Sicherheitslücken nicht auf den Hersteller gewartet werden muss. Die Zeit zwischen der Veröffentlichung einer Sicherheitslücke und des Schließens dieser durch den Hersteller ist unstrittig die Zeit der höchsten Gefährdung. In der Praxis sind derartige Hochrisikozeiten von mehreren Monaten nicht unüblich.

Konsequenzen aus der OpenSSL-Katastrophe

Die 2014 aufgedeckte Sicherheitskatastrophe in der für die Internetkommunikation systemrelevanten Open-SSL-Implementierung zeigt einen unmittelbaren Handlungsbedarf.

> Da staatliche Stellen häufig Open Source Lösungen einsetzen und damit selbst nach konservativen Schätzungen Milliardeneinsparungen realisieren, besteht wegen der Sorgfaltspflicht eine staatliche Verpflichtung, hier für eine Grundsicherheit zu sorgen.

Staatsaufgabe Sicherheit in der Informationstechnik

Die politische und juristische Frage, ob Regierungen Cyberangriffswaffen („Bundes-Trojaner“) zum Schutze hoher Rechtsgüter entwickeln dürfen oder dies verfassungsrechtlich inakzeptabel ist, wie ein entsprechendes Urteil des Bundesverfassungsgericht nahe legt, soll an dieser Stelle nicht diskutiert werden. Aus wissenschaftlicher Sicht muss jedoch in diesem Falle auf ein technisches und organisatorisches Problem hingewiesen werden, das beispielsweise bei der Einblickgewährung in den Windows-Quellcode auftritt.

Die Kenntnis des Quellcodes erleichtert es Angreifern ganz erheblich, ausnutzbare Schwachstellen zu finden. Hier haben staatliche Stellen, die neben dem Schutz der Anwender auch aktive Angriffe entwickeln, einen nicht auflösbaren Zielkonflikt.

> Aus diesem Grunde sollten staatliche Stellen die digitale Verteidigung von Bürgern und Wirtschaft organisatorisch strikt von der Entwicklung von Cyberangriffswaffen trennen.

Die Bundesregierungen haben diesen Punkt schon recht früh durch die Gründung des Bundesamtes für Sicherheit in der Informationstechnik teilweise adressiert. Hier erscheint es sinnvoll eine weitere organisatorische Stärkung, etwa durch die Konstitution einer eigenen Bundesbehörde, umzusetzen.

Diese könnte sich etwa an den Reformvorschlägen der Bundesdatenschutzbeauftragten Andrea Voßhoff zur organisatorischen Ausgestaltung und Stärkung der Unabhängigkeit des Bundesdatenschutzbeauftragten oder dem seit 2000 bestehenden Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein anlehnen.

> Eine unabhängige Bundesbehörde für die Sicherheit in der Informationstechnik könnte, wie bereits seit Jahrzehnten der Datenschutz, ein international beachtetes Modell darstellen.

Wissenschaftliche Empfehlungen

Aus der Sicht der theoriekundigen Praktiker und der praktisch orientierten Theoretiker ergiben sich überraschend einfache Empfehlungen mit zu vernachlässigenden Kosten:

Starke Kryptographie mit extra Sicherheitsspielraum.

Dies bedeutet auf der Algorithmenebene beispielsweise:

- Verwendung von 256 bit Schlüssellänge für AES
- Schlüssellänge größer gleich 4096 bit für RSA

- 512 bit Hash-Funktionen

Ohne volle Schlüsselkontrolle für die Anwender und ohne lesbaren Code und offene Hardware helfen die besten kryptographischen Verfahren natürlich nicht gegen Geheimdiensthintertüren.

- Open Souce fördern.
- Open Source Sicherheit als Staatsaufgabe wahrnehmen

Kryptographie ist eine notwendige Technologie zum Schutz des freiheitlich-demokratischen Gemeinwesens. Trotz der viel diskutierten Angriffe ist es stets die schlechteste Lösung, ungeschützt zu kommunizieren.

Open-Source-Software bietet die Möglichkeit zum Auffinden von Hintertüren und Programmierfehlern. Eine Grundsicherheit für systemrelevante Open-Source-Programme sollte als Staatsaufgabe wahrgenommen werden.

Kryptographie und Offene Software sind mächtige Werkzeuge, um die digitale Gesellschaft menschenwürdig zu gestalten.

Anmerkungen

[1] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Windows_TPM_Pl_21082013.html

Rüdiger Weis ist Diplom-Mathematiker und Kryptograph. Er lebt und arbeitet in Berlin-Wedding und ist Professor für Informatik an der Beuth-Hochschule für Technik Berlin.

13 I Was Looking To See If You Were Looking Back At Me To See Me Looking Back At You

von **Katharina Meyer**

Abbildung 12: What are you looking at? Stencil von Banksy – Fotografie von nolifebeforecoffee / CC BY 2.0

(Überwachungs-)Kunst, der große Bruder, Sphären und das Ich

Turn, Turn, Turn (und am Ende: YOUturn[1]: Seit Dekaden durchlaufen die Sozial- und Kulturwissenschaften sogenannte „turns", die als Gelenkstellen fächerübergreifend Forschungsperspektiven und Theorietransformationen fokussieren.

Auf Linguistic Turn („Sprache konstruiert Gesellschaft") folgte der Iconic Turn („Erkenntnis wird durch die Analyse von Bildern hergestellt"), seit den 1980er Jahren sind die Wissenschaftler nun beim Material Turn angelangt: Geforscht wird (auch) unter der Prämisse, dass allen Objekten die Gesellschaft eingeschrieben ist, die sie hervorgebracht hat. Im Umkehrschluss ist es also ebenfalls möglich, die Gesellschaft und die ihr zugrunde liegenden Werte aus dem Objekt hervorzuholen, wenn man es nur ausreichend lange anstarrt.

Angesichts der Enthüllungen über die Verfasstheit des Internets und der Gesellschaft im Jahr eins nach Snowden scheint nur noch eine Kombination aller drei

oben genannten Analyse-Perspektiven zu verfangen, um zu Erkenntnis zu gelangen.

In einem Artikel zu Creative Disruptors schreibt die Berliner Kuratorin und Wissenschaftlerin Tatiana Bazzichelli über die kollektive Schreckstarre[2]:

> trying to deal with the topic (Überwachung, Anm. d. Red.), it is easy either to become paralysed by its complexity, disillusioned by its grand scale, or deterred by fears of surveillance and repression.

Zu großen Teilen scheint die Bevölkerung nach wie vor überfordert von der Demaskierung der Remilitarisierung des Internets. Es ist nun nicht mehr ausschließlich Teilhabe- und Produktions-, sondern auch: Überwachungsinstrument. Da die Beweisstücke recht ephemer (Infrastrukturarchitektur) und damit unsichtbar sind, fehlt es an Realitätsrückbindung.

Ein möglicher Ausweg aus dem Erkenntnis-Dilemma ist, ähnlich wie angesichts von Datenmassen des Datenjournalismus (welcher Informationen visualisiert und so kognitiv leichter verarbeitbar macht) wie so oft: die Kunst.

Sie ist greifbar, sie zeigt Konsequenzen der tatsächlichen Entwicklung auf, ist somit Vergegenwärtigungsinstrument und spielt gleichzeitig als Heterotopie Alternativen des Ist-Zustandes durch. Stets unter der Prämisse: No punishment. Wo Abkommen längst stocken, gilt immer noch: Kunst- und Gedankenfreiheit. Nach Jacques Rancére geschieht die Emanzipation des Zuschauers jedoch nicht durch didaktische Aufklärung oder das Abbilden von Missständen, sondern durch die Herstellung von Dissens – Befremden[3].

Eine der kreativen Disruptoren ist Laura Poitras, die auf der Klaviatur des Visuellen virtuos spielt und die sich hoffentlich für den ersten Dokumentarfilm verantwortlich zeichnet, der jemals den Oscar gewinnt – nämlich Citizen Four. Sie hat im Zuge der transmediale 2014 die Rede von „Art as Evidence" eingeführt:

> How can we use art to translate evidence or information beyond revealing the facts, so that people experience that information differently, not just intellectually, but emotionally.

Auf dem gleichnamigen Panel „Art as Evidence"[4] wurden im Januar 2014 neue Allianzen aufgezeigt, die diese Vergegenwärtigung bewerkstelligen könnten. Neben Poitras saßen Jacob Appelbaum (Entwickler) und Trevor Paglen (Künstler/Fotograf) auf dem Podium[5]. Alle Akteure verfolgen unterschiedliche Strategien der Darstellung des Überwachungskomplexes, haben aber ein gemeinsames Thema: die Überwachung der Überwacher.

Der Grad der Asymmetrie zwischen Sehen und gesehen werden offenbart die tiefe, komplizierte Beziehung zwischen Sichtbarkeit und Politik.

Betrachtet man den Überwachungsdiskurs, so ist dieser – auch in der Kunst – untrennbar verbunden mit dem Verhältnis von Geografie, öffentlichem Raum, Sichtbarkeit und Politik. Auf diesem Gefälle setzen viele der Arbeiten auf, die man zur „Surveillance Art" zählt. Diese spielt mit dem panoptischen Blick, auf den ich später zurückkomme.

Zunächst jedoch: um den Term „Remilitarisierung des Internets als Überwachungsinstrument"[6] zu rechtfertigen, lohnt ein kleiner Exkurs zum Gründungsmythos des Internets[7]. Eng verbunden mit seiner Geburt sind das Kind sanft bettende Denkschulen, wie z. B. die Kybernetik[8], die entscheidend zur Architektur des technischen Apparates beigetragen haben. Einen Einblick in die Geisteshaltung der Urväter des Internets liefert die Begleitpublikation zu einer Ausstellung, die Diedrich Diederichsen im vergangenen Jahr im HKW in Berlin kuratiert hat: „The Whole Earth. Kalifornien und das Verschwinden des Außen"[9]. Diese reflektiert, wie romantische und technophile Ideen aus dem Umfeld von Gegenkultur und Kybernetik der 1960er Jahre zu den Konzepten des System- und Selbst-Managements im Netzwerkkapitalismus führten, die heute global wirksam sind.

Die positive Besetzung einer Steuerbarkeit der Gesellschaft durch Fremd- und Selbstregulierung ist das grundlegende Problem, das bereits in der Formulierung des Panopticon[10] bei Jeremy Bentham zu finden ist. Dieser entwarf im 19. Jahrhundert das Konzept zum Bau von Gefängnissen, aber auch von Fabriken, das die gleichzeitige Überwachung vieler Menschen durch einen einzelnen Überwacher ermöglicht. Die ständige, potenzielle Beobachtung erhöht den Konformitätsdruck.

Wirkungsvoll übertragen auf den Alltag und den öffentlichen Raum wird dieses Ordnungsprinzip über CCTV. Überwachungskameras sind („zu ihrer eigenen Sicherheit", so der Claim) in Städten weit verbreitet, ihre grundlegenden Funktionsweisen bekannt, ihre Wirkung umstritten. Daher eignen sie sich hervorragend, um Mechanismen offenzulegen. Der Kunstwissenschaftler Andrea Brighenti konstatiert in einem Aufsatz zu Artveillance[11]:

> [...] surveillance does not simply produce substantive social control and social triage, it also contributes to the formation of an ideoscape and a collective imagery about what security, insecurity, and control are ultimately about, as well as the landscape of moods and affects a surveillance society like ours expresses.

Überwachungskameras – obwohl sie mittlerweile getrost als „geringstes Problem" im Kontext der gesellschaftlichen Kontrolle angesehen werden können –

symbolisieren die Kontrollgesellschaft auf spezifische Weise. Als „evokative Objekte“ (Sherry Turkle) erlauben sie eine besondere affektive Aufladung, die sie zu Auslösern verschiedenster Narrative werden lassen.

Die Liste der anschlussfähigen Kunstwerke ist lang: Beginnend mit Vito Acconcis Verfolgungsperformances oder Andy Warhols Experimenten mit Echtzeit und frühem Closed-Circuit-Video in den 60er Jahren; Bruce Naumans Videokorridoren; Dan Grahams Time Delay Room und Rem Koolhaas' Project for the Renovation of a Panoptic Prison in den 70er Jahren; Sophie Calles Dokumentation der beauftragten Überwachung ihrer eigenen Person und Michael Kliers Kompilation von gefundenem Überwachungsmaterial in seinem Film Der Riese in den 80ern; Thomas Ruffs Nachtfotos; den ironischen Überwachungspraktiken des Bureau of Inverse Technology bis hin zur Dokumentation öffentlicher Überwachungskameras durch Frank Thiel und dem systematischen Aufspüren solcher Kameras in Manhattan vom „New York Surveillance Camera Project“ in den 90ern oder dem Internetprojekt „we live in public“ von Josh Harris im Jahre 2000 unter den Bedingungen einer unablässigen Echtzeit-Überwachung. Die Thematik des panoptischen Blicks ist eben nicht neu, auch wenn sie für die aktuelle kulturelle Produktion in immer stärkerem Maß relevant wird (ein Index zu Ausstellungen zu Surveillance Art findet sich unten). Als aktuelles Beispiel sei auf die Installation „Panopticon“[12] hingewiesen, die den Multimediapreis 2014 gewonnen hat.

Hinzu kommen weitere Subkategorien, wie die Sousveillance. Hier werden die Überwachungskamera und ihr Netzwerk verwendet, um Geschichten im Modus des Überwachten zu erzählen. Exemplarisch kann z. B. die Arbeit Tracking Transience[13] von Hasan Elahi genannt werden[14]. Elahi geriet ins Fahndungsraster des FBI, weil er einen arabisch klingenden Vornamen hat und jährlich etwa 100.000 Flugmeilen zurücklegt (Wissenschaftler, curious person!). Als „Terrorverdächtiger“ wurde Hasan Elahi monatelang vom US-Geheimdienst festgehalten und verhört – völlig zu Unrecht. Nach seiner Freilassung ging der Kunstprofessor in die Offensive: Auf seiner Website dokumentiert er nun minutiös seinen Tagesablauf – was er isst, wen er trifft, was er tut. Außerdem kann man dank eines GPS-Peilsenders genau sehen, wo er sich gerade befindet. Diese Art des Gegenangriffs betrachtet Elahi als sein ständiges Alibi. Er glaubt:

> Wenn ich den Geheimdienst mit Informationen überflute, dann hat meine Information irgendwann keinen Wert mehr für sie. Wenn ich ihnen alles erzähle, dann gibt es nichts mehr, was sie über mich herausfinden können.

Ähnlich fatalistische künstlerische Interventionen sind im übrigen auch am Beispiel Google Maps zu belegen. Der allwissende Beobachter verhält sich in Fall der Streetview-Cars nicht statisch, sondern fährt mit stolz erhobenem Stativ durch

Stadt und Land, um zu erfassen und vermessen. Seine Fremdartig- und Sichtbarkeit provoziert Reaktionen.

Angesichts des rollenden Zyklopen entsteht (z. B. bei Hausbesitzern) ein neues Bewusstsein für Privatsphäre. Genauso oft wie den Mittelfinger bekommt die Kamera auch absurde Performances zu sehen. Aufmerksamkeit ist eine harte Währung. Festgehalten werden die Meditationen über Maps nicht nur in Tumblrn wie Fuck You Google Maps[15], die außerhalb des Konsekrationskreislaufs der Kunst stattfinden. Auch arrivierte Vertreter der Medienkunst wie Aram Bartholl, der zu fast jedem Kernbereich des Internets schon ein reflektiertes Kunstprojekt beisteuerte, hat sich unauflöslich mit einer Koordinate auf der virtuellen Landkarte verbunden. Er erklärt seine „15 seconds of fame" wie folgt:

> On the morning of October 13, 2009 I had coffee as usual at Cafe MÖRDER, Berlin Mitte. Suddenly the Google Streetview car entered Borsigstrasse. I dropped my spoon, took the door and ran after it. About a year later on November 18, 2010 Google Streetview Germany went life this spontaneous performance included.

Während Kenntlichkeit der Kern seines Werks ist, geht es z. B. Paolo Cirio statt Glow um Glitch in den Gesichtern seiner Street Ghosts[16]. Er reinszeniert beiläufige Porträtaufnahmen auf Streetview, indem er die Protagonisten als lebensgroße, verschwommene Prints an eben jene Hauswände zurückklebt, vor denen sie aufgenommen wurden.

Kunstgeschichtlich begründet sich die Surveillance Art schon mit der Erfindung der Fotografie. Fotografie kann zugleich Instrument der Überwachung wie auch Ausdrucksmittel in der Sichtbarmachung der negativen Auswirkungen derselben sein (siehe Paglen). Durch die der Technik inhärente Fähigkeit, etwas darzustellen, das gleichzeitig omnipräsent und verdeckt ist, scheinbar überall und nirgends, verwischt Überwachungskultur die Grenzen zwischen privatem und öffentlichem Raum.

Dieser Twist wird auch deutlich am Fotoprojekt „The Neighbours", das in allen Feuilletons 2014 ausführlich besprochen wurde. Fotograf Arne Svenson nutzte ein Teleobjektiv, um aus seiner Wohnung im ersten Stock durch die Fenster in andere Apartments hinein zu blicken. Seine Bilder zeigen unter anderem einen schlafenden Mann, nackte Beine unterm Bademantel und eine Frau im Schaukelstuhl mit Teddybär. Komplette Gesichter sind nie abgebildet, allerdings Partien. Er sagt über das Projekt:

> I looked out the window of my studio and I saw this fascinating amalgam of Mondrian, Hitchcock, and Vermeer, I had to photograph it.

Das Panorama spannte sich vor dem Objektiv allerdings nicht in unberührter, menschenleerer Natur auf – sondern in Wohnzimmern. Zum Streitfall vor Gericht wurden die Momentaufnahmen nur durch den Zufall: Niemand wusste wo der Ort des Shootings war, bis ein Nachrichtensender das Gebäude aufspürte und die Bewohner selbst ihre Anonymität aufbrachen[17]. Es komme auf den Kontext an, urteilen befragte Juristen zu der Deckung durch die Kunstfreiheit. „Die Frage an die klagende Person wäre, wenn sie nicht zu identifizieren ist, wo ist dann der Verlust der Privatsphäre?"

Ja,wo? Schon der Philosoph Paulo Virilio warnte:

> One day the virtual world might overwhelm over the real world. This is that same virtual reality in which monitors you look at your existence.

Freiräume sind wichtig. Ebenso Zonen der Privatheit. Um wieder besser unterscheiden zu können, wo die Grenzen verlaufen, ist es ein wichtiger Möglichkeitsraum, sich selbst durch das „Eye of the Spy-der" zu betrachten. Da die wirklichen Schaltzentralen einem aber die Hoheit über die Bildschirme nicht zugestehen, ist es um so entscheidender, dass die Realität als Versuchsanordnung so oft es geht im Kontext der Kultur durchgespielt und verhandelt wird. So lang, bis man so von seinem eigenen Anblick so befremdet ist, dass auch kein anderer einen mehr sehen soll.

FUN GIMMICK (und alle so: yeah)

Nicht hilfreich in Sachen Überwachungskunst: Ein Promo-Video der One Love Foundation:

https://www.youtube.com/watch?feature=player_embedded&v=EIQQt7Avh7E

Linksammlung zu Surveillance Art

A-Z kreativer Reaktionen auf die Dauerüberwachung (Dazed)
http://www.dazeddigital.com/artsandculture/article/16953/1/the-dazed-guide-to-surveillance

Vice Creators Project http://thecreatorsproject.vice.com/en_au/tag/surveillance+art

ARTE http://www.arte.tv/de/videokontrolle-in-der-medienkunst/765396,CmC=796112.html

Klassiker der Medienkunst zum Thema Überwachung (MedienKunstNetz)
http://www.medienkunstnetz.de/suche/?qt=surveillance

Grundlegende wissenschaftliche Theorien Foucault, Virilio und Deleuze

Zeitschrift „Surveillance&Society" http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/performance

Auswahl von Ausstellungen rund um das Thema Überwachung:

San Francisco Museum of Modern Art
http://www.sfmoma.org/exhib_events/exhibitions/408

Tate Modern London
http://www.tate.org.uk/whats-on/tate-modern/exhibition/exposed

Schirn Kunsthalle Frankfurt
http://www.schirn.de/Privat_4.html

ZKM Karlsruhe
http://ctrlspace.zkm.de/d/

Sydney Institute of Technology
http://art.uts.edu.au/index.php/exhibitions/trace-recordings/,
http://www.tracerecordings.net/About

Open Society Foundation
http://www.opensocietyfoundations.org/moving-walls/22

Anmerkungen

[1] https://www.reporter-ohne-grenzen.de/presse/termine/termin/youturn-ein-ueberwachungsexperiment/

[2] http://www.exberliner.com/features/lifestyle/the-disruptors/

[3] http://www.faz.net/aktuell/feuilleton/buecher/rezensionen/sachbuch/jacques-ranciere-der-emanzipierte-zuschauer-kunst-kommt-nicht-von-kundenbefragung-1999120.html

[4] http://www.youtube.com/watch?v=NEipLr9xLMU und
http://networkingart.eu/2014/04/art-as-evidence/#more-1819

[5] Trevor Paglen fotografiert Orte und Dinge, die es offiziell nicht gibt. Geheimgefängnisse, Spionagesatelliten, Drohnen, Abhörstationen, Spezialeinheiten der US-Streitkräfte – alles, was eigentlich unsichtbar sein sollte, macht Paglen sichtbar.
http://www.galeriezander.com/de/artist/trevor_paglen/information

[6] Geert Lovink vom Institute of Networked Cultures schreibt hierzu treffend: *„Until 1984, a small conglomerate of multinationals such as IBM, Honeywell-Bull, and GE defined the public imagination of computers with their sterile, corporate mainframes that processed punch cards. Until then, computers had been used by large bureaucracies to count and control populations and had not yet shaken off their military origins. Now, thirty years later, the computer is once again the perfect technical instrument of a cold, military security apparatus that is out to allocate, identify, select – and ultimately destroy – the Other. The NSA, with the active support of Google, Facebook, Microsoft, and allied secret services, has achieved „total awareness." Precisely at the moment when the PC is disappearing from our desks, large and invisible data centers take their place in the collective techno-imaginary."*

[7] *„consider art as 'technological', in the sense that art is always tied to a technology of production and a technology of mediation (and re-mediation). From this point of view, new visual and digital technologies cannot fail to have profound impact on contemporary art On the other hand, perhaps less intuitively, artveillance also suggests that we regard surveillance not as a merely technical process focused exclusively on recording images, tracking data flows and processing acquired and stored data, but also as a somewhat 'artful' set of techniques, which may be*

more creative and, with Levi-Strauss, .ore similar to bricolage than usually assumed in surveillance studies." http://www.capacitedaffect.net/2010/Brighenti-2010-Artveillance.pdf

[8] http://de.wikipedia.org/wiki/Kybernetik

[9] http://www.hkw.de/de/media/publikationen/14_the_whole_earth.php

[10] http://www.ucl.ac.uk/Bentham-Project/who/panopticon

[11] http://www.capacitedaffect.net/2010/Brighenti-2010-Artveillance.pdf

[12] http://www.youtube.com/watch?feature=player_embedded&v=uMx8twW3YMo

[13] http://www.mb21.de/p1270353341_777.html

[14] http://elahi.umd.edu/track/; *Projektbeschriebung als TED-Talk (sehr! Unterhaltsam)*. http://www.ted.com/talks/hasan_elahi?language=de

[15] *FYGooglemaps*. http://fygooglemaps.tumblr.com

[16] http://streetghosts.net

[17] http://arnesvenson.com/theneighbors.html

Katharina Meyer ist bevorzugt Technik- und Kulturhistorikerin, von Zeit zu Zeit Kuratorin (z. B. bei der re:publica) und in Teilzeit Research Associate am Hybrid Publishing Lab an der Leuphana Lüneburg. Ausserdem betreut sie für die Open Knowledge Foundation ein Forschungsprojekt zu digitalen Geisteswissenschaften. Sie mäandert an den Schnittstellen von Ästhetik und Technik und publiziert zu Netz- und Medienkunst (z. B. bei Right2Remix) sowie Digitaler Kultur.

14 Grenzen für Überwacher statt grenzenlose Überwachung

von **Peter Schaar**

Nach Beginn der auf Edward Snowden zurückgehenden Veröffentlichungen im Juni 2013 stand zunächst die Aufklärung des Umfangs, der Methoden, der Ziele und der Akteure im Vordergrund. Bis heute halten uns neue Erkenntnisse über entsprechende geheimdienstliche Aktivitäten in Atem. Kontrollgremien und Untersuchungsausschüsse in aller Welt haben sich der Fragen angenommen und zum Teil schon Ergebnisse vorgelegt, die das ungeheure Ausmaß der Überwachung belegen. Dabei ist deutlich geworden, dass es sich nicht nur um einen „NSA-Skandal" handelt, sondern um sehr viel umfassendere, teils arbeitsteilig ausgeführte Aktivitäten einer Vielzahl von Geheimdiensten.

Die inzwischen gewonnenen Erkenntnisse stehen in einem eigenartigen Kontrast zu den Bemühungen, die weltweite Überwachung zu begrenzen und zurückzufahren. Wir brauchen weniger und nicht mehr Überwachung und wir benötigen endlich wirksamere Kontrollen der Geheimdienste. Nur wenn sich bei den politischen Entscheidungsträgern die Einsicht durchsetzt, bei der Überwachung abzurüsten, kann der Ausstieg aus der Überwachungsspirale gelingen.

Zwar wird in den USA und auch in Europa über entsprechende Ansätze diskutiert, aber die Kräfte, die in diese Richtung wirken, sind bei Weitem zu schwach.

Aktivitäten auf internationaler Ebene

Immerhin hatte Deutschland zusammen mit Brasilien eine Entschließung der UN-Vollversammlung initiiert, in der die Wahrung der Menschenrechte bei Überwachungsaktivitäten eingefordert wird. Zudem bemühte sich die Bundesregierung um ein „No-Spy-Abkommen" mit den USA – ein Vorhaben, das offensichtlich keine Chancen auf Realisierung hat.

So hatte ich vorgeschlagen, anknüpfend an die bestehenden rechtlichen Instrumente des internationalen Rechts, die völkerrechtliche Verankerung des Datenschutzes zu verbessern: Die Bundesregierung und die Europäische Union sollten sich für ein internationales Übereinkommen stark machen. Ein Zusatzprotokoll zum Art. 17 des UNO-Paktes für bürgerliche und politische Rechte wäre ein sinnvoller erster Schritt. 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[1]. Immerhin griff Bundeskanzlerin Angela Merkel diesen Vorschlag wenige Wochen später auf: „Das Auswärtige Amt setzt sich als federführendes Ressort auf internationaler Ebene dafür ein, ein Zusatzprotokoll zu Art. 17 zum Internationalen Pakt über bürgerliche und politische Rechte der Vereinten Nationen zu verhandeln." Darin sollten den heutigen modernen technischen Entwicklungen entsprechende internationale Vereinbarungen zum Datenschutz festgeschrieben werden – auch für die Tätigkeit der Nachrichtendienste, meinte die Bundeskanzlerin damals. „Eine gemeinsame Initiative an unsere europäischen Partner ist heute von dem Bundesaußenminister zusammen mit der Bundesjustizministerin ergriffen worden in Form eines Briefs, um hier eine gemeinsame europäische Position zu erhalten."[2]

Nachdem es zunächst so aussah, als würde diese Initiative der Bundesregierung auf breite europäische und internationale Unterstützung treffen, ruderten in den folgenden Wochen und Monaten einige der Regierungen, die zunächst ihre Zustimmung signalisiert hatten, zurück.

Als sich abzeichnete, dass das 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 verstoße. 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. Aufgrund der massiven Intervention der US-Regierung und anderer Mitglieder im exklusiven Überwachungsclub der „Five Eyes" wurde die Resolution schließlich teilweise entschärft, wie der Spiegel unter Berufung auf „UN-Insider" zu berichten wusste. 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 sind verpflichtet, „die vollständige Einhaltung ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen" sicherzustellen. Die Generalversammlung zeigte sich „tief besorgt über die nachteiligen Auswirkungen, die das Überwachen und/oder Abfangen von Kommunikation, einschließlich des extraterritorialen Überwachens und/oder Abfangens von Kommunikation, sowie die Sammlung personenbezogener Daten, insbesondere wenn sie in massivem Umfang durchgeführt werden, auf die Ausübung und den Genuss der Menschenrechte haben können." Die Staaten werden aufgefordert, „Maßnahmen zu ergreifen, um Verletzungen dieser Rechte ein Ende zu setzen und die Bedingungen dafür zu schaffen, derartige Verletzungen zu verhindern, namentlich indem sie sicherstellen, dass die einschlägigen innerstaatlichen Rechtsvorschriften mit ihren Verpflichtungen nach den internationalen Menschenrechtsnormen im Einklang stehen".

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-Menschenrechts-Kommissarin 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. Der im Juli 2014 von der UN-Hochkommissarin für Menschenrechte, Navi Pillay, veröffentlichte Bericht beschreibt in überzeugender Weise die Gefahren, die von der weltweiten Überwachung ausgehen. Offene und verdeckte digitale Überwachungsmaßnahmen seien inzwischen Bestandteil von Rechtsordnungen in aller Welt. Die von Regierungen zu verantwortenden Programme zur Massenüberwachung seien keine Ausnahmeerscheinung, sondern fänden zunehmend regelhaft statt. Die Hochkommissarin erinnerte daran, dass die durch die Menschenrechte definierten Grenzen der Überwachung unabhängig davon gälten, welche Staatsangehörigkeit die Überwachten hätten und an welchem Ort die Überwachung durchgeführt werde[3]. Ihr Stellvertreter Pansieri ergänzte im November 2014, dass „durch digitale Überwachung gewonnene Informationen dazu genutzt wurden, Dissidenten zu identifizieren. Vertrauenswürdige Berichte belegen, dass digitale Technologien auch dazu verwendet wurden um Informationen zu gewinnen, die zur Folter und anderen Verletzungen der Betroffenen geführt haben."[4]

Nationale Ebene

Nationale Handlungsmöglichkeiten gegen globale Überwachungsaktivitäten zu formulieren, erscheint vordergründig als unlösbare Aufgabe – sind doch die Aktivitäten von Regierungen und Parlamenten auf den eigenen Staat ausgerichtet,

während die Überwachung der Datenströme vornehmlich exterritorial, außerhalb des jeweiligen nationalen Territoriums erfolgt. Trotzdem sollte man die Flinte nicht allzu schnell ins Korn werfen und allein auf die Entwicklung und Durchsetzung internationaler Rechtsinstrumente setzen, die der globalen Überwachung Grenzen setzen. So wichtig diese internationalen Regeln sind, so schwierig gestaltet sich ihre Weiterentwicklung und vor allem ihre praktische Durchsetzung, solange große Staaten wie die USA, Russland und China sich verweigern.

Nicht zuletzt wegen dieser Schwierigkeiten macht es also durchaus Sinn, über die Instrumente nachzudenken, die auf nationaler Ebene zur Verfügung stehen.

Zum einen haben nationale Aktivitäten in globalen Netzen auch direkte Folgen außerhalb des eigenen Territoriums. So wirkt sich nationale Gesetzgebung, die den eigenen Behörden beim Überwachen der Kommunikation Grenzen setzt oder entsprechende Aktivitäten ausländischer Geheimdienste unter Strafe stellt, auf die bi- und multilateralen nachrichtendienstlichen Informationstauschbörsen aus – jedenfalls dann, wenn die Bereitschaft dazu bei Regierungen, Behörden und Gerichten besteht.

Auch technologische Maßnahmen zur Härtung von IT-Infrastrukturen schützen die Computersysteme und Netzwerke nicht nur gegen inländische Angreifer, sondern auch gegen Infiltrationsversuche von Nachrichtendiensten. Die Bereitstellung anonymer Nutzungsmöglichkeiten im Netz, robuste Verfahren zur sicheren Authentifizierung, Verschlüsselungsmechanismen nach dem Stand der Wissenschaft und Technik machen es nicht nur Betrügern, sondern auch ausländischen Geheimdiensten schwerer, an begehrte Informationen zu gelangen.

Traditionell entfalten Gesetze ihre Schutzwirkung im jeweiligen territorial definierten Geltungsbereich. Im Unterschied dazu ist das Internet aber so konstruiert, dass Landes- oder auch Kontinentalgrenzen technisch keine Rolle spielen. Wenn etwa ein deutscher Internetnutzer die Webseite eines deutschen Anbieters abruft, können die übertragenen Daten durchaus über amerikanische Netzknoten geleitet („geroutet“) werden. Global agierende Internetunternehmen speichern Daten auf Servern, die auf verschiedene Kontinente verteilt sind. Im Folgenden soll deshalb untersucht werden, wie weit dieses offensichtliche Territorialdilemma durch nationales Recht entschärft werden kann.

Die Tatsache, dass Spionage nicht gegen Völkerrecht verstößt, stellt Spione nicht straffrei. Geheimdienstliche Späh- und Lauschaktionen im Ausland beeinträchtigen regelmäßig die Rechte der davon betroffenen Zielpersonen und sind deshalb strafbar. Zwar heißt es in § 3 Strafgesetzbuch (StGB): „Das deutsche Strafrecht gilt für Taten, die im Inland begangen werden.“ Diese territoriale Begrenzung des deutschen Strafrechts wird aber durch § 5 StGB in Bezug auf Auslandstaten eingeschränkt, die sich gegen inländische Rechtsgüter richten. Zu diesen unabhängig vom Tatort zu ahndenden Straftaten gehört auch die Verletzung von

Betriebs- oder Geschäftsgeheimnissen, nicht jedoch das Post- und Fernmeldegeheimnis oder Verstöße gegen den Datenschutz. Gleichwohl können auch solche Straftaten nach deutschem Recht verfolgt werden, die aus dem Ausland initiiert wurden, aber sich im Inland auswirken („verwirklichen"). Wenn also ein ausländischer Geheimdienstcomputer deutsche Nutzer mittels Trojaner infiltriert und überwacht, erfüllt dies den Straftatbestand des Ausspähens von Daten.

Aus dem Ausland agierende Betrüger, die die Konten deutscher Bankkunden unter Verwendung ausspionierter PINs und Passwörter abräumen, machen sich nach deutschem Recht strafbar. 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. Schon die Vorbereitung einer solchen Straftat, insbesondere das Ausspähen von Passwörtern oder sonstigen Sicherungscodes, die den Zugang zu vertraulichen Daten ermöglichen, ist strafbar.

Ebenso ist nach deutschem Recht strafbar, das nicht öffentlich gesprochene Worte abzuhören oder aufzuzeichnen – dies gilt auch für Telefonate, die mit dem Handy geführt werden. Schließlich verbietet § 99 StGB die geheimdienstliche Agententätigkeit für eine fremde Macht. Der Tatbestand stellt nicht auf konkreten Verrat ab, sondern erfasst jede auf die Beschaffung von Informationen für einen fremden Nachrichtendienst gerichtete Tätigkeit, die deutsche Sicherheitsinteressen beeinträchtigen kann. Geschütztes Rechtsgut ist die äußere Sicherheit Deutschlands im weitesten Sinne. Auch Wirtschaftsspionage kann nach § 99 StGB strafbar sein. Erfasst wird auch die Ausspähung von in Deutschland lebenden Ausländern für Nachrichtendienste ihrer Heimatländer. „Selbst eine Tätigkeit für Nachrichtendienste verbündeter Staaten verletzt deutsche Interessen, wenn sie nicht von deutschen Sicherheitsbehörden abgedeckt ist", heißt es auf der Website des Generalbundesanwalts.[5]

Auch der Bruch des Fernmeldegeheimnisses ist eine Straftat – genauso wie das heimliche Eindringen in geschützte Computersysteme. Heute können kaum noch Zweifel daran bestehen, dass britische und amerikanische Geheimdienste gegen mehrere dieser Strafvorschriften verstoßen haben, etwa beim Abhören des Handys von Bundeskanzlerin Angela Merkel, aber auch beim massenhaften Ausspähen deutscher Kommunikationsverkehre, die über ausländische Netzknoten und Transatlantikkabel geführt werden.

Dies gilt nicht nur für die genannten angloamerikanischen Nachrichtendienste, sondern auch für die Dienste anderer Staaten und auch für den Bundesnachrichtendienst. Wenn etwa der BND Telefone und E-Mails oder Mobilfunknetze im Hindukusch oder in anderen Operationsgebieten überwacht und dabei milliardenfach Metadaten absaugt, widerspricht dies natürlich dem dortigen Recht – und zwar völlig unabhängig davon, ob das deutsche BND-Gesetz derartige Akti-

vitäten erlaubt oder nicht, wie etwa im Untersuchungsausschuss des Deutschen Bundestags zu den NSA-Aktivitäten diskutiert wird.[6]

Bei der Rechtfertigung der geheimdienstlichen Tätigkeit im Ausland wird gern ausgeblendet, dass deutsche Behörden die zentralen Wertentscheidungen des Grundgesetzes, insbesondere die Achtung der Menschenwürde (Art. 1 Abs. 1 GG) stets zu beachten haben, unabhängig davon, wo sie tätig sind. Dies gilt unabhängig davon, ob die Beschränkungen, die etwa das G10- oder das BND-Gesetz dem Bundesnachrichtendienst setzen, nicht uneingeschränkt bei der Auslandsaufklärung gelten. So ist es deutschen Behörden stets verboten, Menschen zu quälen oder zu foltern.

Auch bei nachrichtendienstlichen Lauschaktivitäten kann die Menschenwürde berührt sein: So hat das Bundesverfassungsgericht wiederholt festgestellt, dass es mit der Menschenwürde unvereinbar wäre, wenn staatliche Stellen einen „unantastbaren Kernbereich der Privatsphäre" ausspionieren: „Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung […] nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung […] und dem Strafverfolgungsinteresse findet insoweit nicht statt."[7] In weiteren Entscheidungen hat das Gericht festgestellt, dass zu diesem Kernbereich auch höchstpersönliche Lebensäußerungen gehören, die mittels Telekommunikation übertragen werden.[8]

Das lückenlose Abhören der Telekommunikation ist deshalb generell unzulässig, denn es könnten ja auch Gespräche abgehört werden, die diesem absolut geschützten Bereich zuzurechnen sind. Jedenfalls müssen Vorkehrungen getroffen werden, dass Informationen, die zum Kernbereich privater Lebensgestaltung gehören, nicht aufgezeichnet oder jedenfalls unverzüglich gelöscht werden. Dies gilt nicht nur für inländische Überwachungsmaßnahmen, sondern auch für Aktivitäten des Bundesnachrichtendienstes als Auslandsgeheimdienst. Zudem gilt das deutsche Datenschutzrecht stets dann, wenn der BND personenbezogene Daten im Inland verarbeitet. Wenn der BND – wie durch die Bundesregierung bestätigt[9] – Daten aus der Auslandsaufklärung an die amerikanischen Nachrichtendienste weitergeleitet hat, muss er dabei deutsches Datenschutzrecht beachten.

Man muss also nicht allzu lange suchen, um im juristischen Instrumentenkasten Werkzeuge zu finden, die gegen eine überbordende Geheimdienstüberwachung eingesetzt werden könnten. Als eigentliches Problem entpuppt sich deshalb die zögerliche Anwendung und Durchsetzung der bestehenden rechtlichen Vorgaben, sei es aus außenpolitischer Rücksichtnahme oder aber auch im Interesse der deutschen Sicherheitsbehörden, deren Leitungen immer wieder darauf hinweisen, wie abhängig sie von den Informationen seien, die sie von ausländischen – namentlich amerikanischen – Diensten erhalten.

Technik: Vom Teil des Problems zum Teil der Lösung?

Der kürzlich verstorbene FAZ-Herausgeber Frank Schirrmacher verglich die Erkenntnisse aus den Snowden-Papieren mit dem „Sputnik-Schock", den die Vereinigten Staaten 1959 erlitten hatten, als sie feststellen mussten, dass der erste Weltraumsatellit nicht etwa durch die US-Raumfahrtbehörde NASA auf den Weg gebracht worden war, sondern von den Russen. Unter Bezugnahme auf diese Erfahrung meinte Schirrmacher, es wäre angesichts der Meldungen zu geheimdienstlichen Überwachungsaktivitäten grundfalsch, wenn Europa den Kopf in den Sand stecken und sich mit einer digitalen Opferrolle abfinden würde. Vielmehr müsse die „brachliegende digitale Intelligenz" Europas entfesselt werden, indem man Initiativen für „integre Netzwerke und, wer weiß, auch für Suchmaschinen politisch ins Leben ruft und fördert".[10]

Was könnte diese „digitale europäische Intelligenz" bewirken? Es gibt durchaus verschiedene technische und juristische Stellschrauben für einen besseren Schutz der Daten. Mehr noch: Angesichts des grassierenden Vertrauensverlusts in amerikanische Internetdienste und der begründeten Vermutung, aus den USA oder China stammende Produkte enthielten Hintertüren oder bewusst eingebaute Schwachstellen, lässt sich durchaus europäisches Kapital schlagen.

Dies gilt insbesondere auf dem Feld der Datenverschlüsselung. Seit der Erfindung der E-Mail wird deren Vertraulichkeitsgrad ziemlich zutreffend mit dem einer Postkarte verglichen: Jeder, der Zugriff hat, kann mitlesen. Zudem grassieren Datenmissbrauch und Identitätsdiebstahl im Internet. Auch die übrigen Internetdienste wurden zunächst völlig ohne Verschlüsselung betrieben, die Daten also offen und leicht abhörbar übertragen. Auch wenn seit Jahren an verbesserten Schutzmechanismen gearbeitet wurde, waren viele der inzwischen etablierten Verschlüsselungsverfahren zu schwach, um geheimdienstlichen Angriffen zu widerstehen.

Die NSA und ihr britischer Partnergeheimdienst GCHQ waren offenbar in der Lage, nicht nur die unverschlüsselten Daten, sondern auch den verschlüsselten Internetverkehr großflächig auszuwerten. Viele Informatiker setzen jedoch weiterhin auf die Datenverschlüsselung. Selbst wenn man Überwachung letztlich nicht völlig verhindern könne, bestehe zumindest die Chance, sie den Nachrichtendiensten deutlich zu erschweren und für sie teuer zu machen.

Die Möglichkeit eines absolut sicheren Verschlüsselungssystems mag es theoretisch geben. Praktisch muss man allerdings einige Abstriche machen. Alle funktionierenden kryptographischen Systeme gelten nur unter bestimmten Prämissen hinsichtlich der Fähigkeiten der „Gegenseite", insbesondere in Bezug auf die Rechenkapazitäten als sicher. Die Sicherheit nahezu aller Verschlüsselungsalgorithmen ist zudem nicht vollständig nachgewiesen. Alle Feststellungen zur Sicherheit der jeweiligen Verfahren beruhen vielmehr auf der Prüfung und Diskussion

durch die Fachöffentlichkeit. Deshalb ist es von entscheidender Bedeutung, dass Verschlüsselungsalgorithmen dokumentiert und öffentlich nachprüfbar sind.

Dagegen können Verfahren, deren Funktionsweise geheim gehalten wird, nicht durch unabhängige Experten und eine kritische „Netzcommunity" nachgeprüft werden. Bisweilen wird die Geheimhaltung der Verschlüsselungsalgorithmen sogar als Argument für mehr Sicherheit verkauft. Eine derartige Sichtweise blendet aber aus, dass nicht nur externe Angreifer versuchen, die Verschlüsselung zu durchbrechen, sondern dass auch Insider, die Kenntnisse über Schwachstellen eines Verschlüsselungsverfahrens besitzen, an Angriffen auf gesicherte Daten mitwirken oder ihr Wissen Dritten verkaufen könnten.

An „Security by Obscurity" sollte man spätestens jetzt nicht mehr glauben, nachdem bekannt ist, dass die NSA systematisch auf die Schwächung von Verschlüsselungsverfahren hingearbeitet hat. Deshalb sollten grundsätzlich nur solche Verfahren verwendet werden, deren Programmcode und Funktionsweise öffentlich dokumentiert ist („Open Source").

Die Verschlüsselungsalgorithmen müssen in Software umgesetzt werden. Eine „schlampige" oder bewusst nachlässige Programmierung kann dazu beitragen, dass an und für sich sichere Algorithmen unterlaufen oder umgangen werden können. Bekanntlich bieten derartige Schwachstellen den Geheimdiensten und anderen Insidern Ansatzpunkte zur Kommunikationsüberwachung. Auch hier gilt: Open-Source-Software ist solchen Programmen vorzuziehen, deren Programmcode und Funktionsweise von den Anbietern geheim gehalten werden.

Die Öffentlichkeit allein kann die Sicherheit von Verschlüsselungsverfahren zwar nicht garantieren, sie ermöglicht es aber, dass Fehler und Schwachstellen erkannt und behoben werden können. Ein weiterer Faktor für die Vertrauenswürdigkeit von kryptographischen Verfahren besteht darin, dass weder die Hersteller noch die Anbieter von Diensten rechtlich dazu verpflichtet werden, Hintertüren in ihre Systeme einzubauen, die Geheimdiensten und anderen Sicherheitsbehörden den Zugriff auf die Kommunikation ermöglichen, wie etwa der US-amerikanische Communications Assistance for Law Enforcement Act (CALEA).

Ob bei der Kryptographie, beim Routing, bei der Gestaltung von E-Mail-Diensten oder bei den Anforderungen an Cloud-Speicher: Ansatzpunkte gibt es mehr als genug. Ob die sich hier bietenden Chancen allerdings auch wirklich wahrgenommen werden, ist indes noch ungewiss. Sehr ambivalent verhält sich etwa die Industrie, die bei anderer Gelegenheit nicht zögert, ihre Interessen einzufordern. Frank Schirrmacher weist darauf hin, dass der „deutsche" IT-Branchenverband Bitkom maßgeblich von Ablegern globaler US-Firmen beeinflusst werde und sich auch deshalb kaum als Speerspitze deutscher oder europäischer Interessen eigne. Und die Wirtschaftswoche berichtete über einen heftigen Streit in diesem Verband zum Umgang mit der NSA-Affäre. Aus dessen Protokollen gehe hervor, dass

sich die amerikanischen Mitglieder vehement gegen den Vorschlag deutscher IT-Unternehmen gewehrt hätten, sichere Hard- und Software „Made in Germany" zu forcieren. Insbesondere die Forderung, Datenpakete von und nach Deutschland nicht mehr über Server in den USA und Großbritannien umzuleiten, weil diese von der NSA und dem britischen Geheimdienst GCHQ angezapft werden, sei von den Amerikanern blockiert worden.

Dabei gibt es genügend deutsche – und europäische – Unternehmen, die von einem neuen Geschäftsfeld Datenschutz und Datensicherheit profitieren würden. Bereits jetzt stehen leistungsfähige europäische Cloud-Services zur Verfügung, die ohne US-Beteiligung funktionieren. Dies hat US-Cloud-Anbieter dazu veranlasst, europäischen Kunden zuzusichern, dass deren Daten ausschließlich in Europa gespeichert würden.

Ob damit allerdings der gewünschte Schutz vor Überwachung erreicht wird, ist zumindest offen. Denn die amerikanischen Behörden bestehen darauf, dass die US-Unternehmen – völlig unabhängig von der europäischen Rechtslage – auch solche Daten herauszugeben haben, die nicht auf Servern in den Vereinigten Staaten gespeichert sind. Inwieweit die US-Unternehmen diesen Ansinnen folgen, die gegebenenfalls gegen das Recht der Staaten verstoßen, in denen die Server stehen, ist nicht bekannt.

Immerhin hat die Bundesregierung eine in der Öffentlichkeit kaum wahrgenommene erste Maßnahme getroffen, um rechtliche und technische Hintertüren zu verschließen, die es ausländischen Geheimdiensten ermöglichen, an vertrauliche Daten zu gelangen. In einem an das Beschaffungsamt des Bundesinnenministeriums gerichteten No-Spy-Erlass vom 30. April 2014 ist vorgesehen, dass in Vergabeverfahren des Bundes jeder Bieter Erklärungen abgibt, die heimliche Abflüsse schützenswerter Informationen an ausländische Nachrichtendienste betreffen. Weil dies kaum nachweisbar ist, wurden die Klauseln so ausgestaltet, dass eine Beweiserleichterung zugunsten der Bundesrepublik Deutschland eintritt. Für die Ablehnung eines Bieters bzw. für eine Kündigung des Vertrages soll es ausreichen, dass nachgewiesen wird, dass der Bieter einer rechtlichen Verpflichtung zur Weitergabe von vertraulichen Informationen, Geschäfts- oder Betriebsgeheimnissen an Dritte unterliegt. Gegebenenfalls müssen entsprechende Weitergabeverpflichtungen im Vergabeverfahren offengelegt werden. Damit werden auch Fälle erfasst, in denen entsprechende Auskünfte nach ausländischem Recht geheim zu halten sind[11].

In vielen Bereichen, insbesondere bei E-Mails, gibt es deutsche und europäische Alternativen, die den Vergleich mit der amerikanischen Konkurrenz nicht fürchten müssen. Insbesondere wenn gewährleistet wird, dass die Datenübertragung sicher verschlüsselt erfolgt, könnte die Wahl eines solchen Dienstes einen erheblichen Zugewinn an Sicherheit und Datenschutz bedeuten. Problematisch ist dabei bisher allerdings, dass die meisten Angebote für verschlüsselte E-Mails

lediglich eine „Verbindungsverschlüsselung“ vorsehen, d. h., die verschlüsselt übertragenen E-Mails werden von den Anbietern temporär entschlüsselt und könnten an diesen Schnittstellen gegebenenfalls im Klartext mitgelesen werden. Technisch ist es allerdings möglich, auf professioneller Basis eine Ende-zu-Ende-Verschlüsselung zu gewährleisten. Es ist nur eine Frage der Zeit, bis entsprechende Angebote auf den Markt kommen.

Noch nicht – oder nicht mehr – wirklich konkurrenzfähig ist die europäische Industrie in weiten Bereichen der Netzwerktechnik. Amerikanische und chinesische Unternehmen haben hier außergewöhnlich starke Marktpositionen errungen. Europäische Kunden können bei beiden Herkunftsländern nicht sicher sein, dass die entsprechenden Produkte frei von Hintertüren und nicht dokumentierten Überwachungsschnittstellen sind. Hier hätte eine europäische Industriepolitik gute Chancen, mit gezielter Förderung sicherer und zugleich leistungsfähiger Produkte die Entwicklung marktgängiger Produkte „made in Europe“ zu erreichen, die sich in der Konkurrenz mit chinesischen und US-amerikanischen Anbietern behaupten. Wenn gewährleistet ist, dass die Systeme ohne Einbußen an Qualität und Komfort zugleich die Vertraulichkeit und Integrität der Datenübertragung garantieren, könnte sich hier eine interessante Marktposition gewinnen lassen, weit über Deutschland und Europa hinaus.

Als Reaktion auf die Berichte über die, insbesondere durch die amerikanischen und britischen Geheimdienste betriebenen, globalen Überwachungsmaßnahmen wurde schließlich vorgeschlagen, europäische Datenpakete nicht mehr über Netzknoten in Übersee zu senden. So forderten die Datenschutzbeauftragten des Bundes und der Länder, „zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.“ Das Interntet-Routing sollte so konfiguriert werden, dass die innerhalb eines Gebiets versendeten Nachrichten dieses nicht mehr wie bisher verlassen.

Bemerkenswert ist insbesondere der Vorschlag eines „Schengen-Routing“, benannt nach dem Abkommen über den freien Reiseverkehr in Europa. Dabei würden die Datenpakete ausschließlich über Netzknoten in den Teilnehmerstaaten des Schengener Abkommens geleitet – Umwege über Drittstaaten, etwa die USA, wären auszuschließen. Der Schengen-Raum umfasst die meisten Mitgliedstaaten der Europäischen Union und einige andere europäische Staaten, nicht jedoch Großbritannien und Irland. Die Begrenzung auf die Schengen-Staaten könnte – so die Überlegung – nicht nur die NSA an einem Datenzugriff hindern, sondern auch den britischen Nachrichtendienst GCHQ, der im Rahmen des Programms Tempora maßgeblich an den Überwachungsaktivitäten beteiligt ist. Ein Nebeneffekt könnte darin bestehen, wichtige US-Internetunternehmen mit europäischen Hauptniederlassungen in Großbritannien und Irland zu umgehen.

Technisch ist es heute ohne Weiteres möglich, Datenverbindungen, bei denen beide Kommunikationspartner sich in Europa befinden, nur über europäische

Netzknoten zu leiten. In den letzten Jahren wurden die europäischen Netzinfrastrukturen massiv ausgebaut, sodass jedes Datenpaket heute auf vielen Wegen innerhalb des Schengen-Raums geroutet werden könnte. Tatsächlich werden aber immer noch viele Datenströme über die USA geleitet. Derzeit erfolgt die Wegewahl im Internet im Wesentlichen nach den Kriterien Preis, Entfernung und Service-Qualität. Die Umleitung europäischer Datenpakete über US-Netzknoten hat weniger technische als finanzielle Gründe, denn die US-Anbieter offerieren deutlich günstigere Konditionen als die europäische Konkurrenz. Das Schengen-Routing würde dementsprechend vermutlich zu erhöhten Kosten führen, jedoch kaum mit Einbußen in der Qualität der Verbindungen verbunden sein. Auch die Ausfallsicherheit des europäischen Netzes ist durch vielfach redundante Verbindungen heute weitgehend gewährleistet.

Trotzdem würden entsprechende Vorgaben zum Routing nicht automatisch zum Versiegen der Datenströme über den Atlantik führen. Zum einen werden Daten auch weiterhin stets dann in die USA übertragen, wenn die elektronischen Dienstleistungen von dort aus erbracht werden. Dazu kommt, dass amerikanische Anbieter die Daten ihrer Nutzer über ihre in den USA gelegenen Infrastrukturen leiten und überwiegend dort auf Servern ablegen. Wer einen amerikanischen E-Mail-Dienst nutzt oder Google als Suchmaschine verwendet, muss also – auch wenn das Schengen-Routing kommen sollte – weiterhin damit rechnen, dass seine Daten in den USA landen, auf dem Weg über Netzknoten und Überseekabel durch den GCHQ und die NSA abgehört und auf Anfrage an US-Sicherheitsbehörden herausgegeben werden. Dies gilt auch für Facebook, das seine Dienste seit einigen Jahren europäischen Nutzern offiziell unter der Firma „Facebook Ltd." aus Dublin anbietet, denn technisch wird der Dienst weiterhin überwiegend in den USA betrieben.

Nicht vergessen werden darf dabei, dass Vorgaben zum Routing auch Auswirkungen auf die Konkurrenzsituation europäischer Unternehmen untereinander haben können. So erntete die Deutsche Telekom auf ihren Vorschlag eines „nationalen IP-Routings" empörete Reaktionen bei anderen deutschen Internet-Anbietern. Der Geschäftsführer des größten deutschen Internetknotens DE-CIX Harald Summa bezeichnete die Initiative der Telekom als „reine Marketingaktionen und Irreführung der Politik". Die Telekom selbst behindere den Verbleib der Datenpakete im deutschen Rechtsraum, denn sie organisiere den Transport ihrer Daten direkt mit anderen Netzbetreibern und beteilige sich nicht am öffentlichen, gleichberechtigten Datenaustausch („public peering"). Dies habe zur Folge, dass nicht mit der Telekom verbundene Netzanbieter an Telekom-Kunden gerichtete Datenpakete vielfach nur über das Ausland zustellen könnten. Inzwischen scheinen sich die verhärteten Fronten zwischen den verschiedenen Internetanbietern jedoch aufzulösen.

Wie zu vernehmen ist, verhandelt etwa die Deutsche Telekom mit dem Internetverband Eco über entsprechende Lösungen, die eine sichere Kommunikation über Providergrenzen hinaus ermöglichen.

Anmerkungen

[1] http://www.spiegel.de/netzwelt/netzpolitik/peter-schaar-zu-prism-und-tempora-ueberwachung-zurueckfahren-a-907793.html

[2] http://www.bundeskanzlerin.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/07/2013-07-19-merkel-bpk.html

[3] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[4] http://www.ohchr.org/EN/NewsEvents/Pages/MassSurveillance.aspx;
http://www.ohchr.org/EN/NewsEvents/Pages/MassSurveillance.aspx#sthash.32aEyu1n.dpuf
(eigene Übersetzung)

[5] https://www.generalbundesanwalt.de/de/spionage.php

[6] Vgl. hierzu etwa die Sachverständigengutachten der ehemaligen Bundesverfassungsrichter Papier und Hoffmann-Riem.
https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848

[7] Bundesverfassungsgericht: *Urteil zur akustischen Wohnraumüberwachung („großer Lauschangriff")*. 1 BvR 2378/98, 3. März 2004

[8] Vgl. etwa Bundesverfassungsgericht: *Urteil zur präventiven Telekommunikationsüberwachung durch die Polizei*. 1 BvR 668/04, 27. Juli 2005

[9] *Bundestagsdrucksache 17/14560*, S. 8.

[10] Frank Schirrmacher: *Europas Sputnik-Schock*. FAZ, 31. Oktober 2013

[11] BMI veröffentlicht Erläuterungen zum „No-Spy-Erlass".
http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/08/no-spy-erlass.html

Peter Schaar war von 2003 bis 2013 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Derzeit ist er Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID).

15 Die Aufsicht über Geheimdienste - Ein demokratischer Lackmustest

von **Volker Tripp**

Die Arbeit der Geheimdienste ist naturgemäß opak und dem Blickfeld der breiten Öffentlichkeit entzogen. Als Teil der Staatsgewalt unterliegen diese Behörden jedoch zugleich den Vorgaben des Grundgesetzes, allen voran den Prinzipien von Demokratie, Rechtsstaatlichkeit und Gewaltenteilung sowie der Achtung der Grundrechte. Aus dieser Gemengelage entsteht ein Spannungsverhältnis, dessen Auflösung als Indikator für den Zustand eines demokratischen Rechtsstaates verstanden werden kann.

Formal und rein quantitativ betrachtet fällt der demokratische Lackmustest positiv aus. Gleich drei parlamentarische Gremien sind damit befasst, die Arbeit der drei Nachrichtendienste des Bundes zu kontrollieren. Die generelle Aufsicht obliegt dem mit aktuell neun Abgeordneten besetzten Parlamentarischen Kontrollgremium, während die vier vom Bundestag gewählten Mitglieder der G10-Kommission für die Kontrolle von Eingriffen in die Telekommunikationsfreiheit zuständig sind. Außerdem berät das Vertrauensgremium des Haushaltsausschusses über die Wirtschaftspläne der Dienste. Flankiert wird diese parlamentarische Kontrolle durch Aufsichtsbefugnisse des Bundesrechnungshofes sowie der Bundesbeauftragten für Datenschutz und die Informationsfreiheit.

In qualitativer Hinsicht fällt das Ergebnis hingegen deutlich schwächer aus. Die Sitzungen der parlamentarischen Gremien verlaufen stets unter Ausschluss der Öffentlichkeit und ihre Mitglieder sind zu absoluter Verschwiegenheit über die dort gewonnenen Erkenntnisse verpflichtet. Selbst Kolleginnen und Kollegen der eigenen Fraktion dürfen sie keine dieser Informationen zugänglich machen. Zwar haben die Abgeordneten im Plenum grundsätzlich das Recht, von der Regierung und von Mitgliedern der Gremien Antworten auch auf Fragen zum Bereich der Nachrichtendienste zu verlangen, allerdings gilt dies nur in Fällen besonderer Dringlichkeit. Im Regelfall müssen die Parlamentarier im Plenum ihre Entscheidungen über Befugnisse und Haushalt der Dienste allein auf Grundlage der Empfehlungen ihrer Kolleginnen und Kollegen in den Gremien treffen, ohne die Tatsachenbasis dieser Empfehlungen auch nur im Ansatz zu kennen. An dieser dürftigen Informationslage vermag auch der jährliche Bericht der G10-Kommission wenig zu ändern, da er dem Bundestag üblicherweise erst mit mehreren Jahren

Verzögerung zugeleitet wird. So liegt beispielsweise der Jahresbericht 2012 bislang immer noch nicht vor.

Erschwerend kommt hinzu, dass selbst die mit der Kontrolle beauftragten Gremien nur bedingt Einblick in die Arbeit der Dienste haben. Die Ermittlungsmittel sowohl des Parlamentarischen Kontrollgremiums als auch der G10-Kommission beschränken sich auf Befugnisse zur Befragung von Mitarbeitern der Dienste, zur Akteneinsicht und zum Betreten behördlicher Räumlichkeiten. Diese Instrumente tragen nur in begrenztem Maße zu einer effektiven Informationsbeschaffung bei. So können die Mitglieder der Gremien naturgemäß nur in solche Vorgänge Einsicht nehmen, von denen sie bereits Kenntnis haben und die noch vollständig dokumentiert vorhanden sind, was, wie die geschredderten Akten im Fall des rechtsterroristischen NSU belegen, in Geheimdienstkreisen offenbar keineswegs selbstverständlich ist.

Zudem umfasst das Betretungsrecht lediglich die Möglichkeit, jederzeit Zutritt zu den Räumen der Dienste zu erhalten, nicht jedoch die Befugnis, dort gezielt nach Gegenständen oder Informationen zu suchen, welche die Dienste nicht von sich aus preisgeben wollen. Des Weiteren setzen sämtliche Maßnahmen der Gremien stets einen entsprechenden Mehrheitsbeschluss voraus. Gerade im Parlamentarischen Kontrollgremium, in dem aktuell sieben der neun Mitglieder den Regierungsfraktionen angehören, ist es daher verhältnismäßig leicht, unbequeme Fragen der Opposition gar nicht erst zuzulassen und oder deren Anträge auf Akteneinsicht oder Betreten frühzeitig abzublocken.

Während das System der parlamentarischen Aufsicht über die Nachrichtendienste in den vergangenen Jahren im Wesentlichen unverändert geblieben ist, haben die Möglichkeiten, unbemerkt in die Privatsphäre von Menschen einzudringen und ihre Kommunikation flächendeckend und lückenlos zu überwachen, massiv zugenommen. Mit dieser wachsenden Asymmetrie – zwischen der Intrusionstiefe einerseits und der rechtsstaatlichen Kontrolle andererseits – erhöht sich zugleich die Gefahr der Erosion rechtsstaatlicher Standards und die Entwicklung eines Staates im Staate. Setzt sich diese Entwicklung weiter ungehindert fort, so könnte sich die Demokratie, in der Bürgerinnen und Bürger aktiv am politischen Willensbildungsprozess teilhaben, in einen Untertanenstaat verwandeln, in dem Bevölkerung nur noch potentieller Störenfried ist, den es zu überwachen und zu kontrollieren gilt.

Obwohl es bereits in der Vergangenheit zahlreiche Affären und Skandale rund um deutsche Geheimdienste gab, in denen die parlamentarische Kontrolle versagt und erst mit Jahren Verzögerung eingesetzt hat (etwa in der sogenannten Journalisten-Affäre), vermittelt gerade ein Blick auf die Aktivitäten des BND bei der Überwachung des Internet- und Telefonverkehrs in jüngerer Zeit ein Gefühl dafür, wie schwach die Kontrolle tatsächlich ausgeprägt ist. Die Erhebung von Kommunikationsdaten am Knotenpunkt DE-CIX und ihre Weitergabe an die NSA

von 2004 bis 2007 gelangten erst mit mehreren Jahren Verzögerung zur Kenntnis des Parlamentarischen Kontrollgremiums und der G10-Kommission. Auch von der Ausspähung des NATO-Partners Türkei und dem Abschöpfen der Telefonate der US-Politiker Hillary Clinton und John Kerry erfuhren die Mitglieder der parlamentarischen Kontrollstellen erst aus den Medien. Und obschon die Snowden-Dokumente zahlreiche Hinweise auf verfassungswidriges Verhalten der Dienste liefern – angefangen bei der institutionalisierten massenhaften Übermittlung vom BND abgefangener Verbindungsdaten an die NSA bis hin zur aktiven Beeinflussung der Gestaltung und Auslegung der gesetzlichen Grundlagen für die Datenerhebung und -weitergabe –, stochern selbst die mit der Kontrolle beauftragten Gremien weiterhin im Nebel und sind nicht in der Lage, den Diensten Grenzen aufzuzeigen.

Es wird deutlich, dass die Entwicklung der rechtsstaatlichen Kultur gegenüber dem rasanten technischen Fortschritt und dem damit verbundenen Anwachsen der Überwachungsfähigkeit immer weiter ins Hintertreffen gerät. Zugleich scheint es bei den Diensten zum Sport geworden zu sein, rechtsstaatliche Kontrollen auszuhebeln und zu umgehen, als ginge es um ein lästiges Reglement, das ihrer Arbeit im Weg steht. Um dieser Tendenz entgegen zu wirken und das Aufsichtssystem auf Augenhöhe mit der Tätigkeit der Nachrichtendienste zu bringen, muss es grundlegend neu gedacht und reformiert werden. Leitgedanke eines solchen Systemupdates sollte es sein, die Kontrolle im Sinne der Gewaltenteilung auf möglichst viele unterschiedliche Säulen der Staatsgewalt zu verteilen.

Ausgangspunkt eines solchen Prozesses ist zunächst völlige Transparenz über die Tätigkeit der Dienste, da eine sinnvolle Debatte ebenso wie die politische Willensbildung nur auf der Grundlage ausreichender Informationen möglich ist. Dazu bedarf es insbesondere einer Offenlegung sämtlicher Verwaltungsvereinbarungen über die Kooperation deutscher und ausländischer Dienste. Zwar kann ein gewisses Geheimhaltungsinteresse der Dienste in Bezug auf ihre Tätigkeit nicht bestritten werden, jedoch machen nicht zuletzt die Snowden-Enthüllungen und die zahlreichen Versäumnisse bei der Zusammenarbeit mit den Kontrollgremien deutlich, dass hier die Grundfesten der Verfassung berührt werden. Vor dem Hintergrund des Auftrags und der Daseinsberechtigung der Dienste, nämlich die Verfassung zu schützen, muss das Geheimhaltungsinteresse zum Wohle des Grundgesetzes in diesem Fall zurückstehen.

Dringend verbesserungsbedürftig ist auch die Kontrolle der Dienste selbst. Dazu muss zunächst die personelle Ausstattung der Aufsichtsgremien drastisch ausgeweitet werden. Zur Zeit stehen den drei Nachrichtendiensten des Bundes mit mehreren Tausend Mitarbeitern gerade einmal neun Abgeordnete im Parlamentarischen Kontrollgremium gegenüber, welche die behördliche Tätigkeit neben ihrer eigentlichen Arbeit im Bundestag beaufsichtigen sollen. Um dieses Ungleichgewicht zu beseitigen, benötigt das Gremium neben einem eigenen Mitarbeiter-

stab einen Expertenbeirat, in dem die für eine effektive Kontrolle erforderlichen juristischen, technischen und operativen Fachkenntnisse gebündelt werden. Des Weiteren müssen die Befugnisse des Gremiums um echte Durchsuchungsrechte und Rechte zur Analyse der von den Diensten eingesetzten Hard- und Software ergänzt werden. Damit das Gremium nicht gezwungen ist, sich bei der Ausübung der Kontrolle allein auf offizielle Antworten der Dienste zu verlassen, sollte es zugleich als vertrauenswürdige Anlaufstelle für Whistleblower aus dem Kreis der Dienste fungieren. Dringender Überarbeitung bedarf auch das Verhältnis der Aufsichtsgremien zum Plenum.

Eine effektive Kontrolle der Dienste durch die Legislative setzt voraus, dass die Parlamentarier bei Entscheidungen über geheimdienstliche Befugnisse und Budgets weitgehend so informiert sind, dass ihnen zumindest klar ist, worüber sie eigentlich gerade Beschluss fassen. Daher müssen die Mitglieder des Parlamentarischen Kontrollgremiums und des Vertrauensgremiums im Haushaltsausschuss die Möglichkeit haben, innerhalb ihrer jeweiligen Fraktionen über ihre Erkenntnisse detailliert Bericht zu erstatten. Um sicherzustellen, dass die Kapazitäten der parlamentarischen Aufsicht mit denen der Dienste Schritt halten, sollte die finanzielle Ausstattung der Kontrollstellen zudem an die Budgetentwicklung der Nachrichtendienste gekoppelt werden.

Zur weiteren Stärkung des Gewaltenteilungsgrundsatzes muss der Rechtsschutz gegen Maßnahmen der Telekommunikationsüberwachung aus dem Verantwortungsbereich der G10-Kommission entfernt und vollständig in die Hände von Gerichten gelegt werden. Mit Rücksicht auf das Geheimhaltungsinteresse könnten diese Verfahren so lange nicht öffentlich geführt werden, bis Verstöße der Dienste gegen Verfassung und Grundrechte gerichtlich zweifelsfrei festgestellt sind. Darüber hinaus muss für die Berichte der G10-Kommission ein weitaus engerer zeitlicher Rahmen als bisher bestimmt werden, um dem Parlament eine schnelle Reaktion auf Fehlentwicklungen und Missstände im Bereich der Dienste zu ermöglichen. Auf Seiten der Exekutive schließlich sollte die Bundesbeauftragte für Datenschutz und die Informationsfreiheit aus dem Ressort des Bundesinnenministeriums ausgegliedert werden, da dieses zugleich Dienstherr des Bundesamtes für Verfassungsschutz ist.

Das Zusammenwirken all dieser Veränderungen wäre geeignet, das nötige Maß an Transparenz und Aufsicht über die Nachrichtendienste herzustellen, das eine tiefergehende und grundsätzliche gesamtgesellschaftliche Debatte über die Frage ermöglicht, ob und in welchem Ausmaß die Aktivitäten von Geheimdiensten in einem demokratischen Rechtsstaat akzeptabel sind.

Dieser Beitrag erschien zuerst am 17. September 2014 auf digitalegesellschaft.de.

Volker Tripp ist Jurist und arbeitet als politischer Referent beim Digitale Gesellschaft e.V.. Zuvor betrieb er ein juristisches Repetitorium in Berlin und war als freier Journalist tätig.

16 Modelle zu Reform und Abschaffung der Geheimdienste

von **Markus Reuter** und **Michael Stognienko**

Geheimdienste und Demokratie, das verträgt sich nicht. Denn in einer Demokratie ist der Staat den Bürgerinnen und Bürgern gegenüber zu Transparenz verpflichtet. Er muss Rechenschaft ablegen. Dies können die der Exekutive angegliederten Geheimdienste, weil sie ja geheim operieren, nicht – sie sind deswegen ein Fremdkörper in der Demokratie.

Der NSU-Skandal und der durch Edward Snowden aufgedeckte größte Überwachungsskandal der Menschheitsgeschichte haben eine neuerliche Debatte über die Zukunft der Geheimdienste befeuert und geheimdienstkritische Positionen gestärkt. Schon lange werden von liberaler, bürgerrechtsbewegter, grüner und linker Seite weitgehende Reformen oder die Abschaffung der Geheimdienste gefordert.

Wie kann eine solche Reform aussehen und wie eine Abschaffung? Wo besteht dringender Reformbedarf und wie werden bei einer Abschaffung Aufgaben der Geheimdienste neu verteilt? Welche Probleme bringt das mit sich und an welchen Stellen treten diese auf? Oder sind Geheimdienste gar ersatzlos abschaffbar?

Die Debatte um eine Einhegung oder Abschaffung der Geheimdienste ist nötig, auch vor dem Hintergrund, dass Geheimdienste bislang nach jedem Skandal, und das zeichnet sich auch in der NSA- und NSU-Affäre ab, mit höheren Budgets und erweiterten Kompetenzen[1] ausgestattet wurden.

Zu Reform und Abschaffung von Geheimdiensten gibt es in der Debatte hierzulande unterschiedliche Positionen und auch innerhalb geheimdienstkritischer Parteien wie den Grünen oder der Linkspartei besteht keine Einigkeit. Auffällig ist, dass die Reform und Abschaffung des Inlandsgeheimdienstes „Verfassungsschutz“ weitaus stärker thematisiert wird als die des Auslandsgeheimdienstes BND.

Im Folgenden sollen Reform- und Abschaffungsmodelle, ohne Anspruch auf Vollständigkeit der Varianten innerhalb dieser Modelle, aufgezeigt werden:

Reform: Geheimdienste reformieren, parlamentarische Kontrolle stärken

Diese Position geht davon aus, dass Geheimdienste verfassungsgemäß bzw. von der Verfassung vorgeschrieben seien. Im Grundsatz vertreten die Reformer die

Ansicht, dass Geheimdienste unverzichtbar seien. Als Kritik an denjenigen, die Geheimdienste abschaffen wollen, wird hervorgebracht, dass eine Abschaffung eine Vermischung polizeilicher und geheimdienstlicher Aufgaben mit sich bringen und damit das Trennungsgebot von Polizei und Geheimdiensten verletzen würde.

Vertreterinnen und Vertreter dieser Forderung sind der ehemalige Bundesrichter und Ex-Linkspartei-Abgeordnete Wolfgang Nešković[2], aber auch die Grünen, wo sie in Landesregierungen beteiligt sind.

Reformansätze sind unter anderem:

- Evaluierung des Frühwarnsystems: Gibt es überhaupt Erfolge, die durch geheimdienstliche Tätigkeiten entstanden sind?
- Eine umfassende Revision der Rechtsvorschriften im Bereich der Nachrichtendienste
- Beim Verfassungsschutz: Konzentration auf den Schutz der Verfassungsgrundsätze und Grundrechte vor einem gewaltsamen Umsturz und damit verbunden eine Konkretisierung des Schutzauftrages
- Eine Stärkung der administrativen Kontrolle
- Stärkung der parlamentarischen Kontrolle: Mehr Zeit zur Kontrolle für Mitglieder parlamentarischer Kontrollgremien, mehr Mitarbeiterinnen und Mitarbeiter für die Mitglieder der Gremien, Stärkung der Minderheitenrechte in den Gremien
- Strengere Richtlinien für V-Leute oder Verzicht auf diese

In Neškovićs Positionspapier war zudem die Auflösung und Umwandlung der Landesämter zu Außenstellen des Bundesamtes vorgesehen. Insbesondere diese Forderung löste innerhalb der Linkspartei heftige Kritik aus, weil sie eine Stärkung der Geheimdienste sei. Dort wo die Grünen an Regierungen beteiligt sind, streben sie Geheimdienstreformen an. So ist in NRW im Koalitionsvertrag[3] z. B. eine Stärkung des Kontrollgremiums, eine öffentliche Sitzung des Parlamentarischen Kontrollgremiums, mehr Transparenz durch eine erweiterte Berichtspflicht sowie verbindliche Richtlinien für V-Leute aufgenommen worden.

In Baden-Württemberg hingegen sträubt sich der SPD-Innenminister gegen Reformen[4], insbesondere solche, die Stellenstreichungen und Etatkürzungen für den Landesverfassungsschutz vorsehen.

Im Rot-Grün-regierten Niedersachsen richtete im September 2013 Innenminister Boris Pistorius eine Expertengruppe zur Reform des Niedersächsischen Verfassungsschutzes ein. Diese präsentierte im April 2014 ihre Ergebnisse in „Handlungsempfehlungen der Arbeitsgruppe zur Reform des niedersächsischen Verfassungsschutzes“[5] – die vorgeschlagenen Reformen gehen weniger weit als die oben

aufgezählten Forderungen. Die niedersächsischen Handlungsempfehlungen lassen sich auf folgende Kernaussagen herunterbrechen:

- Es braucht einen Verfassungschutz (Unverzichtbarkeit, Trennungsgebot)
- Gesetzliche Regelungen und Dienstabläufe sollen präzisiert werden
- Der Einsatz von V-Personen soll nur mit Zustimmung der G10-Kommission erfolgen
- Der föderale Aufbau des VS soll erhalten, die Zentralstellenfunktion des BfV gestärkt werden
- Präventiv- und Bildungsprogramme sollen erweitert werden
- Eine Dokumentation der Abläufe/Entscheidungen soll verstärkt erfolgen
- Parlamentarische Kontrollgremien sollen gestärkt werden, z. B. in Sachen Minderheitenrechte

Neustart: Verfassungsschutz auflösen, bei gleichzeitiger Neustrukturierung in Inlandsaufklärung und Demokratieförderung

Die Bundestagsfraktion der Grünen legte 2012 einen Beschluss[6] vor, nach dem der Verfassungsschutz aufgelöst werden solle. Das Papier sieht nach der Auflösung ein 2-Säulen-Modell vor:

> Ein unabhängiges „Institut Demokratieförderung", das keine hoheitlichen Befugnisse hat und insbesondere auch keine nachrichtendienstlichen Mittel anwenden darf, soll ganz überwiegend den Aufgabenbereich des jetzigen BfV übernehmen. Für einen verbleibenden kleinen Teil soll eine „Inlandsaufklärung" mit erheblich beschränkten Aufgaben und Befugnissen neu gegründet werden. Diese ist nur zuständig für die Aufklärung genau bestimmter Bestrebungen mit Gewaltbezug. Nur sie darf sehr eingegrenzt und auch nur als letztes Mittel geheimdienstliche Methoden einsetzen. Ihre Zuständigkeit endet, wenn die Zuständigkeit der Strafverfolgungsbehörden beginnt.

Als Aufgaben des Institutes werden folgende genannt:

> Das Institut ist zuständig für Beobachtung und Analyse von Strukturen und Zusammenhängen gruppenbezogener Menschenfeindlichkeit in Deutschland. Gewaltlose und gewaltbereite Bestrebungen, die sich gegen die Grund- und Menschenrechte, die nicht veränderbaren Grundsätze der Verfassung oder das friedliche Zusammenleben der Völker richten, sollen laufend beobachtet, erforscht und transparent gemacht werden.

Dabei soll das Institut ausschließlich auf öffentlich zugängliche Quellen zurückgreifen und die „Inlandsaufklärung" auf mögliche Zuständigkeiten hinweisen. Die Inlandsaufklärung soll beim Innenministerium angesiedelt sein und nur tätig werden, wenn Personen

- sich gegen die Grund- und Menschenrechte, die nicht veränderbaren Grundsätze der Verfassung oder das friedliche Zusammenleben der Völker richten und
- sich zu diesem Zweck tatsächlich auf die Anwendung von Gewalt und den Aufbau auf Gewalt ausgerichteter Handlungsstrukturen vorbereiten oder fortgesetzt gewalttätige Akteure unterstützen oder Kontakt zu diesen suchen.

Polizeiliche Aufgaben soll die „Inlandsaufklärung" nicht bekommen:

> Der Aufgabenbereich der neuen Inlandsaufklärung ist von dem der Polizei deutlich abzugrenzen. Sobald erkennbar wird, dass es um die Verhütung oder Verfolgung von Straftaten geht, endet die Zuständigkeit der Inlandsaufklärung.

Gleichzeitig fordert der Beschluss der Bundestagsfraktion einen personellen Neuanfang, präzisere Gesetze und eine Stärkung der parlamentarischen Kontrolle sowie eine Beschränkung von polizeilicher und geheimdienstlicher Zusammenarbeit.

Transfer: Geheimdienste abschaffen und notwendige Aufgaben der Geheimdienste teilweise in die Polizei integrieren

Bei allen Geheimdienst-Abschaffungsmodellen wird das Problem diskutiert, dass mit einer Abschaffung Aufgaben der Geheimdienste zur Polizei übergehen müssten oder könnten. Damit verbunden entstehen Probleme einer mächtigeren Polizei mit ggf. erweiterten Befugnissen – auch geheimdienstlicher Art.

Heiner Busch und Norbert Pütter[7] sehen die Abschaffung der Geheimdienste als alternativlos an:

> Die Dienste sind systematisch unkontrollierbar; in ihnen wird die Dominanz der Exekutiven auf die Spitze getrieben; und zugleich sind sie das am wenigsten rechtstaatlich-demokratisch begrenzte Instrument in den Händen herrschender Staatspolitik. Für eine an den Bürgerrechten orientierte Politik gibt es deshalb keine Alternative zur ersatzlosen Abschaffung der Geheimdienste.

Viele ihrer Aufgaben würden dann jedoch an die Polizei übergehen. Das wäre eine Abkehr vom Trennungsgebot[8] von Geheimdiensten und Polizei, das als Lehre aus dem nationalsozialistischen Reichssicherheitshauptamt[9] das Verhältnis von Geheimdiensten und Polizei im Nachkriegsdeutschland bestimmte, jedoch in vielen europäischen Ländern keine Rolle spielt.

Dieses Trennungsgebot ist heute aber schon z. B. durch geheimdienstliche Befugnissen beim BKA, Datenbanken, auf die Polizei und Dienste Zugriff haben, und gemeinsame „Lagezentren" wie das Cyberabwehrzentrum deutlich verwässert. Die Missstände beim Trennungsgebot werden in einem Reader der Grünen im Bundestag kritisiert[10].

Befürworter einer Abschaffung der Geheimdienste und Aufgabenverlagerung zur Polizei argumentieren, dass eine Polizei mit geheimdienstlichen Aufgaben zumindest an Polizei- und Strafprozessrecht gebunden sein müsste, sie müsste ihr Vorgehen in gerichtlichen Verfahren prüfen lassen. Dies wäre ein deutlicher Fortschritt im Vergleich zu den quasi unkontrollierbaren Geheimdiensten.

Wer allerdings heute sieht, wie schwierig es ist, eine transparente Polizei herzustellen oder Polizeigewalt zu ahnden, wird einige Bauchschmerzen mit erweiterten Befugnissen haben. Denkbar ist diese Option nur, wenn die Polizei selbst wirksamer als heute und von extern kontrolliert würde, damit keine Geheimpolizei mit ausufernden Befugnissen entstünde. Folglich sagen Busch und Pütter auch:

> Nicht die mächtigere Polizei ist die Alternative zu den abgeschafften Diensten, sondern die effektiv und extern kontrollierbare Polizei.

Auch Vertreter der ersatzlosen Abschaffung des Verfassungschutzes – wie Leggewie und Meier[11] – befürworten, dass das Personal des Geheimdienstes bei der Polizei weiterarbeitet:

> Die Ämter für Verfassungsschutz können binnen fünf Jahren geordnet abgewickelt werden, fähiges Personal kann man in den polizeilichen Staatsschutz eingliedern. Dieser ist seit jeher die für politisch motivierte Straftaten zuständige „politische Polizei". Die Arbeit speziell ausgebildeter Kriminalbeamter greift nicht ein in ein diffuses Feld des «Extremismus», sondern orientiert sich allein an der Verfolgung und Verhütung von Straftaten (in der Regel Gewalt- und ganz ausnahmsweise Propagandadelikte, wie Volksverhetzung).

Monitoring: Abschaffung der „geheimen“ Tätigkeiten der Geheimdienste, Umwandlung in Institute, die aus offenen Quellen wissenschaftlich arbeiten

Eine weitere Variante ist die Abschaffung eines Geheimdienstes bei gleichzeitiger Schaffung einer Stelle, die öffentlich zugänglich Informationen aggregiert und sammelt.

Im Falle des Verfassungsschutzes ist hier insbesondere der MdB Jan Korte von der Linkspartei mit einem 12-Punkte-Plan[12] in Erscheinung getreten. Hauptidee ist hier:

> Anstelle einer nachrichtendienstlich arbeitenden Behörde tritt eine Informations- und Dokumentationsstelle für Menschenrechte, Grundrechte und Demokratie in Bund und Ländern.

Im Reader der Bundestagsfraktion der Linken zum Thema[13] heißt es u. a.:

> Das BfV wird bis 2014 auf seine ursprünglichen Aufgaben der Informations- und Koordinationsstelle des Bundes für Fragen des Verfassungsschutzes ohne nachrichtendienstliche Kompetenzen reduziert. Alle Landesbehörden werden zu Abteilungen der Landesinnenministerien, wie es jetzt schon in der Hälfte der Bundesländer der Fall ist, umstrukturiert. Eine Ein- oder Unterordnung der Landesämter unter das BfV erfolgt nicht.
>
> Dem BfV und allen Landesbehörden bzw. Abteilungen der Länderinnenministerien werden die Grundlagen zur Informationserhebung mit nachrichtendienstlichen Mitteln entzogen [...]
>
> Der Verfassungsschutz in Bund und Ländern verliert alle Befugnisse zur Bekämpfung der organisierten Kriminalität bzw. seine quasi polizeilichen Befugnisse.
>
> Bundes- und Landesämter für Verfassungsschutz werden spätestens ab dem 01. Januar 2014 aus allen Kooperationsgremien wie GTAZ (Gemeinsames Terrorismusabwehrzentrum) , Gemeinsames Abwehrzentrum Rechts (GAR) und GASIM (Gemeinsames Analyse- und Strategiezentrum illegale Migration) zurückgezogen. Dasselbe gilt für die im Rahmen der Innenministerkonferenz (IMK) und ihrer Arbeitskreise eingerichteten Projekt- und Arbeitsgruppen [...]
>
> Alle Dateien und Akten in Bund und Ländern werden jeglicher nachrichtendienstlichen und polizeilichen Verwendung entzogen. Die entsprechenden automatisierten technischen Verbindungen zwischen

> den Sicherheitsbehörden werden gekappt. Unter Beteiligung der zuständigen Datenschutzbehörden werden Dateien und Akten gesichert, archiviert und der wissenschaftlichen Aufarbeitung sowie zur Information den Betroffenen zur Verfügung gestellt.

Die Zukunft des Verfassungsschutzes sieht in diesem Modell so aus:

> Mit diesen Sofortmaßnahmen sollen die Voraussetzungen geschaffen werden, der Verfassungsaufgabe – die freiheitliche, demokratische und soziale Verfassungsordnung zu schützen – vollumfänglich nachzukommen. An Stelle einer nachrichtendienstlich arbeitenden Behörde tritt eine Informations- und Dokumentationsstelle für Menschenrechte, Grundrechte und Demokratie in Bund und Ländern. Diese soll die Dokumentation neonazistischer, rassistischer, antisemitischer und anderer gegen die Grundsätze der Verfassung gerichteten Aktivitäten und Einstellungen, sowie ihre strukturellen und öffentlichen Erscheinungsformen vornehmen. Zu diesem Zwecke arbeitet sie wissenschaftlich und ist befugt, mit Dritten zu kooperieren. Informationen erhält das Informations- und Dokumentationszentrum nur aus öffentlich zugänglichen Quellen und wissenschaftlichen Studien.

Eine ähnliche Stoßrichtung verfolgt auch Martin Kutscha in einem Aufsatz[14] in der Publikation „Wer schützt die Verfassung?“ der Böll-Stiftung in Sachsen[15]:

> Geheimdienste hingegen sind schon wegen ihrer mangelnden Kontrollierbarkeit ein Fremdkörper im System eines demokratischen Rechtsstaates – daran ändert auch die höchst lückenhafte parlamentarische Kontrolle nichts. Schon vor drei Jahrzehnten brachte der unvergessene Jurist und Politikwissenschaftler Wolfgang Abendroth es treffend auf den Punkt:
>
> Meistens werden die Hilfsmittel der Staatsgewalt, die sich selbst für Verfassungsschutzorgane halten, umgekehrt zu potentiellen Quellen der Gefährdung des Verfassungsrechts. [...] Eine demokratische Verfassung kann stets nur durch die demokratische Willensbildung des Volkes gewährleistet bleiben. Den wirksamsten Schutz der demokratischen Verfassungsordnung können nur die Bürger und Bürgerinnen selbst leisten.

Streichen: Ersatzlose Abschaffung des Verfassungsschutzes (Geheimdienstes)

Die weitestgehende Forderung ist die ersatzlose Streichung der Geheimdienste bzw. des Verfassungsschutzes, die in Teilen der (digitalen) Bürgerrechtsbewe-

gung, in linksalternativen Zusammenhängen und auch bei Grünen und Linken wieder mehr Anklang findet.

Ein Memorandum der Humanistischen Union[16] mit Unterstützung des Arbeitskreises Vorratsdatenspeicherung, des Chaos Computer Clubs, von digitalcourage e.V., des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) und des Komitees für Grundrechte und Demokratie fordert, den Verfassungsschutz ersatzlos abzuschaffen.

Untermauert wird die Forderung in einem Memorandum „Brauchen wir den Verfassungsschutz? NEIN!“[17], das fünf Thesen voranstellt:

1. Eine demokratische Gesellschaft lebt von der Meinungsvielfalt. Radikale Auffassungen und Bestrebungen (die von den vorherrschenden Meinungsbildern abweichen) sind deshalb nicht nur zulässig, sondern auch wünschenswert – solange die Grenzen zur Strafbarkeit bzw. zu gewalttätigem Handeln nicht überschritten werden. Staatliche Behörden dürfen derartige Äußerungen weder als „verfassungsfeindliche“ oder „extremistische“ Bestrebungen abqualifizieren, beobachten oder gar verfolgen. Wir brauchen kein staatliches „Frühwarnsystem“ zur Beobachtung derartiger Auffassungen und Bestrebungen.

2. Geheimdienstlicher Verfassungsschutz ist schädlich, wie auch die zahlreichen Verfehlungen und Skandale in der Geschichte der Bundesrepublik zeigen. Es handelt sich dabei nicht um zufällige, persönliche oder vermeidbare Fehler, sondern systematisch bedingte Mängel eines behördlichen und geheimdienstlichen „Verfassungsschutzes“.

3. Die gesetzlichen Aufgaben der Verfassungsschutzbehörden sind überflüssig. Bei ihrem Wegfall entsteht keine Sicherheitslücke. Eine Aufgaben- und Befugnisüberleitung von den Verfassungsschutzbehörden auf die Polizei ist daher nicht erforderlich. Der Schutz vor Gewalt und Straftaten obliegt der Polizei, der Staatsanwaltschaft und den Gerichten.

4. Eine Kontrolle geheim arbeitender Verfassungsschutzbehörden, die rechtsstaatlichen und demokratischen Ansprüchen genügt, ist nicht möglich. Auch Kontrollverbesserungen sind untauglich: ein transparenter, voll kontrollierbarer Geheimdienst ist ein Widerspruch in sich.

5. Die Verfassungsschutzbehörden sind ersatzlos abzuschaffen – allein schon deshalb, um nicht in Zeiten knapper Kassen und in Beachtung der verfassungsrechtlichen Schuldenbremse jährlich eine halbe Milliarde Euro für überflüssige, ja schädliche Behörden auszugeben. Es bedarf auch keiner ersatzweisen, mit offenen Quellen arbeitenden staatlichen Informations- und Dokumentationsstelle über extremistische Bestrebungen. Das Problem

besteht nicht in einem mangelnden Wissen über radikale, bisweilen auch menschenverachtende Meinungen und Haltungen in unserer Gesellschaft. Die Auseinandersetzung darüber muss mit politischen, demokratischen Mitteln geführt werden; sie ist innerhalb der Gesellschaft zu führen.

Horst Meier und Claus Leggewie fordern in ihrem Aufsatz „Verfassungsschutz – Über das Ende eines deutschen Sonderwegs“:

> Was jetzt auf den Prüfstand muss, ist die gesamte Sicherheitsarchitektur der Berliner Republik. Wer den Verfassungsschutz behutsam aus dieser Konstruktion herausnimmt, braucht nicht zu gewärtigen, das ganze Gebäude der inneren Sicherheit stürze ein. Im Gegenteil: Die auf das Inland bezogene Sicherheitspolitik kann nur übersichtlicher und effizienter werden. Das Ende der Extremistenausspähung wird ein Zugewinn an Freiheit, also ein Gewinn für die Bürgerrechte sein.

Fazit

Nach dem NSU-Skandal und in der heutigen Situation der millionenfachen Überwachung aller Bürgerinnen und Bürger[18] durch ausländische Geheimdienste bei gleichzeitigem Datentausch und Abgleich mit deutschen Geheimdiensten, ist jede Maßnahme demokratisch geboten, die Geheimdiensten Schranken aufweist.

Der Grundwiderspruch Geheimdienst versus Transparenz in der Demokratie[19] wird sich durch zaghafte Reformen und eine leicht verbesserte parlamentarische Kontrolle nicht auflösen. Es wird mutigere Schritte brauchen, die Grundrechte der Bürgerinnen und Bürger zu schützen und gleichzeitig deren Sicherheit zu gewährleisten.

Dieser Beitrag erschien zuerst am 25. Juli 2014 auf der Webseite der Heinrich-Böll-Stiftung

Anmerkungen

[1] http://www.internet-law.de/2014/07/bundesregierung-nutzt-die-aktuelle-entwicklung-zur-ausweitung-von-geheimdienstaktivitaeten.html

[2] http://www.faz.net/aktuell/feuilleton/nsa-affaere-aufklaerung-statt-geheimdienst-12785196.html

[3] http://www.gruene-nrw.de/themen/dokumente/koalitionsvertrag/zusammenfassungen/verfassungsschutz.html

[4] http://www.swp.de/ulm/nachrichten/suedwestumschau/Zankapfel-Geheimdienst-Gruene-und-Innenminister-Gall-uneinig-ueber-Verfassungsschutzreform;art4319,2654455

[5] http://www.mi.niedersachsen.de/download/86620

[6] http://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/fraktion/beschluesse/Beschluss_Geheimdienste.pdf

[7] http://www.cilip.de/ausgabe/100/busch_puetter_dienste_abschaffen.htm

[8] http://de.wikipedia.org/wiki/Trennungsgebot_zwischen_Nachrichtendiensten_und_Polizei

[9]http://de.wikipedia.org/wiki/Reichssicherheitshauptamt

[10]http://www.gruene-bundestag.de/uploads/tx_ttproducts/datasheet/18-10-Reader-PolizeiNachrichtendienste-web.pdf

[11]http://www.weiterdenken.de/sites/default/files/downloads/Verfassungsschutz_Leggewie_Meier.pdf

[12]http://www.taz.de/!99705/

[13]http://http/dokumente.linksfraktion.net/download/130405-verfassungakiii-internet.pdf

[14]http://www.weiterdenken.de/sites/default/files/downloads/Verfassungsschutz_Kutscha.pdf

[15]http://www.weiterdenken.de/de/node/471

[16]http://www.humanistische-union.de/nc/aktuelles/publikationen/publikationen_detail/back/publikationen/article/brauchen-wir-den-verfassungsschutz/

[17]http://www.verfassung-schuetzen.de/wp-content/uploads/2013/09/HU2013_Memo-VS.pdf

[18]http://www.boell.de/de/2014/07/17/leben-im-ueberwachungsstaat

[19]http://www.boell.de/de/2014/07/21/geheimdienste-und-buergerrechte

Michael Stognienko ist Physiker und als Mitarbeiter der Abteilung Politische Bildung in der Heinrich-Böll-Stiftung tätig. Er koordiniert dort u.a. den Bereich EU-Fundraising.

Markus Reuter leitet seit Ende 2009 die Internetredaktion der Heinrich-Böll-Stiftung und ist Chefredakteur von metronaut.de.

17

„Framing“: Wie sich die ACTA-Gegner durchgesetzt haben

von **Katrin Tonndorf**

ACTA. Diese vier Buchstaben machten das Urheberrecht 2012 zum Tagesschau-Thema. Auf einmal wurden große Debatten zu einem netzpolitischen Problem geführt, über das bisher nur die Unterhaltungsindustrie mit ein paar Netzaktivisten stritt. Beide Interessengruppen versuchten, mit ihrer Sichtweise die Öffentlichkeit zu überzeugen. Welches „Framing“ sich durchsetzte, untersuchten Kommunikations- und Politikwissenschaftler der Uni Passau.

Der Konflikt um die Neugestaltung des Urheberrechts begann bereits weit vor ACTA. Seit die Filesharing-Plattform Napster und ihre Nachfolger die Geschäftsmodelle der klassischen Medienindustrie infrage stellten, hat die Unterhaltungsindustrie ihren Einfluss auf die Politik genutzt und erfolgreich für die Verschärfung des Urheberrechts geworben. Ergebnis dieser Bemühungen sind unter anderen das DMCA-Gesetz[1] in den USA und die IPRED-Richtlinie[2] in Europa. Trotz der Mobilisierungsversuche von Netzaktivisten erhielt IPRED im Jahre 2004 in der öffentlichen Berichterstattung nur wenig Aufmerksamkeit und wurde ohne größere Komplikationen vom EU-Parlament angenommen.

Einen ganz anderen Verlauf nahm hingegen das multilaterale Abkommen ACTA[3]. Im Kern sollte es internationale Standards im Kampf gegen Produktpiraterie und Urheberrechtsverletzungen etablieren, weshalb es häufig als Anti-Piraterie-Abkommen bezeichnet wurde. Entwürfe zum ACTA-Abkommen lagen bereits seit 2010 vor; bis dann im Frühjahr 2012 – nur kurz vor der geplanten Ratifizierung – umfangreiche Proteste und eine intensive Medienberichterstattung folgten. Die konkurrierenden Interessengruppen der Unterhaltungsindustrie und Netzaktivisten vertraten in diesen Konflikt grundverschiedene Ansichten.

Argumentationen und Einordnungen werden zu einer Aussagenstruktur verbunden

Um ihre Deutungs- und Interpretationsmuster in der öffentlichen Debatte zu positionieren, waren die Argumentationsrahmen von zentraler Bedeutung. Die Kommunikationswissenschaft spricht hier von Framing, in etwa „Umrahmung“. Beim Framing werden ausgewählte Aspekte eines Themas hervorgehoben und durch Argumentationen und Einordnungen zu einer kohärenten, sprich zusammenhängenden Aussagenstruktur verbunden.

Eben dieses „Framing“ untersuchte ein Lehrforschungsprojekt mit Studentinnen und Studenten der Universität Passau am Lehrstuhl für computervermittelte Kommunikation. Im Laufe der Untersuchung ermittelten die beteiligten Wissenschaftler und Studenten die Argumentationsrahmen (Framing-Strategien) der ACTA-Unterstützer und -Gegner durch eine Analyse von Texten auf deren Webseiten. In einem zweiten Schritt analysierten sie, wie diese Argumentationsrahmen in der Berichterstattung deutscher Leitmedien vorkamen – im Zeitraum vom 1. Januar 2012 bis zum 18. Juli 2012.

Hierfür griffen sie Artikel über ACTA aus reichweitenstarken Print- und Onlinemedien heraus: Süddeutsche Zeitung, FAZ, Rheinische Post, Freie Presse Passau, Spiegel Online, Focus Online, Süddeutsche.de. In den gefundenen 248 Artikeln zählten sie anschließend per Inhaltsanalyse aus, wie häufig die verschiedenen Positionen und Argumente der ACTA-Befürworter und Gegner erwähnt wurden.

Befürworter: Wohlstand und Rechtssicherheit

Der Ausgangspunkt der Debatte lag für die Unterstützer des Abkommens im vorgelagerten Problem der massenhaften Urheberrechtsverletzungen durch Internetnutzer. Dieses Problem sollte durch ACTA gelöst werden. Zur Untermauerung dieser Sichtweise betrachteten die Unterstützer die Thematik in verschiedenen Kontexten: Argumentationen aus rechtlicher, wirtschaftlicher und kultureller Sicht verbanden sie miteinander zu einem „Rahmen“ oder eben „Frame“. In rechtlicher Hinsicht – so argumentierten sie – werde ACTA bessere Möglichkeiten zur Verfolgung von Urheberrechtsverletzungen schaffen, wodurch Rechtssicherheit erreicht werde.

Diese Rechtssicherheit werde sich positiv auf die wirtschaftliche Situation auswirken. So werde der Erfolg von Unternehmen der Unterhaltungsindustrie gesichert, was nicht nur Arbeitsplätze sondern den allgemeinen gesellschaftlichen Wohlstand schütze. Darüber hinaus betonten sie auch positive kulturelle Aspekte. Durch ACTA werde die Existenzgrundlage von Künstlern geschützt, wodurch diese wiederum ein reichhaltiges und innovatives kulturelles Angebot schaffen könnten.

Gegner: Rechtsunsicherheit und vage Formulierungen

Die Gegner des Abkommens diskutierten ACTA in denselben Kontexten – nahmen allerdings vollkommen andere Bewertungen vor. Aus ihrer Sicht werde ACTA Rechtsunsicherheit schaffen, da das Abkommen vage Formulierungen enthalte und eine privatisierte Rechtdurchsetzung fördere. Diese Unsicherheit werde innovative neue Geschäftsmodelle im Mediensektor verhindern. Von dem erweiterten Schutz würden, wenn überhaupt, nur die großen Konzerne und nicht die einzelnen Künstler profitieren.

Sowohl in wirtschaftlicher als auch kultureller Hinsicht werde das Abkommen deshalb negative Auswirkungen haben, so die Gegner. Über diese drei Argumen-

tationsfelder hinaus führten die Gegner mögliche negative Konsequenzen für die Konsumenten- und Bürgerrechte an, zudem das intransparente und von Lobbyeinflüssen geprägte Verfahren. Die ACTA-Befürworter wiesen eine Gefährdung der Grundrechte vehement zurück, entwickelten in diesem Argumentationsfeld allerdings – interessanterweise – keine eigene Aussagen.

Siegeszug der Netzbürger

- Den ersten Höhepunkt erlebte die Berichterstattung, als Deutschland die Ratifizierung des Abkommens am 9. Februar 2012 vertagte und am 11. Februar die erste europaweite Anti-ACTA-Demo stattfand[4].
- Den zweiten Höhepunkt löste kurz danach die Bekanntgabe aus, dass ACTA vom Europäischen Gerichtshof geprüft[5] werden soll. Danach flaute die Berichterstattung deutlich ab.
- Sie setzte erst kurz vor dem Abstimmungstermin des EU-Parlaments am 4. Juli wieder ein[6].

Die untersuchten Artikel verteilten sich in etwa gleichmäßig auf Print-(122) und Onlinemedien (126). Signifikante Unterschiede bei den verwenden Argumenten waren zwischen Print und Online allerdings nicht festzustellen.

Argumente zu Konsumenten-, Bürger- und Freiheitsrechten dominierten

In den 248 analysierten Artikeln wurden die Aussagen der Befürworter und der Gegner von ACTA insgesamt 763 Mal genannt. In den Argumentationsfeldern „Kultur und Wirtschaft" folgte die Medienberichterstattung den Interpretationsmustern der ACTA-Befürworter. Von den 99 Aussagen aus diesen Themenkomplexen waren mehr als 75 Prozent unterstützend. Insgesamt dominierte jedoch die Argumentation im Kontext der Konsumenten- und Bürgerrechte. Die Aussagen der ACTA-Gegner wurden hier 222 Mal aufgegriffen. Die Bedenken der Netzaktivisten, ACTA könnte zu einer Einschränkung der Freiheitsrechte und der privaten Internetnutzung führen, wurden in mehr als 80 Prozent der Artikel aufgegriffen.

Die Behauptung der Befürworter, dass eine solche Gefahr – Einschränkung der Freiheitsrechte und der privaten Internetnutzung – gar nicht besteht, wurde 91 Mal erwähnt. Ebenfalls sehr häufig wurde das Abkommen im Kontext der Rechtssicherheit und -durchsetzung diskutiert. In 119 Fällen gingen die Artikel auf das intransparente und von Lobbyeinflüssen geprägte Verfahren ein. Für diesen Themenkomplex hatten die ACTA-Befürworter keine oder nur wenig schlagkräftige Gegenargumente. Insgesamt nahmen nur 29 Artikel eine positive Position gegenüber ACTA ein; 112 waren neutral, während 117 eine negative Position gegenüber dem Abkommen erkennen ließen.

Die ACTA-Gegner haben es also geschafft, mit der Fokussierung auf Konsumenten-, Bürger- und Freiheitsrechte ihre Sichtweise in der öffentlichen Berichterstattung öfter und wirksamer zu platzieren. Interessanterweise begründete das EU-Parlament seine Ablehnung des Abkommens mit zentralen Aussagen aus dem Argumentationsrahmen (Frame) der ACTA-Gegner.

Der Kampf um das Urheberrecht ist noch lange nicht entschieden

Mit der Ablehnung von ACTA ist der Kampf um eine Erneuerung des Urheberrechts noch lange nicht entschieden. Im Rahmen neuer Abkommen, wie den Freihandelsabkommen TAFTA, TTIP oder auch CETA[7] – zwischen Kanada und der EU – werden bereits neue Regelungen diskutiert, die auch das Urheberrecht im digitalen Zeitalter betreffen könnten. Im Internet formieren sich bereits die Interessengruppen, um ihre jeweiligen Positionen und Argumente durchzusetzen.

Was der Diskussion fehlt, ist eine Auseinandersetzung mit dem Urheberrecht an sich. Um den Konflikt zu lösen, müssen grundsätzlich neue Ansätze diskutiert werden, wie eine Balance zwischen der Entlohnung des Urhebers und dem Gemeinwohl zukünftig ermöglicht werden kann. Wie wichtig dabei klare und nachvollziehbare Argumentationsrahmen sind, zeigt unsere Untersuchung.

Dieser Beitrag erschien zuerst am 10. März 2014 auf iRights.info.

Anmerkungen

[1] http://de.wikipedia.org/wiki/Digital_Millennium_Copyright_Act

[2] http://de.wikipedia.org/wiki/Richtlinie_2004/48/EG_(Schutz_der_Rechte_an_geistigem_Eigentum)

[3] http://irights.info/neue-broschre-acta-der-big-bang-der-netzpolitik

[4] http://irights.info/2012/02/11/warum-acta-nicht-in-kraft-treten-darf/3550

[5] http://irights.info/alexander-alvaro-fdp-acta-ist-nicht-am-ende

[6] http://irights.info/der-spuk-ist-aus-reaktionen-auf-das-scheitern-von-acta

[7] http://irights.info/was-das-ceta-abkommen-fuers-urheberrecht-bedeuten-koennte

Katrin Tonndorf ist wissenschaftliche Mitarbeiterin am Lehrstuhl für computervermittelte Kommunikationen der Universität Passau.

18 TTIP und TISA: Die USA wollen Datenschutz wegverhandeln

von **Ralf Bendrath**

In den Verhandlungen zum transatlantischen Freihandelsabkommen (TTIP) zwischen den USA und der EU wird man sich auch den Themen E-Commerce und transatlantischen Datenflüssen widmen. In diesem Zusammenhang gibt es immer mehr Hinweise darauf, dass die europäischen Datenschutzstandards durch ein solches Handelsabkommen unterwandert werden könnten. Zivilgesellschaft und Verbraucherorganisationen sowohl in der EU als auch den USA[1] warnen, dass die Entwürfe der Kapitel zu E-Commerce und elektronischen Datenflüssen das Datenschutzgrundrecht in der EU bedrohten.

EU: „Haltet den Datenschutz aus den Handelsgesprächen heraus"

Die Verhandlungsführer der EU-Kommision haben wiederholt öffentlich betont, dass sie nicht über ein Mandat für die Verhandlung von Regeln für den Datenschutz verfügten (so zum Beispiel bei der Anhörung der Grünen/EFA-Fraktion im Europaparlament am 5. März 2014[2]). Auch die damalige EU-Justizkommissarin Viviane Reding hat dies in einer Rede in Washington im Oktober 2013 betont[3]:

> [...] Es gibt Themen, die TTIP leicht entgleisen lassen könnten. Eines davon sind Daten und der Schutz persönlicher Daten. In der EU ist dies ein wichtiges Thema, weil Datenschutz ein Grundrecht ist. [...] Aus diesem Grund warne ich davor, Datenschutz in die Handelsgespräche einz. B.ziehen. Datenschutz ist ist kein Verwaltungsaufwand und keine Zollgebühr. Datenschutz ist ein Grundrecht und als solches nicht verhandelbar.

Das Verhandlungsmandat der EU-Kommission bezieht sich stattdessen auf Art. XIV des Allgemeinen Abkommens über Handel mit Dienstleistungen (GATS) der Welthandelsorganisation, welches eine allgemeine Ausnahmeklausel enthält[4]:

> Unter der Voraussetzung, daß Maßnahmen nicht in einer Weise angewendet werden, die ein Mittel zu willkürlicher oder unberechtigter Diskriminierung unter Ländern, in denen gleiche Bedingungen herrschen, oder eine verdeckte Beschränkung für den Handel mit Dienst-

leistungen darstellen würde, darf dieses Übereinkommen nicht dahingehend ausgelegt werden, daß es die Annahme oder Durchsetzung von Maßnahmen eines Mitglieds verhindert [...]

c) die erforderlich sind, um die Erhaltung von Gesetzen oder sonstigen Vorschriften zu gewährleisten, die nicht im Widerspruch zu diesem Übereinkommen stehen, einschließlich solcher: [...]

ii) zum Schutz der Persönlichkeit bei der Verarbeitung und Weitergabe personenbezogener Daten und zum Schutz der Vertraulichkeit persönlicher Aufzeichnungen und Konten

Das Verhandlungsmandat der EU-Kommission besagt in Art. 18[5]:

> Das Abkommen wird der Durchsetzung von Ausnahmen für die Erbringung von Dienstleistungen nicht entgegenstehen, die nach den einschlägigen WTO-Regeln (Art. XIV und XIVbis GATS) zu rechtfertigen sind.

Art. XIV des GATS wurde in der Tat wörtlich in einen Textentwurf für das TTIP-Abkommen übernommen, der von den Verhandlungsführern der EU-Kommission im Juli 2013 vorgeschlagen und im Februar 2014 geleakt wurde[6].

Also ist alles gut? Mit Sicherheit nicht. Dies ist nur das Mandat der EU-Verhandlungsführer. Aber bei jedem internationalen Abkommen gehören zum Tango immer zwei.

„Interoperabilität" oder „Angemessenheit"?

Auf der amerikanischen Seite gab es bereits zahlreiche Versuche, die europäischen Datenschutzregeln im Zusammenhang mit den Handelsgesprächen auszuhöhlen. Neue Lobbyverbände wurden gegründet, wie zum Beispiel die Coalition for Privacy and Free Trade – die Koalition für Privatsphäre und freien Handel, die von der US-Anwaltskanzlei Hogan Lovells gesteuert wird und einige politische Schwergewichte zu seinen Mitgliedern zählen kann[7].

Ein wiederkehrendes Thema dieser Lobby-Bemühungen war in den letzten Jahren der Versuch, auf die „Interoperabilität" zwischen den amerikanischen und den europäischen Regel des Datenschutzes zu drängen. Dies würde im Grundsatz eine gegenseitige Anerkennung der jeweiligen Regeln auf der anderen Seite des Atlantiks bedeuten, möglicherweise mit ein paar juristischen Tricks, um es solide erscheinen lassen.

Der Haken: In der Vereinigten Staaten gibt es derzeit keine umfassenden Datenschutzgesetze. Die Safe-Harbor-Entscheidung von 2000[8], durch welche sich amerikanische Firmen freiwillig den europäischen Standards unterwerfen können,

um damit persönliche Daten aus Europa verarbeiten zu dürfen, ist weitgehend wirkungslos. Das Europaparlament hatte Safe Harbor schon zur Zeit seiner Entwicklung im Jahre 2000 kritisiert. Im Abschlussbericht der Untersuchung zu den NSA-Enthüllungen wurde am 12. März 2014[9] sogar dessen Aufhebung gefordert. Aus europäischer Sicht gibt es also nichts, was als „interoperabel" zu bezeichnen wäre, mit der Ausnahme freiwilliger Maßnahmen zur Selbstregulierung und den üblichen, nicht durchsetzbaren Verpflichtungen zur Transparenz, die dem Verbraucher „Wahlmöglichkeiten" geben, die unter langen und unlesbaren Geschäftsbedingungen versteckt sind[10].

„Interoperabilität" ist ein Versuch, europäische Datenschutzstandards zu untergraben. Die Anforderungen des Datenschutzes in der EU enthalten weit mehr als „Interoperabilität". Art. 25 der Datenschutzrichtlinie von 1995 verlangt, dass

> [...] die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

Kurz: Die europäische Grundlage für die Übermittlung personenbezogener Daten an Drittländer ist die „Angemessenheit" von deren Datenschutzsituation. Auf Seiten der USA versucht man, das durch bloße „Interoperabilität" zu ersetzen.

Einige europäische Datenschutzexperten sind bereits Teil dieses „Interoperabilität"-Manövers. Ende April 2014 haben das Massachusetts Institute of Technology und die Universität Amsterdam eine Reihe von Gesprächsrunden mit dem Titel Privacy bridges – Datenschutzbrücken – veranstaltet.

> mit dem Zweck, Rahmenbedingungen für praktische Interoperabilitätsmöglichkeiten zu entwickeln, um die Lücken zwischen den Rechtssystemen der Europäischen Union und der Vereingten Staaten zu überbrücken. [...] In den nächsten 18 Monaten wird die Gruppe ein gemeinsames Weißbuch vorbereiten, das einen Weg nach vorne aufzeigt zwischen der EU und den USA. Die Bestrebungen zielen darauf ab, einen Rahmen praktischer Möglichkeiten zu schaffen, der starke, weltweit akzeptierte Werte der Privatsphäre in einer Weise voranbringt, die Interoperabilität erschafft und die inhaltlichen und prozeduralen Unterschiede zwischen beiden Rechtssystemen respektiert[11].

Unter den Teilnehmern befinden sich ein paar wohlbekannte Datenschützer und Verfechter der Privatsphäre, wie der frühere Bundesdatenschutzbeauftragte Peter Schaar. Andere haben wiederum enge Verbindungen zur Industrie, die hinter

einer universitären Anbindung verschleiert wird[12]. Alles, was in diesem Kontext entwickelt wird, könnte später in TTIP landen. Der Anspruch des „privacy bridges"-Projektes schließt Änderungen in den Gesetzen der USA aus. Ironischerweise stellt sogar das Weiße Haus in seinem etwa gleichzeitig mit dem Start von Privacy Bridges veröffentlichten Big Data Report explizit fest, dass der rechtliche Schutz von Nicht-Amerikanern im US- Datenschutzrecht ausgeweitet werden müsse[13]. Nach der ersten Publikation dieses Artikels im September 2014 als Statewatch-Analyse diskutiert das Projekt „privacy bridges" nun, den Begriff „Interoperability" fallen zu lassen[14].

Ein paar schwergewichtige Industrie-Player gehen noch einen Schritt über „Interoperabilität" hinaus. Die Business Coalition for Transatlantic Trade, die von der US-Handelskammer gegründet wurde, verlangt nach einem „Rechtsrahmen, der Flexibilität im Umgang mit der Privatsphäre erlaubt und die kooperative Zusammenarbeit in Sicherheitsfragen fortführt." – ganz so, als hätte es nie die NSA-Leaks gegeben und als gäbe es in Europa kein Grundrecht auf Datenschutz.

Sind „Schengen-Routing" und eine „EU-Cloud" Handelshemmnisse?

Auf amerikanischer Seite hat man nun seit einigen Monaten mit einem semantischen Trick gespielt. Es begann im Kontext der europäischen Reaktionen auf die durch Snowden bekannt gewordene Überwachungsaffäre. Von verschiedenen Seiten wurden Vorschläge zur Änderung des Routings von Internetpaketen gemacht. Diese sollten einem bestimmten Pfad folgen und in der EU verbleiben oder sogar nur in Deutschland, wenn sowohl Sender als auch Empfänger sich dort befänden. Solche Vorschläge wurden – aus unterschiedlichen Motiven – von verschiedenen Seiten gemacht, etwa vom Datenschutzexperten Ian Brown[15] von der Universität Oxford, aber auch von der Deutschen Telekom AG[16].

Was auf den ersten Blick als vernünftige Idee erscheint – warum sollte eine E-Mail von Brüssel nach Berlin durch New York oder andere Gegenden mit fragwürdiger Gesetzeslage geleitet werden? – ist technisch nicht einfach und kann sogar durch seine möglichen Nebenwirkungen gefährlich werden. Technisch ist es nicht trivial, weil das Internetprotokoll bei IP-Adressen einen logischen Adressraum verwendet, der nicht weiß, welchen geografischen Standort die IP-Adresse der darunter liegenden physischen Transportebene hat. Dienste, welche die Ortsbestimmung der IP-Adresse ermöglichen, erreichen nur eine Annäherung: Weil es drei offizelle Standorte des Europaparlaments gibt (Brüssel, Luxemburg, Straßburg), sieht meine eigene IP-Adresse im Europaparlament in Brüssel so aus, als wäre ich in Luxemburg.

Aber selbst wenn Geo-Routing technisch machbar wäre, kann es doch nicht unser Ziel sein, die Topologie des transnationalen, weltweiten Internets entlang der Ländergrenzen neu zu formen. Dies würde schnell unerwünschte Folgen nach sich ziehen, beispielsweise Rufe nach „Einwanderungskontrollen" für Datenpa-

kete, was gleichbedeutend mit Internetzensur wäre[17]. Die Grünen haben im Europaparlament eine Änderung zum Abschlussbericht der NSA-Untersuchung eingereicht, derzufolge der gesamte Internetverkehr Ende-zu-Ende verschlüsselt werden soll, weil es dann nicht länger eine Rolle spielt, wo die Daten entlang fließen. Der Änderungsantrag wurde als Teil eines im Februar 2014 im Ausschuss abgestimmten Kompromisses angenommen und anschließend im März 2014 im Plenum des Parlaments bestätigt[18].

Nachdem die Debatte über nationales oder zumindest europäisches Routing zu Anfang des Jahres 2014 schon tot geglaubt war, drängte Bundeskanzlerin Angela Merkel in ihrem wöchentlichen Podcast erneut auf ein europäisches Routing[19]. http://netzpolitik.org/2014/aus-neuland-wird-schengenland-merkel-fuer-aufbau-europaeischer-kommunikationsnetzwerke, 16. Februar 2014. Dies wurde breit in den Medien aufgegriffen – die Debatte köchelt seitdem weiter.

Von amerikanischer Seite wird die Debatte jetzt dazu genutzt, europäische Regeln und Begrenzungen für die Übermittlung personenbezogener Daten an Drittstaaten anzugreifen. Sie werfen Begriffe wie „Schengen-Netzwerk“ und „Cloud Computing“ in einen Topf mit den Drittstaaten-Regeln der EU-Datenschutzrichtlinie und betiteln alles gemeinsam als „Lokalisierung“. Der US-Handelsbeauftragte Michael Froman vertrat dies in der Vorstellung[20] seines Berichts über die Handelsabkommen für den Telekommunikationsmarkt[21]. Er behauptete, die europäischen „Lokalisierungs“-Regeln, die den Datentransport oder die Datenverarbeitung in Europa verlangen, würden ein illegales Handelshemmnis darstellen. Die Business Coalition for Transatlantic Trade argumentiert in die gleiche Richtung. Sie fordert, dass das TTIP-Abkommen „verbietet, dass Dienstleister lokale Server und andere Infrastrukturen verwenden oder eine eine lokale Niederlassung errichten müssen.“[22]

Hier ist es allerdings sehr wichtig, Routing und Datenverarbeitung klar zu trennen[23]. Während das Aufstellen von Regeln für das Routing von Datenpaketen eine schlechte Idee sein mag, ist es auf der anderen Seite sehr entscheidend, wo die Daten verarbeitet werden – insbesondere wenn es sich dabei um personenbezogene Daten handelt. Auch auf europäischer Seite haben viele noch nicht vollständig verstanden, dass die EU-Regeln des Datenschutzes ganz grundlegend auch Regeln für die Lokalisierung sind. Weil Datenschutz in Europa ein bindendes Grundrecht mit Verfassungsrang in der EU-Charta der Gurndrechte ist, können personenbezogene Daten prinzipiell erst einmal nur in Europa verarbeitet werden. Alle Regeln, die die Übertragung von Daten in Drittländer ermöglichen, stellen Ausnahmen von diesem Prinzip dar und müssen deshalb bestimmte Bedingungen erfüllen – wie beispielsweise ein angemessenes Schutzniveau in dem jeweiligen Drittland.

In Zeiten der Post-Snowden-Ära gibt es in Europa eine eine umfassende Debatte über strengere Bedingungen für die Übermittlung personenbezogener Daten in die USA und andere Drittländer. Das Europaparlament hat einen neuen Art. 43a in seine Version der kommenden Datenschutzverordnung eingeführt[24], welcher die Behörden von Drittländern davon abhalten soll, ohne ein gegenseitiges Rechtshilfeabkommen Daten von europäischen Datenverarbeitern zu verlangen. Nun wird der Europäische Gerichtshof entscheiden müssen, ob Datenübertragungen in die USA unter dem Safe-Harbor-Abkommen immer noch legal sind, nach einer Vorabentscheidung des Hohen Gerichts Dublin auf Basis einer Beschwerde des Österreichers Max Schrems und seiner Aktivistengruppe Europe vs. Facebook[25].

Der Digital Trade Act und TTIP

Der amerikanische Handelsbeauftragte Michael Formman steht nicht alleine da. Dem US-Senat wurde im Dezember 2013 ein Entwurf für einen Digital Trade Act vorgestellt[26] Dieser würde Vertretern der Vereinigten Staaten ein bindendes Mandat für internationale Verhandlungen zum E-Commerce in die Hand geben. Regelungen zur „Lokalisierung" würden dann verbannt werden müssen, während die „Interoperabilität" der Datenverarbeitung als Grundprinzip verankert würde. Dieses Gesetz würde natürlich auch für die Verhandlungen der entsprechenden Kapitel in TTIP angewendet werden. Ähnliche Bestimmungen finden sich auch in dem Entwurf des parteiübergreifenden Trade Priorities Act, der im Januar 2014 im US-Senat vorgestellt wurde[27].

Entwürfe von Verhandlungsführern der USA zum E-Commerce in TTIP enthalten bereits diese beiden entscheidenden Aspekte: das Prinzip der „Interoperabilität" europäischer und amerikanischer Datenschutzbstimmungen und das Verbot der „Lokalisierung"[28]. Es ist offensichtlich, dass die amerikanischen Verhandlungspartner, mit Rückhalt durch die Industrie, massiv darauf drängen, diese Punkte im endgültigen Abkommen zu behalten. Im Oktober 2014 haben die US-Verhandlungspartner einen konkreten Textvorschlag zu „Datenflüssen" vorgelegt. Niemand außerhalb der EU-Kommission kann derzeit seine Bedeutung beurteilen. Die Geheimhaltung der Verhandlungen hält sogar den TTIP-Berichterstatter des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) im Europaparlament davon ab, die Schriftstücke einzusehen – dabei ist dieser Ausschuss für den Datenschutz zuständig. Informell bestätigen US-Verhandler aber, dass in dem Text genau die beiden Punkte – „Interoperabilität" und das Verbot von „Lokalisierung" stehen.

Die EU-Kommission ist durch ihr Verhandlungsmandat verpflichtet, den Forderungen der USA zur Aufweichung des Datenschutzes in keiner Weise entgegenzukommen. Allerdings führen internationale Verhandlungen immer zu Kompromissen. Es ist stark anzunehmen, dass TTIP zumindest in abgeschwächter

Form Regulierungen beinhalten wird, die europäische Datenschutzstandards unterwandern, z. B. bei der Limitierung des Interpretationsraumes für die Ausnahmeklausel des GATS auf außergewöhnliche Umstände.

TTIP auf Steroiden: Das Abkommen über den Handel mit Dienstleistungen (TiSA)

Gleichzeitig zu den TTIP-Verhandlugen und ein Jahr lang weitgehend unbemerkt von der Öffentlichkeit, finden die plurilateralen Verhandlungen zum Abkommen über den Handel mit Dienstleistungen statt. Das sogenannte Trade in Services Agreement (TiSA) würde GATS in den beteiligten Ländern ablösen – bis jetzt sind das die USA, die EU und 21 weitere Industrieländer[29]. Die US-Industrie ist durch die in den letzten Monaten zunehmende öffentliche Kritik an TiSA aufgeweckt worden und hat, wie bereits bei TTIP, eine PR-Kampagne zugunsten einer Lockerung von Handelsbeschränkungen begonnen. Die TiSA Business Coalition, auch „Team TiSA"genannt, wurde am 18. Juni 2014 in Anwesenheit des US-Handelsbeauftragten und des Japanischen Botschafters gestartet[30].

Ein erklärtes Ziel der Verhandlungen zu TiSA ist es, die Ausnahmen in GATS abzuschaffen, die bestimmte nicht-tarifäre Handelsbeschränkungen schützen, wie unter anderem den Datenschutz[31]. Dies wird durch ein erstes Leak der TISA-Dokumente veranschaulicht. In einem Entwurf für den Finanzdienste-Anhang zu TiSA, der auf Wikileaks am 19. Juni 2014 veröffentlicht wurde, wird es Finanzinstitutionen wie Banken erlaubt, selbst personenbezogenen Daten frei von einem Land ins andere zu übertragen[32]. Dies würde eine radikale Ausnahme von Europäischen Datenschutzregeln bedeuten. Die Übertragung und Analyse von Finanzdaten aus der EU zum „Terrorist Finance Tracking"-Programm (TFTP) in den USA hat bereits einmal die Beziehungen zwischen den Verhandlungspartnern erschüttert und dazu geführt, dass das Europaparlament 2010 sein Veto für das Abkommen einlegte. Der Textentwurf auf dem TISA-Leak würde nun wirklich alle Schleusen öffnen und den Datenschutz den Bach herunter gehen lassen.

Die Schwächung der Datenschutzgesetze der EU in TiSA umfasst noch mehr als „nur" den Finanzsektor. Quellen zufolge, die in die Verhandlungen involviert sind, enthalte der Entwurf zum Anhang „E-Commerce und Telekommunikation" Bestimmungen, die keine Beschränkungen für grenz. B.rschreitende Informationsflüsse mehr zulassen und auch Lokalisierungsanforderungen für Dienstleister im IKT-Bereich verböten. Von den US-Unterhändlern wurde auch eine Formulierung vorgeschlagen, die jegliche Bedingungen für die Übermittlung personenbezogener Daten an Drittländer, wie sie seit 1995 im europäischen Datenschutzrecht existieren, ausschließen würde. Eine weitere Vorschrift, die ebenfalls von den US-Verhandlern eingebracht wurde, würde jegliche Vorgaben für die elektronische Datenverarbeitung innerhalb des jeweiligen Landes verbieten.

Ortsgebundenheit personengebundener Daten als Grundrecht

Durch die Enthüllungen von Edward Snowden ist offensichtlich geworden, dass Europa dringend in den Wiederaufbau einer eigenständigen IT-Industrie investieren müsste, von der Hardware-Ebene bis hin zu Anwendungen und Diensten, wenn es sich vor der Massenüberwachung der NSA schützen will. Europäische Behörden und Privatunternehmen bestehen immer auf Vorschriften zur Lokalisierung, wenn sie Computerdienste einkaufen, um sicherzugehen, dass ihre sensiblen Daten nicht in Gebieten mit fragwürdiger Gesetzeslage landen.

Sogar der Europäische Gerichtshof hat dies in seinem Grundsatzurteil vom April 2014 hervorgehoben, mit dem die Vorratsdatenspeicherung aufgehoben wurde. Die fehlende Verpflichtung zur Lokalisierung wurde hier offen kritisiert[33]:

> Zweitens schreibt die Richtlinie nicht vor, dass die fraglichen Daten im Unionsgebiet auf Vorrat gespeichert werden, sodass es nicht als vollumfänglich gewährleistet angesehen werden kann, dass die Einhaltung der in den beiden vorstehenden Randnummern angesprochenen Erfordernisse des Datenschutzes und der Datensicherheit, wie in Art. 8 Abs. 3 der Charta ausdrücklich gefordert, durch eine unabhängige Stelle überwacht wird. Eine solche Überwachung auf der Grundlage des Unionsrechts ist aber ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten.

Auf Deutsch: Kein Handelsabkommen darf solch eine bevorzugte Behandlung von europäischen IKT-Unternehmen unterbinden. Oder in noch einfacherem Deutsch: „Nimm das, US-Handelsbeauftragter".

Es bleibt abzuwarten, ob Europa seine Datenschutzbestimmungen unter dem Druck einer Einigung über TTIP und TiSA erreichen, aufrecht erhalten oder gar verstärken können wird.

Dieser Beitrag ist eine aktualisierte Version eines Papers, das zuerst im September 2014 bei statewatch.org erschien.

Anmerkungen

[1] Privacy International, das Center for Digital Democracy, der Europäische Verbraucherverband BEUC und der US-Verbraucherverband waren darin bislang am aktivsten.

[2] Dokumentation: http://www.greens-efa.eu/transatlantic-data-flows-and-the-trade-and-investment-partnership-ttip-11815.html, eine gute Zusammenfassung findet sich auf http://acta.ffii.org/?p=2050

[3] Viviane Reding, Vize-Präsidentin der EU-Kommission und EU-Justizkommissarin: „Towards a more dynamic transatlantic area of growth and investment" *Vortrag auf einer Konferenz die vom Peterson Institute, SAIS und der EU-Delegation ausgerichtet wurde*. http://europa.eu/rapid/press-release_SPEECH-13-867_de.htm, Washington DC/USA, 29. Oktober 2013

[4] World Trade Organization: *Allgemeines Abkommen über den Handel mit Dienstleistungen*. http://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm

[5] Rat der Europäischen Union: *Leitlinien für die Verhandlungen über die transatlantische Handels- und Investitionspartnerschaft zwischen der Europäischen Union und den Vereinigten Staaten von Amerika*. http://www.ttip-leak.eu/media/download/e2ff8f5879aeaf5a40360628db9a0c84.pdf, 17. Juni 2013

[6] http://keionline.org/sites/default/files/eu-kommission-position-in-den.pdf, Art. 64

[7] Unter ihnen befinden sich der frühere EU-Botschafter in den USA Hugo Paemen, der frühere US-Handelsvertreter Clayton Yeutter und Daniel Weitzner, der frühere stellvertretende technische Leiter für Internetpolitik, siehe http://www.hoganlovells.com/hogan-lovells-forms-coalition-for-privacy-and-free-trade-03-18-2013

[8] Kommissionsentscheidung 2000/520/EC vom 26. Juni 2000, entsprechend der Richtlinie 95/46/EC der Europäischen Parlaments und dem Rat über die Angemessenheit des Schutzes durch die Safe-Harbour-Datenschutzprinzipien und damit in Verbindung stehende, häufig aufgekommene Fragen. Herausgegeben vom US-Handelsministerium.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF

[9] *Resolution des EU-Parlaments über die US NSA-Überwachungsprogramme, Überwachungsorgane in verschiedenen Mitgliedsstaaten und ihren Einfluss auf die Grundrechte europäischer Bürger und die transatlantische Zusammenarbeit im Ausschuss für Recht und Innenangelegenheiten*.
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN, 17. Juni 2013

[10] *Terms of Service; Didn't Read*. http://www.tosdr.org

[11] Pressemeldung des MIT CSAIL-Projekts und dem Institut für Informationsrecht der Universität Amsterdam: *EU and US privacy experts in search of transatlantic privacy solutions* (einschließlich einer Teilnehmerliste).http://www.ivir.nl/news/privacy_bridges_launch.pdf. Siehe auch Sam Pfeifle: Will New Privacy Bridge Project Bring EU and U.S. Together?, www.privacyassociation.org/publications/will_new_privacy_bridge_project_bring_eu_and_u.s._together

[12] Z. B. Mitgründer Daniel Weitzner, der in die Industrievereinigung „Coalition for Privacy and Free Trade" involviert ist.

[13] Geschäftsstelle des Präsidenten: *Big Data: Seizing Opportunities, preserving values*. http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014_1.pdf, 1. Mai 2014

[14] *Statewatch-Analyse 257*. http://www.statewatch.org/analyses/no-257-ttip-ralf-bendrath.pdf, September 2014

[15] Ian Brown: *Will NSA revelations lead to the Balkanisation of the internet?*. http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet, 1. November 2013

[16] Jürgen Berke: *Telekom will innerdeutschen Internetverkehr übers Ausland stoppen, Wirtschaftswoche*. http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html, 12. Oktober 2013

[17] Unter ungarischer EU-Ratspräsidentschaft wurde ein Vorschlag für eine „virtuelle Schengengrenze" bereits 2011 diskutiert, siehe http://edri.org/virtual_schengen

[18] *Resolution des EU-Parlaments über die US NSA-Überwachungsprogramme, Überwachungsorgane in verschiedenen Mitgliedsstaaten und ihren Einfluss auf die Grundrechte europäischer Bürger und die transatlantische Zusammenarbeit im Ausschuss für Recht und Innenangelegenheiten*.
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN, 12. März 2014

[19] Matthias Monroy: *Aus #Neuland wird #Schengenland: Merkel für Aufbau „europäischer Kommunikationsnetzwerke"*

[20] Amt des Handelsvertreters der Vereinigten Staaten: *USTR Targets Telecommunications Trade Barriers*, Pressemitteilung.
http://www.ustr.gov/about-us/press-office/press-releases/2014/March/USTR-Targets-Telecommunications-Trade-Barriers, 4. April 2014

[21] Amt des Handelsvertreters der Vereinigten Staaten: *2014 Section 1377 Review On Compliance with Telecommunications Trade Agreements*.
http://www.ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf

[22] Business Coalition for Transatlantic Trade:
Digital Trade. http://www.transatlantictrade.org/issues/digital-trade

[23] Das ist bereits in Regeln für „reine Durchleitung" durch Telekommunikationsanbieter enthalten, die nicht für den Inhalt, den sie transportieren, oder die stattfindende Datenverarbeitung bei Sender oder Empfänger verantwortlich gemacht werden können

[24] *Gesetzesvorlage über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012, Änderungsvorschlag 140*. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402, 12. März 2014

[25] *Urteil des irischen High Court, Richter Hogan, Fall 2013 No. 765JR*.
http://www.europe-v-facebook.org/hcj.pdf,18. Juni 2014

[26] *Digital Trade Act of 2013*, S. 1788. Einbracht am 12. Dezember 2013 von Sen. John Thune (R-SD). https://beta.congress.gov/bill/113th-congress/senate-bill/1788

[27] *Bipartisan Congressional Trade Priorities Act of 2014*, S. 1900. Einbracht am 9. Januar 2014 von Sen. Max Baucus (D-MT). https://beta.congress.gov/bill/113th-congress/senate-bill/1900

[28] Handelsbeamter der EU-Kommission Jan-Willem Verheijden bei der Anhörung von Greens/EFA im EU-Parlament am 5. März 2014. Siehe Ante Wessels: *US wants to undermine privacy in TTIP negotiations*.
http://acta.ffii.org/?p=2050

[29] Unter ihnen befinden sich die Schweiz, Kanada, Japan, Australien, Südkorea, die Türkei und Länder in Lateinamerika und Asien.

[30] http://www.teamTiSA.org

[31] Andreas Zumach: *Geheimverhandlungen in Genf*, taz. http://www.taz.de/!137455, 27. April 2014

[32] Trade in Services Agreement (TiSA): *Anhang zu Finanzdienstleistungen, Konsolidierung der Vorschläge vom 14. April 2014*. https://wikileaks.org/TiSA-financial/WikiLeaks-secret-TiSA-financial-annex.pdf

[33] Abs. 68: *Urteil des Gerichtshofs (Große Kammer) in den verbundenen Rechtssachen C-293/12 und C-594/12*.
http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN, 8. April 2014

Ralf Bendrath ist Politikwissenschaftler und leitender wissenschaftlicher Mitarbeiter von Jan-Philipp Albrecht, Mitglied im Europaparlament für die Grünen/EFA.

19 Wikipedia Zero und Netzneutralität: Wikimedia wendet sich gegen das offene Internet

von **Raegan Mac Donald**

Die Vision der Wikipedia ist „eine Welt, in der jeder Mensch frei die Summe allen Wissens teilen kann." Das ist ein Wert, den wir bei Access teilen. Deswegen waren wir schockiert, als die Wikimedia Foundation, die die Wikipedia hostet und unterstützt, sich gegen den größten Treiber des freien Informationszugangs wandte, den die Welt je gekannt hat: das offene Internet.

In einem Blog-Post bewarb Erik Möller, der stellvertretende Direktor der Wikimedia Foundation, ein relativ neues Angebot: Wikipedia Zero, eine Partnerschaft mit Telekom-Unternehmen, die den priorisierten, gebührenfreien Zugang zur Wikipedia bereitstellt. Die Idee dahinter ist, die hohen Datengebühren zu umgehen, die immer noch viele Menschen auf der ganzen Welt zwingen, offline zu bleiben. In seiner Argumentation für „Zero" beteuert Möller, dass die Wikimedia Foundation der Netzneutralität verpflichtet ist – also der Vorstellung, dass alle Online-Daten gleich behandelt werden sollen – und dass Zero dieses grundlegende Konzept des offenen Internets nicht verletzt. Dem müssen wir, bei allem Respekt, allerdings deutlich widersprechen. Wir glauben, dass Zero klar gegen die Netzneutralität verstößt und ein Angriff auf das offene, freie Internet ist.

Wikimedia ist nicht der einzige, der diese sogenannten „Zero-rating"-Abkommen mit Telekommunikationsunternehmen vorantreibt. Facebook hat auch schon Vereinbarungen geschlossen, um datenreduzierte Versionen seiner Dienste in Industrie- und Entwicklungsländern anzubieten. Aber Wikimedia argumentiert, dass ihre Dienste, im Gegensatz zu Facebook Zero, nicht kommerziell sind. Und deshalb verdiene die Wikipedia spezielle Ausnahmeregelungen, weil im Tausch für die Bevorzugung gegenüber anderen Diensten kein Geld den Besitzer wechsele. Kein Geld, keine Verletzung der Netzneutralität.

Diese Argumentation stinkt ziemlich

In den erst kürzlich aktualisierten Nutzungsbedingungen des Unternehmens steht, dass Zahlung und Nutzung nicht vom Tausch gegen Geld abhängen. Und in der Tat nutzt Wikimedia seine bekannten Marken als Währung in den Verhandlungen mit den Telekom-Partnern, da sie durch Wikipedia Zero mehr Nutzer anwerben wollen.

Den heutigen Nutzern ist klar, dass die revolutionäre Eigenschaft des Internets auf seiner Breite und Vielfalt beruht. Das Internet ist mehr als Wikipedia, Facebook oder Google. Aber für viele würden die „Null-Gebühren-Angebote" den Internetzugang auf die Online-Welt der Web-Schwergewichte begrenzen. Für Millionen von Nutzern wären Facebook und Wikipedia gleichbedeutend mit „Internet." Am Ende würde Wikipedia Zero nicht zu mehr Nutzern des eigentlichen Internets führen, aber Wikipedia könnte einen schönen Anstieg seiner Seitenaufrufe generieren.

Wie die Wikimedia Foundation zu wissen behauptet, liefert die Vielfalt und Tiefe des Wissens im Internet genau das, was Netzneutralität im Wesentlichen so wichtig macht: Gleichbehandlung von Daten führt zu gleichberechtigtem Zugang für alle. Es ist schwer zu erkennen, wie einzelne bevorzugte Dienste mit diesem Prinzip im Einklang sein sollen.

Keine Lösung für den „Digital Divide"

Darüber hinaus ist der Vorschlag, dass Wikipedia oder Facebook die Lösung für den limitierten Internetzugang in Entwicklungsländern ist, etwa so als würde man ein Pflaster auf eine Schusswunde kleben. Die zugrunde liegenden, komplexen Ursachen der digitalen Spaltung bleiben unbehandelt. Außerdem lässt das Angebot von Dienstleistungen, die nicht in begrenzte Datentarife eingerechnet werden – in den entwickelten und weniger entwickelten Ländern gleichermaßen – das Gleichgewicht zugunsten der priorisierten Dienste kippen. Das zerstört die Wachstumsgrundlage für kostengünstige, netzneutrale Alternativen. Die langfristige Wirkung dieser Dienste wird ein Rückgang an Innovation und Wettbewerb im Internet sein – mit einer besonderen Benachteiligung von selbst gebauten, lokalen Dienstleistungen und einer Begünstigung von Unternehmen im Silicon Valley, die Tausende von Meilen entfernt sind. Und ironischerweise führt das zu einer Begrenzung des Zugangs zu Informationen und Wissen.

Wikipedia Zero und ähnliche Dienste spielen den etablierten Telekommunikationsunternehmen in die Hände, die die Märkte überall auf der Welt bereits heute im Würgegriff halten. Priorisierte Angebote machen die Dienstleistungen der „Telkos" attraktiver, verfestigen ihre übermäßig dominante Stellung in den meisten Märkten. Und sie treiben die Idee voran, dass Webseiten zusätzlich bezahlen sollen, um Nutzer zu erreichen, was wiederum den Grundsätzen der Netzneutralität widerspricht und die Entwicklung von Online-Inhalten und -Diensten noch zusätzlich erschwert.

Wikimedia war immer ein Förderer des offenen Zugangs zu Informationen, aber es ist entscheidend, priorisierte, gebührenfreie Angebote als das zu bezeichnen, was sie sind: Kurzsichtige Deals, die für die Zukunft des offenen Internets großen Schaden anrichten. Während immer mehr Menschen das Internet nutzen und weltweit Kämpfe um die Netzneutralität ausgefochten werden, liegt es gerade

in der Verantwortung der angesehenen Organisationen wie Wikimedia, sicherzustellen, dass neue Nutzer ein Internet entdecken können, das tatsächlich „die Summe allen Wissens“ repräsentiert.

Wenn Wikipedia Zero umgesetzt wird, kann es mit einem Schlag die Entwicklung des offenen Internets verändern – und zwar nicht unbedingt zum Besseren. Kein Unternehmen und keine einzelne Plattform – egal ob Facebook oder Wikipedia – sollte alleine dafür verantwortlich sein, den Zugriff auf die Informationen der Welt zu kuratieren. Kurz gesagt: Priorisierte Inhalte unterwandern die Zukunft des offenen Internets und die Rechte der Menschen, die es benutzen.

Dieser Beitrag erschien zuerst am 8. August 2014 auf accessnow.org, die Übersetzung stammt von Kilian Vieth.

Raegan MacDonald ist Policy Managerin von Access. Sie hat sich auf Europapolitik spezialisiert, mit dem Hauptaugenmerk auf Privatsphäre, Datenschutz, Zensur und Netzneutralität. Vorher hat sie bei European Digital Rights gearbeitet, einem Verband von 35 Privacy- und Bürgerrechtsgruppen.

20 Chronisch unterversorgt: Die netzpolitische Dimension des Breitbandausbaus

von **Christian Heise, Christian Herzog** und **Jan Torge Claussen**

Erkannt hat die deutsche Bundesregierung die Wichtigkeit des Breitbandausbaus schon lange. Drei Bundesminister, Thomas de Maizière, Alexander Dobrindt und Sigmar Gabriel beschäftigen sich mit dem Thema. Zusammen haben sie die Digitale Agenda der Bundesregierung veröffentlicht. Darin wird die Bedeutung „flächendeckend verfügbarer leistungsstarker Breitbandnetze [...] für gleichwertige Lebensverhältnisse und eine umfassende Teilhabe an den Chancen der Digitalisierung" hervorgehoben[1]. Auch die Bedeutung von Breitband für die bisher unterversorgten ländlichen Regionen wird betont[2]. Bisher sind das nicht viel mehr als Lippenbekenntnisse, vor allem im ländlichen Raum herrscht nämlich nahezu Funkstille. Im Zeitalter von Cloud-Computing, Video-Streaming und Social Web verfügen nur 5,5 Prozent der Deutschen zum Anfang des Jahres 2014 über einen Internetanschluss mit mindestens 30 Mbit/s[3]. Die BRD nimmt damit Platz 13 der 26 europäischen Mitgliedsstaaten bei der Verfügbarkeit von neuen Zugangstechnologien ein[4], allerdings nur Platz 17 bei der Verbreitung schneller Internetzugänge. Das ist unter Mittelmaß und führt dazu, dass Privatpersonen sowie kleine und mittlere Betriebe in ländlichen Regionen von der sozialen und wirtschaftlichen Entwicklung abgeschnitten sind – ein Armutszeugnis für Deutschland. Was hier versäumt wird, kann netzpolitisch anderswo nicht mehr aufgefangen werden.

Der Plan: Subventionierter Ausbau auf Kosten der Netzneutralität und Frequenzverkauf

Im Oktober 2014 hat die erst im März desselben Jahres gegründete Netzallianz einen Plan für den flächendeckenden Breitbandausbau vorgelegt. Bereits 2015 sollen dafür acht Milliarden Euro ausgegeben werden, insgesamt sind laut TÜV-Studie[5] 20 Milliarden Euro nötig, um bis 2018 das Ziel einer flächendeckenden Verfügbarkeit von schnellem (50 Mbit/s) Internet zu gewährleisten. Allein die Kosten für die Erschließung der letzten fünf Prozent der Haushalte summieren sich auf knapp acht Milliarden Euro.

Eine Möglichkeit diese Lasten zu schultern, stellt die bundesweite finanzielle Förderung im Rahmen verfügbarer Haushaltsmittel über die Einrichtung eines Son-

derfinanzierungsprogramms durch die größte nationale Förderbank, die Kreditanstalt für Wiederaufbau (KfW), dar. Das gilt aber nur für den Anschluss an das Internet. Den Ausbau von Mobilfunknetzen muss der Markt weiterhin selber finanzieren, dafür werden in Deutschland keine Fördermittel an unterversorgte Kommunen bereitgestellt. In Großbritannien wird ein Teil des ländlichen Breitbandkabelausbaus – so eine Auflage aus der letzten Festsetzung der Rundfunkgebühren – von der BBC bezahlt. Parallel beteiligen sich die Kommunen. Allgemein gilt, dass es sich in ländlichen Gebieten ob der weiten Wege und wenigen Kunden für Kabelbetreiber nicht lohnt, den Breitbandausbau voranzutreiben. Um dies zu bewirken, bedarf es entweder positiver Regulierungsanreize oder Auflagen. Immerhin – so eine EU-Richtlinie zum Breitbandausbau – sind bis zu 30 Prozent Kostenersparnis zu erzielen, wenn vorhandene Infrastruktur und Leerrohre genutzt werden sowie zukünftige Bauvorhaben den Ausbau berücksichtigen[6].

Ihren hehren Zielen zum Trotz. B.gegnet die Bundesregierung eigenen Investitionen beim Breitbandausbau bisher eher verhalten. Stattdessen privilegiert sie Kabelanbieter mit weniger Regeln zur Einhaltung der Netzneutralität. So wird im Gegenzug für die privatwirtschaftlichen Investitionen in den ländlichen Breitbandausbau ein essentielles Grundprinzip des Internets neu ausverhandelt: Die Netzneutralität. Man stelle sich vor, auf einer vielbefahrenen öffentlichen Straße gäbe es eine Überholspur, die nur von den Menschen benutzt werden dürfte, die dafür extra zahlten. Ist das fair, wenn doch alle durch Ihre Steuern für klassische Daseinsvorsorgepflichten der öffentlichen Hand – also die grundlegende Versorgung der Bevölkerung mit wesentlichen Gütern und Dienstleistungen durch den Staat – bezahlt haben? Die Antwort auf diese Frage hängt davon ab, wie weit oder eng Daseinsvorsorge ausgelegt wird. Im Rahmen einer weiter gefassten Auslegung, wie sie mitunter von den Autoren vertreten wird, ist das Prinzip der Netzneutralität zentral. Es über Bord zu werfen, würde die Chancen für die Entwicklungen in Deutschland durch den Breitbandausbau konterkarieren. Grundlage für Netzneutralität ist ein offenes Netz und offene Infrastruktur insgesamt. Offen muss es für das größtmögliche Angebot an Medien und Diensten sein, aus denen der Internetnutzer wählt – und nicht der Endkunden-Provider aufgrund seiner Schlüsselposition[7].

Die Hürden: Technologie-Mix, politische Versäumnisse und Störerhaftung

Die letzte große Verkabelung in der Bundesrepublik fand unter Bundespostminister Christian Schwarz-Schilling (1982-1989) statt. Damals ging es um parteipolitische Differenzen. Die Konservativen wollten private Rundfunkveranstalter zulassen und die SPD suchte dies zu verhindern beziehungsweise zu verzögern, um die Frequenzknappheit und damit das öffentlich-rechtliche Rundfunkoligopol aufrechtzuerhalten. Schwarz-Schilling setzte damals gegen viele Widerstände

durch, dass rund 21 Milliarden DM in den Ausbau eines Kupferkoaxialkabelnetzes investiert wurden[8]. Ein gewichtiger Einwand gegen diese Investition bestand damals darin, dass die Nachfrage ungeklärt war. Niemand konnte verlässlich sagen, ob Kabelfernsehen ein Erfolg werden würde und damit die Nachfrage privater Haushalte nach den Kabelverbindungen die Investitionen des Bundes refinanzieren würde. Ironischerweise garantieren heute eben diese Leitungen für das Kabelfernsehen mancherorts Übertragungsgeschwindigkeiten von 100 Mbit/s, während veraltete Telefonleitungen nur geringe Bandbreiten liefern können. Dies liege – so ein Mitarbeiter der Telekom zu einem der Autoren – am geringen Kabeldurchmesser sowie an der Entfernung zum nächsten Knotenpunkt.

Bei den Möglichkeiten für den Ausbau wird zwischen kabelgebundenen und funkgebundenen Maßnahmen unterschieden. Die zum Einsatz kommende (Glasfaseranschluss-)Technologie unterscheidet, an welcher Stelle das Signal über Glasfaser auf die vorhandene Telefonnetz (Kupferinfrastruktur) übertragen wird z. B. direkt am Haus, in der Wohnung oder, wie am häufigsten eingesetzt, zum jeweiligen Hauptverteiler. Eine weitere Option, anstelle der Verwendung der Kupferleitungen, stellen die rückkanalfähigen Kabel-TV-Netze dar. Da diese in ländlichen Regionen oftmals nicht vorhanden sind, bleiben nur Funktechnologien als letzte Alternative gegenüber der Verkabelung. Dabei werden über Richtfunk Verbindungen zwischen einem bereits mit Glasfaserkabel versorgten Verzweiger zu einem unterversorgten Verteiler aufgebaut. Zunehmend werden auch hybride Formen eingesetzt, die beide Technologien vereinen und bereits erfolgreich in den nördlichen Flächenländern wie Norwegen und Schweden eingesetzt werden. (Mobil-)Funk-, reine Kupfer- und Satellitenlösungen sind nicht zukunftsfähig und trotzdem in Einzelfällen in Erwägung zu ziehen. Langfristig kann man dem Breitbandbedarf aber nur mit einer flächendeckenden Anbindung an Glasfaser gerecht werden.

Ein weiterer Hoffnungsträger ist die Versteigerung der 700-MHz-Frequenzen (ehemals DVB-T). Diese haben eine größere Reichweite als höhere Frequenzen und eignen sich vor allem zum kostengünstigen Aufbau der Netz. B.eckung in Flächenländern. Bisher war der von den Mobilfunkbetreibern begonnene Ausbau allerdings keine Erfolgsgeschichte. Zu hohe Kosten und unzuverlässige Bereitstellung der Dienste haben dem LTE-Netz ein eher fragwürdiges Image beim Breitbandausbau beschert. Hinzu kommt die technische Einschränkung, dass beim Einsatz von mobilen Technologien wie LTE (Advanced)[9] zwar faktisch über 50 Mbit/s erreicht werden können, im Gegensatz zu Glasfaser sich aber alle Teilnehmer einer Funkzelle diese Bandbreiteteilen müssen.

Eine weitere Hürde: Der Ausbau von Breitband-Kommunikationsnetzen und die daraus resultierenden Investitionen gehören nicht zu den gesetzlichen Pflichtaufgaben der Kommunen. Hier besteht zu wenig verwaltungspolitischer Druck. Die Lösung von staatlicher Seite kann also nur in einer stärkeren Zusammenarbeit in

interkommunalen Verbünden mit Unterstützung der Landkreise, Länder und des Bundes liegen. Leider gibt es in vielen Kommunen auch heute noch keine direkt ausgewiesenen Verantwortlichkeiten für das Thema Breitband.

Dabei ist der fehlende Zugang zum Breitband nicht ausschließlich auf fehlenden Leitungen zurückzuführen. Viele Zugänge ließen sich zumindest innerhalb von Ballungsräumen oder häuserübergreifend durch die gemeinsame Nutzung von privaten WLAN-Netzen mit Internetzugang herstellen. Solidarität unter privaten Internetnutzern wird jedoch durch den Gesetzgeber verhindert. Das Gesetz zur Störerhaftung[10] sorgt dafür, dass private Anschlußinhaber für eine rechtswidrige Nutzung von Dritten, z. B. Urheberrechtsverletzungen, haften. Auch wenn im Bundestag schon darüber debattiert wird, ist noch keine Lösung in Sicht. Damit behindert der Gesetzgeber mögliche Experimente, freie und offene Netzinfrastrukturen auf kooperativer Basis aufz. B.uen und zu betreiben. Die Verbreitung von offenen Netzen sowie vom Internet unabhängigen Netzwerken wie Freifunk wird nicht nur behindert, sondern auch gegenüber gewerblicher Provider stark benachteiligt, die für das Nutzungsverhalten Ihrer Kunden sinnvollerweise nicht haften müssen.

Die traurige Realität im Jahre 2014: DSL Lite mit 0,3 MBit/s

Ländliche Regionen sind vielerorts besonders attraktiv für Familien mit Kindern. Home-Office und Telearbeit sind keine Seltenheit mehr und machen die ständige physische Präsenz am Arbeitsplatz zumindest in einigen Berufen obsolet. Solange auf deutschen Datenautobahnen außerhalb von Städten aber Geschwindigkeiten auf DSL-Lite (0,3 Mbit/s) oder weniger sinken, werden ebendiese Entwicklungen gebremst oder sogar verhindert. Zwei der drei Autoren waren am 7. November 2014 auf einer Veranstaltung, organisiert vom Wahlkreisbüro der MdB Hiltrud Lotze (SPD) in Lüchow im niedersächsischen Wendland. Diskutiert wurde die Digitale Agenda. Im Rahmen der Vorträge und bei der anschließenden Diskussion wurde deutlich, wie viele weiße Flecken, also von der Breitbandversorgung ausgeklammerte Gebiete, der Landkreis Lüchow verzeichnet. Die davon betroffenen Bürger – die Mehrzahl der Anwesenden – waren vornehmlich am Breitbandausbau interessiert. Mitunter wurden von ihnen Strategien und (genossenschaftliche) Modelle angesprochen, diesen in Eigenregie zu finanzieren. Ohne die Bereitstellung von Breitband, so wurde bei der Diskussion mehr als deutlich, gehörten viele Netzpolitikthemen weiterhin in den Elfenbeinturm. Für Bürger ohne schnelle Internetverbindung bleiben Themen wie Medienkonvergenz, Netzneutralität oder digitale Persönlichkeitsrechte einer digitalen Bohème vorbehalten. Transparenz, Partizipation und Teilhabe in Bezug auf digitale Medien sind ohne die entsprechenden Infrastrukturen nicht vermittelbar.

Anmerkungen

[1] Bundesministerium für Wirtschaft und Energie, Bundesministerium des Innern, Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.) (2014) Digitale Agenda 2014–2017, S. 3.

[2] *Digitale Agenda 2014–2017*, S. 10.

[3] EU-Kommission: *Digital Agenda Scoreboard*.
http://ec.europa.eu/digital-agenda/en/digital-agenda-scoreboard, 2014

[4] Bundesministerium für Verkehr und digitale Infrastruktur: *Kursbuch Netzausbau*, 2014

[5] Szenarien und Kosten für eine kosteneffiziente flächendeckende Versorgung der bislang noch nicht mit mindestens 50 Mbit/s versorgten Regionen. Studie im Auftrag des BMWi.

[6] Rat der EU: *Council adopts new measures to cut broadband costs*. 8. Mai 2014

[7] Eumann, Marc Jan und Lischka, Konrad: *Wir müssen über Peering reden – sieben Thesen zur Netzneutralität*.
https://netzpolitik.org/2014/wir-muessen-ueber-peering-reden-sieben-thesen-zur-netzneutralitaet/

[8] Deutscher Bundestag: *Stenographischer Bericht*, S.5734–5736. 10. Wahlperiode, 78. Sitzung.
Bonn, 29. Juni 1984; Christian Potschka: *Towards a Market in Broadcasting: Communications Policy in the UK and Germany*, S. 189–190.

[9] Long Term Evolution Advanced bezeichnet eine Funktechnologie für mobile Breitbanddatenübertragung mit deutlich erhöhter Leistungsfähigkeit in den Funkzellen unter Einsatz eines weiteren Frequenzspektrums (unterhalb 1000 MHz).

[10] Digitale Gesellschaft: *Störerhaftung beseitigen*.
https://digitalegesellschaft.de/portfolio-items/storerhaftung-beseitigen/;
Live-Blog aus dem Bundestag: *Alle wollen die WLAN-Störerhaftung abschaffen, außer CDU/CSU*.
https://netzpolitik.org/2014/jetzt-live-im-bundestag-debatte-ueber-stoererhaftung/

Christian Heise ist Politikwissenschaftler, wissenschaftlicher Mitarbeiter am Hybrid Publishing Lab (Centre for Digital Cultures) der Leuphana Universität und promoviert zum Thema Open Science. Zuvor war er als Manager bei der Deutschen Presse Agentur, beim ZEIT Verlag und als freier Berater für diverse Unternehmen tätig. Er ist Vorstandsmitglied bei der Open Knowledge Foundation Deutschland sowie im Förderverein für freie Netzwerke e.V..

Christian Herzog ist wissenschaftlicher Mitarbeiter im Projekt Grundversorgung 2.0 am Centre for Digital Cultures an der Leuphana Universität Lüneburg. Er verfolgt Forschungsschwerpunkte in den Bereichen Medienpolitik, Media Governance, Medienregulierung und Rundfunkgeschichte.

Jan Torge Claussen ist Kulturwissenschaftler, Designer, Produzent und Musiker. Er forscht und lehrt zu Themen wie User-Interface, Audio-Kultur, Social Web und Digital Storytelling. Am Centre for Digital Cultures der Leuphana Universität Lüneburg entwickelt er neue Formate und Web-Anwendungen für eine mediale Grundversorgung 2.0 und setzt sich mit der Gestaltung, Nutzer-Partizipation und Mashup-Kultur im Bereich von Videoplattformen auseinander. Er bloggt auf gegenwaerts.com.

21 Sehr geehrte Damen und Herren Abgeordneten, tun Sie endlich etwas für offene (Verwaltungs-)Daten!

von **Christian Heise**

Anfang November 2014 wurden im Rahmen der 21. Sitzung des Bundestagsausschusses „Digitale Agenda" fünf Sachverständige geladen, um in einem Fachgespräch zum Thema Open Data „zu diskutieren, welche Vorteile und Risiken die Bereitstellung offener Daten hat". In diesem Beitrag fasse ich die zentralen Punkte meiner Stellungnahme und den Aussagen vor dem Ausschuss zusammen.

Bereits vor dem Gespräch wurden acht Fragen zum Thema Open Data an die Sachverständigen versandt. Symptomatisch für die bisherige politische Behandlung des Themas Offene Daten ist, dass mehr als die Hälfte der Fragen fast deckungsgleich mit Fragen waren, die bereits im Jahr 2012 im Rahmen eines ähnlichen Fachgesprächs des Unterausschusses Neue Medien mit dem Titel „Entwicklung und Stand Open Data Projekte" an Sachverständige gestellt wurden, und dass diese leider auch heute noch genauso beantwortet werden können.

Zum Mehrwert von offenen Daten

Für mich als Mitglied der gemeinnützigen Open Knowledge Foundation e.V. (OKF DE) steht der gesellschaftliche, politische, wissenschaftliche, kulturelle und soziale Mehrwert von Daten im Vordergrund. Die gesellschaftlichen Potentiale erstrecken sich über alle Bereiche des öffentlichen Lebens und bieten immense Vorteile[1] für alle Mitglieder der Gesellschaft[2].

Natürlich gibt es auch große Potenziale von Open Data für die Wirtschaft in fast allen Wirtschaftszweigen. Freie und offene Daten (egal ob Regierungs- oder andere Daten) können auch als Wirtschaftsförderung verstanden werden, da sie ohne einen einzigen Euro an direkten Subventionen einen enormen Schub an wirtschaftlichen Impulsen und Innovationen bedeuten können: Ob das jetzt die 140 Mrd. Euro der EU-Studie[3], 200 Mrd. Euro laut Steria[4] oder 206 Mrd Euro bis 2020 von einer Microsoft-Studie[5] sind, vermag ich hier nicht zu bewerten. Ich möchte auch davon absehen, solche Dimensionen mantraartig zu wiederholen, da sie einseitige, ausschließlich wirtschaftliche „Interessen" an Open (Government) Data wecken und eine zu einseitige Betrachtungsweise stützen. Dennoch darf bei der Frage nach dem Mehrwert von Offenen Daten nicht unerwähnt bleiben, dass die deutsche Wirtschaft meines Erachtens nach – wenn die Daten zur Verfügung stehen würden – durch die Entwicklung von Anwendungen und Nutzungszenarien profitieren würde. Darüber hinaus könnte eine zusätzliche Fokussierung auf

die Themenbereiche: A) die Veredelung von Rohdaten (z.B. die Aufbereitung der Daten) und B) das Thema Datenschutz und Privacy (Anonymisierung von offenen Daten) ein internationales Alleinstellungsmerkmal darstellen.

Herausforderungen bei der Öffnung von Datenbestände der Verwaltung in Deutschland

Das letztendliche Potenzial von offenen Daten hängt von dem kurzfristigen Willen und dem daraus resultierenden Handeln ab, das Thema endlich umfassend zu adressieren, konkrete Maßnahmen zu verabschieden und die dafür zwingend notwendigen politischen Rahmenbedingungen (technisch und rechtlich) zu schaffen.

Bisher überwiegen noch viele Schwierigkeiten und/oder Widerstände. Ein Beispiel: Im Rahmen meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Centre for Digital Cultures (CDC) der Leuphana Universität habe ich mit einem Kollegen eine explorative Befragung unter Daten- und Investigativ-Journalisten durchgeführt[6]. Die Ergebnisse, die als offener und anonymer Datensatz zur Verfügung stehen[7], sind exemplarisch auch auf andere Bereiche des öffentlichen Lebens und die Wirtschaft übertragbar. Dabei gaben 66 Prozent der Befragten an, dass Behörden die Auskunftspflicht verweigern bzw. die Arbeit durch lange Bearbeitungszeiten und hohe Kosten behindern. Rund 59 Prozent der Befragten kritisierten, dass die relevanten Daten schlichtweg nicht vorhanden seien.

Wünschenswert wäre diesbezüglich mindestens die Ausweitung des § 5 Abs. 2 Urheberrechtsgesetz zur Gemeinfreiheit von Werken der öffentlichen Verwaltung oder ein nationales Transparenzgesetz. Bei § 5 UrhG sollte klarer herausgearbeitet werden, dass im Abs. 1 und Abs. 2 Urheberrechtsfreiheit angestrebt wird. Damit entfällt die Möglichkeit, durch Lizenzen Einschränkungen zu machen. Die Auslegung des § 5 UrhG sollte sich am Konzept der „Public Domian" orientieren, wie es seit Jahrzehnten in den USA gepflegt wird. Lizenzen können nur von einem Lizenzgeber vergeben werden, der über die Rechte an den Werken verfügt. Dies trifft bei Gemeinfreiheit nicht zu. Der Regelfall in Bezug auf öffentliche Daten sollte Urheberrechtsfreiheit und damit Lizenzfreiheit sein. Lizenzen nützen in diesem Bereich nichts, sie behindern. Dies zeigt auch die langwierige Diskussion durch die Beschränkungen des Innenministeriums (BMI).

Positiv muss in diesem Zusammenhang erwähnt werden – auch wenn wir als OKF DE immer gegen eine eigene nationale Lösung waren –, dass nach einer sehr konstruktiven Zusammenarbeit mit dem BMI vor kurzem die Datenlizenz Deutschland 2.0 als mit der OpenDefinition vereinbar anerkannt worden ist[8]. Der Aktionsplan zur G8 Open Data Charter ist ein weiterer positiver (wenn auch kleiner) Schritt. Die im Aktionsplan avisierte Öffnung von wenigstens zwei Datensätzen je Behörde und die weiteren Maßnahmen sind nicht ausreichend, um den Vorsprung anderer Länder aufzuholen[9]. Insgesamt ist die Bundesregierung leider noch sehr weit davon entfernt, den Bereich offene Daten aktiv (mit)zugestalten.

Zwingend notwendige (politische) Maßnahmen

Größtes Manko ist, dass eine gesetzliche Festlegung zur Veröffentlichung von (allen) Inhalten der Verwaltung nach Open-Government-Data-Prinzipien fehlt, z. B. über ein novelliertes Informationsfreiheitsgesetz, Anpassung der eGovernment-Gesetze, über ein eigenes Open-Data-Gesetz oder ein nationales Transparenzgesetz. Will Deutschland wirklich die im Koalitionsvertrag und in der Digitalen Agenda formulierte „Vorreiterrolle" einnehmen, so ist ein rascher Open-Government-Partnership-Beitritt, die Schaffung gesetzlicher Rahmenbedingungen für Open Data, die Etablierung einer zentralen Anlaufstelle für das Thema im Bereich der ministerienübergreifenden Bundesverwaltung und die Schaffung einer Digital-Service-Einheit wie z. B. der GDS[10] in UK oder dem Etalab[11] in Frankreich unausweichlich. Ebenfalls notwendig ist eine konstruktiv-kritische Auseinandersetzung mit dem Konzept von Open Data in Politik, Wissenschaft und Gesellschaft. In diesem Bereich sind mehr Ressourcen für die wissenschaftliche Auseinandersetzung mit Offenheit nötig.

Werden diese oder ähnlich effektive Maßnahmen nicht ergriffen, wird Deutschland weiter im internationalen Vergleich zurückfallen und die angesprochenen Potenziale werden sich für Deutschland nicht entfalten können.

Persönlichkeitsrechte, Datenschutz und die Angst vor Manipulation von offenen Datensätzen

Auch bei der Frage nach dem Schutz von Persönlichkeitsrechten schließe ich mich uneingeschränkt den Auffassungen meiner Kollegen und den Aussagen von 2012 an[12]. Grundsätzlich gilt hier die vom Kollegen von Wikimedia e.V. 2012 erwähnte[13], zwingende Verpflichtung, genau diese Schutzaspekte ganzheitlich sicherzustellen. Dabei liegt die Verantwortung bei der herausgebenden Stelle. Denn der Schutz von Daten beginnt bereits bei der Erhebung und nicht erst bei der Freigabe und Veröffentlichung. Was den Daten- und Geheimschutz betrifft, so werden diese hinreichend durch eigene Gesetze geregelt. Betriebsgeheimnisse sollten beim Handeln des Staates nicht auftreten. Als Beispiel ist hier Hamburg zu nennen, das für die Eigenbetriebe keine Betriebsgeheimnisse im Transparenzgesetz mehr will. Urheberrecht sollte nach § 5 UrhG bei öffentlichen Daten keine Rolle mehr spielen. Lizenzen sind hier unangebracht.

Was die Gewährleistung der Sicherheit und Vertrauenswürdigkeit der Daten angeht, könnte etwa zusätzlich eine offene Lizenz mit Attribution gewählt werden, z. B. CC-BY, um die Vertrauenswürdigkeit sicherzustellen. Zur weiteren Gewährleistung der Sicherheit, Vertrauenswürdigkeit und Manipulationssicherheit von offenen Verwaltungsdaten sollten darüber hinaus sämtliche Daten mit einer ausreichend sicheren kryptographischen Signatur veröffentlicht werden. Ferner sollten Datensätze mittels aussagekräftiger Metadaten eine Prüfbarkeit der Herkunft der Daten gewährleisten.

Grundsätzlich muss an dieser Stelle auch erwähnt werden, dass in einigen Bereichen von Open Data die Veröffentlichung von Daten überhaupt erst zu einer Erhöhung der Datenqualität geführt hat. Ein Beispiel hierfür wäre die Veröffentlichung von Daten zur Entwicklungszusammenarbeit im IATI-Standard. Darüber hinaus ermöglicht die Veröffentlichung, dass Fehler in den Daten von mehr Nutzern gesehen und korrigiert werden können. Die Gefahr der Manipulation besteht meines Erachtens nicht. Von keiner Behörde ist glaubwürdig vorgetragen worden, dass durch nachträgliche Manipulationen von Informationen Schaden entstanden sei. Bei Gesetzen und Urteilen ist das seit Jahrzehnten unproblematisch[14].

Die im Koalitionsvertrag von CDU/CSU und SPD vereinbarte Vorreiterrolle der Bundesverwaltung bei der Bereitstellung offener Daten

Um ernsthaft eine Vorreiterrolle bei der Bereitstellung offener Daten einzunehmen, brauchen wir ein nationales Transparenzgesetz (mindestens aber eine ambitionierte Neufassung des Gesetzes über die Weiterverwendung von Informationen öffentlicher Stellen (IWG) bzw. Umsetzung der EU PSI-Richtlinie[15]), saubere Daten, eine bessere Ressourcenausstattung in der Bundesverwaltung im Bereich Open Government, einheitliche Standards und die genannte ressortübergreifende Einheit bzw. zentrale Ansprech-/Clearingstelle (und damit ist explizit nicht der IT-Plannungsrat gemeint!). Das forderte auch eine Mehrzahl der Teilnehmer der genannten Befragung des CDC auf die Frage „Wie bzw. mit welchen konkreten Maßnahmen Ihre Arbeit mit Daten und/oder Informationen erleichtert werden könnte“ und die Sachverständigen im Jahre 2012. Solange es keine bessere Koordinierung und umfassendere Behandlung des Themas „Open Data“ gibt, wird die deutsche Bundesverwaltung weit unter dem internationalem Durchschnitt bleiben.

Kostenregelungen für die Bereitstellung offener Daten

Verwaltungsdaten heißen nicht so, weil sie der Verwaltung gehören, sondern weil sie diese verwaltet. Die Refinanzierung knapper Kassen durch den Vertrieb und Verkauf offener Regierungsdaten ist für mich unvertretbar und als Relikt aus der gescheiterten Verwaltungsmodernisierung vergangener Dekaden anzusehen. Das bedeutet nicht, dass Verwaltungen von offenen Daten nicht selbst profitieren können. In dem zweitgrößten Landkreis Deutschlands, Ludwigslust-Parchim, ist z. B. die Verwaltung selbst der größte Treiber und Nutzer (für die Verwendung) von Verwaltungsdaten. Auch in Hamburg sind erste Vorteile für den Verwaltungsalltag selbst ersichtlich. Auch die Stadt Moers muss man hier als positives Beispiel für die Entwicklung von Open Data aus der Verwaltung selbst erwähnen. Open Data ermöglicht eine einfache Zusammenarbeit unterschiedlicher Abteilungen. Fehler und Abweichungen in unterschiedlichen Versionen ursprünglich gleicher oder ähnlicher Datensätze können einfacher erkannt bzw. verhindert werden.

Open Data hat damit auch das Potenzial, die Prozesse in den öffentlichen Verwaltungen zu modernisieren und durch Synergieeffekte Kosten signifikant zu reduzieren.

Aus meiner Sicht sind bis auf eine Ausnahme keine Rahmenbedingungen erforderlich, um maschinenlesbare Rohdaten der öffentlichen Hand für die – insbesondere wirtschaftliche – Nutzung durch Private auszugleichen. Einzige Ausnahme sind die Kosten, die ggf. für eine notwendige Anonymisierung der Rohdaten entstehen. Sollte eine Konkurrenz zwischen öffentlichen Angeboten und denen von kommerziellen Anbietern entstanden sein, sehe ich es eher als Problem an, dass es überhaupt dazu gekommen ist. Einschränkungen und die Debatte um die Nutzung der Regierungsdaten für kommerzielle Zwecke offenbaren ein fehlgeleitetes Verständnis der Chancen, die Open Data eröffnet. Geschäftsmodelle, die auf Freigabe der Rohdaten beruhen, bieten gute Möglichkeiten, den Spagat zwischen ökonomischen Imperativen und der Bereitstellung von Wissen für die Allgemeinheit zu meistern. Ein weiterer Punkt sind eventuell höhere Steuereinnahmen durch neue Produkte privatwirtschaftlicher Anbieter – darum geht es ja in der EU- und Microsoftstudie. Wer diesen wirtschaftlichen Mehrwert will, kann nicht mit dem Argument „Deckung von Verwaltungskosten" das Potenzial abwürgen.

Die Erfahrung zeigt, dass die Freigabe von Daten häufig auch dazu führt, dass Bürger sich aktiv an der Pflege, Verbesserung und Fehlerbeseitigung dieser oder abgeleiteter Daten beteiligt haben (Wikipedia, OpenStreetMap, etc.). Open Data sollte also nicht als „Daten-Einbahnstrasse" gesehen werden, sondern als ein bidirektionaler Prozess.

Novellierung des IFG oder Open-Data-Gesetz?

Es spricht nichts gegen ein eigenes Open-Data-Gesetz und die Ausweitung der Informationsfreiheit, im Gegenteil: Wir haben in Deutschland eine rechtstreue Verwaltung und das normale Steuerungsmedium ist das Recht. Dennoch wäre die m. E. beste Option ein nationales Transparenzgesetz, um der zwanghaft-technokratischen Herangehensweise der Verwaltung in Bezug auf Informationsfreiheit und Open Data zu begegnen. Transparenzgesetze vereinen außerdem den Ansatz von Open Data (Push) und IFG (Pull)[16]. Auch das wurde schon 2012 von den Sachverständigen gefordert. Die noch jungen Erfahrungen aus Hamburg zeigen, dass ein Transparenzgesetz mit einer proaktiven Informationstätigkeit einfacher und schneller umzusetzen ist als gedacht. Nur eine gesetzliche Verpflichtung der Verwaltung kann den Prozess vorantreiben, weil nur so die Priorisierung der abzuarbeitenden Themen die nötige Reihenfolge erhält und eine Struktur aufgebaut werden kann.

Warum ein Beitritt zur Open Government Partnership (noch) sinnvoll ist

Bislang blieb es nur bei dem Lippenbekenntnis im Koalitionsvertrag der Bundesregierung[17] und einer Ankündigung des SPD-Abgeordneten Klingbeil bezüglich eines OGP-Beitritts[18]. Dabei hätte ein frühzeitiger Beitritt zur OGP sicher auch dazu beigetragen, dass die Zivilgesellschaft, andere gesellschaftliche Gruppen und die Länder schon frühzeitig an der Arbeit des digitalen Wandels im Bereich Open Data hätten teilnehmen können. Auch das BMI ist im März 2012 in einer Stellungnahme zu dem Schluss gekommen, dass „dieser Standpunkt (der Open Government Partnership nicht beizutreten) nicht dauerhaft beibehalten werden kann, ohne eine (vor allem zivilgesellschaftliche) Unterstützung für bereits laufende Aktivitäten zu verlieren".

Ein weiterer Vorteil der OGP ist der (durch den prozessorientierten Ansatz und die höhere internationale und politische Verbindlichkeit) gestärkte Austausch der Ministerien untereinander[19]. Bei einem raschen Beitritt könnte darüber hinaus auch die internationale Gemeinschaft von einem Beitritt Deutschlands profitieren. In einem Zeitalter, in dem Regierungen und Unternehmen immer mehr private Daten sammeln, bedarf es klarer Regeln und effektiver Mechanismen, um die Rechte und den Schutz des Einzelnen zu garantieren. Deutschland hat international den Ruf einer Nation, in dem Datenschutz und Schutz der Privatsphäre einen hohen Stellenwert haben. Die Erfahrungen, die Deutschland bei der Entwicklung von Gesetzen und Institutionen diesbezüglich gemacht hat, und hoffentlich noch machen wird, dürften anderen Nationen von großem Nutzen sein. Das gilt auch für die Aktivitäten im Rahmen der Europäischen Union: Wenn wir nicht endlich aktiv werden, dann können wir bei der dringend notwendigen Harmonisierung auf EU-Ebene nicht mitgestalten.

Offenheit der im Bundestag anfallenden Daten

Bundestagspräsident Nobert Lammert hat beim letzten Relaunch der Webseite des Bundestags im Jahre 2009 auf die Anfrage eines Pressevertreters geantwortet, er halte es nicht für „notwendig oder zweckmäßig", die Inhalte „auf einem virtuellen silbernen Tablett zu präsentieren"[20]. Ich möchte ihm widersprechen. Ein konkretes, praktisches Beispiel: Sie alle haben die Möglichkeit nach § 31 Abs 1. GOBT nach einer Abstimmung eine Abgeordnetenerklärung abzugeben – in der letzten Wahlperiode wurde fast 2500 Mal davon Gebrauch gemacht. Diese Erklärungen werden gesondert im Protokoll aufgenommen und als PDF veröffentlicht. Leider ist es nicht ohne Weiteres möglich, diese Daten auszulesen und maschinenlesbar zu verarbeiten. Dabei würden diese Erklärungen bestimmt einen Teil der Fragen zu Ihrem Abstimmungsverhalten, die über abgeordnetenwatch.de gestellt werden oder aus Ihren Wahlkreisen kommen, beantworten.

Der Bundestag kann und muss endlich als gutes Beispiel vorangehen und alle Daten maschinenlesbar und unter einer offenen Lizenz zur Verfügung stellen. Der Standardeinstellung muss auf 'offen' gesetzt werden und die Veröffentlichung von Daten muss die Regel, nicht die Ausnahme darstellen. Bisher geht die Bundestagsverwaltung nach unseren Erfahrungen aber genau den entgegengesetzten Weg. Es kann nicht sein, dass eine gemeinnützige Organisation einen transparenteren Zugang zu den Inhalten des Bundestags ermöglicht als der Bundestag selbst. Ein erster, konkreter Schritt wäre eine Unterzeichnung der Erklärung zur Parlamentarischen Offenheit[21] und die Schaffung eines einheitlichen Zugriffs auf die Bundestagsinformationssysteme[22]. Das würde die Demokratie stärken, wäre ein gutes Zeichen für die Entwicklung von Open Data in Deutschland und könnte sicher auch einen Beitrag gegen Politikverdrossenheit und mangelnde Glaubwürdigkeit leisten[23].

Sehr geehrte Damen und Herren Abgeordnete, wenn der Staat ernsthaft „Vorbild für die Digitalisierung in Deutschland" sein möchte und wir nicht in zwei Jahren in einem ähnlichen „Fachgespräch" dieselben Fragen mit denselben Antworten diskutieren wollen, müssen sie endlich für einen raschen Open-Government-Partnership-Beitritt und für die gesetzlichen Rahmenbedingungen für Open Data und proaktive Informationsfreiheit (auch maschinenlesbar) sorgen sowie eine zentrale Anlaufstelle für das Thema im Bereich der ministerienübergreifenden Bundesverwaltung schaffen!

Anmerkungen

[1] Z. B. die OKF-Projekte http://codefor.de oder http://codingdavinci.de.

[2] Eine beispielhafte Auflistung der Bereiche finden Sie unter http://okfn.de/opendata/.

[3] http://europa.eu/rapid/press-release_MEMO-11-891_en.htm?locale=en

[4] http://www.steria.com/your-business/government/beyond-efficiency/

[5] http://www.bigopendata.eu/

[6] http://digitale-grundversorgung.de/blog/2014/10/16/nachrichtenkonferenz-prasentation-und-daten-open-data-und-investigativer-journalismus/

[7] https://zenodo.org/record/12252

[8] http://okfn.de/2014/09/erfolg-fuer-open-data-datenlizenz-deutschland-version-2-0-ist-eine-offene-lizenz/

[9] http://okfn.de/2014/09/stellungnahme-zum-nationalen-aktionsplan-der-bundesregierung-zur-umsetzung-der-open-data-charter-der-g8-g7/

[10] https://www.gov.uk/government/organisations/government-digital-service

[11] http://www.etalab.gouv.fr

[12] http://webarchiv.bundestag.de/archive/2013/1025/bundestag/ausschuesse17/a22/a22_neue_medien/oeffentliche_Sitzungen/open_data/Protokoll.pdf

[13] http://blog.wikimedia.de/wp-content/uploads/20120622-Stellungnahme-UANM-Wikimedia-Opendata.pdf

[14] Obwohl auch hier großes Optimierungspotential besteht, siehe dazu: http://www.collaboratory.de/w/Datei:OpenGovFactsheet2Legislative20v1.pdf

[15] http://okfn.de/2014/07/gemeinsame-stellungnahme-zum-entwurf-eines-gesetzes-ueber-die-weiterverwendung-von-informationen-oeffentlicher-stellen-iwg/

[16] http://www.carta.info/58468/alt-fur-ein-nationales-transparenzgesetz/

[17] *Koalitionsvertrag für die 18. Legislaturperiode (2013–2017)*, Seite 153

[18] http://opengovpartnership.de/ Disclamer: Ich bin Mitgründer des AK OGP DE

[19] Das belegen z. B. konkrete Erfahrungen aus UK.

[20] http://www.zeit.de/online/2009/33/bundestag-website-relaunch

[21] http://www.openingparliament.org/declaration

[22] http://oparl.de/

[23] http://www.slideshare.net/StephenAbbott2/opening-parliaments-strengthening-democracy

Christian Heise ist Politikwissenschaftler, wissenschaftlicher Mitarbeiter am Hybrid Publishing Lab (Centre for Digital Cultures) der Leuphana Universität und promoviert zum Thema Open Science. Zuvor war er als Manager bei der Deutschen Presse Agentur, beim ZEIT Verlag und als freier Berater für diverse Unternehmen tätig. Er ist Vorstandsmitglied bei der Open Knowledge Foundation Deutschland sowie im Förderverein für freie Netzwerke e.V..

22 Open Access: Auf dem Weg zur politischen Erfolgsgeschichte?

von **Jeanette Hofmann** und **Benjamin Bergemann**

Einleitung: Open Access wider die Umzäunung des Wissens?

Aus der Ferne besehen mag das akademische Publikationswesen Kopfschütteln auslösen. Zunächst werden öffentliche Mittel bereitgestellt, damit die Wissenschaft forschen und ihre Ergebnisse veröffentlichen kann. Nachdem die WissenschaftlerInnen ihre Beiträge bei Zeitschriften eingereicht und den Verlagen die Verwertungsrechte für die Veröffentlichung übertragen haben, kaufen die Universitätsbibliotheken dieses Wissen wieder zurück – zu Preisen, die die Verlage festlegen. Die öffentliche Hand zahlt also mehrfach, erst für die Produktion wissenschaftlichen Wissens und anschließend für dessen Zugänglichmachung.

Die Open-Access-Bewegung will Alternativen zu den Regeln des Zeitschriftenmarktes entwickeln. Ihr Ziel besteht in einem ungehinderten Zugang zu wissenschaftlichen Erkenntnissen und, dieser Aspekt gerät gelegentlich aus dem Blick, möglichst umfangreichen Nachnutzungsmöglichkeiten für Dritte. Öffentlich finanzierte Forschung soll im Internet frei zirkulieren können und die wissenschaftliche Kommunikation nicht länger durch Verlage kontrolliert werden. Die Vorzüge von Open Access (OA) liegen auf der Hand: Die Allgemeinheit bekommt Zugang zu wissenschaftlichem Wissen, die Kosten für dessen Verbreitung sinken und der Wissensfluss innerhalb der akademischen Welt wird erleichtert.

Auch wenn OA nicht nur Freunde hat und seine Durchsetzung in den jeweiligen Ländern und Disziplinen sehr unterschiedlich verläuft, weisen die Statistiken doch durchweg nach oben. Eine zunehmende Zahl von Forschungs- und Forschungsförderorganisationen forcieren OA durch spezielle Regelungen, die sogenannten OA-Mandate und Empfehlungen. Die Erfolgsgeschichte von OA innerhalb der letzten 10 Jahre erstaunt, weil sie dem vielfach diagnostizierten Trend der Ausdehnung des Urheberrechts (Propertisierung) in der Informationsgesellschaft widerspricht. James Boyle, einer der bekanntesten Vertreter dieser These, meint, dass wir im Internetzeitalter eine zweite Phase der Privatisierung kollektiver Güter durchlaufen. So wie einst die Aristokratie Weideland und Weiher einfriedete, beobachten wir heute die Umzäunung von „intellectual commons“. Man denke nur an die Debatten um das Leistungsschutzrecht oder ACTA.

In diesem Beitrag fragen wir uns, warum ausgerechnet der Bereich des wissenschaftlichen Wissens eine Ausnahme von der allgemeinen Ausweitung des Urheberrechts darstellen sollte und, wenn dem so sei, welche Tücken hat der Weg in den Mainstream für OA? Der erste Teil widmet sich dem Markt für wissenschaftliche Zeitschriften. Die sogenannten „Journals" dokumentieren heute das Gros des wissenschaftlichen Wissensgewinns. Der hohe Konzentrationsgrad und die immensen Gewinnspannen auf dem Journalmarkt vermitteln einen Eindruck von dem starken Gegenwind, der OA entgegenweht.

Vom Gift Exchange zu Big Deals: Die Privatisierung des akademischen Publizierens

Der Markt für wissenschaftliche Zeitschriften ist noch relativ jung. Bis Ende der 1960er Jahre wurden akademische Journale überwiegend von den Fachgesellschaften der einzelnen Disziplinen herausgegeben. Wissenschaftliche Werke galten als öffentliche Güter, die in öffentlichen Einrichtungen erzeugt und nach dem Prinzip des „gift exchange" verbreitet wurden: WissenschaftlerInnen gaben Zugang zu ihren Forschungsergebnissen und erhielten im Gegenzug die der anderen. Das heißt, die Kontrolle über den akademischen Wissensfluss lag in den Händen der Organisationen, die auch die Inhalte produzierten. Bis heute sind weite Teile des akademischen Betriebs nicht-marktförmig organisiert. Die Privatisierung des Handels mit wissenschaftlichen Zeitschriften bildet eine gewichtige Ausnahme davon.

Akademische Zeitschriften standen im Ruf eines wenig lukrativen Geschäfts, weil ihr Inhalt sehr speziell und die Abnehmerschaft entsprechend klein war. Mehrere Faktoren trugen dazu bei, dass sich trotzdem ein Markt für akademische Journale formieren konnte. Eine große Rolle spielte die anhaltende Expansion der Universitäten im letzten Drittel des 20. Jahrhunderts, die für einen stetigen Anstieg der Nachfrage sorgte. Gleichermaßen wichtig war die Einführung des Science Citation Indexes (SCI) im Jahre 1963. Der SCI ist ein bibliometrisches Instrument, das ursprünglich entwickelt wurde, um die relevantesten Zeitschriften der einzelnen Disziplinen zu identifizieren. Der SCI fasste die bestehenden Zitationsregister erstmals zu einem übergreifenden Index zusammen und schuf auf diese Weise das Konstrukt der „core journals", ein neues „generic concept with universal claims", wie Jean-Claude Guédon feststellt[1]:

> „Core science" suddenly existed and it could be displayed by pointing to a specific list of publications.

In dem Maße, in dem der SCI zum allgemein akzeptierten Auswahlkriterium für relevante, unverzichtbare Zeitschriften avancierte, entwickelten sich die „core journals" zu einer Art Monopolgut. Die Zeitschriften, die laut SCI den Forschungsstand der Disziplinen repräsentieren, sind durch andere Zeitschriften

nicht ersetzbar; Bibliotheken müssen ihren Nutzern den Zugang zu diesen ermöglichen – gleichgültig wie hoch der Preis dafür ist. Die Nachfrage nach den wichtigen Zeitschriften ist – ökonomisch formuliert – unelastisch geworden. Zusammengenommen machten die internationale Expansion von Bildung und Forschung und der SCI wissenschaftliche Zeitschriften lukrativ. In der Folge begannen die Verlage gezielt, Journale aufzukaufen.

Den Fachgesellschaften schien der Verkauf der Journale zunächst vorteilhaft, weil er finanzielle und administrative Entlastung vom Publikationsgeschäft versprach. Es dauerte allerdings nur wenige Jahre, bis sich die Schattenseiten der Privatisierung bemerkbar machten. Wissenschaftliche Einrichtungen verloren die Kontrolle über den Zugang und die Verbreitung wissenschaftlichen Wissens. An die Stelle des „gift exchange" trat die Macht der Verwertungsrechte, die AutorInnen an die Verlage abtreten. Innerhalb kurzer Zeit begannen die Zeitschriftenpreise drastisch zu steigen und bereits in den 1970er-Jahren kündigte sich die sogenannte Zeitschriftenkrise an: Moderat wachsenden Bibliotheksbudgets standen explodierende Subskriptionskosten gegenüber. Tatsächlich erhöhten sich die durchschnittlichen Preise für Zeitschriften seit den 1970er-Jahren um ein Vielfaches stärker als die Verbraucherpreise. Allein zwischen 1990 und 2000 stiegen sie laut einem OECD-Bericht[2] um etwa 180 Prozent. Andere AutorInnen sprechen für den Zeitraum zwischen 1986 und 2003 von ca. 300 Prozent Preissteigerung[3].

Die Privatisierung der wissenschaftlichen Zeitschriften konnte weder gestoppt, noch konnten ihre Auswirkungen ernsthaft eingedämmt werden. Hinzu kam ein Lock-in-Effekt, der durch die neue Rolle der „core journals" im Rahmen der Qualitätsmessung akademischer Leistungen verursacht wurde: In vielen Disziplinen avancierte das Ranking von Artikeln und AutorInnen auf der Basis der Impact Faktoren von Zeitschriften zum allgemeinen, karriereentscheidenden Standard.

Im Zuge der Digitalisierung haben sich die Geschäftsmodelle verändert. Seit den 1990er Jahren hat der lizenzierte Zugang zu digitalen Inhalten zunehmend den Verkauf von wissenschaftlichen Zeitschriftenabos abgelöst. Seit dem Ende der 1990er Jahre begannen die Verlage, sogenannte „Big Deals" mit Bibliotheken zu verhandeln, die sich zu diesem Zweck nach und nach zu Konsortien zusammenschlossen. Big Deals sind langfristige Lizenzverträge, die den Zugang zu großen Zeitschriftenpaketen regeln. Big Deals verbessern zweifellos den Zugang zu Zeitschriften, auch für kleine wissenschaftliche Einrichtungen. Allerdings sind Bibliotheken bei Big Deals gezwungen, ganze Zeitschriftenpakete zu erwerben. Sie bezahlen somit zwangsläufig auch für Journale, die sie nicht brauchen. Zudem gehen mit Big Deals Geheimhaltungsvereinbarungen („non-disclosure agreements") und damit intransparente Preismodelle einher. Die Abhängigkeit von großen Verlagen bleibt somit bestehen.

Das Milliardengeschäft mit wissenschaftlichen Zeitschriften

Heute bildet das Verlegen wissenschaftlicher Zeitschriften einen kleinen, aber hoch profitablen globalen Markt. Laut einem Report der International Association of Scientific, Technical and Medical Publishers[4] erwirtschafteten die Verlage 2011 einen weltweiten Umsatz von etwa 9,4 Milliarden USD, wobei mindestens 70 Prozent auf die Subskriptionsgebühren öffentlicher Bibliotheken zurückgehen. Schätzungen zufolge liegt die durchschnittliche Rendite der Verlage wissenschaftlicher Zeitschriften zwischen 20 Prozent und 30 Prozent[5]. Eine beeindruckende Größe, wenn man bedenkt, dass nur sehr wenige Branchen derart lukrativ sind: Profitträchtiger als das Verlegen wissenschaftlicher Zeitschriften ist nur der Finanzmarkt. Allerdings besteht zwischen den Verlagen ein erhebliches Gefälle. Während das Gros der 5.000 bis 10.000 Verlage kaum die Gewinnschwelle erreicht, weisen die „Big 5" kontinuierliche Erlösspannen zwischen 35 Prozent und 40 Prozent oder sogar darüber hinaus aus.

Ermöglicht werden diese außerordentlichen Gewinne durch die unbezahlte Arbeit der zumeist öffentlich finanzierten WissenschaftlerInnen, die sowohl die Inhalte produzieren als auch die Qualitätskontrolle übernehmen. Die Verlage selbst „add relatively little value to the publishing process", wie eine – viel zitierte[6], aber leider nicht online verfügbare – Analyse der Deutschen Bank nüchtern feststellt.

Nach einer Phase der Fusionen und Aufkäufe ist der wissenschaftliche Zeitschriftenmarkt heute durch einen hohen Konzentrationsgrad geprägt. In dieser Hinsicht ähnelt er der internationalen Musikbranche. Die fünf größten Verleger halten einen Marktanteil von etwa 35 Prozent. Die größten drei, Elsevier, Springer und Wiley-Blackwell, publizieren jeweils mehr als 2.000 Journale und in 2011 immerhin 42 Prozent aller Artikel[7].

Der Markt für wissenschaftliche Zeitschriften bildet einen wichtigen Entstehungskontext für die Open-Access-Bewegung. Kennzeichnend für diesen Markt sind sehr stabile, wenig innovative, jedoch enorm profitable und oligopolförmige Strukturen. Die Marktmacht der Verlage beruht unter anderem darauf, dass die AutorInnen ihnen – in Abwesenheit eines effektiven Zweitveröffentlichungsrechts[8] – üblicherweise die ausschließlichen Verwertungsrechte für ihre Werke übertragen. Die Verwertungsrechte bilden die Grundlage für die Lizenzbedingungen, mit denen die Verlage die wissenschaftliche Kommunikation einschließlich der Zugangs- und Nutzungsbedingungen von Werken weitgehend bestimmen. Die hohen Profite wiederum erklären sich aus einer Kombination von geringer Wertschöpfungsleistung und dem Monopolgüterstatus von „core journals".

Die Open-Access-Bewegung entstand interessanterweise im gleichen Zeitraum wie die ersten kommerziellen Experimente mit der Vermarktung des elektronischen Zugangs zur wissenschaftlichen Literatur. In diesem Sinne stellen die Big

Deals der Verlage und die akademische Open-Access-Bewegung zwei gegensätzliche Antworten auf die Digitalisierung der wissenschaftlichen Kommunikation dar.

Die Gründungsmythen von Open Access

Die zentrale Idee von OA ist, mit öffentlichen Mitteln finanzierte wissenschaftliche Werke allgemein zugänglich zu machen. Allerdings ist OA selbst wiederum ein Sammelbegriff für verschiedene Programme, Ziele und Verfahren, die sich im Laufe der vergangenen Jahre herausgebildet haben. Explizit definiert wurde OA erstmals 2001 im Rahmen der Budapest Open Access Initiative[9], die die bis heute bekannteste Begriffsbestimmung vorgelegt hat:

> „Open Access" meint, dass Peer-Review-Fachliteratur kostenfrei und öffentlich im Internet zugänglich sein sollte, sodass Interessenten die Volltexte lesen, herunterladen, kopieren, verteilen, drucken, in ihnen suchen, auf sie verweisen und sie auch sonst auf jede denkbare legale Weise benutzen können, *ohne finanzielle, gesetzliche oder technische Barrieren* jenseits von denen, die mit dem Internet-Zugang selbst verbunden sind. In allen Fragen des Wiederabdrucks und der Verteilung und in allen Fragen des Copyrights überhaupt sollte die einzige Einschränkung darin bestehen, den Autoren Kontrolle über ihre Arbeit zu belassen und deren Recht zu sichern, dass ihre Arbeit angemessen anerkannt und zitiert wird.

Über die Entstehung von OA kursieren mindestens zwei Erzählungen, die beide mit der Digitalisierung beginnen. Die bekanntere Variante führt die Entstehung von OA auf die Zeitschriftenkrise zurück. Demnach waren es rasch steigende, überhöhte Preise für Zeitschriften und restriktive Nutzungsbedingungen, die die Open-Access-Bewegung begründet haben. Die zweite Erzählung erklärt die Entstehung von OA mit dem Wunsch einiger ForscherInnen, die wissenschaftliche Kommunikation mithilfe des Internets zu revolutionieren.

Vor allem in den Technik- und Naturwissenschaften hatte sich schon in den 1970er Jahren eine „Pre-Print-Kultur" entwickelt. Um den Kommunikationsprozess zu beschleunigen, zirkulierten die AutorInnen ihre zur Begutachtung eingereichten Artikel zeitgleich unter KollegInnen. Ende der 1980er Jahre ersetzte das Internet den Postverkehr und die ersten Disziplinen begannen, ihre Artikel elektronisch zu archivieren. 1991 richtete Paul Ginsparg „arXiv", den ersten Pre-Print-Server für Physiker ein, der Vorabdrucke nicht nur archivierte, sondern auch allgemein zugänglich und durchsuchbar machte. Im gleichen Zeitraum entstanden die ersten elektronischen OA-Zeitschriften. 1989 gründete Stevan Harnad das Online-Journal Psycoloquy, das der Idee des „scholarly skywriting" ge-

widmet war: Untereinander verbundene Texte, Kommentare und Revisionen sollten für alle sichtbar sein, als wären sie in den Himmel geschrieben.

Die treibende Kraft hinter den ersten Initiativen zur Selbstarchivierung, später als „Grüner Weg" bezeichnet, und Online-Journalen waren also nicht primär hohe Preise oder die Macht der Verlage, sondern die Faszination über die neuen Möglichkeiten, die das elektronische Kommunizieren bot[10]:

> Although I knew about the price of subscriptions and the serials crisis at the time, that was not my primary motivation: open online access and interaction was (and still is).

Die verschiedenen Gründungsmythen von OA sind bis heute relevant, denn sie verweisen auf unterschiedliche Zielsetzungen und Lösungspfade. So können die Zeitschriftenkrise und das Problem der Finanzierbarkeit im Prinzip durch Big Deals großer Bibliothekskonsortien und Nationallizenzen abgemildert werden. Der Verwirklichung von „skywriting"' kommt man durch Big Deals nicht näher. Weder dehnen diese den Zugang zu wissenschaftlichen Werken auf alle BürgerInnen aus, noch erlauben sie eine Nachnutzung von Texten und Daten. Die wissenschaftliche Kommunikation wird auch weiterhin durch die Lizenzpolitik der Verlage bestimmt.

Die OA-Erzählung, die in den Selbstarchivierungs- und Kooperationspraktiken der 1980er und 1990er Jahre wurzelt, begnügt sich also nicht mit einem lizensierten Zugang für WissenschaftlerInnen, sondern sie führt über den Grünen Weg zu „Libre OA" (siehe unten) und von dort aus weiter zu „Open Science".

Als wissenschaftliche Graswurzelbewegung beschränkte sich OA zunächst auf wenige Disziplinen, wie Physik, Kognitionsforschung und Biologie bzw. Biomedizin. Ein „subversive proposal"[11], das dazu aufforderte, Publikationen künftig grundsätzlich online zugänglich zu machen, fand kein breites Echo. Allerdings entstanden im Laufe der 1990er Jahre immer mehr Repositorien und Literaturdatenbanken und gegen Ende der 1990er Jahre gewann der Unmut über die Preispolitik der Verlage allmählich Momentum. Neben Kampagnen, Deklarationen, Manifesten und Boykottaufrufen kam es zu Rücktritten ganzer Zeitschriftenredaktionen und Neugründungen von OA-Journalen. Gleichzeitig zeigten sich Institutionalisierungstendenzen, die die OA-Mythen bzw. Ansätze miteinander verknüpften.

Open Access etabliert sich

1999 gründete sich die Open Archives Initiative, die plattformübergreifende Metadaten für die Suche von OA-Publikationen entwickelt. Einen weiteren wichtigen Schritt zu mehr Interoperabilität bildete die Entwicklung der EPrints Software im Jahre 2000, mit der Forschungseinrichtungen OA-Repositorien schaffen

können. Im Jahre 2003 entstand das Directory of Open Access Journals und damit zugleich Mindeststandards für die Definition von OA-Zeitschriften. Zugleich dehnte sich der OA-Gedanke auf weitere Bereiche aus. So führte das MIT 2002 das OpenCourseWare-Projekt ein, um Lehrmaterialien kostenlos zugänglich zu machen. Im gleichen Jahr startete eine Gruppe um Lawrence Lessig die Creative Commons Initiative. Die modularen Lizenzen sind im Kontext von OA wichtig, um (Nach-)Nutzungsmöglichkeiten für Texte, Daten und andere wissenschaftliche Erzeugnisse festlegen zu können. Davon kann etwa abhängen, ob Textmining oder Übersetzungen ohne Weiteres möglich sind.

Um die Jahrtausendwende hatte sich OA so weit etabliert, dass erste OA-Verlage entstanden und eine Ausdifferenzierung von Geschäftsmodellen einsetzte. Wiederum bildeten die Biomedizin sowie die Natur- und Technikwissenschaften die Vorreiter. Zwei ikonische Beispiele sind der im Jahre 2000 gegründete britische Verlag Biomed Central und der gemeinnützige US-Verlag Public Library of Science (PLoS), die beide als Wegbereiter von OA gelten.

Biomed Central gilt als der erste erfolgreiche kommerzielle OA-Verlag. Sein Gründer, Vitek Tracz, experimentierte mit Geschäftsmodellen für OA-Verlage und führte im Jahre 2002 das „author pays"-Prinzip ein[12]:

> So we said: „OK, we will turn the current model upside down and offer the research articles free to readers and charge for services to authors."

Im Jahre 2008, als sich Biomed Central als weltweit größter OA-Verlag etabliert hatte und knapp 200 Zeitschriften herausgab, kaufte Springer das Unternehmen – ein Beleg nicht nur für den Gesinnungswandel der Wissenschaftsverlage, die OA bis dato bekämpft hatten, sondern auch für die Erfolgsaussichten des Geschäftsmodells.

Die Ursprünge von Public Library of Science (PLoS) liegen in einer erfolglosen Initiative von WissenschaftlerInnen im Umfeld der Biomedizin. Im Jahre 2000 hatten sie die Wissenschaftsverlage aufgefordert, Forschungsliteratur in öffentlichen Repositorien wie PubMed Central zugänglich zu machen und zudem angedroht, künftig nur noch in OA-Journalen zu publizieren. Nachdem die von mehr als 30.000 WissenschaftlerInnen unterstützte Petition weitgehend folgenlos blieb und der Boykott mit Durchsetzungsproblemen zu kämpfen hatte, entschieden sich die Initiatoren, PLoS zu einem nicht-kommerziellen OA-Verlag auszubauen. Den Gründern von PLoS ging es neben dem Zugang vor allem auch um die Verfügbarkeit öffentlich finanzierter Forschung[13]:

> Should the reward for the publishers' small contribution be permanent, private ownership of the published record of scientific research,

> and monopoly control over how, when and by whom a paper can be read or used and how much this access will cost? No!

Die seit 2003 bei PLoS erscheinenden Journale veröffentlichen ihre Artikel unter der Creative-Commons-Lizenz CC-BY. Die Finanzierung von PLoS orientiert sich jedoch interessanterweise am „author pays"-Modell des kommerziellen BioMed Central Verlags.

Grün, Gold, Freiheit oder Freibier: Die Spielarten von OA

Spätestens mit der Etablierung von Verlagen gabelten sich die OA-Strategien. Auf der einen Seite breiteten sich Repositorien für die öffentliche Selbstarchivierung aus. Auf der anderen Seite entwickelte sich eine Zeitschriften- und Verlagslandschaft, die unter dem Vorzeichen unterschiedlicher Ziele mit kommerziellen bzw. nicht-kommerziellen Publikationsmodellen experimentierte. Um 2004 haben sich für diese zwei wichtigsten Verbreitungsmodelle die Bezeichnungen „Grüner" und „Goldener Weg"' durchgesetzt. Der Grüne Weg bezeichnet die Archivierung von Beiträgen in Repositorien (öffentlichen Dokumentenservern). Die Veröffentlichung in OA-Zeitschriften entspricht dem Goldenen Weg.

Eine weitere wichtige Unterscheidung betrifft die Art und den Umfang der Offenheit. „Gratis OA" signalisiert das Fehlen von Preisbarrieren; „Libre OA" steht für den Verzicht zumindest eines Teils der urheberrechtlichen Nutzungsrestriktionen. Diese Unterscheidung entspricht jener zwischen „free beer" und „free speech" in der Debatte um freie Software.

Orientiert an diesen vier Grundtypen haben sich einige Mischformen von OA entwickelt. An erster Stelle ist hier das zeitverzögerte („delayed") OA zu nennen, das AutorInnen erst nach einer Embargophase die Selbstarchivierung ihrer Artikel erlaubt. Ferner sind viele Verleger zu Hybridlösungen übergegangen. Sie bieten ForscherInnen an, ihre Beiträge, die sie in konventionellen Journalen veröffentlichen, für durchschnittlich 3.000 USD „freizukaufen". Dieses Hybridmodell steht im Ruf des „double dipping", einer Praxis, bei der Verlage gleichzeitig Subskriptions- und Publikationsgebühren erheben. Open Access wird auf diesem Wege zur Zusatzeinnahmequelle der Verlage, während das dysfunktionale wissenschaftliche Publikationssystem auf Basis von Subskriptionsgebühren unangetastet bleibt.

Ein Tropfen im Ozean: Zur Verbreitung von Open Access

Auf den ersten Blick weisen die Zahlen zur Verbreitung von OA seit vielen Jahren kontinuierlich nach oben. Obwohl die Mehrzahl wissenschaftlicher Veröffentlichungen nach wie vor nicht allgemein zugänglich ist, liegt der Anteil von OA schätzungsweise zwischen 10 und 20 Prozent. Eine aktuelle Studie im Auftrag der EU-Kommission[14] stellt eine noch höhere OA-Verbreitung fest. Ihr zufolge liegt der OA-Anteil bei neueren Veröffentlichungen bei bis zu 50 Prozent.

In einigen EU-Mitgliedsstaaten wie Großbritannien scheint der Umschlagpunkt inzwischen sogar überschritten zu sein, sodass mehr als 50 Prozent aller neueren Artikel in irgendeiner Form frei zugänglich sind.

Zahlen zu OA – nicht nur jene aus der EU-Studie – sind jedoch mit Vorsicht zu genießen. Wie oben gezeigt, gibt es mehrere mögliche Definitionen von OA. Was die jeweiligen Studien unter „frei zugänglich" verstehen und subsumieren, differiert stellenweise enorm. Das führt zu unterschiedlichen Ergebnissen und Schlussfolgerungen. Kurzum wird mit diesen Zahlen auch Politik gemacht. So heißt es in der erwähnten EU-Studie:

> Despite what several authors thought, and argued for, green OA only appears to be moving slowly, whereas gold and hybrid OA (such as pay-per-article for OA release) appear to be driving in the fast lane.

Auch die Anzahl der OA-Journale ist im Wachstum begriffen. So weist das Directory of Open Access Journals augenblicklich knapp 10.000 Zeitschriften und rund 1.7 Millionen Artikel aus. Diese Erfolgsmeldungen täuschen allerdings darüber hinweg, dass die Bedeutung der etablierten „core journals" in den meisten Disziplinen ungebrochen und die Mehrzahl wichtiger Artikel weiterhin hinter Bezahlschranken verschlossen ist. Nur in den Disziplinen Biologie, Physik und Gesundheitswissenschaften haben sich OA-Journale als ernsthafte Alternative etablieren können.

Ob Gold oder Grün: Eine US-amerikanische Biologin profitiert bislang ungleich mehr von Open Access als eine deutsche Sozialwissenschaftlerin. Im EU-Vergleich gehört Deutschland nämlich zu den Schlusslichtern und die Human- und Sozialwissenschaften zählen wiederum zu jenen Fächern, in denen sich OA bis heute nicht durchgesetzt hat. OA stellt in den meisten Disziplinen nach wie vor ein Randphänomen dar; die große Masse der akademischen Veröffentlichungen ist nicht frei zugänglich. Man setze sich an seinen Rechner und versuche die relevante Literatur zu einem Forschungsproblem im Internet zu recherchieren, ohne auf eine Universitätsbibliothek zurückgreifen zu können. Auch um diesen Artikel zu schreiben, mussten wir auf Informationen zurückgreifen, die nur Angehörigen gut situierter Wissenschaftseinrichtungen zugänglich sind.

Die politische Dimension von Open Access

Die großen internationalen Unterschiede in der Verbreitung von Open Access resultieren aus unterschiedlichen OA-Politiken. Diese können als nationale OA-Policies sowie als „Mandate" der Forschungs- und Forschungsförderungsorganisationen daherkommen. OA-Politiken können den Charakter bloßer Empfehlungen (wie in Deutschland) haben oder aber obligatorisch sein und dadurch enormen Einfluss entfalten.

Open Access Policies: Schlupflöcher, Mandate, Zweitverwertungsrecht

OA-Mandate schreiben vor, dass begutachtete Arbeiten entweder in Repositorien deponiert oder in OA-Journalen veröffentlicht werden müssen. Erlassen werden können sie entweder von den wissenschaftlichen Einrichtungen, bei denen die WissenschaftlerInnen beschäftigt sind, oder von den Forschungsförderern, die die Finanzierung bereitstellen.

Die ersten institutionellen OA-Mandate entstanden um 2004. Derzeit gibt es weltweit etwa 230 institutionelle Mandate und weitere 90 Mandate von Förderungsinstitutionen. OA-Mandate variieren untereinander im Hinblick auf den Umfang der obligatorischen öffentlichen Zugänglichkeit, die Ausnahmen von der OA-Regel und auch bezüglich ihrer Sanktionsmechanismen. Anders formuliert lassen sich OA-Mandate entsprechend des institutionellen Gegengewichts kategorisieren, das Forschungs- und Förderungseinrichtungen gegenüber Verlagen und Veröffentlichungskonventionen in die Waagschale legen. Je weitgehender und strikter die Regelungen der wissenschaftlichen Einrichtungen, desto enger die Handlungsspielräume der Verlage – und AutorInnen.

Peter Suber[15] unterscheidet zwischen drei verschiedenen Mandatstypen – eine Art OA-Durchsetzungshierarchie: die schwächste Form des Mandats sind „Loophole"-Regelungen, die eine Selbstarchivierung nur dann erfordern, wenn der Verlag dieser zustimmt. „Deposit mandates" wiederum verlangen eine Selbstarchivierung unter allen Umständen, aber die Zugänglichkeit der Texte orientiert sich an Sperrfristen und ist somit ins Belieben der Verlage gestellt. Die weitestgehende Regelung enthält eine „rights retention" Pflicht, mit der sich Universitäten grundsätzlich ein Zweitveröffentlichungsrecht vorbehalten, sodass AutorInnen erst gar keine ausschließlichen Verwertungsrechte an Verlage übertragen können (auch hier bestehen Ausnahmeregelungen).

Als internationales Vorbild und Kompromisslösung für OA-Mandate gilt derzeit das von der Universität Liège im Jahre 2008 eingeführte „deposit mandate"[16], das alle AutorInnen dazu verpflichtet, ihre Arbeiten im Repositorium der Universität zu deponieren, sobald diese den Begutachtungsprozess erfolgreich durchlaufen haben und zur Veröffentlichung angenommen worden sind; unabhängig davon, ob der Verlag eine Sperrfrist für Zweitveröffentlichungen verhängt oder nicht. Um die Befolgung der „immediate-deposit clause" sicherzustellen, werden bei Evaluationen grundsätzlich nur die im universitätseigenen Repositorium befindlichen Veröffentlichungen berücksichtigt. Neben diesem offenbar sehr erfolgreichen Durchsetzungsmechanismus besteht ein besonderes Merkmal des Liège-Modells im „email-eprint-request button", der es ForscherInnen erlaubt, auch Sperrfristen unterliegende Artikel mit einem Klick von der AutorIn per E-Mail anzufordern.

Passt Grün zu Gold? Die Zukunft des OA-Publizierens

Rund zehn Jahre nach der Berliner Erklärung lautet die zentrale Frage derzeit nicht, ob sich OA durchsetzt, sondern verhandelt werden die Bedingungen und der Umfang der freien Zugänglichkeit zu wissenschaftlicher Literatur. Die Verlage bevorzugen den Goldenen Weg und das damit verbundene „author pays"-Modell, weil es die Struktur des Zeitschriftenmarktes im besten Fall nur geringfügig ändert. Universitäten und Förderungseinrichtungen geben zumeist einer Kombination aus Grünem und Goldenem Weg den Vorzug. Beide Verfahren sind allerdings mit spezifischen Vor- und Nachteilen behaftet.

Als großer Vorteil des Goldenen Wegs gilt, dass Texte und Daten ohne Umweg über Embargos sofort verfügbar sind. Zudem können über „gratis OA" hinausgehende Lizenzmodelle, d. h. „Libre OA" mit den Verlagen explizit vereinbart werden oder sind bereits vorgesehen. Nachteilig an der Goldenen Lösung ist, dass sich die (Preissetzungs-)Macht der Verlage auf die AutorInnengebühren ausdehnt. Ein weiteres – umstrittenes[17] – Argument ist, dass das „author pays"-Modell die Gefahr sinkender Qualitätsstandards mit sich bringt. Denn AutorInnengebühren könnten Anreize schaffen, die Anzahl der Veröffentlichungen zu erhöhen und Begutachtungs- und Selektionsprozesse durchlässiger zu gestalten.

Die Vorteile des Grünen Wegs sind, dass nahezu keine zusätzlichen Veröffentlichungskosten anfallen. Anders als beim Goldenen Weg können die Förderungsinstitutionen – wie oben anhand des Liège-Modells erklärt – den Grünen Weg verpflichtend vorschreiben, ohne in die Wissenschaftsfreiheit einzugreifen. (Wissenschaftsfreiheit ist wiederum ein umstrittener Begriff im OA-Diskurs[18].) Der Nachteil des Grünen Wegs besteht vor allem in seiner schwierigen Durchsetzbarkeit, weil in vielen Ländern (darunter Deutschland) keine OA-Mandate bestehen oder diese durch Embargoregeln und die verbreitete Nichtbefolgung unterlaufen werden. Hinzu kommt, dass die Selbstarchivierung zumeist die Form von Gratis-OA annimmt, weil viele AutorInnen und Repositorien nicht ausdrücklich auf die Urheberrechte verzichten.

Die AdvokatInnen des Grünen Wegs sind der Meinung, dass eine flächendeckende Durchsetzung von Selbstarchivierungsregeln Voraussetzung dafür ist, dass die Nachteile des Goldenen Wegs begrenzt und faire Goldene Geschäftsmodelle möglich werden. Erst wenn alle Artikel und Daten zumindest im Rahmen von Gratis-OA allgemein zugänglich sind und Bibliotheken überteuerte Zeitschriften tatsächlich abbestellen können, so das Argument, wird sich die Verhandlungssituation im Zeitschriftenmarkt zugunsten von AutorInnen und Bibliotheken ändern. Die VerfechterInnen des Goldenen Wegs halten dem entgegen, dass nur dieser die sofortige und vollständige Verfügbarkeit von qualitätsgeprüften Texten und Daten garantiert.

Obwohl viele Stimmen betonen, dass die jeweiligen Wege nicht als konkurrierende, sondern als komplementäre Verfahren[19] verstanden werden sollten, be-

steht aufgrund ihrer unterschiedlichen Konsequenzen für die weitere Entwicklung des Zeitschriftenmarkts ein unübersehbares Spannungsverhältnis zwischen Grün und Gold. Die BefürworterInnen des Goldenen Modells sehen sich dem Vorwurf ausgesetzt, den Interessen der Verlage Vorrang gegenüber jenen der Forschung einzuräumen.

„Pay to say"? Die britische Open-Access-Politik

Einer der wichtigsten Schauplätze der gegenwärtigen Aushandlung von OA-Policies ist Großbritannien, eines der OA-Pionierländer. Bereits 2004 hatte das Science and Technology Committee des Britischen Unterhauses empfohlen[20], dass AutorInnen ein Zweitveröffentlichungsrecht erhalten und Kopien ihrer Artikel in öffentlich zugänglichen Repositorien deponieren. Heute ist Großbritannien das Land mit der weltweit höchsten Anzahl von OA-Mandaten, einer respektablen Anzahl von Repositorien und einem Anteil von öffentlich zugänglichen Veröffentlichungen von rund 40 Prozent[21].

Im Jahre 2011 setzte die britische Regierung die OA-Politik erneut auf die Tagesordnung und berief[22] eine unabhängige Arbeitsgruppe mit dem Ziel ein, Vorschläge zur Verbesserung des Zugangs zu Forschungsergebnissen zu entwickeln. Die aus VertreterInnen der Wissenschaft, der Förderungseinrichtungen, des zuständigen Wirtschaftsministeriums und der Verlage zusammengesetzte ExpertInnengruppe sprach sich für eine grundlegende Neuausrichtung der britischen OA-Politik aus. In Abkehr von der bisherigen OA-Politik favorisierte der „Finch Report"[23] den Goldenen Weg und reduzierte den Grünen Weg auf eine Rückfalloption für graue Literatur (z. B. Abschlussarbeiten und Arbeitspapiere), Forschungsdaten und die Fälle, in denen eine Publikation in Goldenen Journalen nicht möglich ist. Zugleich empfahl die ExpertInnengruppe, das bisherige subskriptionsbasierte Finanzierungsmodell wissenschaftlicher Zeitschriften auf ein „author pays"-Modell umzustellen. Die Begründung für diesen radikalen Schritt lautet, dass die Selbstarchivierung das Ziel einer allgemeinen Zugänglichkeit wissenschaftlicher Arbeiten nur unzureichend erfüllt. Der Goldene Weg erlaube demgegenüber einen nachhaltigen Wandel in der Publikationspraxis unter Beibehaltung der akademischen Qualitätsmessungsverfahren und Zusammenarbeit mit den etablierten Verlagen.

Die britische Regierung folgte den Empfehlungen des Finch Reports und stellte sogleich eine Anschubfinanzierung für den Aufbau von Publikationsfonds[24] bereit. Der britische Research Council reagierte auf die Empfehlungen des Finch Reports noch im gleichen Jahr mit einer Änderung seiner Förderungsrichtlinien. Seit 2013 müssen RCUK geförderte Veröffentlichungen nicht nur öffentlich zugänglich gemacht werden, sondern dem Goldenen Weg ist Priorität einzuräumen, sofern öffentliche Mittel für die Publikationsgebühren zur Verfügung stehen.

Der Finch Report und die darauf gründende Förderungspolitik des RCUK haben national wie international Kritik ausgelöst[25]. Ein Committee des britischen Unterhauses reagierte auf den Finch Report mit einem eigenen Konsultationsverfahren und einer Stellungnahme[26], die sich sehr kritisch gegenüber der Kehrtwende in der britischen OA-Politik äußerte. Auch WissenschaftlerInnen meldeten sich zu Wort und wiesen auf die problematischen Folgen einer verbindlichen Einführung des Goldenen Wegs hin. So stehe angesichts knapper Ressourcen zu befürchten, dass die Publikationsfonds für das „author pays"-Modell nicht ausreichten und die Universitäten daher gezwungen würden, diese nach Kriterien zu verteilen, die nicht wissenschaftlichen Standards und der Praxis des Peer-Reviews entsprächen. Publikationsmöglichkeiten würden unter diesen Umständen künftig weniger von der wissenschaftlichen Qualität als von den vorhandenen Publikationsressourcen abhängen. Die Autonomie und Qualitätskontrolle der Wissenschaft werde hierdurch geschwächt. Zudem bestehe die Gefahr, dass öffentliche Forschungsmittel dauerhaft in Publikationsfonds umgewandelt werden und somit an die Verlage abfließen. Das „pay-to-say"-Modell bedrohe mithin die Freiheit der Wissenschaft[27].

Die Kritik an der Privilegierung des Goldenen Wegs hat inzwischen einen Niederschlag in den neuen Richtlinien des Higher Education Funding Council for England (HEFCE)[28] gefunden, der für die Ressourcenzuteilung und Evaluierung der britischen Forschungseinrichtungen zuständig ist. Ab der Evaluierungsperiode 2016 bezieht HEFCE ausschließlich Publikationen in die Begutachtung ein, die frei zugänglich sind. Die neuen Richtlinien stützen sich ausdrücklich auf das Verfahren der Université de Liège[29]. Es können daher nur Veröffentlichungen geltend gemacht werden, die nach einer positiven Begutachtung innerhalb von drei Monaten in einem Repositorium der Universität deponiert wurden.

Die jüngeren Entwicklungen in der britischen OA-Politik vermitteln einen guten Eindruck von den relevanten AkteurInnen, ihren Zielen und Einflussmöglichkeiten. Regierungen, Universitäten, Förderungsorganisationen, Verlage und WissenschaftlerInnen ringen um die Ausgestaltung der künftigen Evaluierungs- und Förderungsrichtlinien, und sie verhandeln damit nichts Geringeres als die Kontrolle über die wissenschaftlichen Inhalte und die Modi ihrer Verbreitung. Die Verlage sind an der Etablierung von Publikationsfonds interessiert, die das „author pays"-Modell und damit verknüpfte Gewinnerwartungen absichern. Die Wissenschaft wiederum befürchtet eine Umverteilung von Forschungsressourcen zugunsten der Verlagswirtschaft und neue Publikationsengpässe. Die Regierung, die Forschungs- und Forschungsförderungsorganisationen hingegen sind in der Position, verbindliche OA-Regelungen durchzusetzen, aber dem voraus geht eine Abwägung der beteiligten öffentlichen und privaten Interessen; eine schwierige Gratwanderung mit offenem Ausgang, wie die britische Entwicklung demonstriert.

Die Auseinandersetzungen in Großbritannien bieten auch Anhaltspunkte für die Bewertung der europäischen OA-Politik. Das neue EU-Forschungsrahmenprogramm Horizon 2020 enthält erstmals ein OA-Mandat[30]. Alle durch das Programm geförderten Forschungsergebnisse müssen in einem Repositorium abgelegt werden, auch wenn sie in einem Goldenden OA-Journal erscheinen. Es bleibt abzuwarten, ob die europäische Regelung Impulse für Länder mit schwachen OA-Politiken wie etwa Deutschland geben kann.

Fazit: Der Zaun um die wissenschaftliche Allmende

Die OA-Bewegung hat den von James Boyle beklagten Zaun um die Wissensallmende zwar nicht eingerissen, aber sie hat ihn zweifellos auf die (wissenschafts-)politische Tagesordnung gesetzt. Das große Verdienst von OA besteht in der Politisierung der akademischen Publikationsbedingungen und der privatwirtschaftlichen Kontrolle über Forschungsergebnisse. Nach und nach geraten etablierte Geschäftsmodelle und akademische Veröffentlichungskonventionen unter Rechtfertigungsdruck und müssen sich den Vergleich mit OA gefallen lassen.

Unterdessen ergibt die Entwicklung von OA bislang ein sehr uneinheitliches Bild mit großen Unterschieden zwischen einzelnen Disziplinen und Ländern. Allerdings werden die konkreten OA-Politiken und ihre Durchsetzungsmechanismen von einzelnen Pionierorganisationen und großen Förderorganisationen ausgehandelt. Zur Diskussion steht hier nicht mehr die Einführung von OA, sondern dessen Ausgestaltung: Bleibt die Selbstarchivierung eine wählbare und gleichberechtigte Option oder wird sie durch verlagsfreundliche Förderpolitiken und lange Sperrfristen marginalisiert? Offen ist auch die weitere Entwicklung der Verwertungsrechte. Können sich Creative-Commons-Lizenzen gegenüber Gratis-OA durchsetzen, sodass die erlaubnisfreie Nachnutzung von Texten und Daten die Norm wird? In der Verbindung zur Lizenzierungsfrage zeigt sich, dass die Bedeutung von OA über den reinen Zugang zu Forschungsergebnissen hinausgeht und die Forschungsbedingungen in einem viel weiteren Umfang betrifft.

Lässt sich Open Access also als eine Abkehr von der Umzäunung der „intellectual commons“ deuten? Zumindest sollte der verbreiteten Annahme über die lineare Expansion von Ausschlussrechten in der Informationsökonomie nicht mehr widerspruchslos gefolgt werden.

Anmerkungen

[1] http://www.arl.org/storage/documents/publications/in-oldenburgs-long-shadow.pdf

[2] http://www.oecd-ilibrary.org/science-and-technology/digital-broadband-content-scientific-publishing_9789264065901-en

[3] http://southernlibrarianship.icaap.org/content/v09n03/mcguigan_g01.html

[4] http://www.stm-assoc.org/industry-statistics/the-stm-report/

[5] http://www.nature.com/news/open-access-the-true-cost-of-science-publishing-1.12676

[6] http://southernlibrarianship.icaap.org/content/v09n03/mcguigan_g01.html

[7] http://www.theguardian.com/commentisfree/2011/aug/29/academic-publishers-murdoch-socialist

[8] http://irights.info/artikel/zweitveroffentlichungsrecht-die-richtung-stimmt-die-details-enttauschen/15422

[9] http://www.budapestopenaccessinitiative.org

[10] http://poynder.blogspot.de/2014_06_01_archive.html

[11] https://groups.google.com/forum/?hl=en#!topic/bit.listserv.vpiej-l/BoKENhK0_00

[12] http://www.infotoday.com/it/jan05/poynder.shtml

[13] http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1084138/

[14] http://europa.eu/rapid/press-release_IP-13-786_de.htm

[15] https://mitpress.mit.edu/sites/default/files/titles/content/openaccess/Suber_11_chap4.html#chap4

[16] http://www.eprints.org/openaccess/policysignup/fullinfo.php?inst=Universit%C3%A9%20de%20Li%C3%A8ge

[17] http://svpow.com/2013/10/03/john-bohannons-peer-review-sting-against-science/

[18] http://www.inf.uni-konstanz.de/netethicsblog/?p=247

[19] https://mitpress.mit.edu/sites/default/files/titles/content/openaccess/Suber_10_chap3.html#chap3

[20] http://www.publications.parliament.uk/pa/cm200304/cmselect/cmsctech/399/399.pdf

[21] http://www.publications.parliament.uk/pa/cm201314/cmselect/cmbis/99/9906.htm#a3

[22] http://www.theguardian.com/science/2011/dec/08/publicly-funded-research-open-access

[23] http://www.researchinfonet.org/wp-content/uploads/2012/06/Finch-Group-report-FINAL-VERSION.pdf

[24] https://www.gov.uk/government/news/government-invests-10-million-to-help-universities-move-to-open-access

[25] http://openaccess.eprints.org/index.php?/archives/904-Finch-Report,-a-Trojan-Horse,-Serves-Publishing-Industry-Interests-Instead-of-UK-Research-Interests.html

[26] http://www.publications.parliament.uk/pa/cm201314/cmselect/cmbis/99/9902.htm

[27] http://thedisorderofthings.com/2012/12/04/open-access-hefce-ref2020-and-the-threat-to-academic-freedom/

[28] http://www.hefce.ac.uk/news/newsarchive/2014/news86805.html

[29] http://blogs.lse.ac.uk/impactofsocialsciences/2014/04/01/hefce-open-access-ref-gamechanger/

[30] http://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Open_Access_in_H2020.pdf

Jeanette Hofmann leitet am Wissenschaftszentrum Berlin für Sozialforschung die Projektgruppe Politikfeld Internet. Sie ist Ko-Direktorin des Alexander von Humboldt Instituts für Internet und Gesellschaft und leitet dort den Bereich Policy und Governance und ist Professorin für Internetpolitik an der Universität der Künste. Sie war Sachverständige in der Enquete-Kommission Internet und Digitale Gesellschaft und beteiligt sich aktiv im Internet Governance Forum.

Benjamin Bergemann studierte Politikwissenschaft in Berlin und forscht nun am Wissenschaftszentrum Berlin für Sozialforschung. Er interessiert sich für Datenschutz, Überwachung und das große Ganze der Informationsgesellschaft. Benjamin ist zudem im Digitale Gesellschaft e.V. aktiv.

23

Open the Snowden Files! Das öffentliche Interesse am freien Zugang zu den Dokumenten des NSA-Gate

von **Krystian Woznicki**

In der Snowden-Debatte kommen immer größere Zweifel an dem Auswertungsverfahren der Dokumente auf. Die exklusiven Partnerschaften, die der Whistleblower mit Journalisten und Redaktionen eingegangen ist, stoßen an ihre Grenzen: Könnte die Arbeit im Dienste der Öffentlichkeit nicht inklusiver und dadurch auch effizienter gestaltet werden? Berliner Gazette-Herausgeber Krystian Woznicki erklärt in seinem Essay, warum wir über einen offenen Zugang zu den Snowden-Dokumenten nachdenken sollten.

Gibt es eine globale Überwachungsindustrie, in der Staaten und Konzerne gemeinsamen Interessen nachgehen – all das jenseits von demokratischer Legitimation und Kontrolle? Die Enthüllungen durch Edward Snowden haben diese Frage aufgeworfen und in Teilen beantwortet. Deshalb sind sie von öffentlichem Interesse. Unterstrichen wird das dadurch, dass die Enthüllungen eine beispiellose Medienerzählung ausgelöst haben; allein die Dauer ist historisch (über ein Jahr lang hat sie sich entfaltet und im Zuge dessen verschiedene Debatten stimuliert). Doch die politische und gesellschaftliche Wirkung dieser Erfolgsgeschichte ist begrenzt. Warum sind Massenproteste ausgeblieben? Warum hat es keinen Umsturz gegeben?

Meine These: Das öffentliche Interesse ist bislang nicht ausgereizt worden. Das liegt nicht zuletzt daran, dass der Zugang zu den Dokumenten des NSA-Gate nicht offen ist. Nachdem ein mutiger Bürger „unter Lebensgefahr" (Constanze Kurz) Material zusammengetragen hat, weil er glaubte, dass es von öffentlichem Interesse sei, ist es nicht in der öffentlichen Hand gelandet. Und untersteht auch nicht ihrer Kontrolle. Das blockiert das demokratische Potenzial der Snowden-Enthüllungen.

Kann der Datenberg geöffnet werden?

Nur ein kleiner Teil des Snowden-Materials wurde bislang als Original-Dokument veröffentlicht (weniger als 5 Prozent). Entscheidungen darüber gehen auf einen kleinen Kreis von Leuten zurück, die das Material bearbeiten, lesen, analysieren, interpretieren und publizieren. Jene, die zu dem kleinen Kreis gehören, darunter Glenn Greenwald, argumentieren damit, dass all das aus Sicherheitsgründen geschehe. In diesem Sinne könnte man sagen, dass das Snowden-Material von den richtigen Leuten „sichergestellt" wurde, um größeren Schaden

zu verhindern. Es gibt auch das offensichtliche Argument, dass diese Methode jene lang anhaltende Medienerzählung und dem Whistleblower damit eine nachhaltige Sichtbarkeit ermöglicht hat – bekanntlich eine Art Lebensversicherung.

Es gibt einen weiteren Blickwinkel. Daten gelten als das „Öl des 21. Jahrhunderts." In diesem Sinne könnte man davon sprechen, dass das Snowden-Material privatisiert worden ist von Leuten, die versuchen, die Daten im Sinne ihrer eigenen Interessen auszubeuten. Das klingt zunächst nach einer höhnischen Unterstellung. Etwa auf der Wellenlänge angesiedelt wie auch der Unmut, der sich gegenüber Greenwald entlädt, er werde von „Eitelkeit" und „Karrierismus" getrieben. Doch niemand stellt grundlegende Fragen über den Umgang mit dem historischen Daten-Leak. Etwa, ob es einen Weg gibt, den betreffenden Datenberg zu öffnen. Wenn man die aktuellen Umstände in Betracht zieht – der Whistleblower steckt aussichtslos in Moskau fest – ist ein solcher Vorschlag ziemlich weit hergeholt. Kaum jemand, der das Anliegen unterstützt, würde die Lebensversicherung Snowdens gefährden wollen.

Doch ich glaube, dass wir die Frage, ob der Datenberg geöffnet werden kann, stellen müssen. Nicht deshalb, weil die Akteure, die an dieser Sache im Dienste der Öffentlichkeit arbeiten, unseren Erwartungen nicht gerecht werden. Nein, in vielen von uns, die sich der so genannten Öffentlichkeit zugehörig fühlen, schlummert diese Frage, weil die Prozesse im Dienste der Öffentlichkeit (um den hehren Ansprüchen gerecht zu werden) so gestaltet werden müssen, dass sie ein Höchstmaß an Inklusivität und Durchlässigkeit ermöglichen. Doch genau das ist in diesem Fall nicht gegeben.

Adorno hat einmal gesagt (ich paraphrasiere), dass die „Wirkung eines Werks dort anfängt, wo die Intention des Autors endet." Analog zu Snowden ließe sich sagen: Die Wirkung des Snowden-Materials beginnt dort ihr volles Potenzial zu entfalten, wo die Intention des Whistleblowers endet (z. B. mit einer exklusiven Gruppe von Leuten zu arbeiten). Viele Forscher, Aktivisten und Technologie-Experten (nicht zu sprechen von den ganzen Journalisten, die nicht zu den „wenigen Glücklichen" gehören) haben ein großes Interesse daran, mit dem Snowden-Material zu arbeiten.

Es ist übrigens dasselbe Interesse wie auch schon in Zeiten der größten WikiLeaks-Projekte[1] vor einigen Jahren. Stellen wir uns nur einmal vor, welche historische Wirkung es hätte, etwa im Bereich der Wissenschaften, sozialen Bewegungen und IT-Branchen, wenn das Snowden-Material in die öffentliche Hand überführt werden könnte. Und hier als Grundlage für Studien und alle erdenklichen Lernprozesse zur Verfügung stehen würde. Es ist kaum auszumalen, so weitreichend wären die Auswirkungen.

Luke Harding und die Überforderung der Analysten

Bei der netzwerk recherche Jahrestagung in Hamburg (das große, internationale Treffen des Investigativ-Journalismus) habe ich Luke Harding, Autor des Buchs „The Snowden Files", mit dieser Angelegenheit bei der Q&A-Session seines Vortrags konfrontiert. Vor meiner Intervention hatte Harding bereits einige Hinweise auf die Beschränkungen der laufenden Untersuchung geliefert. Er spielte auf verschiedene Gründe an, warum die „wenigen Glücklichen" nicht in der Lage sind, der analytischen Herausforderung angemessen zu begegnen. „Wir sind keine Technik-Experten." Oder: „Nach zwei Stunden fallen einem die Augen aus." Dennoch schien Harding völlig unvorbereitet, vor seinem geistigen Auge die Option durchzuspielen, den Kreis der „wenigen Glücklichen" grundlegend zu erweitern.

Um seine Antwort zu paraphrasieren: Ja, es ist ein Dilemma, dass nur wenige Leute sich das Snowden-Material anschauen können und ihre eigenen Schlüsse daraus ziehen können. Jedoch ist diese Begrenzung ein natürliches Ergebnis ihrer prekären Natur (Dokumente, die Staatsgeheimnisse beinhalten) und darüber hinaus eine Folge des anhaltenden Drucks der Regierung. Dennoch, wer „ein besonderes Projekt" hat, sollte nicht zögern, Alan Rusbridger zu kontaktieren und ihn um Zugang zu den betreffenden Dokumenten zu bitten.

Eine Auskunftsanfrage an The Guardian? So eine Anfrage richtet sich üblicherweise an obskure Organisationen oder intransparente Firmen und wird von der Presse artikuliert unter Verweis auf das Informationsfreiheitsgesetz und andere legale Instrumente. Der Antrag wird für gewöhnlich zunächst abgelehnt. Doch wer dran bleibt und nicht davor zurückschreckt, vor Gericht zu ziehen, hat Aussicht auf Erfolg, wie die Geschichte des Investigativ-Journalismus zeigt.

Seymour Hersh und die Accountability der Presse

Die Auskunftsanfrage ist ein wichtiges Instrument für die freie Presse. Doch in diesem Kontext ist es die Presse selbst (beziehungsweise einige ihrer Vertreter), an die wir eine solche Anfrage richten müssen. Das wirkt absurd und wirft verschiedene Fragen auf, darunter: Wem gegenüber sind Organisationen wie The Guardian, Washington Post, New York Times, Der Spiegel und Akteure wie Glenn Greenwald eigentlich Rechenschaft schuldig? Welcher demokratischen Kontrolle sollten sie unterzogen werden?

Als ich den renommierten Investigativ-Journalisten Seymour Hersh mit dieser Angelegenheit konfrontierte, hatte ich den Sound eines Kämpfers im Ohr und engagierte Aussagen, darunter: „In Anbetracht der massiven Vergehen gegen die Verfassung – darf die Presse tatsächlich darum besorgt sein, das Gesetz zu brechen, wenn es um Entscheidungen geht, welche Materialbestände zur Veröffentlichung freizugeben und mit welchen Akteuren zu teilen sind?"

Hersh sagte nein, er schrie solche Dinge heraus bei seinem Vortrag auf der netzwerk recherche Tagung. Als ich ihn wegen dieser Angelegenheit ansprach, zunächst von Angesicht zu Angesicht nach dem Vortrag, dann via E-Mail, vertrat er einen nicht ganz so, sagen wir, „aggressiven" Standpunkt. Hersh über die Tatsache, dass das Snowden-Material von Leuten unter Verschluss gehalten wird, die die Idee der Presse- und Meinungsfreiheit repräsentieren:

> Ich sehe kaum Chancen, Greenwald oder jemanden von The New York Times, The Washington Post oder von Guardian dazu zu bewegen, ihre Materialbestände zu öffnen. Die betreffenden Akteure werden behaupten, dass ihr Vorgehen dem Interesse der Öffentlichkeit geschuldet ist. In der Zwischenzeit horten sie, was sie haben und teilen es mit niemandem. Zeitungen sind nicht allzu interessiert daran, den Reichtum zu verbreiten.

Das Paradoxon der Informationsanfrage

Dieser Pessimismus ist nachvollziehbar. Dennoch: Gibt es nicht Dinge, die wir unternehmen könnten? Auskunftsanfragen mögen aussichtslos erscheinen. Aber sie sind ein wichtiges Instrument. Die Erfahrung zeigt: Man kann den Kampf gewinnen. In Großbritannien kann man in Betracht ziehen, eine Beschwerde bei der Press Complaints Commission einzulegen - in Bezug auf die Tatsache, dass ein Medienhaus exklusive Kontrolle über das Snowden-Material ausübt. In Deutschland, wo dieses quasi-monopolistische Vorgehen gegen den Pressekodex verstößt, könnte man beim Deutschen Presserat eine Klage einreichen.

An dieser Stelle wird sehr deutlich: Die Auswertung des Snowden-Materials im Zeichen des öffentlichen Interesses offenbart eine beunruhigende Diskrepanz – sollten wir in der Presselandschaft nicht grenzübergreifend zusammenarbeiten, um die großen Probleme unserer Zeit zu lösen, statt uns gegenseitig zu verklagen? Hier bekommen wir 1) die Defizite des aktuellen Modells und 2) den Anreiz, ein neues Modell für die Zukunft zu ersinnen, direkt zu spüren. Vor diesem Hintergrund sollte man damit beginnen, ein Konzept für die Überführung des Snowden-Materials in die öffentliche Hand zu erarbeiten. Ein Modell, das sowohl die offensichtlichen Probleme der „Sicherheit" und des „Regierungsdrucks" als auch Fragen nach Snowdens „Lebensversicherung" in Betracht zieht.

All das sollte auf der internationalen Bühne behandelt werden. Ausgangspunkte sollten die USA, Großbritannien und Deutschland sein. Also Länder, in denen die Unterlagen derzeit bearbeitet werden. Vielleicht sollte alles in Deutschland anfangen, wo das zivilgesellschaftliche Interesse an den Snowden-Enthüllungen wahrscheinlich am größten in der Welt ist. Die zentralen Akteure hier, darunter Journalisten und Hacker, arbeiten sehr eifrig an diesem Fall. Im Zuge dessen akkumulieren sie aufgrund ihres exklusiven Zugangs „kulturelles Kapital" (Bour-

dieu), während sie weitgehend intransparente Entscheidungen treffen, was von dem Material zugänglich sein sollte und was nicht. Kurz, es gibt genügend Reibungspotenzial in dieser Stadt, um ein Modell des offenen Umgangs mit großen Daten-Leaks zu konzipieren.

Probleme mit „uneingeschränktem Zugang"

Auf den ersten Blick gibt es nicht allzu viele Gründe, warum wir diesbezüglich allzu optimistisch sein sollten. Schließlich sind wir „in jedem Fall der drei großen Daten-Leaks der vergangenen Jahre vor jeweils unterschiedliche Probleme gestellt worden, als wir das Material offen zugänglich gemacht haben. Insofern lässt sich ein globales Modell nicht ohne Weiteres konstruieren. Jeder neue Datensatz wird mit einem neuen Set von Problemen behaftet sein", wie Stefan Candea, eine zentrale Figur im Offshore Leaks-Projekt, zu verstehen gibt.

Andere, die seit vielen Jahren im Feld des Investigativ-Journalismus aktiv sind, sehen ebenfalls grundlegende Probleme, „uneingeschränkten Zugang" anzubieten. „Da können auch Zulieferer drinstehen, die gar nicht wissen, dass sie mit den Diensten zu tun hatten", so Ewan Tarkan[2], der (verdeckte) Recherchen zu Themen wie Überwachung betreibt. „Bei allen großen Leaks der Vergangenheit waren immer auch 'Unschuldige' erfasst. In Afghanistan etwa Namen von Übersetzern oder lokalen Ansprechpartnern. Bei geheimerkrieg.de (kein Daten-Leak, sondern eine Auswertung) standen in den Daten auch die Namen von Menschen, die ganz normale IT-Wartung gemacht oder andere Aufträge erledigt haben."

Sollten wir deshalb nicht weitergehen in diese Richtung? Nur, weil große Daten-Leaks schier unmöglich zu „regulieren" sind, sollten wir nicht erst anfangen, darüber nachzudenken?

Mit Blick auf seine lange Berufserfahrung meint Tarkan:

> Ich bin strikt dagegen, Leaks ohne zumindest selektiv geschwärzte Namen zu veröffentlichen. In der Vergangenheit sind immer wieder Menschen in Papieren aufgetaucht, die nur ausgelagerte Dienste erledigt haben. Deren Leben ist in höchstem Maße gefährdet bei einer ungeschwärzten Veröffentlichung. Gleichzeitig kann dies kein Argument dafür sein, nun alle Papiere zurückzuhalten. WikiLeaks hat es schließlich auch geschafft, Namen aus Dokumenten zu entfernen und diese dann zu veröffentlichen.

Denken wir also weiter, nehmen aber zunächst einmal noch einen weiteren wichtigen Hinweis zur Kenntnis: „Es ist die Entscheidung des Leakers, dem Journalisten zu sagen, was er mit dem Material machen soll", wie wiederum Candea herausstreicht. Offenbar wollte Snowden nicht, dass sein Material in der öffentlichen Hand landet. Leute wie Snowden sollten deshalb überzeugt werden – vielleicht

nicht unmöglich in Anbetracht der Tatsache, dass auch er nicht vollumfänglich zufrieden sein dürfte, was bislang mit seinem Material passiert ist (wie nicht wenige Beobachter mutmaßen). Da steht eine Menge Arbeit vor uns in Sachen Bewusstseinsbildung, sowohl im Hinblick auf Whistleblower als auch im Hinblick auf ein Modell für Plattformen, die offenen Zugang zu ihrem Material erlauben.

Das Zukunftsmodell in sechs Punkten

Zu *allererst* sollte jede verantwortungsbewusste Enthüllung mit „Informationen über das Material des gesamten Korpus angereichert sein, solang diese Art der Information nicht die Identität des Whistleblowers preisgibt", sagt der erfahrene IT-Journalist Detlef Borchers von heise.de. „Dies bringt mit sich, dass jeder interessierte Leser mit einer gewissen Souveränität nachvollziehen kann, ob die Veröffentlichung in einem Massenmedium durch eine (verdeckte) Agenda gesteuert wird."

Zweitens sollten bei einem öffentlich zugänglichen Leak alle Namen entfernt werden. Doch wer löscht die Namen? Wer gestaltet die Benutzeroberfläche auf eine Art und Weise, dass sie auch für ein nicht-technisches Publikum leicht zu bedienen ist? Hier würde eine Programmier- oder Kontrollinstanz ins Spiel kommen. Im Hinblick darauf müsste der „Verantwortung, die diese Instanz trägt, eine zentrale Bedeutung zukommen", denkt wiederum Borchers und erinnert daran, „dass immer wieder viele Fehler passieren, etwa, dass in der deutschen Ausgabe des Greenwald-Buches Namen von NSA-Leuten drinstehen, die im englischsprachigen Original geschwärzt sind."

Drittens müsste sichergestellt werden, dass die Dateien in einer Art und Weise zugänglich gemacht werden, die auch die Anonymität der User schützt. Man will brisante Dateien nicht auf dem persönlichen Computer haben, sondern in der Cloud, an einem öffentlich bekannten Ort, der einen gesicherten Zugang erlaubt. Doch wer soll die Dateien dann hosten? Ideal wäre eine öffentliche Institution, zum Beispiel eine Bibliothek.

Viertens wären die Bearbeitungsmöglichkeiten der geleakten Dokumente von zentraler Bedeutung für unser Modell: Sind die fraglichen Dateien maschinenlesbar? Oder müssen sie erst noch in diesen Zustand gebracht werden? Es gibt verschiedene Werkzeuge, die dieses Problem lösen könnten, beispielsweise DocumentCloud.

Fünftens müsste der User die Sprache verstehen, in der die Dokumente verfasst sind. Hier gibt es verschiedene Möglichkeiten: Jemanden zu Rate ziehen, der sie spricht, sie selbst lernen oder sich einer Maschine bedienen, die es kann.

Die vom Datenjournalismus bereitgestellten Werkzeuge (man findet sie online oder bekommt sie bei einer der vielen Datenjournalismus-Veranstaltungen vorgestellt) unterstützen einen dabei, die Systematisierung, die Analyse und die öffent-

lichkeitsfähige Interpretation vorzunehmen. Jede Veröffentlichung, die auf solch einer Auswertung basiert, sollte natürlich die benutzten Quellen offen legen.

Und schließlich, *sechstens*, müsste unser Modell die Sicherheit des Whistleblowers bedenken, sofern er sich entschieden hat, an die Öffentlichkeit zu treten wie im Falle Snowdens. Hier müsste sichergestellt werden, dass er seine Lebensversicherung und somit sein Leben nicht verliert. „Ed", wie Unterstützer ihn nennen, hat seine Strategie schon mehrfach gewechselt. Anfangs, Sommer 2013, wollte er sich an der von ihm angestoßenen Debatte nicht beteiligen, sondern die Dokumente für sich selbst sprechen lassen. Wenige Monate später, Ende 2013, hat er seine Haltung geändert und begann eine Reihe von öffentlichen Auftritten. Der nächste große Schritt wäre es, den Zugang zu den Dateien zu öffnen. Zumindest zu 50 Prozent. Hierbei sei an Assange erinnert: In seinem Falle blieben einige Dateien (vielleicht große Leaks zu den US-Banken) unveröffentlicht. So konnte er seine publizistische Aktivität aufrechterhalten. Dieser Ansatz könnte auch für Snowden funktionieren.

Grundpfeiler unserer Demokratie

Ist das alles, was bei diesem hier vorgeschlagenem Modell berücksichtigt werden müsste? Vermutlich nicht. Jedes Feature, ob es nun bereits vorgeschlagen wurde oder nicht, müsste von der Öffentlichkeit genaustens überprüft werden. Um die Debatte in Gang zu bringen, könnten wir zunächst fragen: Warum gibt es eigentlich nur einen öffentlich zugänglichen Zähler der Snowden-Files? Dieser wird, unter dem Projektnamen „Tally Update", von John Young auf cryptome.org betrieben. Warum bieten diesen Service nicht die „wenigen Glücklichen" an, die im Besitz der Dokumente sind? Oder warum helfen sie nicht zumindest, die Exaktheit des Zahlenstands zu überprüfen?

Warum werden die Snowden-Dokumente so restriktiv behandelt? Ist das der einzig mögliche Weg? Was ist in diesem Kontext von öffentlichem Interesse? Wollen wir lückenlose Aufklärung qua offenem Zugang zu den Dokumenten? Oder die Zurückhaltung von Informationen, um den Whistleblower zu schützen? Müssen wir uns zwischen diesen beiden Optionen entscheiden? Oder gibt es einen Weg, um beide Anliegen miteinander zu versöhnen? Diese Fragen ziehen Fragen nach sich, die allesamt an den Grundpfeilern unserer Demokratie rütteln. Die Zeit für diese Auseinandersetzung ist mehr als reif.

Dieser Beitrag erschien zuerst am 9. Juli 2014 bei der Berliner Gazette.

Anmerkungen

[1] http://berlinergazette.de/wikileaks-nachhaltigkeit-cablegate

[2] Der Name Ewan Tarkans wurde von der Redaktion geändert.

Kristian Woznicki gründete 1999 die Online-Zeitung Berliner Gazette. Das Verhältnis von Kultur und Internet beschäftigte ihn auch in früheren Projekten: Er war Teil eines interdisziplinären Forschungsprojekts zur digitalen Kartierung von Diskursen im sozialen Netzwerk und Ko-Direktor eines digitalen Archivs der Globalisierung.

24 Freie Software in München: Fakten sind stärker als Fiktion

von **Matthias Kirschner**

Die Stadt München ist ein Leuchtturmprojekt für den Einsatz Freier Software in der öffentlichen Verwaltung. Die Stadt betreibt mittlerweile auf mehr als 15.000 Arbeitsplatzrechnern Freie Software und hat dabei bereits über 11.000.000 Euro gespart. Während der Migration auf Freie Software haben sie ihre heterogene IT an 51 Standorten mit 1.000 IT-Angestellten und 22 IT-Abteilungen konsolidiert. Trotz dieser Herausforderungen und widrigen Vorraussetzungen seitens der Bundes- und Landespolitik sind die meisten Benutzer[1] mit der Migration zufrieden und wollen nicht zurückwechseln. Und all das geschieht im Vorgarten der deutschen Microsoft-Hauptzentrale.

Aber was könnte man tun, wenn man etwas gegen den Erfolg Freier Software in München hat? Man könnte mit Emotionen spielen und Gerüchte darüber streuen, dass die Münchner IT-Leute weder den Interessen der normalen Benutzer noch denen der Leitungsebene Beachtung schenken. Natürlich müsste man dabei sehr vage bleiben und darauf hoffen, auch ein paar der Stimmen hervorzulocken, die sowieso immer unzufrieden sind. Damit hätte man einen einfachen Weg, um den schon geschaffenen Prozess zu diskreditieren.

Das ist in den letzten Monaten in München durch die Bemerkungen des neuen Oberbürgermeisters Dieter Reiter (SPD) und seines zweiten Bürgermeisters Josef Schmid (CSU) geschehen. Wobei einige Kommentatoren über eine Verbindung zwischen dem Umzug von Microsofts Hauptzentrale von Unterschleißheim nach München und der Aussage Reiters, bei diesem Deal geholfen zu haben[2], spekulierten. Da Microsoft der größte Steuerzahler in Unterschleißheim war[3], wird München finanziell stark von dem Umzug profitieren.

Antwort auf Anfrage kann bisherige Kritik nicht belegen

Sicher ist, Reiter und Schmid konnten ihre Kritik an Freier Software bisher nicht mit Fakten belegen. Mitte Oktober antwortete Reiter mit fast dreiwöchiger Verspätung auf eine Anfrage von Bündnis 90/Die Grünen[4], in der um Klarstellungen bezüglich GNU/Linux in der Stadt München gebeten wurde. Dabei musste Reiter bei allen vorherigen Äußerungen zurückrudern.

So bezog sich die Mitarbeiterumfrage „Great Place to Work“ von Ende 2013 – auf die sich Reiter und Schmid in ihrer Kritik berufen hatten – laut Reiters neuen Aussagen auf diverse Facetten der IT-Struktur, wie z. B. Hardware, Support, oder Telearbeit. Die Umfrage lässt aber ungeklärt, ob und wie die Probleme der Nutzer überhaupt etwas mit Freier Software zu tun haben: Dies sei „zum aktuellen Zeitpunkt nicht erhoben“, so musste Reiter nun eingestehen. In einem Interview mit der Stadtbild[5] – einer Zeitschrift für Münchner Behörden und Institutionen – hatte er im Juli auf die Frage „Sie gelten als Fan von Microsoft. Wird München von Linux auf Microsoft umsteigen?“ geantwortet:

> Ich gebe zu, die Entscheidung der Stadt, Linux einzuführen, hat mich überrascht. Wir sind auf den Open-Source-Zug aufgesprungen, doch Open-Source-Anwendungen hinken *gelegentlich* den Microsoft-Anwendungen hinterher. Ich kann ein Lied davon singen… Auch bei den Mitarbeiterinnen und Mitarbeitern ist das ein großes Thema. Das haben die Kommentare im „Great Place to Work“-Forum gezeigt. […]

Die Computerwoche hat zu der behaupteten Mitarbeiterunzufriedenheit eigene Recherchen betrieben und Mitarbeiter befragt[6]. Die Ergebnisse widersprechen Reiters und Schmids Behauptungen.

Weiterhin musste Reiter zugeben, dass die von den Medien oft zitierte Wartezeit auf die dienstlichen Mobiltelefone „in keinem Zusammenhang“ mit dem „Betriebssystem LiMux“ steht. Stattdessen sei der Hauptgrund für die Wartezeiten, dass „bislang keine Smartphones mit iOS-Betriebssystem in der Verwaltung eingesetzt wurden“. Schmid hatte dazu im Juli noch in der Münchner Abendzeitung gesagt[7]:

> Es ist ärgerlich. […] Da werden Vorurteile, die man als Normalbürger gegenüber der Verwaltung hat, bestätigt. Da ist das ganze Thema LiMux, den Anwender-Programmen fehlen zahlreiche Funktionen, die sonst gängig sind und vieles ist nicht kompatibel mit den Systemen außerhalb der Verwaltung. Ich habe vier Wochen auf mein Smartphone gewartet und, als ich es endlich hatte, Glückwünsche vom Oberbürgermeister bekommen – denn bei ihm hat es noch länger gedauert.

Bezüglich der laut Schmid fehlenden einheitlichen Software zur E-Mail- und Kalender-Verwaltung stellte sich in der Antwort auf die Grünen-Anfrage außerdem heraus, dass die Einführung der Freien-Software-Lösung „Kolab“ überhaupt erst Anfang 2014 in Auftrag gegeben wurde und deshalb frühestens 2015 in den produktiven Betrieb gehen soll.

Breite Unterstützung für Freie Software in München

Im Antwortschreiben zeigte sich außerdem, dass die politische Unterstützung für GNU/Linux in München weiterhin stark ist. Sowohl die städtische IT-Verwaltung als auch die dritte Bürgermeisterin Christine Strobl stehen hinter der Münchner Freien-Software-Strategie. Damit distanzieren sie sich von den vorherigen Äußerungen Reiters und Schmids. So ist Bürgermeisterin Strobl „nach gründlicher Prüfung" weiterhin der Ansicht, dass die Umstellung auf Freie Software richtig war. Auch der Stadtrat hält unverändert zu Freier Software und verteidigte seine Haltung nochmals im Juli[8]. IT-Experten aus den eigenen politischen Reihen haben ihre Stimme erhoben, um Reiter und Schmid zu korrigieren und als Einzelmeinungen zu deklarieren.

Auch die wirtschaftlichen Aspekte sprechen für Freie Software. Reiter selbst beziffert die durch wegfallende Lizenzkosten entstandenen Einsparungen auf 11.000.000 Euro. Allein die Hardware-Kosten bei einer Migration zu Windows 7 würden sich auf ca. 3.150.000 Euro belaufen, und bei „einem Umstieg auf Windows 8 wären die Kosten noch wesentlich höher". Dazu würden noch weitere Kosten anfallen, die derzeit nicht bezifferbar seien. Neben dem Kostenargument werden im Antwortschreiben die Erfolge bei der Unterstützung Offener Standards durch die Umstellung erwähnt. Dies ermöglicht der Stadt die Hoheit über die eigenen Daten und stellt den diskriminierungsfreien Zugang zu städtischen IT-Diensten sicher.

Zusammenfassend scheint es, dass Reiter und Schmid den bisherigen Erfolg Freier Software in München unterschätzt haben und vorschnell unhaltbare Kritik in die Öffentlichkeit getragen wurde.

Unsere Erfolge feiern

Doch die wichtige Frage ist: Wie machen wir weiter?

Zuallererst einmal sollten wir unseren Erfolg feiern. Dafür nehmen wir uns oft nicht die Zeit, da schon wieder neue Probleme anstehen und der nächste Angriff subtiler und besser vorbereitet sein wird. Allerdings sind Erfolge – und seien sie noch so klein – für eine Bewegung wichtig. Wenn Freie Software bei widrigen Ausgangsvorrausetzungen auf EU-, Bundes- und Landesebene sogar eine solche Schmutzkampagne der Bürgermeister übersteht, dann zeigt das, wie viel gute Arbeit bereits gemacht wurde.

Richtlinie für Offene Standards

Daneben beinhaltet die Antwort auf die Anfrage der Grünen einen anderen entscheidenden Punkt: Das Problem der Dokumentenformate. Der Münchner IT-Verantwortliche stellte fest, dass die deutschen Bundesländer und die Bundesregierung zu Beginn der Migration die Wichtigkeit von Freier Software und Offenen Standards betont, aber danach nie konsequent diesen eingeschlagenen Pfad weiterverfolgt haben.

In Deutschland blockiert das Fehlen eines klaren Grundsatzes über Offene Standards die öffentlichen Verwaltungen, wenn sie auf Freie Software umsteigen wollen. In den letzten Jahren haben andere europäische Länder wie Großbritannien, Frankreich, Italien und Schweden mehr dafür getan, Freie Software und Offene Standards zu fördern.

Auf europäischer Ebene hat der frühere Münchner Oberbürgermeister Ude die Europäische Kommission darum gebeten[9], zwei Maßnahmen zur Teilhabe mit Freier Software an EU-Projekten umzusetzen: Erstens sollten alle Dokumentvorlagen, die in Microsoft Office-Formaten vorhanden sind, auch im „Open Document"-Text-Format (ODT) verfügbar sein. Zweitens sollten alle Präsentationsnotebooks in den EU-Institutionen auch ein Programm zum Anzeigen von „Open Document"-Präsentationen (ODP) installiert haben. Diese Forderungen sind aus dem Jahr 2011 und die europäischen Gremien haben seither keine bedeutsamen Richtlinien für Offene Standards umgesetzt.

Bei Dokumentenstandards müssen wir also weiter dafür arbeiten, dass die Europäische Union, Bund und Länder öffentlichen Einrichtungen keine Hürden für den Einsatz Freier Software in den Weg stellen.

Öffentlich finanzierte Software als Freie Software veröffentlichen

Nachhaltig können wir den Einsatz Freier Software in der öffentlichen Verwaltung nur unterstützen, wenn wir erreichen, dass öffentlich finanzierte Software unter einer Freien-Software-Lizenz veröffentlicht werden muss. Bürger und Unternehmen haben für die Software mit ihren Steuern bezahlt, also sollten sie – sowie andere Behörden – diese Software für jeden Zweck verwenden, verstehen, verbreiten und verbessern dürfen.

Anmerkungen

[1] http://www.computerwoche.de/a/wohin-steuert-linux-in-muenchen,3043464,2

[2] http://www.zeit.de/politik/deutschland/2013-11/reiter-muenchen-spd/komplettansicht

[3] http://www.merkur-online.de/lokales/muenchen-lk-nord/unterschleissheim-umzug-nach-muenchen-microsoft-prueft-neue-standorte-2766978.html

[4] http://www.ris-muenchen.de/RII2/RII/DOK/ANTRAG/3456728.pdf

[5] http://www.linux-magazin.de/NEWS/Microsoft-Fan-Muenchens-neuer-OB-Reiter-will-in-Sachen-Limux-neue-Loesung-finden

[6] http://www.computerwoche.de/a/wohin-steuert-linux-in-muenchen,3043464,2

[7] http://www.abendzeitung-muenchen.de/inhalt.az-interview-josef-schmid-alles-ist-jetzt-viel-schwieriger.b29923b0-0c35-4866-bad7-cca8d9054f0b.html

[8] http://www.heise.de/newsticker/meldung/Linux-in-Muenchen-Stadtrat-verteidigt-LiMux-gegen-Buergermeister-2262506.html

[9] https://blogs.fsfe.org/mk/prasident-des-deutschen-stadtetags-an-europaische-kommission-mehr-fur-freie-software-einsetzen/

Matthias Kirschner ist Vize-Präsident der Free Software Foundation Europe. Er ist verantwortlich für die Öffentlichkeitsarbeit, koordiniert die politische Arbeit der FSFE in Deutschland und führt das Berliner Büro der FSFE. Er hilft Journalisten, Politikern, der Öffentlichen Verwaltung, Unternehmen und der Öffentlichkeit zu verstehen, warum Freie Software wichtig für Wirtschaft und Gesellschaft ist.

25 Die Entwicklung des Medienmarktes – zwischen Insolvenzen, Oligopolisierung und Aufbruch

von **Christian Humborg** und **Benedict Wermter**

Deutschland ist der größte Zeitungsmarkt Europas und der fünftgrößte der Welt[1]. Die Auflagen gehen allerdings zurück. 1992 wurden noch 26 Millionen Tageszeitungen verkauft, 2011 nur noch 18,8 Millionen – ein Minus von 19 Prozent. Es geht weiter abwärts: Forscher gehen von 11 Millionen verkauften Exemplaren pro Tag im Jahre 2022 aus, bis die letzte verkaufte Zeitung 2034 über den Tisch geht[2]. Allein im Jahre 2014 ging die verkaufte Auflage um 4,16 Prozent zurück[3]. Die Auflagenzahlen aller Regionalzeitungen ergeben ein negatives Bild; überregional zeigt sich mit wenigen Ausnahmen das selbe Minus.

Mit den Auflagen gehen auch die Einnahmen zurück: Im Jahre 2012 haben die Verlage in Deutschland mit Anzeigen und Beilagen und mit dem Vertrieb von Zeitungen einen Umsatz von 8,23 Milliarden Euro gemacht. Das bedeutet einen Verlust von 3,3 Prozent zu 2011. Gerade das Anzeigengeschäft bricht ein: Das vierte Jahr in Folge waren in Deutschland die Einnahmen aus Anzeigen und Werbung geringer als die Einnahmen aus dem Vertrieb der Zeitungen[4]. Ein Trend von weltweiter Gültigkeit: Von 2007 bis 2011 sanken die Einnahmen aus dem Anzeigengeschäft der Verlage weltweit um 41 Prozent. Der US-Markt verzeichnet dabei die größten Einbußen[5].

Superreiche und transnationale Medienkonzerne

Die 50 größten globalen Medienkonzerne haben ihren Umsatz in den vergangenen zwanzig Jahren von 155 auf 473 Milliarden Euro verdreifacht. Dabei klafft die Schere zwischen Mega-Konzernen und dem kleinen Rest zunehmend auseinander. 60 Prozent des Gesamtumsatzes gehen an die Top Ten der Medienwelt, 20 Prozent alleine an die Marktführer Google und Comcast[6]. In den USA deuten sich große Übernahmen an, die kennzeichnend für den Trend der Oligopolisierung in der Branche sind: Comcast will den Konkurrenten Time Warner Cable schlucken, AT&T möchte den Satelliten-Pay-TV-Anbieter DirecTV kaufen[7].

Mit im Spiel sind Medienmogule und Superreiche wie Warren Buffet, dessen Holding Berkshire Hathaway eine global operierende Media Group unterhält, die beispielsweise im Vereinigten Königreich Marktführer unter den Zeitungsverlegern ist. Ebenso einflussreich ist Rupert Murdoch mit seiner News Corporation – einem Mediengiganten, der 21st Century Fox, die britische Sun und Times besitzt.

Der derzeit reichste Mann der Welt, der Mexikaner Carlos Slim, stieg im Jahre 2008 bei der New York Times ein. In den Händen von Amazon-Gründer Jeff Bezos ist seit 2013 eine der einflussreichsten US-Zeitungen: die Washington Post. Für 250 Millionen Dollar hat sich Bezos jene Zeitung gesichert, die den Watergate-Skandal aufdeckte oder über das Geheimdienstprogramm Prism berichtete.

Wie Medientycoons im Westen haben in Osteuropa Oligarchen das Medienzepter in der Hand. In jüngster Vergangenheit sind Übernahmebestreben von Finanzoligarchen auf Zeitungen aus Tschechien und der Slowakei bekannt geworden. Die slowakische Investment-Gruppe Penta hat sich in die Tageszeitung SME, ein Leitmedium des Landes, eingekauft. Daraufhin ist die gesamte redaktionelle Leitung zurückgetreten, da sie den Einstieg als Bedrohung ihrer Unabhängigkeit wertet. SME hatte zuvor innerhalb eines Korruptionsskandals die Privatisierung staatlicher Unternehmen durch Penta enthüllt[8]. Im Juni 2013 sicherte sich der zweitreichste tschechische Unternehmer und gleichzeitig Finanzminister und Regierungsvize Andrej Babis den Verlag Mafra. Die mächtigste Mediengruppe betreibt die größten Zeitungen, Radio- und Fernsehsender des Landes. Zuvor hatte die Axel Springer Ringier (eine deutsch-schweizerische Kooperation des Springer-Verlags) ihre tschechischen Blätter an einen Energieriesen des Landes verkauft[9].

Oft folgen Übernahmen massive Sparpläne. So werden kleine Regionalzeitungen in den USA von den Medienriesen geschluckt. Die Roanoke Times wurde 2013 von der Berkshire Hathaway Media Group übernommen. „Your paper will operate from a position of financial strength", kündigte Warren Buffet an – und entließ 31 Mitarbeiter[10]. In den letzten fünf Jahren wurden 14 Tageszeitungen eingestellt – darunter traditionsreiche Blätter wie die Oakland Tribune. Im Oktober 2014 strich die New York Times wegen sinkender Anzeigenerlöse 100 Stellen[11]. *Downsizing* scheint ein Trend von globaler Gültigkeit zu sein: In Frankreich geben viele Blätter auf oder erscheinen ausschließlich im Netz – wie die Wirtschaftszeitung La Tribune. Die spanische El Pais hat ein Drittel ihres Teams verloren.

Deutsche Medienhäuser unter Anpassungsdruck

Auch in Deutschland zeigen sich grundlegende Veränderungen in der Marktpositionierung der führenden Medienhäuser mit journalistischem Schwerpunkt, die unter den Stichworten „Zentralisierung" und „digitale Neuausrichtung" zusammengefasst werden können. Das Hamburger Verlagshaus Gruner + Jahr mit seinen bekannten Zeitschriften Stern, Geo, Capital, Neon und Brigitte gehört seit Herbst 2014 zu 100 Prozent zum deutschen Marktführer Bertelsmann. Das drittgrößte Medienhaus in Deutschland, die Axel Springer SE, sah offenbar in der Sparte Regionalzeitung keine Zukunft mehr und verkaufte einen bedeutenden Teil seiner Print-Sparte an die Funke-Mediengruppe. Zu den verkauften Zeitungen gehören das Hamburger Abendblatt oder die Berliner Morgenpost sowie Zeitschriften wie Hörzu und BILD der Frau[12].

Meist bleiben die Übernahmen nicht ohne Konsequenzen: Nach der Übernahme von Gruner + Jahr durch Bertelsmann kündigte der Medienriese an, 400 Mitarbeiter und Journalisten zu entlassen. Zu den ersten, die gehen müssen, gehören alle elf Textredakteure von Brigitte und 14 Redakteure von GEO. Der Betrieb der Financial Times Deutschland wurde 2012 komplett eingestellt[13]. Die Funke Mediengruppe wurde in den letzten Jahren durch Massenentlassungen verschlankt: Die Redaktion der Westfälische Rundschau wurde gänzlich geschlossen[14], zudem werden zahlreiche Lokalredaktionen eingestampft, zuletzt in Dorsten, Lüdenscheid und Castrop-Rauxel[15].

So manches überregionales Traditionsblatt sieht sich in Gefahr: Die Frankfurter Allgemeine Zeitung bestätigt große Verluste. 200 von 900 Arbeitsplätzen sollen wegfallen, ein Fünftel davon Redakteure[16]. Die Frankfurter Rundschau galt als erstes prominentes Opfer der überregionalen Medienkrise, als im November 2012 Antrag auf Insolvenz gestellt wurde[17]. In den Regionen müssen viele Blätter aufgeben – wie die insolvente Münchener Abendzeitung im Frühjahr 2014 – oder sie existieren als „Zombie-Zeitungen" mit fremden Mänteln und Lokalteilen weiter – so wie die Münstersche Zeitung seit November 2014[18].

Die Verunsicherung der Leser und Nutzer bezüglich der Objektivität von Informationsinhalten wird im globalen Korruptionsbarometer von Transparency International für 2013 abgebildet. Demnach glaubt die Mehrheit der Menschen in Deutschland, dass Verlage und Rundfunkanstalten von Korruption beeinflusst werden. Die Medien schneiden schlechter ab als öffentliche Verwaltung und Parlamente[19]. Einer Umfrage des Statistik-Portals statista zufolge belegen Journalisten beim Vertrauen in verschiedene Berufsgruppen den viertletzten Platz. Mit nur 37 Prozent Zustimmung rangieren sie hinter Beamten, Unternehmern oder Schauspielern[20].

Krise heißt Innovation

Dem multimedialen Zugang zu Informationen sind kaum mehr technische Grenzen gesetzt. Eine Studie der Newspaper Association of America legt den Wandel des Medienkonsums amerikanischer Rezipienten offen: Mehr als 137 Millionen Erwachsene lesen wöchentlich ein Printprodukt. Im Gegensatz dazu haben Online-Inhalte alleine im Januar 2014 mehr als 145 Millionen Bürger erreicht. Die Einnahmen aus Online-Angeboten sind in 2012 um 275 Prozent gestiegen; 43 Millionen erwachsene Amerikaner haben sich 2013 im Schnitt mindestens einmal im Monat über Smartphones und Tablets informiert[21]. Die Forschung zum Journalismus in der digitalen Moderne konstatiert der Branche einen zunehmenden Anpassungsdruck. Einerseits ergibt der Sparzwang und die stetige Verwandlung des Journalismus in einen Niedriglohnsektor ein Professionsparadox[22]: Viele Medienhäuser und Journalisten sahen sich gezwungen, im PR-Bereich tätig zu werden und die Nähe zu Unternehmen zu suchen. Die Medien richteten sich dia-

logorientiert aus und suchten die Interaktion mit den „Prosumenten" – den Konsumenten, die selbst Inhalte produzieren. Durch die Explosion von User generated Content wurde Journalismus vom *Gatekeeper* zum *Gatewatcher* – der Ein- und Ausgang von Informationen wird immer weniger gesteuert, sondern mehr beobachtet und moderiert[23].

Die etablierten Medienhäuser reagierten mit unterschiedlicher Intensität und Geschwindigkeit: Die New York Times legte im Frühjahr 2014 einen Innovation Report vor, dessen Task Force grundlegende digitale Transformationen für das wirtschaftlich strauchelnde US-Leitmedium ausgearbeitet hat: „digital-first" lautet die Devise – alle Inhalte sollen zuerst digital ablaufen, außerdem steht Interaktion mit dem Leser in sozialen Medien ganz oben auf der Agenda[24]. Andere Zeitungen wie The Philadelphia Inquirer starten exklusive Kooperationen mit Tabletherstellern. Indikator dieses Wandels sind Medien, die nie ein Presswerk von innen gesehen haben.

Die Huffington Post ist ein bekanntes Beispiel, jüngere Gründungen sind Portale wie Vox oder Quartz. Die Grenzen zwischen einer professionellen vierten Gewalt und dem sich informierenden Bürger sind verschwommen. Das schafft Platz für Neues: Das Gebot der digitalen Moderne ist der onlinebasierte, interaktiv produzierte, journalistische Inhalt auf transparenter Basis – ein demokratischer Zugewinn. Das multimediale Storytelling gilt als Zukunftstrend. *Crowdsourcing* und *Crowdfunding* gewinnen an Bedeutung.

Doch wie können im beschleunigten Zeitalter bei medialer Konzentration tiefgründige Recherchen, die objektive und umfassende Hintergrundinformationen liefern, durchgeführt und aufwendige Geschichten von großer Bedeutung erzählt werden?

In den USA ist spendenbasierter Investigativjournalismus schon seit Jahrzehnten erfolgreich. Eines der bekanntesten Beispiele ist der 2007 gegründete Non-Profit Newsroom ProPublica, der mit mehr als 30 Reportern zentrale Themenfelder wie Überwachung oder die Waffenlobby bearbeitet. Bei manchen Recherchen beziehen die Reporter mehrere Tausend Freiwillige in die Recherche mit ein.

Andere Beispiele dieser spendenbasierten Redaktionen sind das Center for Investigative Reporting oder das Center for Public Integrity, die schon vor gut 25 Jahren gegründet wurden. Mittlerweile gibt es in den USA rund 100 solcher Büros, von der kleinen lokalen Redaktion bis hin zum zweifachen Pulitzerpreis-Gewinner ProPublica.

In Deutschland gibt es seit Juli 2014 CORRECT!V, das erste gemeinnützige Recherchebüro im deutschsprachigen Raum. CORRECT!V setzt auf datengetriebenen Investigativjournalismus. Aussagekräftige und sensible Daten- und Dokumentenschätze werden beschafft, aufbereitet, und die Geschichte dahinter erzählt.

CORRECT!V hat einen Bildungsauftrag: Bürger werden mit journalistischen Werkzeugen ausgestattet, die sie unterstützen, selbst unabhängigen und transparenten Journalismus zu betreiben. Dabei wirkt CORRECT!V als Multiplikator: Je mehr Nutzer in der Community journalistischen Austausch betreiben, desto stärker können die Recherchen werden. So schafft CORRECT!V Vertrauen und will in Zukunft auch mithilfe der Bürger große Rechercheprojekte stemmen. Unabhängig von großen Konzernen und Medienhäusern entstehen so Projekte, die Missstände aufdecken, die aufgrund des Spardrucks der Verlage sonst nicht oder nicht in dieser Tiefe angegriffen werden könnten. Investigativer Journalismus als demokratisches Schwert ist in Zeiten von Lobbyismus und Machtmissbrauch in Wirtschaft, Politik und Medien immer wichtiger.

Und CORRECT!V ist gemeinnützig: Die Ergebnisse finden zunächst durch exklusive Kooperationspartner in den Flächenmedien statt. Um die Reichweite zu erhöhen, werden aber alle digital veröffentlicht und sind über „steal-our-story" für jeden frei verfügbar – denn sie sind Allgemeingut.

Doch es gibt viele neue journalistische Ansätze. NDR, WDR und Süddeutsche Zeitung haben einen großen Rechercheverbund gegründet. Das Forum VOCER für Debatten und Kritik, die sich auf den Medienumbruch beziehen, möchte die digitalen Herausforderungen analysieren und innerhalb von Themenschwerpunkten einen langfristigen Kontrast zur schnellen Medienwelt setzen. Die Krautreporter sind ein Crowdfunding-Projekt im Journalismus, das im vergangenen Jahr für Aufsehen gesorgt hat. netzpolitik.org hat sich als führendes Medium in Fragen der Netzpolitik durchgesetzt. Die Plattform BuzzFeed ist mittlerweile von einem Labor von Technikbegeisterten MIT-Absolventen zu einem bedeutenden Nachrichten-Portal geworden. Die BuzzFeed-Webseite hat mehr Besucher als jedes andere Medium der Welt.

Das Online-Magazin VICE spricht *reader interests* wie *sex*, *drugs* und *crime* an und fällt dabei durch ungeschönte und direkte Erzählformate in gesellschaftlichen Grenzbereichen auf. Weitere Beispiele wie CARTA zeigen, dass Neues entstanden ist und dass experimentiert wird. Aber auch die Alteingesessenen experimentieren, wie taz und Zeit Online. Was sich durchsetzen wird, wird die Zukunft zeigen. Aber eines ist sicher: Die neuen Akteure werden nicht verschwinden, sondern viele von ihnen werden sich durchsetzen, vermutlich auf Kosten der Alteingesessenen.

Anmerkungen

[1] Anja Pasquay: *Die deutschen Zeitungen in Zahlen und Daten 2014*. Bundesverband Deutscher Zeitungsverleger e.V. (Hrsg.)

[2] Klaus Meier: *Statistisch berechnet: Im Jahr 2034 erscheint die letzte gedruckte Tageszeitung* in *Journalistik – Das Blog zum Buch*. https://journalistiklehrbuch.wordpress.com/2012/03/06/statistisch-berechnet-im-jahr-2034-erscheint-die-letzte-gedruckte-tageszeitung/

[3] (IFM) Institut für Medien- und Kommunikationspolitik (2014): *Deutsche Medienkonzerne 2014*. http://www.mediadb.eu/rankings/deutsche-medienkonzerne-2014.html

[4] Pasquay, Anja: *Die deutschen Zeitungen in Zahlen und Daten 2014*. Bundesverband Deutscher Zeitungsverleger e.V.

[5] Henning Kornfeld: *Wan-Ifra veröffentlicht World Press Trends. Leser hui, Einnahmen pfui* Kress.de, 3. September 2012

[6] Till Wäscher: *Die größten Medienkonzerne der Welt 2014: Das Jahr der Mega-Fusionen*. http://www.carta.info/72937/die-groessten-medienkonzerne-der-welt-2014-das-jahr-der-mega-fusionen/

[7] ebenda

[8] Alexander Mostyn: Mit Geld gezähmt. In: http://www.taz.de/1/archiv/digitaz/artikel/?ressort=fl&dig=2014%2F11%2F11%2Fa0098&cHash=8db585507f5b76de3ded53ee7dcfbf46

[9] ebenda

[10] Clay Shirky: *Last Call. The end of the printed newspaper*. https://medium.com/@cshirky/last-call-c682f6471c70

[11] Frankfurter Allgemeine Zeitung: *New York Times streicht hundert Redaktionsstellen*. http://www.faz.net/aktuell/feuilleton/medien/medienkrise-new-york-times-streicht-hundert-redaktionsstellen-13186156.html

[12] (IFM) Institut für Medien- und Kommunikationspolitik: *Deutsche Medienkonzerne 2014*. http://www.mediadb.eu/rankings/deutsche-medienkonzerne-2014.html

[13] ebenda

[14] ebenda

[15] David Hein: *Funke gibt Redaktionen in Castrop-Rauxel und Dorsten auf*. http://mobil.horizont.net/medien/nachrichten/Zeitungen-Funke-gibt-Redaktionen-in-Castrop-Rauxel-und-Dorsten-auf-117260

[16] Spiegel Online: *Zeitungskrise: FAZ streicht bis zu 200 Stellen*. http://www.spiegel.de/wirtschaft/unternehmen/frankfurter-allgemeine-zeitung-faz-streicht-bis-zu-200-stellen-a-991803.html

[17] Christoph Sydow: *Insolvenz der Frankfurter Rundschau: Das Blatt hat sich gewendet*. http://www.spiegel.de/kultur/gesellschaft/die-insolvenz-der-frankfurter-rundschau-ist-keine-ueberraschung-a-867084.html

[18] *Zeitungssterben*. https://zeitungssterben.wordpress.com/page/2/

[19] Transparency International: *Globales Korruptionsbarometer 2013: Medien werden erstmals als korrupter wahrgenommen als Öffentliche Verwaltung und Parlament*. http://www.transparency.de/2013-07-09-GCB-2013.2322.0.html

[20] Statista: *Vertrauen Sie den folgenden Berufsgruppen?*. http://de.statista.com/statistik/daten/studie/1470/umfrage/vertrauen-in-verschiedene-berufsgruppen

[21] (NAA) Newspaper Association of America: *The Evolution of Newspaper Innovation (Infographik)*. http://www.naa.org/innovation

[22] Leif Kramp: *Profession am Scheideweg* in Leif Krampf et al. (Hrsg.): *Journalismus in der Moderne*

[23] Bernd Oswald: *Vom Produkt zum Prozess* in Leif Krampf et al. (Hrsg.): *Journalismus in der Moderne*

[24] Myles Tanzer: *Exclusive: New York Times Internal Report Painted Dire Digital Picture*. http://www.buzzfeed.com/mylestanzer/exclusive-times-internal-report-painted-dire-digital-picture

Christian Humborg ist Geschäftsführer des gemeinnützigen Recherchebüros CORRECT!V, vorher war er bei Transparency International Deutschland tätig. Er ist promovierter Betriebswirt und kennt sich besonders mit dem Aufbau von NGOs aus.

Benedict Wermter ist Volontär beim gemeinnützigen Recherchebüro CORRECT!V.

26 Öffentlich-Rechtlich und offen lizenziert: Creative Commons in ARD & Co

von **Leonhard Dobusch**

Mit der Bedeutung wachsen häufig Begeisterung und Bedenken gleichermaßen. Das gilt nicht nur für neue Technologien, sondern auch für neue Ideen und Konzepte. Beobachten ließ sich diese Dynamik im Jahre 2014 rund um den Vorschlag, mehr öffentlich-rechtliche Inhalte unter offenen Lizenzen wie Creative Commons zugänglich zu machen.

Der öffentlich-rechtliche Rundfunk in Deutschland ist einer der größten Produzenten öffentlich finanzierter Inhalte. Allerdings bedeutet auch dort – ähnlich wie bei universitärer Forschung oder bei Schulbüchern – öffentlich finanziert nicht automatisch öffentlich zugänglich oder gar nutzbar. Von Verlagen herbeilobbyierte Löschpflichten zwingen öffentlich-rechtliche Sender dazu, viele ihrer Inhalte bereits nach 7 Tagen wieder aus dem Netz zu entfernen. Aufgrund von „ungeklärten Musik- oder Bildrechten", wie in der FAQ der ARD-Mediathek erklärt wird, können viele Reportagen und Dokumentation überhaupt nicht online wiedergegeben werden. Und selbst wenn Inhalte online verfügbar sind, ist damit noch lange nicht das Recht der BeitragszahlerInnen verbunden, diese weiterzuverbreiten und weiter zu nutzen. Auch für öffentlich-rechtliche Inhalte gilt das „alle Rechte vorbehalten" des Urheberrechts.

Diese Einschränkungen der Verfügbarkeit öffentlich-rechtlicher Inhalte stehen dabei in eklatantem Widerspruch zum gesetzlichen Programmauftrag. So möchte die ARD etwa „möglichst viele Menschen" mit ihrem „Programm rund um Information, Bildung, Beratung und Unterhaltung" erreichen. Obwohl Digitalisierung und Internet die Erfüllung dieses Auftrags eigentlich einfacher denn je machen sollten – so könnten Inhalte unabhängig von Sendezeiten und -frequenzen dauerhaft abrufbar gehalten werden –, werden diese Potenziale bislang nicht einmal im Ansatz ausgeschöpft.

Bericht der AG Creative Commons in der ARD

Eine Möglichkeit, um diese Situation auch ohne Gesetzesänderungen zumindest ein wenig zu verbessern, ist der verstärkte Einsatz von offenen Lizenzen wie Creative Commons im öffentlich-rechtlichen Rundfunk. Zumindest im Bereich von Eigenproduktionen ohne Fremdmaterial und GEMA-Musik könnten Creative-Commons-lizenzierte Inhalte ohne aufwändige Rechteklärung weiterverbreitet,

dauerhaft verfügbar gehalten und, eine entsprechend offene Lizenz vorausgesetzt, auch dafür genutzt werden, neue Werke zu schaffen[1].

Zu einer ähnlichen Einschätzung kommt mittlerweile auch eine Arbeitsgruppe (AG) Creative Commons in der ARD. In einem im Oktober 2014 geleakten Entwurf für einen Bericht der AG[2] wird der verstärkte Einsatz von Creative Commons prinzipiell befürwortet und das mit dem öffentlich-rechtlichen Programmauftrag begründet:

> Die Nutzung von CC-Lizenzen unterstützt die Erfüllung dieses Auftrags: Der Zugang zu Bildungsinhalten oder Inhalten, die die Meinungsbildung fördern, wird erleichtert. Die ARD kann Beitragszahler, vor allem jüngere, besser erreichen. Werden mehr Menschen erreicht, erhöht sich die Beitragsakzeptanz. Redaktionen in der ARD nutzen selbst CC-lizenzierte Inhalte. Die ARD sollte daher auch Inhalte unter CC zur Verfügung stellen. (S. 3)

Bevor jedoch öffentlich-rechtliche Inhalte unter Creative Commons veröffentlicht werden können, sind eine Reihe von Voraussetzungen zu prüfen. Dazu zählt beispielsweise die Frage, ob die Rundfunkanstalten überhaupt über die erforderlichen Urheberrechte verfügen, ob Persönlichkeitsrechte davon betroffen sein könnten und wie die erforderliche Kennzeichnung und Downloadmöglichkeit praktisch realisiert werden kann. In einigen Nischen wie beispielsweise den NDR-Fernsehsendungen „Zapp“ und „Extra 3“ oder der ZDF-Sendung „Elektrischer Reporter“ wurden diese Fragen aber bereits gelöst, die Inhalte sind unter Creative Commons und damit dauerhaft online verfügbar.

Kritisch-offener Brief zu Creative Commons

Kurz nach Bekanntwerden der Arbeitsgruppe sowie deren Berichtsentwurfs wurde aber deutlich, was die größte Hürde für die verstärkte Nutzung von Creative Commons im öffentlich-rechtlichen Rundfunk darstellen könnte: Fragen rund um angemessene Vergütung. So wandte sich der Berufsverband der AuftragskomponistInnen in Deutschland, der CC Composers Club e. V., mit einem ausführlichen offenen Brief[3] gleich direkt an „die Intendanten der ARD-Sender“ und meldete umfassende Bedenken gegen die Nutzung von Creative Commons an.

Befürchtet wird darin unter anderem „das Ziel eines Vergütungs-Dumpings bei Kreativschaffenden“ und die mit Creative Commons verbundene Förderung von “Drittanbieter-Plattformen sowie Suchdienste[n]“. Vor allem der erste Punkt, die Sorge um angemessene Vergütung von AutorInnen sowie anderen Kreativschaffenden ist dabei ein durchaus relevanter Punkt. Auch nur der Eindruck, dass Creative Commons als Sparprogramm missbraucht werden könnte, könnte die Akzeptanz der Lizenzen untergraben und damit mehr Schaden anrichten als nützen.

Vor einer Umsetzung der Empfehlungen der ARD-Arbeitsgruppe bedarf es also verbindlicher Klarstellungen, dass es durch Creative Commons zu keiner auch nur mittelbaren Kürzung von Honoraren kommen wird, sondern allenfalls zusätzliche Vergütung für die Einräumung von weitreichenderen Rechten erforderlich ist. Gleichzeitig ist es aber so, dass Wiederholungs- und Nachnutzungshonorare in vielen Bereichen keine oder eine sehr geringe Rolle spielen. Selbst eine anfängliche Beschränkung des Creative-Commons-Einsatzes auf diese Bereiche, zu denen etwa Wort- und Textbeiträge angestellter RedakteurInnen zählen, würde eine enorme Steigerung von offen lizenzierten Inhalten bedeuten.

Darüber hinaus gilt es aber auch, mittel- bis langfristige Perspektiven für eine größere Selbstverständlichkeit bei der Nutzung von offenen Lizenzen zu formulieren. Eben weil der öffentlich-rechtliche Auftrag mit Creative Commons besser erfüllt werden kann, müsste die Begründungspflicht mittelfristig umgedreht werden: Begründungspflichtig sollte also nicht die Nutzung von Creative Commons sein, sondern jene Fälle, in denen Inhalte nicht offen lizenziert werden. Mit anderen Worten: Wo rechtlich eine Creative-Commons-Lizenzierung möglich ist, sollte sie zur Regel werden. Bis dorthin ist es wohl noch ein weiter Weg.

Sowohl der optimistische Bericht der ARD-Arbeitsgruppe zu Creative Commons als auch die teilweise kritische Resonanz in Form des offenen Briefs der Auftragskomponisten sind aber ein Beleg für die gestiegene Bedeutung von Creative Commons – und die größere Ernsthaftigkeit, mit der im öffentlichen Sektor an der stärkeren Nutzung von Creative Commons gearbeitet wird.

Anmerkungen

[1] Dazu ausführlich das D64 White Paper *Creative Commons im öffentlich-rechtlichen Rundfunk*. http://cc.d64.serpens.uberspace.de/wp-content/uploads/sites/2/2014/01/White-Paper-CCimOR-D64.pdf

[2] irights.info: *Endlich Creative Commons im öffentlich-rechtlichen Rundfunk?*. http://irights.info/artikel/endlich-creative-commons-im-oeffentlich-rechtlichen-rundfunk/24015

[3] *Offener Brief an die Intendanten der ARD-Sender*. http://www.composers-club.de/offener-brief-an-die-intendanten-der-ard-sender/

Leonhard Dobusch ist Juniorprofessor für Organisationstheorie am Management-Department der Freien Universität Berlin. Er twittert als @leonidobusch und bloggt privat unter leonidobusch.blogspot.com sowie gemeinsam mit anderen am englischsprachigen Forschungsblog governancexborders.com.

27 Der gläserne Leser – Wie Amazon unsere Lesegewohnheiten ausspäht

von **Daniel Leisegang**

Das E-Book kommt – langsam aber stetig: Schon heute greift ein Viertel aller Bundesbürger regelmäßig zum digitalen Buch[1]. Mehr als 22 Millionen E-Books wurden hierzulande 2013 verkauft – im Vergleich zum Vorjahr ein Umsatzplus von rund 60 Prozent.

Dieses dynamische Wachstum hat einen heftigen Wettstreit um die Marktanteile auf dem digitalen Buchmarkt ausgelöst. An dessen Spitze steht der US-Konzern Amazon: Er kontrolliert hierzulande nicht nur etwa 20 Prozent des Buchmarktes und rund 80 Prozent des Onlinehandels, sondern hält auch über 40 Prozent des deutschen E-Book-Marktes fest in seiner Hand[2].

Allerdings ist die Konkurrenz Amazon auf den Fersen: Im März 2013 brachten Thalia, Weltbild, Hugendubel, Club Bertelsmann sowie die Deutsche Telekom in einer überraschenden Allianz gemeinsam den E-Reader Tolino auf den Markt. Das deutsche Gemeinschaftsprodukt steht in direkter Konkurrenz zu Amazons Kindle. Dessen Marktanteil lag 2013 bei rund 43 Prozent; der Tolino konnte immerhin einen Anteil von rund 12 Prozent für sich verbuchen.

Das E-Book tritt somit mehr und mehr neben das gedruckte Buch und verändert zugleich das Machtgefüge auf dem Buchmarkt. Die Folgen sind dramatisch – auch und gerade für die Konsumenten: Denn im Zuge der Digitalisierung auf dem Buchmarkt werden deren Nutzungsdaten zu einer immer wertvolleren Ressource. Diese Entwicklung bedroht nicht nur die Privatsphäre der Leser, sondern auch deren Recht, frei über die gekauften Bücher zu verfügen.

Der Kindle: Die Vorzüge des digitalen Lesens

Besonders deutlich zeigt sich diese Gefahr am Lesegerät des Marktführers Amazon. Dieses spielt in der Zukunftsstrategie des Konzerns eine zentrale Rolle.

Seit 2009 ist der Kindle (zu Deutsch: „etwas entfachen“) in Deutschland verfügbar. Inzwischen gibt es ihn in der siebten Generation. Er verfügt über ein lesefreundliches und energiesparsames Graustufen-Display, ist kaum dicker als ein Bleistift und wiegt rund 200 Gramm. Das Gerät kann Tausende Bücher speichern und seine Akkulaufzeit beträgt etwa zwei Monate bei einer durchschnittlichen Lesezeit von einer halben Stunde pro Tag.

Je nach Ausstattung kostet der E-Reader zwischen 49 und 189 Euro[3]. Mit dem subventionierten Preis versucht Amazon dauerhaft, die Konkurrenz zu unterbieten, um so möglichst rasch Marktanteile zu gewinnen; Profite wirft der Kindle erst ab, wenn der Kunde regelmäßig Bücher bei Amazon kauft.

E-Reader wie der Kindle sind so komfortabel zu nutzen, dass selbst hartgesottene Buchwürmer in Versuchung kommen. Die Geräte liegen angenehm in der Hand und klappen nicht versehentlich zu. Dank ihres geringen Gewichts lassen sie sich bequem in jeder Haltung nutzen – selbst im Liegen. Wer mal versucht hat, auf dem Rücken liegend in der gedruckten Ausgabe von „Krieg und Frieden" zu schmökern, weiß dies zu schätzen. Die Bildschirme der E-Reader sind gestochen scharf und kontrastreich; lange Texte lassen sich ohne Anstrengungen auf ihnen lesen. Da neuere Geräte zudem über eine integrierte Beleuchtung verfügen, sind sie nicht nur unter heller Sonneneinstrahlung, sondern selbst im Dunkeln einsetzbar.

Neben der Haptik und der Lesefreundlichkeit ist aus Sicht der Kunden auch die unmittelbare Verfügbarkeit von Büchern entscheidend. Die meisten E-Reader bieten einen direkten Zugang zu einem Online-Shop, der es erlaubt, zu jeder Stunde und an nahezu jedem Ort der Welt neue Bücher zu erwerben – sofern eine Datenverbindung besteht.

So auch beim Kindle: Er bietet Zugang zu Amazons gesamtem digitalen Bücherangebot. Ähnlich einem Webbrowser können Nutzer auf der dem Bildschirm angepassten Amazon-Website nach Büchern suchen und diese auf dem Gerät speichern. Die ersten Seiten eines E-Books lassen sich vorab kostenlos lesen. Erst wenn ihnen ein Buch zusagt, schließen die Kunden den Kauf ab. Daraufhin wird das gesamte Werk innerhalb weniger Sekunden per Funkverbindung heruntergeladen und steht zur Lektüre bereit.

Bei Amazon gekaufte E-Books lassen sich zudem nahtlos auf unterschiedlichen Geräten weiterlesen. Der Konzern ermöglicht es dem Nutzer beispielsweise, die morgens auf dem Tablet begonnene Lektüre unterwegs in der U-Bahn auf dem Smartphone per Kindle App fortzusetzen. Abends auf dem Sofa kann der Kunde dann zum Kindle E-Reader greifen. Dabei wird der Lesefortschritt auf sämtlichen Geräten über die firmeneigenen Server synchronisiert. Darüber hinaus können die Kunden die Markierungen und Lesezeichen anderer Leser einblenden, besonders beliebte Stellen sind als *Popular Highlights* gekennzeichnet. Die digitalen Bücher enthalten somit bereits beim Kauf Spuren anderer Amazon-Kunden. Zugleich wandelt sich das Lesen eines Buches von einer intimen Handlung zu einem Kollektiverlebnis, vergleichbar mit dem gemeinsamen Schauen eines Kinofilms[4].

Lizenz zum Lesen

Allerdings zahlen die Kunden für das komfortable Lesen einen hohen Preis. Denn Amazons E-Reader ist in seiner Nutzung massiv eingeschränkt. So kann er nur

das von Amazon entwickelte und geschlossene E-Book-Format Mobi nutzen. Das von zahlreichen Händlern angebotene offene ePub-Format ist dagegen nicht verwendbar. Kauft der Kunde also ein E-Book bei einem Konkurrenten, muss er dieses erst umständlich in das Amazon-Format umwandeln, um es auf dem Kindle lesen zu können.

Somit erhalten Amazon-Kunden mit dem Kauf eines E-Books nur ein Nutzungsrecht – oder anders ausgedrückt: eine Lizenz zum Lesen. Ein Besitzverhältnis wie bei einem gedruckten Buch, das sie nach Belieben verwenden und verleihen dürfen, besteht nicht.

Welche Folgen dieses Modell hat, wird den meisten Kunden erst bewusst, wenn sie sich für einen anderen Anbieter entscheiden. Kündigen sie nämlich ihr Konto bei Amazon, verlieren sie damit auch den Zugriff auf sämtliche digitale Bücher, die sie zuvor dort gekauft haben. Der Grund: Die Kindle-Bücher liegen nicht nur im Amazon-eigenen Format vor, sondern verfügen zudem über einen Kopierschutz; sie sind daher nicht ohne weiteres auf einem anderen E-Reader verwendbar.

Das Geschäft mit den Daten

Damit aber nicht genug: Darüber hinaus geben die Nutzer viel über sich preis. Denn Amazon schaut seinen Kunden bei der Lektüre von E-Books quasi unentwegt über die Schulter und zeichnet deren Leseverhalten auf. Dabei werden neben der genauen Leseposition auch die Lesedauer sowie sämtliche Hervorhebungen und Anmerkungen an Amazon übermittelt. Damit weiß der Konzern exakt, wie viel Zeit ein Leser für ein Buch benötigt, ob er es bis zum Ende liest und mit welchen Begriffen er nach neuen Büchern sucht. Auch die Kindle-App auf Smartphone, Tablet oder Rechner erfasst, wie oft ein Leser das Programm nutzt und wie viel Zeit er mit der Lektüre verbringt.

Die abgefangenen Daten geben dem Konzern tiefe Einblicke in die Vorlieben jedes einzelnen Kunden – auf deren Grundlage dann weitere Kaufempfehlungen gemacht werden. Schätzungen zufolge sollen rund 30 Prozent des Umsatzes auf Produktempfehlungen beruhen, denen Big-Data-Analysen zugrunde liegen[5].

Inzwischen verfügt Amazon – wie Facebook und Google – auch über ein eigenes soziales Netzwerk, das ihm zusätzliche Daten liefert. Im März 2013 kaufte der Konzern die Plattform Goodreads. Auf ihr verfassen die Nutzer Rezensionen von Büchern und empfehlen diese weiter. Das Angebot wird rege genutzt: Insgesamt gibt es mehr als 25 Millionen Besprechungen, und besonders auf mobilen Geräten verzeichnete die Community in den vergangenen Monaten hohe Zuwächse bei den Neuanmeldungen.

Die angehäuften Kunden- und Nutzungsdaten setzt Amazon auch in anderen Geschäftszweigen ein. So hat das Unternehmen jüngst eine Plattform für Display-Werbung gestartet. Dem Wall Street Journal zufolge will der Konzern in einem

ersten Schritt Werbeanzeigen auf den eigenen Shopping-Sites anzeigen, langfristig soll das System auch außerhalb von Amazon zum Einsatz kommen. Die Werbeplattform funktioniert dabei ähnlich wie Google AdSense, bei dem Werbung in Abhängigkeit zu bestimmten Suchbegriffen platziert wird. Damit tritt Amazon zugleich in direkte Konkurrenz zu dem Suchgiganten Google, an den es bisher Werbeplätze auf Amazon.com vermietet hat. Und dank der detaillierten Datengrundlage wird Amazon in der Lage sein, Werbung noch zielgenauer als dieser zu schalten.

Der „Mainstream-Lover": Bestseller dank Big Data

Aus den Nutzungsdaten lässt sich aber noch weitaus mehr Kapital schlagen. Langfristig werden diese auch die Buchproduktion selbst grundlegend verändern. Denn auch das Schreiben von Büchern verändert sich unter dem Einfluss der gewonnenen Daten. Verlage konkurrieren heute mit den neuen Produkten des wachsenden digitalen Unterhaltungsmarktes – dazu gehören Fernsehserien, die Sozialen Medien aber auch Handyspiele. Für die Buchhändler wie auch für die Verlage werden die Nutzerdaten der Kunden somit zunehmend wichtiger, um ihre Produkte besser auf die Interessen der Kunden zuzuschneiden und verkaufen zu können.

Die mittels der E-Reader gewonnen Daten bieten hierfür eine wichtige Grundlage. So dauert es durchschnittlich etwa sieben Stunden, um das letzte Buch von Suzanne Collins „Hunger Games"-Trilogie zu lesen. Im zweiten Band der Trilogie haben rund 20.000 Kindle-Leser den gleichen Satz angestrichen: „Because sometimes things happen to people and they're not equipped to deal with them." („Weil den Menschen manchmal Dinge widerfahren, auf die sie nicht vorbereitet sind.") Und die meisten Nutzer luden, gleich nachdem sie den ersten Band ausgelesen hatten, unmittelbar den zweiten herunter.

Welche Veränderungen diese Erkenntnisse mit sich bringen, zeigt schon jetzt eindrucksvoll der unabhängige Verlag Coliloquy mit Sitz in San Francisco. So können die Leser dessen Mystery-Reihe „Parish Mail" wählen, ob der jugendliche Protagonist über Zauberkräfte verfügen soll oder nicht. In „Great Escapes" können sie hingegen die Intensität der Liebesszenen bestimmen und das Erscheinungsbild der Hauptfigur anpassen: Diese hat – so Coliloquy – idealerweise schwarze Haare und grüne Augen, verfügt über eine kräftige Statur und eine leicht behaarte Brust.

Mit diesem Wissen können Autoren noch während des Schreibens – so wie es bei Fernsehserien bereits üblich ist – den Verlauf ihrer Geschichten anpassen. Beispielsweise spielt in der romantischen Gaunerkomödie „Getting Dumped" eine junge Frau die Hauptrolle. Die Leser wurden gefragt, welcher der Verehrer ihr Herz gewinnen soll. Mehr als die Hälfte wählte Collin, der dem Typus Hugh Grant entspricht, rund 30 Prozent mochten hingegen Daniel am liebsten, zu dem

die Romanheldin allerdings eine abgekühlte Liebesbeziehung pflegt, und knapp 17 Prozent bevorzugten Pete, den attraktiven aber vergebenen Kollegen.

Das Votum der Leser bewahrte den Charakter Daniel vor seiner Marginalisierung oder gar Auslöschung: Die Autorin Tawna Fenske nahm die Leservorlieben zum Anlass, ihn nicht wie geplant ins Gefängnis zu schicken, sondern ihm stattdessen eine zentrale Rolle in ihrem Roman zu geben. Der Anteil seiner Fans war offensichtlich zu groß, um diese zu verprellen.

Welche Auswirkungen diese veränderten Produktionsweisen auf den Buchmarkt haben werden, lässt sich derzeit nur erahnen. Fest steht aber: Bislang lebte der Buchmarkt davon, dass sich der Erfolg einzelner Produkte nicht eindeutig vorhersagen ließ. Und gerade dies gewährleistete ein überaus ausdifferenziertes Angebot an Publikationen. Allerdings zeichnet sich bereits seit einigen Jahren ein dramatischer Wandel ab: Lieblos produzierte „Hits" und Buchserien à la Harry Potter dominieren mehr und mehr den Markt. Werden Bücher künftig nun noch mehr auf einen mittels Big Data ermittelten Massengeschmack zugeschnitten, droht die Vielfalt auf dem Buchmarkt weiter zurückzugehen.

Amazon: Produktion eigener Inhalte

Auch Amazon hat erkannt, dass es mithilfe der Nutzungsdaten seiner rund 230 Millionen Kunden Bücher maßschneidern und zu Verkaufsschlagern machen kann.

Zu diesem Zweck hat der Konzern in den Vereinigten Staaten seit 2009 Schlag auf Schlag neue Verlage gegründet; auch mehrere renommierte Verlagshäuser kaufte der Konzern auf. Amazons unternehmerisches Ziel liegt auf der Hand: Der Internetkonzern möchte die Verlage als Mittler ausschalten und tritt daher in direkte Konkurrenz zu ihnen. Langfristig will sich Amazon so die gesamte Wertschöpfungskette des Buchmarktes unter den Nagel reißen. „Die Einzigen, die für den verlegerischen Prozess noch nötig sind, sind der Autor und der Leser", verkündete bereits 2011 Amazon-Verlagsmanager Russell Grandinetti.

Ein Angebot, mit dem der Konzern den Verlagen als erstes zu Leibe rückte, heißt Kindle Direct Publishing (KDP). Amazon startete es parallel zur Markteinführung seines Kindle im Jahre 2007, um so exklusive Inhalte für diesen E-Reader anbieten zu können. Mit KDP können Autoren direkt und in Eigenregie Bücher bei Amazon veröffentlichen. Obwohl es kein Lektorat im klassischen Sinne gibt, ist das Programm äußerst beliebt. Viele Hobbyautoren, die zuvor bei anderen Verlagen abgelehnt wurden, können hier ihre Texte einem Millionenpublikum zum Kauf anbieten – und dabei sogar auf einen Überraschungserfolg hoffen. Laut Amazon stammten 2012 etwa jede fünfte Novität und fünf der zehn meistverkauften deutschsprachigen Kindle-Bücher von Selbstverlegern.

Zwei Jahre nach dem Start von KDP stieg Amazon ins klassische Verlagsgeschäft ein. Mehr als ein Dutzend Verlage hat der Konzern seit 2009 in den Vereinigten

Staaten unter dem Dach von Amazon Publishing ins Leben gerufen. Als besonders erfolgreich gilt der im Mai 2010 gegründete Verlag AmazonCrossing. Er ist zuständig für englischsprachige Übersetzungen fremdsprachiger Bücher und gehört heute zu den führenden Lizenzeinkäufern der USA. Dabei übersetzt er vor allem jene Werke, die Amazon-Kunden in anderen Ländern überdurchschnittlich gut bewerten; allein 2012 übertrug er 29 ausländische Titel ins Englische.

Die höchsten Verkaufszahlen erzielte dabei der Historienroman „Die Henkerstochter" des Deutschen Oliver Pötzsch. Die Übersetzung schaffte es bis auf Platz eins der Kindle-Bestsellerliste und verkaufte sich bis Ende 2012 über 500.000 Mal. Zuvor erschienen Pötzschs Bücher beim Ullstein Verlag. Der verkaufte immerhin 300.000 Exemplare, bevor er Amazon die englischsprachigen Weltrechte an vier Romanen für jeweils 25.000 Euro überließ. Nicht nur für Amazon hat sich dieser Kauf somit gelohnt, sondern auch für Oliver Pötzsch: Er wurde in den Vereinigten Staaten zum gefeierten Starautor.

Der direkte Angriff auf die Verlage

Nach KDP und den ersten verlegerischen Gehversuchen läutet Amazon nun die dritte Phase seiner Verlagsstrategie ein. Gezielt greift der Konzern die großen Verlagshäuser an, indem er deren Autoren abwirbt. Dabei nimmt Amazon zu Beginn – wie schon bei der Eroberung des Buchhandels – hohe Verluste in Kauf. So erhalten Amazon-Autoren Tantiemen in Höhe von 30 bis 70 Prozent des Verkaufspreises – ein Angebot, dass keiner der traditionellen Verlage dauerhaft überbieten kann. Sie beteiligen ihre Autoren in der Regel mit 5 bis 15 Prozent des Verkaufspreises.

Auch die Verlagsbranche in der „Alten Welt" hat Amazon ins Visier genommen. Im Jahre 2013 expandierte Amazon Publishing nach Europa und richtete eine Dependance in Luxemburg ein. Und im Frühjahr 2014 gab Amazon zum Auftakt der Leipziger Buchmesse bekannt, sein Verlagsgeschäft in Deutschland massiv ausbauen zu wollen. Die Verlage sollten alarmiert sein: Denn um ihnen nachhaltig zu schaden, muss Amazon nur einige Bestsellerautoren abwerben und für sich gewinnen. Gerade sie garantieren den Verlagshäusern jene hohen Umsätze, mit denen weniger umsatzstarke Werke subventioniert werden. Amazon hingegen ist auf eine solche Querfinanzierung nicht angewiesen.

Was aber folgt aus alledem? Gelänge es Amazon tatsächlich, jeden anderen Mittler zwischen den Autoren und den Lesern auszuschalten, hätte dies fatale Folgen für die Buchkultur. Amazon wüchse zu einem mächtigen Gatekeeper an, der allein darüber entscheidet, welche Bücher veröffentlicht werden – und welche nicht. Daran dürften aber weder die Kunden noch die Politik ein Interesse haben. Bis heute ist das Buch – neben der Presse, dem Rundfunk und den neuen Medien – ein Initiator unentbehrlicher Debatten und damit Leitmedium unserer politischen Öffentlichkeit. Aus diesem Grund ist die Auseinandersetzung um Amazon

nicht nur eine um den Schutz unserer Privatsphäre und den Erhalt einer vielfältigen Buchkultur. Im Zentrum steht auch die Frage nach der Zukunft unserer Demokratie.

Dieser Beitrag basiert auf dem Buch „Amazon. Das Buch als Beute", das 2014 im Schmetterling Verlag erschienen ist.

Anmerkungen

[1] *Ergebnis einer repräsentativen Umfrage des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien (BITKOM)*. www.bitkom.org/de/presse/8477_80388.aspx

[2] In den Vereinigten Staaten fällt die Marktdominanz von Amazon noch deutlicher aus: Seit 2007 führt der Konzern den amerikanischen Buchmarkt an. Er verkauft heute schätzungsweise 40 Prozent aller gedruckten und 67 Prozent aller digitalen Bücher.

[3] Schon seit längerem bietet Amazon auch Lesegeräte zu einem reduzierten Preis an, wenn der Kunde im Gegenzug zustimmt, auf dem Kindle Werbebanner angezeigt zu bekommen. Um die Anzeigen gezielt schalten zu können, greift Amazon auf die Kauf- und Lesehistorie der Kunden zurück.

[4] Der auf Amazons Tablets („Kindle Fire") installierte Webbrowser „Silk", den Amazon eigens für sein Tablet programmiert hat, späht standardmäßig sämtliche Datenströme aus, die der Nutzer abruft. Amazon zufolge dient dies allein dem beschleunigten Datenaustausch: Die Abfragen würden über die firmeneigenen Server geleitet, dort ausgewertet und komprimiert, um so angeblich schneller auf die Endgeräte zu gelangen. Tatsächlich weiß Amazon auf diese Weise genau, welche Internetseiten der Kunde mit dem Gerät aufruft und wie lange er sich wo im Netz aufhält.

[5] Vgl. Viktor Mayer-Schönberger: „Ich wünsche mir ein Recht auf Irrationalität" (Interview), www.spiegel.de, 20.12.2013.

Daniel Leisegang ist Politikwissenschaftler und Redakteur der Monatszeitschrift „Blätter für deutsche und internationale Politik" (www.blaetter.de). Er schreibt vor allem zu medien- und netzpolitischen Themen.

Er engagiert sich zudem bei LOG.OS e.V. (www.log-os.info). Der Verein verfolgt das Ziel, eine unabhängige, am Gemeinwohl ausgerichtete E-Book-Plattform aufzubauen.

28 Recht auf Vergessen – Kommentare zum Urteil des Europäischen Gerichtshofs

von **Joe McNamee, Jan Schallaböck** und **Thomas Stadler**

Das Urteil des Europäischen Gerichtshofs zu personenbezogenen Daten und Suchmaschinen sorgt noch immer für Aufregung. netzpolitik.org hat verschiedene Spezialexperten™ angefragt, ihre Meinung zum Urteil und Erwiderungen auf gängige Argumente auszuführen, drei davon sind hier abgedruckt.

Kommentar von Joe McNamee

Als der Europäische Gerichtshof über den Fall „Google Spanien" urteilte, stürzte sich die Presse auf die Entscheidung und nahm in als ein Beispiel für das „Recht auf Vergessen". Der Guardian erklärte, Google müsse Links zu zwei Seiten der La-Vanguardia-Website löschen und dass Rechtsexperten sagen würden, das Urteil könne den Startschuss für Löschanträge geben. Ebenso erklärte die BBC, dass dem EuGH zufolge Links zu irrelevanten und veralteten Informationen auf Anfrage gelöscht werden sollten. Diese schockierende Geschichte verbreitete sich in beeindruckender Geschwindigkeit um die Welt. Einziges Problem: Die Geschichte war zwar schockierend, aber trotzdem nicht wahr.

In Wirklichkeit, wie der Gerichtshof in seiner Presseerklärung und nicht weniger als fünfzehn Mal in seinem Urteil erklärte, beschränkt sich dieses nur auf Fälle, in denen Suchanfragen auf Basis des Namens des Klagenden ausgeführt werden. An keiner Stelle wird von dem Gerichtshof das Löschen von Inhalten vorgeschlagen. Der Gerichtshof urteilte, dass Google Situationen korrigieren solle, in denen eine Suchanfrage mit dem Namen eines Individuums „inadäquate, irrelevante oder nicht länger relevante, oder übermäßige" Suchergebnisse hervorbringt. Das Gericht verwies auf Googles Behauptung, das Entfernen von Seiten aus seinem Index wäre unverhältnismäßig, und widersprach dieser Ansicht weder implizit noch explizit.

Die falsche Presseanalyse scheint zumindest teilweise von Google selbst angeheizt worden zu sein. Die BBC berichtete, dass die Firma angedeutet hatte, Suchergebnisse über Individuen, die irrelevant oder veraltet seien, zu löschen. Diese Analyse wurde von zahlreichen Presseagenturen wiederholt. Der Telegraph berichtete über die Geschichte unter der Überschrift „EU urteilt: Google muss deine Daten löschen, wenn du dazu aufforderst", und – separat – dass Google alle sieben Sekunden eine Anfrage bekomme, „Informationen zu unterdrücken". Bloomberg berichtete, dass Menschen Google dazu auffordern könnten, sensible Informa-

tionen von Internetsuchergebnissen zu entfernen. Der eingeladene Experte fügte hinzu, Daten könnten für immer aus dem Internet entfernt werden und Google würde die Daten aus seinem System löschen.

Seltsamerweise gibt es wenige direkte Zitate von Google zu diesem Thema. Reuters beschränkte sich darauf, namenlose „Quellen" innerhalb der Firma zu zitieren und berichtete, dass Jeffrey Rosen von der George Washington Universität von Google aufgefordert worden sei, mit Reportern zu sprechen, obwohl er keine formelle Verbindung zu Google hat. Ein anderer Akademiker, der zwar mit aber nicht direkt für Google arbeitet, Luciano Floridi, erklärte dass die „Ära frei verfügbarer Informationen in Europa jetzt vorbei" sei. Wie man diese Schlussfolgerung aus dem Urteil ziehen können sollte, wird nicht erklärt. Kurz gesagt: Anscheinend haben Googles eigene Interaktionen mit der Presse ein „Recht auf Vergessen". Sichtbare Spuren gibt es nur wenige.

Es gibt einen wichtigen Punkt der bezüglich der Weisheit des Gerichts angesprochen werden muss. Nämlich gänzlich in Googles Verantwortung zu lassen, welchen Beschwerden stattgegeben werden sollte und welchen nicht. Wie dem auch sei, Google löscht keine Daten. Google wurde nicht dazu aufgefordert, Daten zu löschen. Die betreffenden Websiten sind weiterhin über die Google-Suche zu finden. Auf der anderen Seite löscht Google Hunderte Millionen Suchergebnisse weltweit auf der Grundlage von US-Recht und hat ein Abkommen mit dem Weißen Haus, um weltweit Strafmaßnahmen vorzunehmen. Außerhalb der Rechtsstaatlichkeit, gegen Online-Dienste, die verdächtigt werden, gegen amerikanisches Recht auf Geistiges Eigentum zu verstoßen. Außerdem hat es Adhoc-Vereinbarungen auf nationaler Ebene, Suchergebnisse ohne Rechtsaufsicht zu entfernen. Merkwürdigerweise wurde diesen Aktivitäten nie ein solches Level an Medienaufmerksamkeit gewidmet.

Als Ergebnis dieses Urteils werden keine Seiten gelöscht. Das Urteil schafft kein „Recht auf Vergessen". Nichts wurde vergessen, außer der Wahrheit – der einen Sache, bei der niemand das Recht zu vergessen hat.

Kommentar von Jan Schallaböck

Der Europäische Gerichtshof (EuGH) hat in letzter Zeit zwei vielbeachtete Entscheidungen zum Thema Datenschutz gefällt. Während seine Entscheidung zur Vorratsdatenspeicherung, die auch einige Schwächen der Entscheidung des deutschen Bundesverfassungsgerichts zur gleichen Frage korrigiert, in der Zivilgesellschaft allgemeinen Jubel ausgelöst hat, gibt es zur jüngeren Entscheidung, die unter der Überschrift „Recht auf Vergessen" rezipiert wird, allerdings von vielen Seiten kritische, bisweilen auch polemische Stimmen.

Der Sachverhalt und das damit zusammenhängende Urteil lassen sich schnell skizzieren: Ein Spanier (genaugenommen: die spanische Datenschutzbehörde) war gegen Google vorgegangen, weil eine Suchanfrage nach seinem Namen einen

Link auf einen Zeitungsartikel zum Ergebnis hatte, in dem es um eine 16 Jahre zurückliegende Pfändung gegen den Kläger ging.

Nach den Vorgaben europäischen Datenschutzrechts ist eine Verarbeitung personenbezogener Daten unter anderem dann zulässig, wenn das berechtigte Interesse der datenverarbeitenden Stelle gegenüber dem Interesse des Betroffenen überwiegt. Das Gericht hat diese Abwägung vorgenommen und ist zu dem Ergebnis gekommen, dass das Interesse des Betroffenen überwiegt, sich nicht mit einem lange erledigten Fehltritt konfrontiert zu sehen. Das Interesse von Google, diesen Datensatz anzuzeigen, muss dagegen zurücktreten. So weit, so schlüssig.

Ein Kernpunkt der Kritik an dem Urteil ist, dass das Gericht das Suchergebnis als rechtswidrig bewertet und nicht die Veröffentlichung des ursprünglichen Artikels. Abstrahiert man das Urteil, könnte das heißen, dass eine rechtmäßige Veröffentlichung über eine Suchanfrage nach einem Namen unter Umständen nicht auffindbar sein soll. Kann das richtig sein?

Ja. Eine Suchmaschinenanfrage ist nicht dasselbe wie eine Archivrecherche. Bei der Google-Anfrage werden nahezu sämtliche im Internet offen verfügbaren Inhalte im Zusammenhang mit einem Namen zusammengeführt. Es entsteht ein umfassendes Dossier, mitunter sogar ein weitreichendes Profil einer Person. Mit einer Archivrecherche ist das nicht möglich. Hier kann allenfalls der vergleichsweise kleine, im Archiv verfügbare Bestand, zusammengeführt werden. Es bedarf zudem meist einer ungefähren Vorstellung davon, was man sucht. Quantitatives schlägt hier in Qualitatives um. Es handelt sich also nicht um denselben Lebenssachverhalt, entsprechend bedarf es vielleicht auch einer anderen Regelung.

Die grundlegende Frage ist: Sollte man mit publizierter Information immer alles machen dürfen? Ein solcher Grundsatz ist einfach und daher verlockend, trifft aber nicht auf alle Fälle zu. So werden die meisten Menschen wohl zustimmen, dass private und staatliche Überwachungsmechanismen, die alle möglichen Quellen abgrasen, um mittels Korrelationsanalysen Listen von Menschen anzufertigen, die wahrscheinlich insolvent, schwul oder narzisstisch gestört sind, nicht wünschenswert sind. Diese Möglichkeiten bietet das Netz derzeit.

Nach allem was wir hören, existieren solche Programme und Algorithmen und werden genutzt. Das Recht muss das aber durchaus nicht goutieren. Es widerspricht übrigens auch dem datenschutzrechtlichen Prinzip der Zweckbindung, das seit Jahrzehnten anerkannt ist. Entsprechend sind eben diese Anwendungen und Prozesse nicht oder nur eingeschränkt zulässig – man könnte das als prozessorientierten Datenschutz bezeichnen.

Was hier im Einzelnen zulässig sein soll und was nicht, ist leider schwierig abzugrenzen. Das Urteil schreibt eine Abwägung vor. Hier kommt ein zusätzliches Problem ins Spiel: Maschinen können nicht gut abwägen, sie können nur rechnen. Wollen wir uns aber mit Rechenmaschinen das Leben erleichtern, brauchen

wir berechenbare Sachverhalte. Die Entscheidung, ob etwas verarbeitet werden darf, muss automatisch gefällt werden können. Recht und Technik müssen hier zusammenspielen.

Eine mögliche Lösung wäre dabei beispielsweise ein neues Element in der HTML-Auszeichnungssprache, mit der Webseiten beschrieben werden, das verhindert, dass Namen und ähnliche Angaben von Suchmaschinen gespeichert werden. Die Verpflichtung ein solches „noindex tag"' zu verwenden, müsste dann jene Publizierenden treffen, die auf Auffindbarkeit in Suchmaschinen setzen. Hier ist die Aufgabe auch aus vielerlei Gründen besser verortet.

Hiergegen kann man – zu Recht – einwenden, dass das Recht die technische Möglichkeit der Verarbeitung nicht ausschließt. Das Recht verkommt zu „snake oil". Es entstehen Gatekeeper (und Akteure, die sich nicht gar an das Recht gebunden fühlen), die die Informationen mit erhöhter Exklusivität auswerten können. Letzteres ist auch ein Problem für die Demokratie. Es muss daher das, was als richtig (und als Recht) anerkannt wurde, auch in Technologie übersetzt werden. Hierfür brauchen wir perspektivisch neue technische Ansätze, nämlich durchsetzungsstarkes Privacy by Design.

Ein weiterer Kritikpunkt ist, dass eine effektive Rechtsdurchsetzung nur denjenigen zugute kommt, die sich eine solche leisten können. Dem könnte man entgegenhalten: Die private Rechtsdurchsetzung ist im Datenschutzrecht eher zu schwach ausgeprägt. Es grenzt an eine Absurdität, dass urheberrechtlich geschützte Wirtschaftsinteressen effektiver durchgesetzt werden können als das im Datenschutzrecht verbürgte Persönlichkeitsrecht.

Es ist einer der Konstruktionsfehler des derzeitigen Datenschutzrechtes, die Durchsetzung der Einhaltung im wesentlichen bei Datenschutzbehörden zu verorten – die zwangsläufig daran scheitern müssen, weil es einfach derart viele Datenverarbeiter gibt. Was dringend erforderlich wäre, ist ein pauschaliertes Mindestschmerzensgeld bei Datenschutzverstößen, kombiniert mit einem Verbandsklagerecht. Dann wäre dem Problem des viel beschworenen „Umsetzungsdefizits" schnell beizukommen. Die Unternehmen sähen sich dann deutlich veränderten Risikoabwägungen gegenüber, würden sich dagegen versichern wollen und auf Druck der Versicherer ihre Verarbeitungsprozesse anders entwickeln.

Journalisten müssen regelmäßig abwägen, ob sie Personen, die in ihren Recherchen aufgetaucht sind, namentlich erwähnen. Hierfür gibt es über Jahre entwickelte Grundsätze. Diese Aufgabe kann gesellschaftlich nur durch abstrakte Vorgaben gelöst werden, die Einzelfallabwägung kann und sollte nicht durch staatliche Einrichtungen durchgeführt werden. Eine staatliche Aufsichtsbehörde mit der Aufgabe der Abwägung öffentlicher Informationsinteressen für jeden Einzelfall wäre nicht nur unpraktisch und geradezu monströs, sie wäre auch kaum mit den Vorgaben aus Art. 5 des Grundgesetzes, der Presse- und Meinungsfreiheit, zu vereinbaren.

Kritisieren kann man das Urteil jedoch insoweit, als das Gericht für die Abwägung wenige konkrete Kriterien nennt, wann ein Suchmaschinenbetreiber einen Eintrag löschen muss und wann nicht, so dass ein nicht unerheblicher Auslegungsspielraum bleibt. Das Gericht hat eine Linie vorgegeben, die Suchmaschinenbetreibern nahelegt, im Zweifel zu löschen.

Gegen Gelöschtes wird vermutlich selten geklagt. Es ist daher nicht zu erwarten, dass viele Gerichte in die Verlegenheit kommen, sich mit einer differenzierteren Auslegung zu befassen. Diese Konkretisierung müsste der Gesetzgeber nachliefern, auch dadurch, dass er den Löschpflichten Indizierungspflichten gegenüberstellt. Eine solche rechtliche Vorgabe zu einer Suchmaschinenneutralität zu formulieren ist eine wichtige, aber auch eine schwierige Aufgabe.

In der Tat sorgt eine stärkere Verrechtlichung wohl stets auch für Markteintrittshürden. Für ein kleines Startup wird der Aufbau einer Rechtsabteilung in der Regel nicht oberste Priorität haben. Allerdings ist es unwahrscheinlich, dass die Entscheidung viele aufstrebende, junge Wettbewerber für Google vom Markt gefegt hat. Die Markteintrittshürden für Suchmaschinen sind aus vielerlei Gründen bereits jetzt erheblich. Monopolen muss man anders begegnen – ein Vorbild könnte man sich im Kartell- oder im Medienaufsichtsrecht suchen.

Für Suchmaschinen, die sich auf Personensuchen spezialisieren wollen, mag es nun nahezu unmöglich geworden sein, sich zu etablieren. Aber auch jenseits der vom Gericht festgestellten Rechtslage ist es gesellschaftlich vielleicht wünschenswert, dass für solche Angebote ein paar Hürden existieren.

Kommentar von Thomas Stadler

Vor ein paar Tagen hat der Europäische Gerichtshof entschieden, dass Suchmaschinenanbieter wie Google verpflichtet werden können, Suchergebnisse aus ihrem Index zu löschen, wenn diese Treffer auf Inhalte verweisen, die personenbezogene Daten enthalten. Geklagt hatte ein Spanier, der eine amtliche Mitteilung auf eine ihn betreffende Zwangsversteigerung, die allerdings schon einige Jahre zurücklag, nicht mehr von Google indiziert haben wollte.

Die Entscheidung des Europäischen Gerichtshofs (EuGH) zur datenschutzrechtlichen Verantwortlichkeit von Google enthält zwei begrüßenswerte Klarstellungen:

1. Suchmaschinen verarbeiten personenbezogene Daten und zwar als Verantwortliche im Sinne der Datenschutzrichtlinie der EU.

2. Google ist an europäisches Datenschutzrecht gebunden, weil es Daten auch innerhalb der EU verarbeitet. Im Rahmen einer weiten Auslegung der Richtlinie hält es der EuGH für ausreichend, dass Google in Spanien eine Niederlassung unterhält, die die Aufgabe hat, Werbeflächen für Google zu vermarkten. Da die Trefferergebnisse und die Werbung (Ad-Words) auf denselben Seiten angezeigt werden, erfolgt die Datenverarbeitung nach Ansicht

des EuGH auch im Rahmen der Werbetätigkeit der spanischen Zweigniederlassung von Google. Und daraus folgt dann, nach Ansicht des EuGH, die datenschutzrechtliche Verantwortlichkeit. Diese alles andere als zwingende Annahme wird in der Rechtswissenschaft zu Diskussionen führen. Im Interesse einer effektiven Durchsetzung des europäischen Datenschutzrechts darf man sie aber zumindest rechtspolitisch begrüßen.

Problematisch ist das Urteil des EuGH vor allen Dingen aber deshalb, weil es das Spannungsverhältnis zwischen Persönlichkeitsrecht/Datenschutz einerseits und Meinungs-, Presse- und Informationsfreiheit andererseits höchst einseitig zugunsten des Datenschutzes auflöst.

Der EuGH betont, dass das Recht auf Schutz personenbezogener Daten im Allgemeinen gegenüber dem Interesse der Internetnutzer auf Zugang zu Informationen überwiegt und dieses Regel-Ausnahme-Verhältnis auch nur in besonders gelagerten Fällen durchbrochen werden kann. Diese Position des EuGH bricht mit der bisher bekannten, ergebnisoffenen Abwägung zwischen Persönlichkeitsrecht und Meinungsfreiheit wie sie vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für Menschenrechte seit langer Zeit praktiziert wird.

Die Annahme eines regelmäßigen Vorrangs des Schutzes personenbezogener Daten führt dazu, dass aus Sicht der Suchmaschine die Indizierung solcher Inhalte, die sich mit einer bestimmten oder auch nur bestimmbaren Person auseinandersetzen, regelmäßig als problematisch zu betrachten ist. Jeder, der über Google Informationen über seine Person findet, wird durch das Urteil in die Lage versetzt, von Google eine Löschung solcher Treffer aus dem Index zu fordern. Zumindest ist dieses Szenario nach der Entscheidung des EuGH jetzt als Regelfall definiert worden.

Der EuGH postuliert also nichts weniger als einen regelmäßigen Vorrang des Datenschutzes vor der Meinungs- und Informationsfreiheit. Die Heerschar an Journalisten, die hierzu in den letzten Tagen Beifall geklatscht hat, sollte sich jetzt vielleicht mal darüber Gedanken machen, was das tatsächlich auch für ihre Arbeit bedeuten kann.

Das Urteil des EuGH geht desweiteren davon aus, dass die Suchmaschine auch verpflichtet sein kann, selbst solche Informationen aus ihrem Suchindex zu tilgen, die sich rechtmäßig im Netz befinden. Insoweit könnte es nach Ansicht des EuGH nämlich sein, dass derjenige, der die Informationen veröffentlicht hat, sich anders als Google auf ein Medienprivileg berufen kann. Das bedeutet im Ergebnis, dass Google und andere Anbieter nicht einmal mehr rechtmäßige Inhalte bedenkenlos indizieren können. Diese Annahme des EuGH deutet zudem auf eine äußerst befremdliche Vorstellung der Reichweite der Pressefreiheit hin. Nach ständiger Rechtsprechung des Bundesverfassungsgerichtes können sich nämlich

auch Transporteure und Informationsmittler auf das Grundrecht der Pressefreiheit berufen. Das hat einen ganz einfachen Grund: Presseerzeugnisse müssen und mussten schon immer zu ihren Lesern transportiert werden. Der Schutz dieses, für einen demokratischen Staat so essentiellen, Rechts ist deshalb nur dann effektiv gewährleistet, wenn auch der Transport von Presseerzeugnissen nicht beeinträchtigt wird. Ohne den Schutz der Informationsmittler ist der Schutz der Pressefreiheit also unvollständig. Diesen notwendigen Schutz will der EuGH Informationsmittlern wie den Suchmaschinen offenbar aber nicht (mehr) zukommen lassen. Das allerdings wäre im Vergleich zur Pressefreiheit, wie wir sie kennen, ein erheblicher Rückschritt.

Die Entscheidung des EuGH weist darüber hinaus eine erhebliche sachliche Nähe zu Netzsperren auf.

Bei Access-Sperren und den Löschpflichten, die der EuGH Google abverlangt, geht es im Kern um dasselbe. Nämlich darum, durch staatlichen Zwang den Zugang zu Inhalten im Internet zu erschweren. In beiden Fällen geschieht dies durch die Inpflichtnahme eines Netzdienstleisters, der dafür sorgen soll, dass die Mehrheit der Nutzer nicht mehr auf bestimmte Inhalte zugreifen kann. Man kann sowohl Suchmaschinenbetreiber als auch Access-Provider als Zugangsanbieter betrachten. Zwischen dem Phänomen der Netzsperren und den vom EuGH postulierten Löschpflichten besteht also kein inhaltlich relevanter Unterschied.

Die Entscheidung des EuGH ist in seiner Kernaussage meinungs- und informationsfeindlich. Sehr treffend hat das Ansgar Koreng auf Twitter zusammenfassend so formuliert:

> Was das heutige EuGH-Urteil zeigt: Datenschutz hat auch eine zutiefst freiheitsfeindliche Seite.

Den Treppenwitz zu seiner Entscheidung hat der EuGH übrigens auch gleich mitgeliefert. Im Urteil stand der volle Name des spanischen Klägers, mit der Folge, dass jetzt ganz Europa die Geschichte seiner Zwangsversteigerung kennt und Google es jetzt eigentlich auch unterlassen müsste, das Urteil des EuGH zu indizieren.

Die Fokussierung der gesamten Diskussion auf Google dürfte übrigens ebenfalls an der Sache vorbei gehen. Das Urteil betrifft letztlich alle Dienste mit hoher Reichweite, also insbesondere auch soziale Medien wie Facebook oder Twitter.

Es bleibt die Hoffnung, dass das Urteil des EuGH einfach nur nicht durchdacht und schlecht begründet ist. Auch diese Möglichkeit sollte man in Betracht ziehen.

Diese Beträge erschienen zuerst im Mai und Juni 2014 auf netzpolitik.org, wo sich auch zwei weitere Kommentare von Leonhard Dobusch und Rigo Wenning nachlesen lassen.

Joe McNamee ist Direktor von European Digital Rights (EDRi).

Jan Schallaböck forscht beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zu Identitätsmanagement- und Datenschutztechnologien im Rahmen nationaler und internationaler Forschungskonsortien und -netzwerke.

Thomas Stadler ist Fachanwalt für IT-Recht.

29 #Icebucketchallenge: Soziales Groß-Experiment in Sachen Selbstdarstellung

von **Julius Endert**

Sozial- und Netzwissenschaftler oder Psychologen müssen zur Zeit wohl abwechselnd staunen und jubeln. Die Ice Bucket Challenge ist quasi ein unverlangt angelegtes Großexperiment zur Psychologie des Menschen unter besonderer Berücksichtigung von Netzwerkmechaniken. Sie liefert so viele Erkenntnisse über das Verhalten der teilnehmenden Probanden und die Funktionsweise von Netzen, dass man gar nicht weiß, wo man mit der Auswertung anfangen sollte.

Anlass zur vermeintlich uneigennützigen Selbstdarstellung

Vielleicht ist es so: Der vernetzte Mensch pflegt die fortwährende Selbstdarstellung in den Netzen (der Autor nimmt sich da nicht aus, nicht zuletzt durch diesen Eintrag) und fühlt sich doch nie so ganz wohl dabei. Darf man, soll man seine vernetzten Mitmenschen dauernd mit persönlichem Scheiß belästigen? Andererseits: Man muss es ja – wie sonst würde man noch als relevant wahrgenommen werden?

Und dann kommen da diese ALS-Leute daher, bieten ein emotionales Thema und diesen nicht mehr kritisierbaren Anlass zu einer ebensolchen Präsentation im Netz – und nicht nur das: Durch den geschickt eingebauten Schneeball-Effekt der Nominierung – ein Teilnehmer nominiert drei neue – gibt es gleich doppelte Absolution für das eigene Posen und Posten. Man ist regelrecht gezwungen, bei dem Eiswassertreiben mitzumachen – dicke Gänsefüßchen bei gezwungen. Weil: Man tut es ja nicht für sich selbst, sondern für die gute Sache eines Dritten. Und selbst die, die sonst im Netz nicht ständig posten, bloggen, twittern, haben endlich einen Grund, hier (erstmalig) aufzuspringen. Das ist einfach perfekt – vielleicht zu perfekt. Dazu unten mehr.

Doch ein Eimer mit Eiswasser ist nicht ein Eimer voller Eiswasser. Die Prozedur bietet eine fast nicht für möglich zu haltende Variationsbreite an Differenzierungs- und eben Selbstdarstellungsmöglichkeiten. Das eigene Profil kann in Richtung Gutmensch geschärft werden. Gleichzeitig bilden sich durch das Kübeln mit Eis vorhandene Netzwerkstrukturen der Teilnehmer ab, was vielleicht die interessanteste Beobachtung sein dürfte.

Mein linker Platz ist leer, da wünsche ich mir den/die XY her

Da sind beispielsweise die Eiswassergießer, die Englisch sprechen, wie Herr Steingart, Chef der Verlagsgruppe Handelsblatt[1]. Er richtet sich, seiner Funktion und Natur gemäß, an ein größeres Publikum. Als Ausweis des persönlichen Status und der eigenen Gruppenzugehörigkeit dienen die Personen, die man sich zu nominieren traut – wie Frau Meckel, bald Chefredakteurin der Wirtschaftswoche[2], die dann standesgemäß mit Frau von der Leyen eine Ministerin nominiert – wichtige Frau nominiert sehr wichtige Frau.

Eine (kleine) Stichprobe ergibt: Die Netzwerkkreise bleiben geschlossen, Ausbrechen aus den eigenen Kreisen nach unten oder oben kommt nicht vor. Allenfalls gibt es leichte Abweichungen, wie im Fall Chefredakteurin / Ministerin. Es ist ein wenig wie früher im Kindergarten: Mein linker Platz ist leer, da wünsche ich mir XY her. Das war schon für die Kindergärtnerin (oder den Gärtner) sehr aufschlussreich. Und wer nicht herbeigewünscht oder nominiert wurde, der schaute eben traurig aus der Wäsche – so wie die Kollegen von handelsblatt.com[3], die sich folgerichtig selbst nominieren, damit sie auch ein wenig vom viralen Hype abbekommen, Netzverständnis bekunden können und sich vor allem – nämlich auf ihrer Webseite – in eine Reihe mit Bill Gates, Kai Diekmann und George W. Bush stellen können (war das nicht der, dem wir jetzt die Lage im Irak zu verdanken haben?).

So lässt sich aus den Nominierungen und Handlungen vor der Kamera ein sehr präzises Bild der bestehenden Netzwerke und handelnden Personen nachzeichnen. Viele von ihnen werden erstmalig vor der Kamera gestanden haben. Man sieht es ihnen an.

Verschwundene Eiswürfel

Aber die Chance, dies zu tun, weil ohne vordergründiges Eigeninteresse, ist einfach zu verlockend. Wenn man dann wie Herr Müller von Blumencron[4] theatralisch noch ein paar eiskalte Eiswürfel in seinen Eimer packt ("This has to be really cold!") – die man aber im geschnittenen Video selbst in der Zeitlupe nicht mehr erkennen kann –, wird das Ganze vollends als Schauspiel entlarvt. Natürlich darf man ihn nicht kritisieren (und vielleicht tue ich ihm Unrecht), weil er im Video davon spricht, dass seine Mutter vor 20 Jahren an der Krankheit gestorben sei.

Was uns das lehrt? Sicher, dass Wohltätigkeit dann am besten funktioniert, wenn sich beide Seiten davon einen Gewinn versprechen. Schon mit Plaketten beschriftete Parkbänke zeugen davon, dass man als Spender auch gesehen und erkannt werden möchte. Doch viel mehr lernt man über den Wert von Persönlichkeit im Netz und die Attribute, die wir dieser durch eine derartige Aktion hinzufügen können – und was wir bereit sind, dafür zu tun.

Aufschaukelungseffekte

Mehr noch lernt man über das Funktionieren von Netzwerken und Verstärkungseffekte. Denn die Verbreitung hängt nicht nur mit dem guten Zweck und dem System der Nominierungen zusammen, sondern auch mit dem Umstand, dass viele der Nominierten selbst dicke Netzwerkknoten sind. Sie konnten den Schneeball wirkungsvoll weiterrollen, bis schließlich die Medien wegen der Relevanz dieser Persönlichkeiten an der Relevanz des Themas nicht mehr vorbeikamen.

Schlussendlich wurden so auch hochrangige Unternehmer und Politiker legitimiert, eine Handlung vor einer Kamera und der Netzöffentlichkeit zu vollziehen, die sie sicher noch kurz vorher unter Androhung von Strafe von sich gewiesen hätten. Wie mittlerweile die ganze Welt erfasst wurde, zeigt eine geogetaggte Visualisierung der Tweets, die #icebucketchallenge beinhalten[5], sehr eindrucksvoll.

Shareability

Zugleich erfüllen die Videos ganz im Sinnes von YouTube das Merkmal der sogenannten Shareability: Sie sind kurz, bisweilen lustig, zeigen eine ungewöhnliche Handlung, appellieren zugleich an unsere Gefühle und sind mit einem *Call to Action* verbunden. Das reicht aus, um bei vielen Nutzern den Reflex des Teilens und Empfehlens auszulösen. Die sogenannte Challenge ist so in sehr kurzer Zeit zum Meme geworden, ist mutiert, hat sich verselbstständigt und eine eigene Richtung genommen, die nur noch begrenzt mit der Ursprungsidee zu tun hat.

Vielleicht ist #icebucketchallenge bezogen auf das Thema ALS auch längst ins Gegenteil gekippt – und irgendwie aus dem Ruder gelaufen, weil es zu gut auf die Netzwerkmechanismen aufsetzt (und das, was laut Peter Kruse in den Netzen resonanzfähig ist). Jedenfalls ist der Netzwerkeffekt erstmalig in der Elite der Gesellschaft angekommen und damit ein Beleg, dass nun auch diese Schichten "mit drin hängen", bzw. sich nicht mehr entziehen wollen oder können, wenn im Netz ein Meme die Runde macht. Es ist nach meiner Kenntnis nach Kony 2012 erst der zweite Fall einer derartigen Aufschaukelung.

Hoffentlich bleibt es bei den guten Zwecken, hier gibt es ein wahrlich unerschöpfliches Betätigungsfeld: Man stelle sich vor, diese Art der Solidarität würde für Frieden in Gaza oder in der Ukraine genutzt. Auf sozialpsychologische Studien bin ich gespannt.

Dieser Beitrag erschien zuerst auf navigarenecesseest.wordpress.com.

Anmerkungen

[1] http://www.handelsblatt.com/video/video-news/panorama/handelsblatt-herausgeber-gabor-steingart-nimmt-nominierung-an-gabor-steingart-nimmt-ice-bucket-challenge-an/10366596.html

[2] http://youtu.be/KVjWIopVMq4

[3] http://www.handelsblatt.com/panorama/aus-aller-welt/promi-dusche-mit-eiswasser-stefan-menzel/10369302-11.html

[4] http://youtu.be/o25jK5RXbcE

[5] http://srogers.cartodb.com/viz/89e638ac-2a2c-11e4-9cb7-0e73339ffa50/embed_map

Julius Endert ist freier Journalist und Autor und koordiniert das Hyperlandblog im Auftrag von heute.de. Er ist Inhaber der Journalisten-Agentur Netz-Lloyd GmbH und aktiver Gesellschafter der European Web Video Academy.

30 Waffen und Brüste: Kultureller Imperialismus und die Regulierung von Sprache auf kommerziellen Plattformen

von **Jillian C. York**

Als die Starkomikerin Chelsea Handler ein Statement über den russischen Präsidenten Vladimir Putin setzen wollte, wählte sie ihr Markenzeichen – direkte Komik – und bestieg oben ohne ein Pferd, um sich über die Angeberei des autoritären Führers lustig zu machen. Sie postete ein Foto des Stunts auf Instagram, einer Photo-Sharing-Plattform, die Facebook gehört. Es hatte die Überschrift: „Egal was ein Mann tun kann, eine Frau hat das Recht, es besser zu machen."

Beinahe sofort wurde das Bild aus dem Netz genommen und Handler bekam mitgeteilt, dass ihr Posting gegen Instagrams Community-Regeln verstoßen habe. „Denke daran, dass unsere Community sehr verschieden ist und dass deine Postings auch von 13-Jährigen gesehen werden", besagen die Regeln. „Wir respektieren die künstlerische Integrität von Fotos und Videos, aber unser Produkt und dessen Inhalte müssen mit den Kriterien für Nacktheit und Inhalten für Erwachsene übereinstimmen. In anderen Worten: Bitte poste keinerlei Nacktheit oder Inhalte für Erwachsene."

Handler antwortete und wies dabei darauf hin, dass diese Regeln sexistisch seien und sie drohte damit, Instagram zu verlassen. Wie viele zuvor entdeckte sie eine der großen Einschränkungen der Meinungsfreiheit in den Zeiten von Social Media: Instagram, im Gegensatz zu den meisten anderen „Rathausplätzen", ist in Privatbesitz.

Plattformen von Unternehmen haben in vielerlei Hinsicht die Rolle des Rathausplatzes oder des öffentlichen Raums übernommen. Es sind Orte, an denen Menschen sich versammeln, um Neuigkeiten zu diskutieren, über Politik zu reden und mit anderen Ähnlichdenkenden in Verbindung zu treten. Doch, wie in modernen Einkaufszentren, sind das private – nicht öffentliche – Räume und sie werden auch so reguliert. Entscheidungsträgerinnen und -träger aus Unternehmen setzen Beschränkungen auf diesen Plattformen durch, die Meinungsfreiheit und Privatsphäre behindern.

Obwohl Inhaltsbeschränkungen sich von Plattform zu Plattforum unterscheiden, sind die Mechanismen zur Überwachung und Entfernung von Postings oder Nutzerkonten ziemlich ähnlich. Die meisten Plattformen verlassen sich auf Nutzerberichte: Das heißt, eine Nutzerin oder ein Nutzer sieht Inhalte, die sie oder er un-

angemessen findet und nutzt das Meldungstool der Plattform, das eine Nachricht an die Aufsicht des Unternehmens sendet. Der unerwünschte Inhalt wird dann noch einmal betrachtet und entfernt, wenn man zu dem Ergebnis kommt, dass er gegen die Allgemeinen Geschäftsbedingungen oder die Community-Regeln verstößt.

In Handlers Fall war die Sache klar: Nacktheit ist auf Instagram streng verboten. Aber es gibt noch eine Menge anderer Beispiele. Beispiele, bei denen der fragliche Inhalt sozial oder politisch schwierig oder kontrovers war und die Grenze von der Prüfperson, die den Bericht bekommen hat, so oder anders gezogen hätte werden können. Noch schlimmer ist, dass manchmal Inhalt entfernt wird, der ganz offensichtlich nicht gegen Regeln verstoßen hat. Es bleiben dann dem Nutzer oder der Nutzerin nur wenige Möglichkeiten, zu widersprechen und die Abläufe des Unternehmens infrage zu stellen.

Nehmen wir zum Beispiel eine andere Geschichte, in der Instagram eine Rolle spielt. Eine Frau mit größerem Körperumfang postete Bilder von sich in Unterwäsche auf der Plattform und bekam kurz darauf mit, dass ihr gesamtes Nutzerkonto gelöscht worden war. Nur nach beträchtlicher Medienaufmerksamkeit entschuldigte sich Instagram für die Situation und reaktivierte das Nutzerkonto. Dabei wiesen sie darauf hin, dass sie „manchmal einen Fehler" bei der Einschätzung von Inhalt machen.

Nicht nur die Falschanwendung von Regeln ist das Problem, oft ist es die Regulierung an sich

Social-Media-Plattformen aus den USA – wie YouTube, Google, Twitter und Instagram – sind durch Abschnitt 230 des US Communications Decency Act von Haftung ausgenommen[1]. Das bedeutet, dass jeglicher Online-Zwischenanbieter, der Meinungsinhalte hostet, nicht rechtlich für nutzergenerierte Inhalte haftbar gemacht werden kann, mit einigen strafrechtlichen Ausnahmen. Im Wesentlichen ermöglicht das Unternehmen, eine Plattform für kontroverse Meinungen bieten zu können und gibt ihnen rechtliche Rahmenbedingungen, die freie Meinungsäußerungen fördern. Aber gleichzeitig ermöglicht Abschnitt 230 es diesen Plattformen auch, den Charakter ihrer Dienste selbst zu bestimmen. In anderen Worten:

Es besteht keinerlei Verpflichtung, sich für freie Meinungsäußerung einzusetzen.

Dennoch nutzen die zuvor genannten Plattformen oft den rhetorischen Begriff der Meinungsfreiheit, um ihre Produkte zu bewerben. Twitters CEO Dick Costolo hat das Unternehmen als „Meinungsfreiheitsflügel der Meinungsfreiheitspartei" bezeichnet. Facebook brüstete sich stolz mit seiner Rolle im Arabischen Frühling. Währenddessen sind diese Unternehmen zunehmend zu Zensoren geworden. Sie verbannen eine ganze Reihe von Inhalten, von Gewalt bis Nacktheit. Während sich das in ihrem Handlungsspielraum befindet, sind die globalen Implikationen

großer US-Plattformen, die in die Rolle eines Zensors schlüpfen, noch weitgehend unerforscht.

Exportieren amerikanischer Werte durch Inhaltsregulierung

In den Vereinigten Staaten gibt es eine klare Doppelmoral, wenn es um Gewalt und Sex in den Medien geht. Gewalt hält sich im Massenfernsehen. Dort belegt eine ganze Reihe gewalttätiger Programme – von CSI („Crime Scene Investigation") bis The Blacklist (über einen Kriminellen, der sich dem FBI anschließt) – regelmäßig Spitzenplätze bei den beliebtesten Fernsehsendungen. Gleichzeitig wurde die Darstellung von Sexualität schon immer strenger reguliert.

Die Telekommunikationsbehörde der USA beispielsweise beschränkt die Ausstrahlung von „unanständigen" Sendungen auf die späte Nacht und definiert sie als „Sprache oder Material, das Sexual- oder Ausscheidungsorgane oder -aktivitäten darstellt oder beschreibt, in Begriffen, die offenkundig anstößig sind, folgend den gegenwärtigen Gemeinschaftsstandards für das Sendemedium." Obwohl Nacktheit nicht explizit erwähnt wird, wurden die vagen Formulierungen oft so interpretiert, dass auch nicht-sexuelle Inhalte als „anstößig" galten.

Auf ähnliche Art wurde auch das Filmbewertungssystem der Motion Picture Association of America (MPAA), einer undurchsichtig geführten Handelsorganisation, für seine Doppelmoral hinsichtlich Nacktheit und Gewalt kritisiert. Wie die feministische Autorin Soraya Chemaly treffend beschrieb:

> Es ist ein ernsthaftes Problem, dass Menschen mit ihren 14-jährigen Kindern in R-gerankte[2] Filme gehen können, in denen Enthauptungen, abgetrennte Organe, blutige Körper, Vergewaltigungen und Schlimmeres gezeigt werden, aber nicht in einen Film, der zwei Frauen zeigt, die Spaß am gemeinsamen Sex haben.[3]

This Film Is Not Yet Rated, eine Dokumentation von 2006, beschäftigt sich direkt mit diesem Problem und weist auf bestimmte Filme und ihre Wertungen hin. Daraus wird klar, wie Gewaltdarstellungen im Allgemeinen Bewertungen als jugendgeeignet erhalten während Filme, die nackte Haut und Sex beinhalten, erwachsenen Zuschauerinnen und Zuschauern vorbehalten bleiben. Obwohl die MPAA die allgemeinen Bedenken bezüglich ihres Systems betreffend Sex und Gewalt adressiert hat, beziehen sie sich dabei lediglich auf die Bedürfnisse anonymer Massen amerikanischer Eltern, mit denen sie angeblich in Kontakt stünden.

Unglücklicherweise spiegeln sich diese Standards in den Regeln und Praktiken der weltweit beliebtesten sozialen Netzwerke wieder. Obwohl Facebooks Community Standards mit einer Erklärung beginnen, dass die Regeln dazu da sind, um „die Bedürfnisse und Interessen einer globalen Bevölkerung in Einklang zu bringen", könnte der Umgang mit Gewalt und Sex auf der Plattform nicht widersprüchlicher dazu sein.

Die Community Standards „schränken die Darstellung von Nacktheit ein". Der Abschnitt zu Gewalt und Bedrohungen hingegen bezieht sich auf terroristische Vereinigungen und gewalttätige Straftaten, aber nicht auf das Zeigen oder Teilen von Bildern und Videos mit Gewaltdarstellungen, egal ob real oder fiktiv. Grafische (Gewalt-)Darstellungen werden in einem späteren Abschnitt behandelt, der besagt, dass „Menschen ihre Zuschauer vor der Art der Videoinhalte warnen sollten, damit die Zuschauer eine bewusste Entscheidung treffen können, ob sie diese sehen wollen oder nicht."

Und so zieren Videos von Enthauptungen in Syrien die Feeds von Nutzerinnen und Nutzern und Seiten, die automatische Waffen verherrlichen, bleiben erreichbar, währenddessen ein geschmackvolles Bild eines Aktmodels wahrscheinlich offline genommen würde. Praktisch bedeutet das – trotz Facebooks Beteuerungen von Ausnahmen für „Inhalte mit persönlicher Relevanz", wie Familienfotos mit Bildern von stillenden Müttern – , dass hin und wieder Malereien mit nackten Personen, ein *New Yorker*-Cartoon, der Brustwarzen zeigt, und Bilder von Frauen, die stolz die Narben ihrer Brustamputation präsentieren, von der Plattform entfernt wurden.

Es wurde damit argumentiert, dass populäre soziale Netzwerke amerikanische Werte wie Meinungsfreiheit und Offenheit exportieren. Sie exportieren auch diejenigen amerikanischen Normen und Werte, die ein gutes Gefühl bei Gewalt und ein Unbehagen beim menschlichen Körper mitbringen. Die Befürworter dieses Exportkonzeptes weisen darauf hin, dass die Unternehmen unter dem Strich positive Auswirkungen auf die Meinungsfreiheit in Ländern mit strengen Regierungsbeschränkungen haben. Sie zeigen immer nur auf Fälle, in denen Aktivisten und Aktivistinnen ihre Plattformen für gemeinsame Aktionen genutzt haben und argumentieren, dass diese nur durch die Existenz ihrer Seite möglich gewesen seien. Die Gegnerinnen und Gegner bringen an, dass eine derartige Einmischung die staatliche Souveränität verletze und sind angeekelt von der Dreistigkeit, mit der US-Unternehmen sich das Recht nehmen, zu bestimmen, was anderswo angemessen ist.

Es wird nur selten erwähnt: Die Räume, in denen ein großer Teil der Welt täglich öffentlich diskutiert, sind den Launen privater Unternehmen unterworfen, die von primär weißen, primär der Oberschicht angehörigen, primär amerikanischen Männern besessen und geführt werden. Berichte zum Stand der Vielfalt in den letzten Monaten zeigen das ganz klar: Facebooks Angestellte sind zu 69 Prozent männlich, zu 57 Prozent weiß. Bei Google sind 70 Prozent männlich und 61 Prozent weiß. Twitter ist ebenfalls zu 70 Prozent männlich und 59 Prozent weiß. Diese demografischen Eigenschaften sollten nicht unberücksichtigt bleiben.

Diejenigen Personen an der Spitze dieser Unternehmen haben die Aufgabe, Normen und Abläufe zu bestimmen, die den Großteil unserer täglichen Online-Konversation regeln.

Deshalb ist es nicht einfach eine Frage des Exports amerikanischer Werte, sondern der Werte dieser spezifischen Bevölkerungsgruppe. Im Wesentlichen bestimmt genau diese Gruppe an Menschen die amerikanischen Werte für die Milliarden an Nutzerinnen und Nutzer sozialer Medien, die ihnen sonst kaum begegnet wären. Der nicht hinterfragte Transfer überalterter Mediennormen in die digitale Welt, zusammen mit der Dominanz einer gewissen Klasse innerhalb der Unternehmen, macht eine neue Definition von „Online-Freiheit" notwendig.

Die Unterstützung spezieller Interessen

Obwohl die Regeln und Abläufe auf Unternehmensplattformen von den Unternehmen selbst festgelegt werden, gibt es deutlichen Einfluss von externen Akteuren, seien es Lobbyisten, Nichtregierungsorganisationen oder Regierungen. Diese Akteure haben spezielle Sichtweisen zur Rolle von Unternehmen in der Meinungsregulierung und versuchen Regeln so zu beeinflussen, dass es manchmal um kaum mehr als Eigeninteressen geht.

Zum Beispiel haben im letzten Jahr europäische Regierungen versucht, proaktiv terroristische Inhalte in sozialen Netzwerken zu zensieren. Organisationen für Meinungsfreiheit und Bürgerrechte lobbyieren regelmäßig Unternehmen, damit sie Meinungsfreiheit schützen. Zur selben Zeit hat sich Twitter mit Women, Action & the Media (WAM) zusammengetan, um „bestätigte Berichte (von Belästigungen) an Twitter heranzutragen und die Antworten Twitters auf verschiedene Arten genderbezogener Belästigung nachzuverfolgen."[4]

Die letztere Maßnahme wurde für den Versuch gelobt, das Problem der Belästigung von Frauen in sozialen Netzwerken zu lösen. Kritik an dem Plan kam primär von Konservativen, die WAM als feministische Interessensvertretung sehen, die versucht, anti-feministische Meinungen zu zensieren.

Auch wenn diese Kritik zweifellos überzogen ist, lohnt es sich doch, die Idee von Interessensvertretungen – die in Beziehung mit Unternehmen stehen, um Inhalte zu regulieren – näher zu beleuchten. Und WAM ist bei Weitem nicht die einzige Gruppe dieser Art. Die Anti-Defamation League (ADL), die sich selbst als jüdische NGO beschreibt, die „Antisemitismus und alle Formen von Gottlosigkeit" bekämpft und „demokratische Ideale"[5] verteidigt, hat ebenso die Regeln von Unternehmen beeinflusst. Allen voran überzeugten sie Google davon, ein Top-Suchergebnis für das Wort „Jude" zu setzen, das die abwertenden Gebrauchsarten des Wortes erklärt. Vor Kurzem traf die Gruppe eine Vereinbarung mit Twitter, Facebook, Google und Microsoft, um „strengere Sanktionen" gegen diejenigen durchzusetzen, die beleidigende Botschaften posten.

Diese Maßnahmen allein mögen nicht von Natur aus problematisch sein, aber die ADL hat eine Historie, Zensur und Spezialinteressen zu fördern. Die Gruppe hat sich prominent gegen die Errichtung einer Moschee in Lower Manhattan ausgesprochen, da sie sich zu nah am früheren World Trade Center befunden hätte.

Letztes Jahr hat eine Lokalgruppe der Organisation ein Museum dazu gebracht, eine Ausstellung mit Kinderkunstwerken aus Gaza zu schließen. Die Organisation trat auch als Unterstützerin einer kontroversen Werbekampagne auf, die Muslime als „Wilde" bezeichnet. Mit einer derartigen Historie ist es schwer zu glauben, dass die ADL sich als ehrlicher Akteur in Verhandlungen mit Social Media Unternehmen verhalten wird.

In der Zwischenzeit treffen Interessensgemeinschaften aus anderen Teilen der Welt oft auf verschlossene Türen. Ein kürzlich veröffentlichter Bericht von Facebook zeigte, dass das Unternehmen Tausende Inhalte auf Anfrage der pakistanischen Strafverfolgungsbehörden offline genommen hatte, obwohl pakistanische Bürgerrechtsgruppen sich dagegen ausgesprochen hatten. In ähnlicher Weise blieben Fragen von Aktivistinnen und Aktivisten weltweit unbeantwortet, inwieweit das Unternehmen mit der NSA zusammenarbeitet. Die Möglichkeit, Einfluss zu nehmen, ist typischerweise US-Unternehmen vorbehalten.

Auch wenn die Einbeziehung von Interessensgemeinschaften in den Regelungsprozess in vielen Fällen Bedenken über demografische Strukturen innerhalb der Unternehmen lindern kann, darf man das Risiko von unangebrachtem Einfluss auf derartige Regelungen nicht unterschätzen – vor allem, wenn Einfluss hinter verschlossenen Türen geltend gemacht wird. Es verdient nähere Betrachtung. Und da private Regulierung im Wettbewerb mit Regierungsbeschränkungen von Redefreiheit steht – und sie manchmal übertrifft – sind derartige Räume zunehmend ein Schlachtfeld für Meinungsfreiheitsaktivistinnen und -aktivisten und den Befürworterinnen und Befürwortern stärkerer Regulierung gleichzeitig.

Verantwortung gegenüber den Nutzerinnen und Nutzern

Zu häufig werden Argumente, die eine genauere Prüfung von unternehmensseitiger Regulierung befürworten mit „Das Recht auf Meinungsfreiheit gilt hier nicht!" niedergebrüllt. Dieses Gegenargument, das von Laien und Entscheidungsträgerinnen und -trägern in Unternehmen gleichermaßen vorgebracht wird, geht in die Richtung, die Diskussion über den Einfluss von unternehmensseitiger Regulierung auf unsere Meinung einfach abzubrechen.

Und auch wenn hier tatsächlich das Recht auf freie Meinungsäußerung in diesen Räumen nicht gilt, ist es unmöglich, den Effekt zu ignorieren, den Meinungsfreiheitsbeschränkung durch Unternehmen auf die Gesellschaft haben kann. Dazu muss man sich bloß die Größe der Plattformen ansehen: Facebook brüstet sich mit 864 Millionen täglichen Nutzerinnen und Nutzern, 82 Prozent davon befinden sich außerhalb der USA und Kanada.

284 Millionen Menschen weltweit – 77 Prozent nicht in den USA – nutzen Twitter zumindest monatlich. Instagram hat 200 Millionen aktive Nutzerinnen und Nutzer im Monat, von denen sich 65 Prozent außerhalb der USA befinden. Und die Liste lässt sich fortsetzen.

Der Einfluss dieser Plattformen kann nicht bestritten werden: Von den Aufständen in der arabischen Welt bis hin zu den gegenwärtigen Protesten in Ferguson, Missouri, haben sich soziale Medien als wichtiges Werkzeug politischer Beteiligung, Protest und Bürgerbeteiligung herausgestellt. Ihre Rolle für künstlerischen und persönlichen Ausdruck ist gleichermaßen wichtig. Wo Räume öffentlicher Interaktion zunehmend privatisiert werden, werden Meinungen, die bereits jetzt als Randmeinung wahrgenommen werden, zunehmend marginalisiert.

Jedes Mal wenn Unternehmensplattformen Inhalte zensieren – sei es aufgrund öffentlicher Aufforderung, Markt- oder Regierungsdruck – hat das einen abschreckenden Effekt für die Meinungsfreiheit. Ja, Facebook ist ein privates Unternehmen, aber es ist auch die größte gemeinsame Meinungsplattform, die es je auf der Welt gab. Und es ist an der Zeit, dass wir uns der zusätzlichen Verantwortung zuwenden, die solch ein Privileg mit sich bringt.

Anmerkungen

[1] http://www.law.cornell.edu/uscode/text/47/230

[2] Anm. der Redaktion: Filme, die erst ab 18 Jahren zum eigenständigen Ansehen freigegeben sind.

[3] http://www.salon.com/2013/11/06/the_mpaas_backwards_logic_sex_is_dangerous_sexism_is_fine/

[4] http://www.womenactionmedia.org/2014/11/06/harassment-of-women-on-twitter-were-on-it/

[5] http://www.adl.org/about-adl/

Jillian C. York ist Direktorin für Internationale Meinungsfreiheit bei der Electronic Frontier Foundation. Sie arbeitet an der Schnittstelle von Technik und Policy mit einem Fokus auf der arabischen Welt. Sie hält oft Vorträge und schrieb bereits für die New York Times, Al Jazeera, den Guardian, Foreign Policy und CNN. Zusammen mit Katherine Maher macht sie die Webshow Interrobang.

31 Rechtsextremismus in Sozialen Netzwerken

von **Johannes Baldauf**

In netzpolitischen Fragen spielt der Umgang mit Hate Speech bisher noch eine untergeordnete Rolle. Nur langsam findet eine Debatte über den Umgang mit menschenverachtenden Inhalten im digitalen Raum ihren Weg in die öffentliche Wahrnehmung. Dabei handelt es sich keineswegs um ein neues Phänomen. Dies gilt insbesondere, wenn es um Rechtsextremismus geht. Denn das Internet ist für Rechtsextreme das Propagandamedium Nummer eins. Führende Köpfe hatten das Potential des Mediums früh erkannt, sodass rechtsextreme Aktivitäten schon in Mailboxsystemen, dem Usenet und später mit diversen Domains im WWW verzeichnet werden konnten. Entsprechend stellen rechtsextreme Inhalte in Sozialen Netzwerken kein neues Phänomen dar, sondern lediglich die Anpassung an die aktuellen Gegebenheiten und Möglichkeiten des Mediums.

Neben Propagandazwecken werden Soziale Netzwerke zur Rekrutierung und Mobilisierung der AnhängerInnenschaft genutzt, aber auch zur Einschüchterung von GegnerInnen. Plattformen wie Facebook, YouTube, Twitter oder auch VK werden zu verschiedenen Zwecken genutzt. Dort wird Propaganda bereitgestellt, GegnerInnen bloßgestellt und eingeschüchtert und neue AnhängerInnen mobilisiert. Jede moderne rechtsextreme Kampagne bzw. Bewegung hat heutzutage eine starke Netzanbindung. Die Zahl rechtsextremer Social-Media-Angebote steigt jährlich und die Bandbreite ist groß, wie einige Beispiele der letzten Jahre verdeutlichen:

Im Mai 2011 kursierte das Video eines nächtlichen Fackelumzugs von mehreren Dutzend weiß maskierten Menschen im Netz – das Phänomen der „Unsterblichen" betrat die Bühne der Öffentlichkeit. Da der nächtliche Fackelumzug in einer sächsischen Kleinstadt naturgemäß wenig bis gar keine Öffentlichkeit mit sich bringt, wurde der Aufmarsch auf Video aufgenommen und mit dramatischer Musik unterlegt.

Aus einer einzelnen Aktion wurde innerhalb der rechtsextremen Szene ein virales Phänomen, das europaweit noch heute NachahmerInnen findet. Inhaltlich stellt das Phänomen lediglich eine Neubearbeitung der rechtsextremen Volkstod-Kampagne dar, nach der „die Deutschen" aussterben würden, weil sie statistisch gesehen weniger Kinder bekommen als Menschen, die als nicht-deutsch angesehen werden. Doch die popkulturellen Anleihen – Flashmobs, „The Matrix", Guy-Fawkes-Masken, Musik aus dem „Herr der Ringe"-Trailer – lassen die „Die

Unsterblichen“ innovativ und besonders für Jugendliche attraktiv wirken. Eine moderne Webseite, gut geschnittene und vertonte Videos: Die „Unsterblichen“ verdanken ihren Erfolg dem Netz und bilden damit exemplarisch den Prototyp moderner rechtsextremer Kampagnen. Doch nicht nur der traditionelle Rechtsextremismus nutzt das Netz geschickt. Auch der modernisierte Rechtsextremismus weiß um die Macht und Reichweite des Internets:

Im November 2012 trat die Identitäre Bewegung Deutschland, das deutsche Pendant zur französischen Generation Identitaire, an die Öffentlichkeit. Wieder war es ein Video, welches tausende Nutzer erreichte. Zeitgleich wurden diverse Seiten auf Facebook eröffnet und eine breit angelegte Kampagne gestartet. Das Ziel der Identitären Bewegung: die Gründung einer neuen Jugendbewegung und das mithilfe des Internets, speziell der Sozialen Netzwerke. In diesem Video formuliert die Gruppe ihr Hauptanliegen: eine Kampfansage an die „Herrschaft des Multikulti-Wahns“. Multikulturalismus sei schuld an der „Überfremdung“ bzw. der „Islamisierung“, welche Europa zu zerstören drohe.

Dieses Manifest wird im Video sehr eindringlich von verschiedenen jungen Menschen vorgetragen, womit eine weitere Botschaft unterstrichen wird: Die Politik habe durch den „Multikulti-Wahn“ die europäische Kultur, die Identität verkauft. Die Jugend aber, denn aus ihr komme die Identitäre Bewegung und an diese wolle sie sich richten, besinne sich nun auf die europäische Kultur und kämpfe gegen die „Islamisierung“ und für die eigene Identität.

Dem Feindbild Islam und der Drohkulisse der „Islamisierung“ wird ein Europa gegenübergestellt, das frei von äußeren, „fremden“ Einflüssen sein soll, um so jeweils die „nationale Identität“ bewahren zu können. Dahinter verbirgt sich die Idee eines „Europa der Vaterländer“, also „Frankreich den Franzosen“ oder „Spanien den Spaniern“. Dieses Konzept des sogenannten Ethnopluralismus ist einer der ideologischen Kernpunkte der Neuen Rechten. Der Rassismus der traditionellen Rechtsextremen wird ersetzt durch einen kulturalisierten Rassismus. An die Stelle des Wortes „Rasse“ treten die Ersatzbegriffe „Ethnien“ und „Kultur“. Wenn also in diesem Kontext von Identität gesprochen wird, dann ist damit „kulturelle Identität“ gemeint. Bei der neuen Rechten ist dies gleichbedeutend mit der „nationalen Identität“, die durch Einflüsse von außen und den „Multikulturalismus“, gestört und bedroht werde. Schuld am „Multikulti-Wahn“ sei die 68er-Generation, die dadurch ebenfalls zum Feindbild aufsteigt.

Mit dieser Haltung steht die Identitäre Bewegung nicht allein da: Islamfeindliche Kampagnen rechtspopulistischer Bewegungen wie Pro Köln, Pro NRW und Die Freiheit sorgen seit Jahren für Schlagzeilen; auch die 2013 gegründete AfD versteigt sich zu ähnlichen Äußerungen. In den Niederlanden positioniert sich Geert Wilders auf diese Weise mit der Partij voor de Vrijheid, in der Schweiz die SVP, in Österreich die FPÖ. Auch finden sich europaweite Netzwerke, deren Kernthema die Islamfeindlichkeit darstellt. Hierzu gehören Zusammenschlüsse wie Ci-

ties against Islamisation und die Defense League Bewegung. Spätestens seit dem Erfolg von Thilo Sarrazins Buch „Deutschland schafft sich ab“ wurde klar, dass islamfeindliche Parolen nicht nur ein Thema des rechtsextremen Lagers darstellen, sondern entsprechende Ängste und Vorurteile in der Gesellschaft weit verbreitet und anschlussfähig sind. In diesem Kontext wirken aktuelle Phänomene wie HoGeSa (Hooligans gegen Salafisten) oder PEGIDA (Patriotische Europäer gegen die Islamisierung des Abendlandes) nicht überraschend und verdeutlichen den Versuch, durch einen modernisierten Rechtsextremismus massentauglicher werden zu wollen.

Diese Massentauglichkeit ist vor allem dann noch einfacher zu erreichen, wenn auf Bezüge zum traditionellen Rechtsextremismus verzichtet wird. Auch hier dient die Identitäre Bewegung als Beispiel: Dies beginnt beim Symbol und den Farben der Bewegung. Als Symbol wurde der griechische Buchstabe Lambda gewählt, der auch das Zeichen der spartanischen Hopliten im antiken Griechenland war. In der Schlacht bei den Thermopylen 480 v. Ch. sollen die Hopliten eine entscheidende Rolle gespielt und die persische Armee lange in ihrem Vormarsch aufgehalten haben. Eine überspitzte Darstellung der von Herodot überlieferten Ereignisse findet sich in der Graphic-Novel-Serie „300“ von Frank Miller, die 2007 von Zack Snyder verfilmt wurde. Die Perser werden als dekadent und degeneriert, als eine nicht enden wollende Flut von Invasoren dargestellt. Dem gegenüber stehen die spartanischen Hopliten, die als reine, muskulöse, unbezwingbare und unerbittliche Krieger konträr zur persischen Streitmacht gezeichnet werden.

Snyders Filmadaption ist für das Selbstverständnis und die Selbstdarstellung der Identitären zentral. Die persische Streitmacht als Invasion aus dem Orient wird von ihnen als Analogie zu der befürchteten „Islamisierung“ Europas interpretiert; sich selbst verstehen die Identitären als spartanische Hopliten, die – der Analogie folgend – das Bollwerk gegen die „Islamisierung“ bilden.

Auch wenn durch historische Bezüge wie die spartanischen Hopliten intellektuelle Unterfütterung geboten wird, sind die Slogans der Identitären Bewegung eher jugendaffin und vordergründig simpel: „0 Prozent Rassismus – 100 Prozent Identität“ oder “Nicht rechts, nicht links – identitär“. Diese Slogans verdeutlichen den Versuch, die mit der rechtsextremen Etikettierung verbundene Tabuisierung zu umgehen, indem man sich rhetorisch von rassistischen Gruppen distanziert. Um das Identitätskonzept jugendaffin aufzubereiten, werden weitere popkulturelle Anleihen genommen. Neben „300“ wird auf „Avatar“ und die Ewoks aus „Star Wars“ verwiesen und die Lesart eines „Kulturkampfes“ gegen eine Invasion betont, die den Frieden und die Harmonie der eigenen Welt zu zerstören droht.

So wie sich die Identitäre Bewegung als spartanische Hopliten inszeniert, versucht auch die europaweit vernetzte Defense League sich das Image von Kriegern zu geben. Jedoch bezieht dieser Zusammenschluss seine Anleihen nicht aus der Antike, sondern findet sie im Bild des mittelalterlichen Kreuzritters. Auch der

norwegische Rechtsterrorist Anders Behring Breivik lehnt sich an das Selbstverständnis des Kreuzritters an, der gegen eine drohende „Islamisierung" Europas kämpft.

Auch bei der NPD ist die strategische Öffnung zur Mitte der Gesellschaft hin zu beobachten. Durch verschiedene Kampagnen, die jeweils mit eigenen Facebook-Seiten operieren, hat es die NPD geschafft, zu einer der erfolgreichsten Parteien auf Facebook zu werden. Mit über 110.00 Likes liegt sie deutlich vor den Volksparteien CDU und SPD. Noch deutlicher wird der Vorsprung, wenn es um die Viralität, also die Interaktion mit den bereitgestellten Inhalten geht Mittels breit angelegter Kampagnen erreicht die NPD auch Menschen, welche in der Offline-Welt eine direkte Nähe zur Partei eher scheuen würden. Dazu werden primär sehr emotional besetzte Themen genutzt: Die rechtsextreme Kampagne „Todesstrafe für Kinderschänder" findet sich auch auf Facebook, allerdings in der leichter verdaulichen Formulierung „Deutschland gegen Kindesmissbrauch". Über die reflexartige Zustimmung der NutzerInnen – denn wer ist schon für Kindesmissbrauch – gelingt es den Rechtsextremen dieses Thema im Web 2.0 zu platzieren und mit der eigenen Partei zu verknüpfen.

Die Taktik der Instrumentalisierung der Ängste der Menschen wird auch bei der seit dem Sommer 2013 laufenden Kampagne gegen Flüchtlingsunterkünfte angewendet. Im Zuge der bundesweiten Debatte über die Unterbringung von Asylsuchenden, gründeten sich in den Sozialen Netzwerken vermeintlich ehrlich besorgte BürgerInneninitiativen mit lokalem Bezug, wie beispielsweise „Nein zum Heim in Eisenhüttenstadt", „Bürgerbewegung Hellersdorf" oder „Schneeberg wehrt sich". Aktuell können über 70 derartiger Facebook-Seiten gezählt werden. Ein Vergleich der verschiedenen „Bürgerinitiativen" offenbart jedoch, dass sie kampagnenartig mit ähnlichen Logos und Slogans von der NPD orchestriert werden. Entsprechend der Kampagne gegen vermeintliche „Kinderschänder" gelingt es der Partei, online ein Klientel zu mobilisieren, welches quantitativ weit über den tatsächlichen WählerInnenzahlen und der Gruppe von direkten SympathisantInnen liegt.

Zumeist tritt die NPD dabei zunächst nicht direkt als offensichtliche Drahtzieherin auf den entsprechenden Seiten, Gruppen und Events auf. Dies führt dazu, dass sich mehr Menschen der populistischen Forderung vorschnell anschließen, da sie nicht durch die gesellschaftliche Tabuisierung der Neonazi-Partei abgeschreckt werden. Nach und nach werden dann jedoch auf den entsprechenden Seiten auch Inhalte der NPD verbreitet, die sich weiter in den Distributionskanälen des Netzwerkes, der Timeline, an die UserInnen verteilen.

Die Kampagnenseiten gegen Flüchtlingsheime und gegen Kindesmissbrauch stellen nur zwei Beispiele dar, die verdeutlichen sollen, wie die NPD eine so große Zustimmung in Sozialen Netzwerken generiert. Als Satellitenseiten eingesetzt, dienen sie dazu den Tabuisierungs-Reflex zu umgehen, den die NPD auslöst. Wei-

ter zeigen sie auch, dass die strategische Ausrichtung auf die Mobilisierung hin zur Mitte und Rekrutierung neuer Anhängerschaft ausgerichtet ist. Traditionelle Propaganda mit NS-Bezug wird nicht angeboten, auch weil Facebook entsprechende Inhalte deutlich stärker sanktioniert. Daher wenden sich geschlossene Kaderstrukturen als harter Kern des traditionellen Rechtsextremismus von populären Angeboten wie Facebook ab und ziehen sich auf Plattformen – wie beispielsweise dem russischen VK Netzwerk - zurück, die weniger stark im Fokus der Öffentlichkeit stehen.

Doch Rechtsextremismus und gruppenbezogene Menschenfeindlichkeit sind keine statischen Phänomene – sie entwickeln sich stetig weiter. Regelmäßig gibt es neue rechtsextreme Kampagnen und Strategien, die versuchen, die Ängste und Vorurteile der UserInnen zu instrumentalisieren. Diese Strategien sind, wie oben beschrieben, beeinflusst durch den gesellschaftlichen Konsens „gegen Nazis" zu sein.

Aber der Konsens sorgt auch dafür, dass das Problem Rechtsextremismus in personeller Hinsicht externalisiert („Nazis sind die Anderen") und die dahinter stehende Ideologie exotisiert wird („Das hat doch heute keine Bedeutung mehr"). Im digitalen Raum sind die Übergänge zu rechtsextremen Gedankengut jedoch fließend und eine effiziente Arbeit gegen Rechtsextremismus in diesem Bereich kann nur funktionieren, wenn über die Grenzen dessen hinausgegangen wird, was gemeinhin als rechtsextrem bezeichnet wird. Ausprägungen der Gruppenbezogenen Menschenfeindlichkeit, also zum Beispiel Antisemitismus, Homophobie, Sexismus und Rassismus, finden sich zwar unter dem Dach des Rechtsextremismus, sind aber auch jeweils unterschiedlich stark in der Gesellschaft verbreitet. Wenn sich der Rechtsextremismus jedoch stetig wandelt und gerade online eine Anschlussfähigkeit zur Mitte hin intendiert, dann besteht die praktische Arbeit gegen ihn aus mehr, als nur Hakenkreuze und Horst-Wessel-Lieder aus dem Netz zu entfernen. Rechtsextremismus darf grade im Netz nicht gesondert von anderen Hate-Speech-Phänomenen betrachtet werden.

Plattformbetreiber unterschätzen diese Gefahr, die Politik hat sie lange ignoriert und die Zivilgesellschaft versucht, sich mit „Bunt statt Braun"-Parolen des Problems anzunehmen. Dabei müssen die Lösungen so modern sein, wie es das Medium ist. Es wird deutlich, wie wichtig die stetige Beobachtung dieses Sektors ist, denn nur die Kenntnis solcher Phänomene und Entwicklungen befähigt uns und andere, entsprechende Antworten formulieren zu können.

Johannes Baldauf studierte Literaturwissenschaft, Jüdische Studien und Deutsch als Fremdsprache in Jena, Potsdam und Berlin. Seit 2008 beschäftigt er sich mit Rechtsextremismus, Antisemitismus und Verschwörungstheorien im Internet. Für die Amadeu Antonio Stiftung referiert er über Erscheinungsformen von Neonazis und wirkungsvolle Gegenstrategien in sozialen Netzwerken und koordiniert seit 2014 das Projekt no-nazi.net.

32 Die Hearings der neuen EU-Kommissare aus netzpolitischer Sicht

von **Angela Sobolciakova**

Zwischen dem 29. September und dem 7. Oktober fanden die Anhörungen der designierten Kommissare im Europäischen Parlament statt. Dies ist eine kurze Zusammenfassung der sechs Anhörungen, in denen die designierten Kommissare die Fragen der Abgeordneten des Europäischen Parlaments in Bezug auf digitale Rechte, Schutz der Privatsphäre und Handelsabkommen beantwortet haben.

Günther Oettinger (Deutschland) ist der Nominierte für digitale Wirtschaft und Gesellschaft. Cecilia Malmström (Schweden) wurde als designierte Kommissarin für Handel nominiert. Dimitris Avramopoulos (Griechenland) ist der designierte Kommissar für Migration und Inneres. Věra Jourová (Tschechische Republik) ist für die Position der Kommissarin für Justiz, Verbraucher und die Gleichstellung der Geschlechter nominiert. Andrus Ansip (Estland) will das Amt des Vize-Präsidenten für Digitalen Binnenmarkt übernehmen. Frans Timmermans (Niederlande) wird voraussichtlich erster Vize-Präsident und Kommissar für Regulierung, inter-institutionelle Beziehungen, Rechtsstaatlichkeit und die Charta der Grundrechte.

Günther Oettinger wurde zu den notwendigen Schritten für einen erfolgreichen Umgang mit Cloud Computing und dem Big-Data-Bereich befragt. Er antwortete, dass wir eine EU-weite Gesetzgebung für Cloud-Dienste bräuchten. Bei den Themen des „Rechts auf Vergessenwerden", der Vorratsdatenspeicherung und Verarbeitung blieb er strikt auf der Linie der bereits existierenden Kommissionspolitik. Er sagte, dass Daten nicht dauerhaft gespeichert werden sollten und Bürger Zugang zu den über sie gespeicherten Daten bekommen sollten. Das „Recht auf Vergessenwerden" biete seiner Aussage nach zusätzlichen Schutz. Er sieht es als Grundrecht an.

Schlagzeilen machte Oettinger, als er die Prominenten, die ihre sensiblen Daten in den kürzlich gehackten Cloud-Diensten gespeichert hatten, als dumm bezeichnete. Gleichzeitig lobte er Cloud-Dienste für ihre wirtschaftliche Effizienz und Umweltfreundlichkeit sowie für ihre Fähigkeit, „den Kunden maßgeschneiderte Produkte und Dienstleistungen bieten zu können".

Cecilia Malmström bezeichnete das transatlantische Freihandelsabkommen (TTIP) in ihrer Eröffnungsrede als die wichtigste Herausforderung der näheren

Zukunft. Die durch TTIP ermöglichten Streitbeilegungsverfahren zwischen Investoren und Staaten (ISDS) wurden ausgiebig erörtert. Malmström versprach, dass beide verhandelnden Seiten an einem Einverständnis inklusive ISDS sehr interessiert seien. Ausweichend erklärte Malmström, dass ISDS nicht zwangsweise in TTIP integriert werden müsse, wohingegen das ebenfalls geplante Freihandelsabkommen mit Kanada (CETA) ohne ISDS nicht zustande kommen werde. In diesem Falle würde sie ISDS unterstützen, während sie sich durchaus gewillt zeigte, dies im TTIP nicht zu tun. Sie wurde auch zu ihrer geheimen Diskussion mit der US-Regierung über eine unveröffentlichte Entwurfsfassung der EU-Datenschutzverordnung befragt, die es laut einer von EDRi publizierten E-Mail gegeben habe. Sie bestritt zunächst die Echtheit der „geleakten" E-Mail, die tatsächlich auf eine Anfrage im Namen der Informationsfreiheit herausgegeben worden war. Anschließend wurde sie aufgefordert, die Echtheit dieser E-Mail öffentlich anzuerkennen.

Dimitris Avramopoulos beantwortete die Fragen des Europäischen Parlaments zur Umsetzung des EuGH Urteils über Vorratsdatenspeicherung wie folgt: „In Ermangelung einer EU-Gesetzgebung ist eine Vorratsdatenspeicherung auf nationaler Ebene notwendig. Mitgliedstaaten können immer noch eine eigene, nationale Gesetzgebung zur Vorratsdatenspeicherung einführen, die sowohl der sogenannten E-Privacy-Richtlinie entspricht als auch den jeweils eigenen konstitutionellen Prinzipien." Der Verweis auf die E-Privacy-Richtlinie ist deshalb bedeutend, weil er zeigt, dass der Kommissionsabgeordnete bereit ist, die Position, dass Vorratsdatenspeicherung unter EU-Recht fällt, zu verteidigen. Avramopoulos musste sich auch den Fragen der Abgeordneten zur Gültigkeit des Fluggastdatenspeicherung (Passenger Name Record – kurz PNR) nach dem Gerichtsbeschluss zur Vorratsdatenspeicherung stellen. Er antwortete, dass Gerichtsbeschlüsse Voraussetzung für jede zukünftige politische Handlung seien. In Europa würden bald neue Entscheidungen gültig und sie sollten horizontal eingeführt werden.

Věra Jourová zählte die schnelle Einführung einer modernen EU-Datenschutzreform in den ersten sechs Monaten ihrer Amtszeit zu ihren Prioritäten. Auf die Fragen bezüglich eines „Regenschirm-Abkommens", also einem Datenaustausch mit den USA zur Strafverfolgung und Safe Harbor (einer Entscheidung über die allgemeinen Regeln dieses Datenaustausches) hob sie hervor, beide seien entscheidend, um das Vertrauen zwischen der EU und den USA wiederherzustellen. Die Bedingungen von Safe Harbor müssten allerdings wirklich sicher sein. Sie versprach, diese Themen zu analysieren und versicherte, den Schutz von Privatsphäre und Datensicherheit immer ernst zu nehmen.

Andrus Ansip will sich auf Datenschutz, die Regulierung von Telekommunikationsunternehmen und Cyber-Sicherheit konzentrieren, um so faire Wettbewerbsbedingungen für alle Unternehmen zu sichern. Außerdem betonte er die Bedeutung von E-Commerce und E-Government. Er sagte, dass Europas Binnenmarkt

noch nicht für das digitale Zeitalter bereit sei. Dennoch möchte er, dass nicht alles über die EU reguliert wird. Ansip versprach, auf die Urheberrechtsreform zu achten und Hindernisse für den grenzüberschreitenden Online-Handel abzubauen. Weiterhin versprach er die Einführung von E-Invoices (Elektronische Rechnungen) und E-Procurement in die EU-Kommission bis 2015 ebenso wie elektronische Unterschriften bis zum Ende seines Mandats. Auch Ansip verlangte Änderungen von Safe Harbor. Desweiteren fand er die Ausnahmen zur „nationalen Sicherheit" der USA darin beunruhigend und war bereit, das Abkommen aufzuheben, sollten die zukünftigen Verhandlungen mit den Vereinigten Staaten dahingehend keine zufriedenstellenden Resultate bringen. Ansip sprach sich auch gegen das Geoblocking von Online-Inhalten aus.

Frans Timmermans versprach ein starkes Engagement für die Achtung der Grundrechte. Er möchte als Kommissar für Grundrechte weiter gehen als sein bereits sehr aktiver und ehrgeiziger Vorgänger. Zudem will er ein verpflichtendes Register für Lobbyisten einführen. Ob er in der Lage ist, seine Vorhaben für Transparenz und Demokratie durchzusetzen und so das schreckliche Verhalten beim Zugang zu Dokumenten der scheidenden Kommission umzukehren, bleibt abzuwarten.

Dieser Beitrag erschien zuerst am 8. Oktober 2014 auf edri.org, die Übersetzung stammt von Justin Hanney. Mittlerweile haben alle der oben genannten designierten Kommissare ihr Amt angetreten.

Angela Sobolciakova war von September bis Dezember 2014 Praktikantin bei European Digital Rights (EDRi) in Brüssel. Zuvor studierte sie Rechtswissenschaften in der Slowakei und in Norwegen und arbeitete als Rechtsanwältin beim slowakischen Zentrum für Rechtshilfe.

33 Vom Internet der Dinge, algorithmischer Gesetzgebung und dem Ende der Politik

von **Kirsten Fiedler**

Das „Internet der Dinge" war in diesem Jahr ein viel gehypter Begriff, was an der wachsenden Erkenntnis liegen mag, dass es längst nicht mehr Science Fiction sondern allgegenwärtige Realität ist. Wir tragen Computer am Handgelenk, in der Hosentasche, wir bewegen uns in Computern fort und tragen sie in Form von Implantaten im Körper.

Unsere Kommunikation wurde in den letzten zehn Jahren globaler und interaktiver, das Netz wurde gesellschaftlich und wirtschaftlich unumgänglich. Und nun dringt es bis in die letzten Ecken und Dinge unseres Alltag vor. Web-2.0-Pionier Tim O'Reilly vertritt die Ansicht, dass Regierungen an dieser „Big Data Revolution" teilnehmen sollten und fragt in „Beyond Transparency"[1]: Wenn schon so viel in unserem Alltag erfasst und analysiert wird, warum sollte man weiterhin an theoretischen Regulierungsansätzen festhalten? Und warum sollte man schnell überholte Gesetze verabschieden, wenn man heutzutage so viele Sensoren und damit Möglichkeiten für flexibles Feedback hat? Das Internet der Dinge ist eine Herausforderung für Politik und Gesellschaft, und zwar nicht nur für den Datenschutz und die Sicherheit. O'Reilly's Vorschläge lassen ahnen, wie tiefgreifend das Internet der Dinge unsere Gesellschaft verändern wird.

In einer Welt von Milliarden vernetzten Geräten, Systemen und Dienstleistungen ist die Frage naheliegend, wie die Regeln für den Umgang mit unseren persönlichen Daten aussehen und Grundrechte gesichert werden. Schon heute sind es nicht mehr nur PCs oder Laptops, die miteinander über das Internet kommunizieren, längst ist das Netz mobil geworden und begleitet uns im Verkehr, in Aufzügen, beim Einkaufsbummel oder auf Partys. Der Kühlschrank warnt, dass mal wieder Milch fehlt, die Zahnbürste erinnert uns ans Zähneputzen, die Herdplatten optimieren den Energieverbrauch, unser Armband wacht über unseren Schlaf und mahnt, heute noch ein paar Schritte mehr zu gehen.

Experten der Investment-Firma Wedbush erklärten die Automatisierung von Haushalten zu einer der größten Geschäftsmöglichkeiten unseres Jahrzehnts. Kein Wunder also, dass Google im Januar 2014 den Thermostat- und Rauchmelderhersteller Nest Labs kaufte und damit den Einzug in unsere intelligenten Häuser vorbereitete. Die private Sammel-Industrie dringt mit dem Internet

der Dinge noch viel weiter in unsere Privatsphäre vor, als es derzeit NSA, GCHQ oder BND tun. Der Europäische Datenschutzbeauftragte warnte bereits vor zwei Jahren, dass intelligente Messsysteme „eine massive Erhebung personenbezogener Daten" ermöglichen, „die Rückschlüsse auf häusliche Aktivitäten zulassen". Kurz gesagt: Es lässt sich leicht herausfinden, welche Fernsehsendungen in einem Haus laufen, wie wohlhabend die Bewohner sind, wie sehr sie sich um die Sauberkeit bemühen, wann die Kinder zu Hause sind und wann nicht.

Das Internet der Dinge rückt den Computer ins Zentrum sozialpolitischer Diskussionen. Wie wird sich Google in unsere Heizgewohnheiten einmischen, wenn das Unternehmen heute schon darüber entscheidet, welche Suchergebnisse wir angezeigt bekommen und welche nicht? Gibt es bald Staatstrojaner für Implantate oder Kühlschränke? Werden Kinder mit Sehstörungen zukünftig nur noch spezielle Implantate bekommen, die nicht jugendfreie Inhalte filtern? Oder werden Hörimplantate billiger angeboten, wenn man sich personalisierte Werbespots ins Ohr säuseln lässt?

Auch unsere Straßen werden schlauer. Im Rahmen eines neuen Mautsystems, das lange diskutiert und nun von Verkehrsminister Dobrindt vorgeschlagen wurde, sollen alle Nummernschilder elektronisch erfasst werden. Im Arbeitsprogramm des technischen Polizeinetzwerks der EU (ENLETS) stand Anfang des Jahres der Wunsch, die Polizei mit technischen Hilfsmittel auszustatten, um Autos per Fernsteuerung anzuhalten. In Wien denkt man seit einigen Jahren über „intelligente Straßen" nach, um gegen Parkplatznot und Staus vorzugehen und Singapur entwickelt sich mit Tausenden Sensoren zur ersten smarten Nation. Es ist also nur eine Frage der Zeit, bevor sich gegenwärtige netzpolitische Diskussionen in die hypervernetzte Welt verlagern: Müssen wir demnächst etwa für eine Verkehrsnetzneutralität kämpfen, damit alle fahrerlosen Autos potenziell gleich schnell ans Ziel kommen und nicht bestimmte Verkehrsteilnehmer diskriminiert werden?

Web-2.0-Pionier Tim O'Reilly erklärte auf der SolidCon 2014, dass Versicherungen zum Geschäftsmodell des Internets der Dinge werden – so wie die Werbung bereits das Geschäftsmodell des Internets ist. Je mehr das Internet der Dinge weiß, desto mehr Daten stehen den Versicherungen zur Verfügung, um zu verhindern, dass wir nicht vom rechten Weg abkommen. In den USA wird daher das schlaue Armband Fitbit auf dem amerikanischen Markt massenweise an Firmen verkauft, um bei der Verwaltung der Gesundheitsvorsorge ihrer Angestellten zu helfen. Denn das Programm „Obamacare" belohnt Arbeitgeber für Initiativen, die zu einem gesünderen Leben ermuntern, mit Prämien und Steuervorteilen. Auch in Europa fasst diese Idee Fuß. Im November 2014 kündigte die Generali-Gruppe an, für die elektronische Kontrolle von Fitness und Ernährung Gutscheine für Reisen und sogar Prämiennachlässe zu gewähren.

Was bedeutet das Internet der Dinge also für die Politik? Tim O'Reilly meint, dass wir uns an einem einzigartigen Zeitpunkt befinden, an dem wir die Anzahl der Gesetze verringern und Regierungen stattdessen von der Datenerhebung profitieren können, um Gesetzgebungsprozesse zu optimieren. Er nennt dies „algorithmische Regulierung". Ein Beispiel hierfür ist das italienische Data-Mining-Programm „redditometro", welches in der Steuererklärung angegebene Einkommen und Ausgaben mittels Algorithmen abgleicht, um Steuerhinterziehungen aufzudecken. Ein weiteres Beispiel ist ein Bericht des Thinktanks 2020health, in dem der britischen Regierung vorgeschlagen wurde, Steuervorteile für diejenigen einzurichten, die mit dem Rauchen aufhören oder mehr Sport machen. Wie auch bei Obamacare und den Plänen der Generali-Gruppe gilt hier die unausgesprochene Annahme, dass ungesunde Lebensweisen der Gesellschaft zur Last fallen und daher steuerlich benachteiligt werden sollten – nach anderen Ursachen wird nicht gesucht, an der Lobbyarbeit mächtiger Lebensmittelkonzerne oder an wirtschaftlichen Ungerechtigkeiten liegt es natürlich nicht.

O'Reilly trennt mit seinen Thesen das Mittel vom Zweck und vergisst dabei, dass Ersteres in einer demokratischen Gesellschaft fast ebenso wichtig wie das Ergebnis ist. Während wir uns darüber einig sind, dass Bildung, Gesundheit und Sicherheit erstrebenswerte Ziele sind, herrscht keine Einigung darüber, wie wir diese Ziele erreichen. Bisher waren die ideologischen Linien einigermaßen klar – wird die politische Debatte nun im Internet der Dinge überflüssig? Internet-Theoretiker Evgeny Morozov kritisiert[2] den Glauben, dass sich alle Probleme der Welt, vom Übergewicht bis zum Treibhauseffekt, mit ein paar Daten und vernetzten Geräten lösen lassen. Auch Frank Schirrmacher hinterfragte im letzten Jahr diese Entwicklung (wobei man im Hinblick auf O'Reilly den „Markt" durch „Staat" ersetzen kann): „Der automatisierte Markt analysiert Präferenzen, und ob es bei der Wahl des Konsumenten um Bücher oder Regierungen geht, ist für diesen Markt nur ein Preisunterschied."[3]

Edward Snowdens Enthüllungen haben gezeigt, wie gerne sich staatliche Behörden bei den Datenbeständen privater Unternehmen bedienen. Man kann bezweifeln, dass unsere Regierungen der Versuchung von „Big Data" widerstehen werden. Wenn wir es jetzt nicht schaffen, universell geltende Rechte und Freiheiten zu verankern, riskieren wir womöglich mit einer „algorithmischen Regulierung" eine politische Ordnung, in der private Unternehmen alles entscheiden. Aber vielleicht behält auch Stanislaw Lem Recht, da die Menschen „gern selbst entscheiden möchten, in welchem System sie leben, welches Wirtschaftsmodell sie verwirklichen und welche Ziele die Gesellschaft verfolgen soll [...]; berücksichtigt man das, dann ist die Regelung gesellschaftlicher Systeme mithilfe von Maschinen, obwohl möglich, nicht ratsam".[4]

Anmerkungen

[1] Tim O'Reilly: *Open Data and Algorithmic Regulation* in Brett Goldstein, [et al.]: *Beyond Transparency*. Code for America Press, 2013.

[2] Evgeny Morozov: *To Save Everythig, Click Here*, 2013.

[3] Frank Schirrmacher: *Ego – Das Spiel des Lebens*, 2013.

[4] Stanislaw Lem: *Summa Technologiae*, 1964.

Kirsten Fiedler ist Geschäftsführerin des Netzwerkes European Digital Rights (EDRi), das in Brüssel 34 Bürgerrechtsorganisationen aus ganz Europa vertritt. In ihrer Freizeit engagiert sie sich beim Digitale Gesellschaft e. V. und bloggt ab und zu auf netzpolitik.org. Auf Twitter heißt sie @Kirst3nF.

34 Partizipation als Kontrollinstrument: Internet Governance in Zeiten Snowdens

von **Arne Hintz** und **Stefania Milan**

Als 2002 die Vorbereitungen zum Weltgipfel Informationsgesellschaft (World Summit on the Information Society - WSIS) begannen, stand ein Begriff im Zentrum der Debatte: Multistakeholderism. Nicht nur Regierungen sollten die brennenden Themen der Informationsgesellschaft diskutieren, sondern Staaten, Wirtschaft und Zivilgesellschaft gemeinsame Positionen erörtern. Den zivilgesellschaftlichen Akteuren aus Nichtregierungsorganisationen, der Wissenschaft, nichtkommerziellen Internet-Service-Providern und aktivistischen Gruppen kam dabei die Rolle zu, ihr spezifisches Wissen zu Themen wie Technologie und Recht einzubringen, aber auch BürgerInnen und InternetnutzerInnen zu repräsentieren und somit die Legitimation der Gipfelergebnisse auf breitere Beine zu stellen. Zu einer Zeit globaler Konfrontationen, in der die Gipfel und Konferenzen großer Institutionen, wie etwa der Welthandelsorganisation (WTO) und des Weltwirtschaftsforums (WEF), regelmäßig Massenproteste auslösten und nur noch hinter Zäunen, Mauern und Polizeibarrieren stattfinden konnten, sollte der WSIS Gemeinsamkeit symbolisieren und die Legitimität globaler Politik erneuern. Das Multistakeholder-Prinzip wurde zur zentralen Innovation des Gipfels, die meisten Reden und Pressemitteilungen konzentrierten sich auf den partizipativen Prozess (statt der substanziellen Entscheidungen des Gipfels) und Straßenproteste blieben weitgehend aus.

Rund zehn Jahre später, während der Eröffnungsveranstaltung des Internet Governance Forum (IGF) in Istanbul im September 2014 tweetete @pondswimmer: „All I'm saying is, if #multistakeholder were a drinking game, I'd be in the hospital with alcohol poisoning right about now." Wieder ist das Multistakeholder-Prinzip omnipräsent und als rhetorischer Bezug in Eröffnungsreden, Stellungnahmen und Arbeitspapieren unerlässlich. Sehen wir also den Siegeszug partizipativer Internetpolitik? Oder soll wieder etwas legitimiert werden?

Multistakeholderism

Die Geschichte der Internet Governance ist durchaus ein Modellbeispiel für neue Politik- und Regulierungsformen. Technische Arbeitsgruppen entwickelten grundlegende Standards und Protokolle, zivilgesellschaftliche Experten nehmen Schlüsselpositionen ein, in etwa der Internet Corporation for Assigned Names

and Numbers (ICANN), Regierungen stellen lediglich ein Beratungsgremium und verschiedene 'stakeholder' diskutieren relevante Regulierungsfragen miteinander im IGF. 'Multistakeholder governance' hat traditionelle Prozesse internationaler Politik dramatisch verschoben. Zivilgesellschaftliche Organisationen und Individuen haben neue Möglichkeiten, Themen zu setzen, Politik- und Regulierungsvorschläge zu erarbeiten und Entscheidungsprozesse zu beeinflussen. Viele von ihnen sitzen nun mit am Tisch, wenn die Zukunft der Internetpolitik diskutiert wird.

Wenngleich die Resultate oft nicht den eigenen Zielen entsprachen, wurde das Multistakeholder-Prinzip selten infrage gestellt. Als neue Politikform, die das Entscheidungsmonopol von Regierungen hinterfragt und zivilgesellschaftlichen Akteuren eine wichtige Rolle zuweist, wurde es bislang stets verteidigt. Allerdings hat sich gleichzeitig die Rhetorik der Multistakeholder-Prozesse verselbständigt. Sämtliche beteiligte Akteure predigen nun das Mantra der Multistakeholder-Politik. Vom WSIS zur IGF-Eröffnung 10 Jahre später wurde diese strukturelle Innovation von der Zivilgesellschaft, aber auch der Wirtschaft und vielen Regierungen gefeiert. Sind wir also Zeugen einer harmonisch-partizipativen Entwicklung hin zu gemeinsamen Zielen der Internetpolitik? Zwei aktuelle Entwicklungen können uns dabei helfen, diese Frage zu beantworten – die Enthüllungen des Whistleblowers Edward Snowden und die Gründung der 'NETmundial Initiative', der neuesten Internet-Governance-Organisation.

Der Snowden-Faktor

Die Enthüllungen des NSA-Whistleblowers Edward Snowden ab Juni 2013 änderten nicht nur unser Verständnis von Online-Kommunikation, sondern auch die internationalen Diskussionen zu Internetfreiheit und Internet Governance. In den Jahren zuvor war von Seiten des US-Außenministeriums und Hillary Clintons 'Internet Freedom Agenda' ein Ost-West Diskurs inszeniert worden, in dem der freie Westen dem autoritären Osten gegenüberstand, insbesondere Ländern wie China und dem Iran. Aufgrund der Enthüllungen über die massenhafte Überwachung digitaler Kommunikation durch Behörden wie die amerikanische NSA und den britische GCHQ waren nun plötzlich jene Länder als Feinde der Internetfreiheit bloßgestellt. Die Überwachung ganzer Länder und ihrer Bevölkerungen, Regierungen und Konzerne führte zu diplomatischen Konfrontationen. Im September 2013 beschuldigte etwa die brasilianische Präsidentin Dilma Roussef in einer Rede vor der UN-Vollversammlung die USA, Menschenrechte zu brechen und die Demokratie zu untergraben:

> In the absence of the right to privacy, there can be no true freedom of expression and opinion and therefore no effective democracy. In the absence of the respect for sovereignty, there is no basis for the relationship among nations.

Regierungen in Ländern wie Deutschland und Brasilien diskutierten Möglichkeiten, ihre Online-Kommunikation unabhängiger zu machen von amerikanischen Firmen und den Telekommunikationsstrukturen, die von amerikanischen Spionagebehörden überwacht wurden. Regierungen und Firmen, die zuvor die internationale Diskussion bestimmt hatten, waren nun in der Defensive.

NETmundial

Im April 2014 lud die brasilianische Regierung zu einer Konferenz ein, um die Zukunft der Internetregulierung in der Post-Snowden-Ära zu diskutieren. Delegierte nationaler Regierungen, der Wirtschaft und der Zivilgesellschaft trafen sich in São Paulo, um neue Prinzipien der Internet Governance zu entwickeln und einen Plan für die Zukunft zu entwerfen. Insbesondere TeilnehmerInnen der Zivilgesellschaft und aus dem Globalen Süden freuten sich über den offenen und partizipativen Charakter von NETmundial und konnten ihre Belange einbringen. ICANN, die wichtigste technische Regulierungsbehörde des Internets, war oft für ihre engen Verbindungen zur Wirtschaft und zur US-Regierung kritisiert worden, und die Versuche einiger Länder, der International Telecommunications Union (ITU) mehr Kompetenzen zu übertragen und somit Regierungen mehr Einfluss auf die Internetregulierung zu gewähren, war ebenso kontrovers. Im Kontext der Konflikte über die zukünftige Internet Governance konnte NETmundial ein Zeichen setzen und die durch Snowden aufgeworfenen Diskussionen ins Zentrum rücken.

NETmundial 2.0 – Das Imperium schlägt zurück

Wenige Monate später führte diese Dynamik scheinbar zur Gründung einer Initiative, die die Themen der NETmundial-Konferenz fortführen und institutionell untermauern könnte. Die neue 'NETmundial Initiative', der unter anderem wieder Brasiliens Internetorganisation CGI.br angehört, versprach, in einem partizipativen Prozess gemeinsame Lösungen für die anstehenden Probleme zu entwerfen. Allerdings waren nun plötzlich andere Akteure mit von der Partie. Die Führungsgruppe der neuen Initiative beinhaltete insbesondere das Weltwirtschaftsforum (WEF) – ein Treffpunkt globaler Wirtschafts- und Politik-Eliten. Ein exklusiver Klub mächtiger Entscheidungsträger hatte sich damit an die Spitze der NETmundial-Agenda gesetzt. Statt der Fortführung eines kritischen Dialoges und einer Post-Snowden-Agenda ähnelte die neue Initiative eher der Kaperung des NETmundial-Diskurses durch diejenigen, die die 'Occupy'-Bewegung als die '1 Prozent' bezeichnet hatten. Akteure, die für die Exklusivität globaler Politik stehen und somit traditionell eher das Gegenteil partizipativer Multistakeholder-Prozesse vertreten, besetzten ein progressives und kritisches Label.

Die NETmundial-Initiative, so der Plan, soll von einem Koordinationsrat geleitet werden, dem fünf 'ständige Mitglieder' angehören (ähnlich dem UNO-Sicherheitsrat) sowie 20 weitere Mitglieder. ICANN, CGI.br und das WEF erklär-

ten sich selbst zu ständigen Mitgliedern, während die weiteren 20 aus Wissenschaft, Zivilgesellschaft, Regierungen und Wirtschaft rekrutiert werden sollen. Wenngleich dies formell dem Multistakeholder-Prinzip entsprechen würde, löste die zentrale Rolle einer Institution wie des WEF doch deutliche Zweifel aus, ob die neue Initiative wirklich – wie vom ICANN-Vorsitzenden Fadi Chehade angekundigt, „the mother of all bottom-up processes" wird. ICANNs Rolle wurde ebenfalls bereits kritisiert, da nicht zwangsläufig ersichtlich war, warum ICANN als explizit technische Organisation ein Hauptakteur in einer nicht-technischen Initiative sein sollte.

Zivilgesellschaftliche Teilnahme?

Infolge der Ankündigung der neuen Initiative diskutierten zivilgesellschaftliche Gruppen und Organisationen kontrovers ihre mögliche Teilnahme an diesem Projekt. Nicht nur kritische Netzwerke wie die JustNet Coalition lehnten dankend ab, sondern auch die Internet Society (ISOC), ein zentraler Akteur in internationalen Internet-Governance-Strukturen. Die Internet Governance Civil Society Coordination Group (CSCG), eine Koalition wichtiger zivilgesellschaftlicher Organisationen wie etwa der Association for Progressive Communication (APC), der Diplo Foundation und der ICANN Non-Commercial Stakeholders Group (NCSG) sagten vorsichtig und nach langen Beratungen zu, aber nicht ohne eine ganze Reihe von Konditionen zu verlangen.

Sowohl das Interesse vonseiten der NETmundial-Initiative an zivilgesellschaftlicher Beteiligung als auch die kontroversen Diskussionen auf zivilgesellschaftlicher Seite, bezeugen die zentrale Rolle partizipativer Strukturen in der Legitimation neuer Institutionen. Während die eine Seite nicht-staatliche und nichtwirtschaftliche Akteure benötigt, um ihre Ziele durchsetzen zu können, will sich die andere Seite möglichst teuer verkaufen und ihren eigenen Einfluss stärken.

Post-Snowden-Konflikte

Dieses Spiel gegenseitiger Legitimierung und gemeinsamer (wenn auch vorsichtiger) Kooperation mag sinnvoll sein, solange gemeinsame Zielsetzungen zumindest denkbar sind. Dies ist in der Post-Snowden-Ära jedoch zunehmend fraglich. Der Überwachungsskandal hat den Blick auf die einstigen Verfechter der Internetfreiheit (insbesondere der amerikanischen und britischen Regierungen) gelenkt und ihre autoritären Züge offenbart. Kommerzielle soziale Medienplattformen wie Google und Facebook sind integraler Bestandteil der Überwachungsmaschinerie. Internetzensur hat sich rapide Richtung Westen verbreitet, und die neuen 'Parental Control Filters' in Großbritannien sind nur ein Beispiel dafür, wie Internetinhalte auch in demokratischen Ländern zunehmend gefiltert und blockiert werden. Der Kampf um die Deutungshoheit gegenwärtiger Entwicklungen und die Einflusspositionen für zukünftige Regulierungen werden durch die neue NETmundial-Initiative nur allzu deutlich.

Der Multistakeholder-Diskurs legt den Mantel der Harmonie über die diametral entgegengesetzten Interessen, die in den Foren der Internet Governance aufeinandertreffen – ICANNs Fadi Chehade beschwor explizit die 'Harmonie' zwischen allen beteiligten Akteuren während der Auftaktveranstaltung zum ICANN-Treffen in London im Juni 2014, unterlegt von den harmonischen Tönen eines walisischen Männerchors. Allerdings lässt sich in Zeiten zunehmender Kontrolle der Internetkommunikation die Frage stellen, ob ausgerechnet Multistakeholder-Kompromisse ein geeigneter Weg sind, sich jener Kontrolle entgegenzustellen. Alternative Foren wie etwa das 'Ungovernance Forum', das parallel zum IGF in Istanbul stattfand, gehen einen anderen Weg. Sie dienen als Diskussionsforum zur Entwicklung einer eigenen zivilgesellschaftlichen Agenda und Strategien, die sich vom Multistakeholder-Dialog über Kampagnen und Proteste bis hin zur Arbeit an alternativer technischer Infrastruktur ziehen.

In Zeiten, in denen das offene Internet massiven Bedrohungen ausgesetzt ist, ist nicht zwangsläufig ersichtlich, warum der sinnvollste Ausweg darin liegen sollte, mit jenen zusammenzuarbeiten, die für diese Bedrohung verantwortlich sind. Wenngleich das Multistakeholder-Prinzip einen Fortschritt internationaler Politik darstellt, brauchen wir möglicherweise mehr Konflikt als Konsens, mehr Konfrontation als Zusammenarbeit.

Weder über die zukünftige Rolle, noch die Struktur und Aktivitäten der NETmundial-Initiative herrscht zum gegenwärtigen Zeitpunkt Klarheit. Und selbst die zunächst zentrale Stellung des WEF kann sich verschieben und reduzieren. Die Ökologie der Internet Governance ist im Fluss, und das ist in diesem Fall nicht anders. Die NETmundial-Initiative verdeutlicht allerdings die Konflikte, die die Internetpolitik der Gegenwart durchziehen, und die Rolle, die Partizipation und Multistakeholder-Prinzip dabei spielen.

Arne Hintz lehrt und forscht an der Cardiff School of Journalism, Media and Cultural Studies. Seine Forschung verbindet Kommunikationspolitik, Medienaktivismus und technologischen Wandel. Er leitet das Forschungsprojekt „Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations After the Snowden Leaks".

Stefania Milan lehrt an der Universität Tilburg Datenjournalismus. Die Sozial- und Politikwissenschaftlerin beschäftigt sich vor allem mit den Themen Cloud Protesting, der Politik von Code und Datenaktivismus.

35 Netzpolitik 2014: Von der Neuformatierung politischer Strukturen

von **Julia Krüger**

August 2014: Nach mehreren Monaten der Verhandlung beschließt das Bundeskabinett das Regierungsprogramm „Digitale Agenda 2014-2017“. Das schon vor seiner Veröffentlichung geleakte und über Monate umstrittene Dokument enthält die inhaltlichen Leitlinien, mit denen die Koalitionsregierung die Digitalisierung in Wirtschaft und Gesellschaft gestalten und vorantreiben möchte und sie markiert die Bedeutung, welche netzpolitischen Fragen nunmehr zukommt.

Im Kontext dieser Agenda wurden im Frühjahr zugleich Umstrukturierungen im politisch-administrativen System der Bundesrepublik vorgenommen: Zum einen erhielt der Bundestag einen Ausschuss „Digitale Agenda“, der allerdings nicht mit relevanter Federführung ausgestattet ist und in erster Linie beratende Funktionen übernehmen soll[1]. Zum anderen wurden Ressourcen und Zuständigkeiten zwischen den Bundesministerien und der Bundesregierung neu verteilt. Das Wirtschafts-, das Innen- und das Verkehrsministerium übernahmen federführend die Ausgestaltung des Arbeitsprogramms. Weitere Zuständigkeiten fielen an das Bundesministerium der Justiz und für Verbraucherschutz, das Bundesministerium für Bildung und Forschung, das Auswärtige Amt, das Bundesministerium für Gesundheit, das Bundesministerium für Familie, Senioren, Frauen und Jugend, das Bundesministerium für Arbeit und Soziales sowie einzelne Ressorts der Bundesregierung.

Die Digitale Agenda war und ist hoch umstritten. Sie sei weit hinter den Empfehlungen der interfraktionellen Enquete-Kommission „Internet und Digitale Gesellschaft“ (2010-2013) zurückgeblieben und überhaupt visionslos. Im Angesicht des rasanten Wandels digitaler Technologien, weit reichender gesellschaftlicher Veränderungen und folgenschwerer Herausforderungen wie der Infragestellung rechtsstaatlicher Standards durch flächendeckende Kommunikationsüberwachung ist sie in weiten Teilen der Öffentlichkeit als leere Phrasendrescherei der Bundesregierung eingeordnet worden[2]. Die Häme blieb nicht aus, man konnte sie sogar nachfeiern[3].

Doch jenseits aller Kritik ist mit der Digitalen Agenda nicht nur die Netzpolitik im politischen Establishment angekommen. Politische Strukturen selbst ändern sich infolge der Digitalisierung – und dies ist mit der Reorganisation insbeson-

dere administrativer Zuständigkeiten manifest geworden: Im Vorfeld dessen gab es eine breite Diskussion, ob Netzpolitik ein Internetministerium braucht, auf verschiedene Ministerien aufgeteilt oder doch gleich beim Bundeskanzleramt angesiedelt werden sollte. Ausschlaggebend war nicht nur die Bedeutung, die Netzpolitik von verschiedenen Akteuren zugeschrieben wird. Vielmehr stand zur Debatte, ob Netzpolitik ein Politikfeld oder ein Teil etablierter Politikfelder ist. Kann man netzpolitische Fragen klassischen Politikbereichen wie der Wirtschafts-, Wettbewerbs- oder Medienregulierung zuordnen? Oder braucht man für eine den Herausforderungen adäquate Bearbeitung eine neue, integrierende, koordinierende und zentralisierende politische Institutionalisierung auf allen Ebenen?

Auf der Oberfläche bildet der Querschnittscharakter netzpolitischer Fragen den Hintergrund für die Diskussion, denn diese tangieren zumeist mehrere politische Handlungsbereiche. Die Frage der Netzneutralität beispielsweise verknüpft Infrastrukturausbau mit Wirtschaftspolitik und Grundrechten. Urheberrechte nur aus juristischer Perspektive zu betrachten, würde dem Thema nicht gerecht werden, denn das vernachlässigt essentielle Bezüge zu Innovation und Datenschutz (in der Durchsetzung). Datenschutz überhaupt tangiert fast alle netzpolitischen Fragen und ist mit technischer Infrastruktur und Design verknüpft – wodurch Fragen der Verfügungsgewalt über infrastrukturelle Kernressourcen, der Produktion technischer Standards wie auch der Geschäftsmodelle und Unternehmensorganisationen im IT-Sektor unvermeidbar mitbetroffen sind, um nur ein paar wenige Beispiele zu nennen. Netzpolitische Fragestellungen verschränken also etablierte politische Problem- und Handlungsfelder wie die Wirtschafts- und Wettbewerbs-, Medien- und Technologie- oder Innen- und Justizpolitik stärker miteinander.

Es ist allerdings davon auszugehen, dass diese stärkere Verschränkung etablierter politischer Handlungsfelder nicht nur charakteristisch ist, sondern eine konstitutive Wirkung entfaltet: Denn die in den jeweiligen Bereichen bislang als funktional und angemessen erachteten Problemwahrnehmungs- und Problemlösungsmodi sowie Regulierungskonzepte stoßen durch die Verknüpfung der Handlungsfelder aufeinander und an ihre Grenzen. In der Folge werden Konzepte für alle tangierten gesellschaftlichen Problembereiche neu entwickelt werden müssen – auf Basis veränderter Akteurskonstellationen und inklusive der Entwicklung integrierender Sichtweisen und Regulierungsansätze.

Betrachtet man diesen Aushandlungsprozess von neuen Konzepten für etablierte, aber nun digitalisierte gesellschaftliche Problembereiche als Netzpolitik, dann ist Netzpolitik längst in der Politik angekommen. Die Herausforderung besteht dann vielmehr darin, den Aushandlungsprozess bestmöglich zu gestalten – und hierbei gibt es mit Sicherheit mehrere Optionen. Von großer Bedeutung erscheint zunächst natürlich die Beteiligung aller relevanten Akteure. Adäquate Verfahren und Institutionen könnten die Akteure aus den unterschiedlichen Bereichen,

mit ihren jeweils spezifischen Wahrnehmungen, Ideen und Denkweisen, darin unterstützen, gemeinsame Sichtweisen und konstruktive Regulierungskonzepte zu entwickeln. Denn die dafür notwendige, interdisziplinäre Verständigung ist schwierig. Wie schaffen wir einen Raum und einen Prozess, indem Techniker, Juristen, Wirtschaftspolitiker, Sozialwissenschaftler usw. gemeinsame und bindende Lösungsansätze für komplexe Probleme der unterschiedlichen gesellschaftlichen Handlungsbereiche finden? Dass ein solcher Prozess transparent und demokratisch verlaufen sollte, ist klar. Denn zur Debatte steht: Eine digitale Gesellschaft, die letztlich von Bürgern, Arbeitnehmern und Arbeitgebern, Eliten und der Öffentlichkeit akzeptiert sein muss.

Gut, die Digitale Agenda war nicht der große Wurf, im Kompetenzgerangel nach den Wahlen wurde Netzpolitik eben wieder auf verschiedene Ministerien und Behörden aufgeteilt, dazu ein mit keinem Ministerium korrespondierender und grundsätzlich lediglich beratender Bundestagsausschuss eingerichtet, der auch klassischerweise nicht-öffentlich tagt. Wie gut, dass ein kleines, aber feines Blog immer wieder nachhakt, wo denn jetzt eigentlich welche Zuständigkeiten liegen[4]. Diese werden nun auch irgendwie koordiniert, seit September in der „Koalitionsarbeitsgruppe Digitales", die als Ansprechpartner für die jeweilig zuständigen Staatssekretäre dienen soll.

Es bleibt abzuwarten, wie gut das gewählte Modell, eine Aufteilung und Koordinierung ministerialer Zuständigkeiten in Verbindung mit einem theoretisch integrierenden, praktisch zahnlosen Bundestagsausschuss in der Bearbeitung netzpolitischer Fragen, funktioniert. Die Skepsis ist groß[5]. Zu erwarten sind viele Konflikte – zwischen den unterschiedlichen Problemwahrnehmungs- und Problemlösungsmodi, den jeweiligen Akteurspositionen, den Politikergenerationen usw. Aber Fakt ist: Egal ob Netzpolitik nun in einem Internetministerium, in einem Koordinierungsgremium oder im Bundeskanzleramt verortet ist – die Digitalisierung der Gesellschaft ist in vollem Gange, die Emergenz neuer politischer Probleme, welche zu ihrer Bearbeitung die konstruktive und visionäre Zusammenarbeit von Akteuren verschiedener Politikbereiche benötigen, längst sichtbar geworden und Struktur bereits verändert. Eine zufriedenstellende Gestaltung wäre wünschenswert.

Man kann, wie Don Quijote es einst tat, Windmühlen als Riesen begreifen, die man bekämpfen muss, um der eigenen, längst verlorenen Position zu Ruhm und Ehre zu verhelfen. Man kann Müller werden. Oder man kann dazu beitragen, dass verarmte Junker, Bauern und gesellschaftliche Autoritäten den technischen Wandel verstehen, dessen sozioökonomische Konsequenzen vermitteln und gesellschaftliche Konzepte entwickeln, die Chancen und Risiken der Entwicklungen für möglichst viele soziale Gruppen händelbar machen. Ist wohl eine Frage der Einsicht und Verantwortlichkeit.

Anmerkungen

[1] Nachdem der Ausschuss zunächst komplett ohne Federführung ausgestattet wurde, wurde ihm diese im September für das Arbeitsprogramm „Digitale Agenda“ zugebilligt. Allerdings sollen konkrete Gesetzesvorhaben weiterhin in den jeweiligen Fachausschüssen federführend bearbeitet werden. Mehr Informationen zu der Debatte: Konstantin Notz: *Federführende Zuständigkeit des „Internet-Ausschusses“ für die „Digitale Agenda?“ – schön wär's!*. http://gruen-digital.de/2014/09/federfuehrende-zustaendigkeit-des-internet-ausschusses-fuer-die-digitale-agenda-schoen-waers/

[2] Zu den Reaktionen siehe: Markus Beckedahl: *Kommentare und Reaktionen zur Digitalen Agenda in anderen Medien*.
https://netzpolitik.org/2014/kommentare-und-reaktionen-zur-digitalen-agenda-in-anderen-medien

[3] A. Bense: *Die Hymne zur Digitalen Agenda*, *„Cyber, Cyber“*. Kann nachgehört werden unter:
https://soundcloud.com/atbense/ritscheratsche-cyber-cyber-mix

[4] Markus Beckedahl: *Welche Ministerien sind für die Digitale Agenda zuständig?*.
https://netzpolitik.org/2014/welche-ministerien-sind-fuer-digitale-agenda-zustaendig/;
Anna Biselli: *Wer ist eigentlich für Netzpolitik zuständig? Bundesregierung so: „Keine Ahnung, ist eben Querschnittsthema“*.
https://netzpolitik.org/2014/wer-ist-eigentlich-fuer-netzpolitik-zustaendig-bundesregierung-so-keine-ahnung-ist-eben-querschnittsthema/

[5] Eine systematische Aufarbeitung kritischer Punkte findet sich in Sebastian Rieger, Sebastian (Stiftung Neue Verantwortung): *Hintergrundanalyse: Braucht die Digitale Agenda das Kanzleramt?*.
http://www.stiftung-nv.de/153251,1031,111427,-1.aspx

Julia Krüger ist Sozialwissenschaftlerin aus Berlin. Sie interessiert sich für die Entwicklung der digitalen Gesellschaft und hat sich mit der Regulierung von Inhalten, Internet Governance und Datenschutz beschäftigt. Zurzeit forscht sie zu Internet Policy am Social Science Center Berlin.

Zehn Gründe, um einen Dauerauftrag für netzpolitik.org einzurichten

1. Wir sind eines der ersten fast komplett leserfinanzierten Netz-Medien in Deutschland. Wir sind niemandem verpflichtet, außer unseren Leserinnen und Lesern und unserer Haltung. Das sehen wir als Auftrag.

2. Wir sind der zentrale Ort für die netzpolitische Debatte im deutschsprachigen Raum. Ob Politiker, Journalistin, Aktivist oder BND-Mitarbeiterin – an netzpolitik.org kommt keiner vorbei.

3. Wir sind ein Frühwarnsystem. Wer netzpolitik.org liest, weiß was in der Zukunft debattiert wird. ACTA, Vorratsdatenspeicherung, Totalüberwachung, Netzneutralität oder Netzsperren sind dabei nur einige Themen, die wir schon von Beginn an begleitet haben.

4. Wir sind kein Geschäftsmodell, sondern gemeinnützig und gemeinwohlorientiert. Die Spenden unserer Leserinnen und Leser sind nicht nur steuerlich absetzbar, sondern fließen direkt in unsere journalistische Arbeit. Mit Eurem Dauerauftrag können wir mehr Themen bearbeiten und der Politik noch besser auf die Finger schauen.

5. Wir reden nicht nur, was man tun sollte. Wir tun etwas. Seit über zehn Jahren. Mit Leidenschaft, zu wenig Geld und derzeit 2,5 festen Stellen. Und mit einem großen Netzwerk um uns herum – deutschlandweit und international.

6. Wir sind transparent und legen unsere Finanzierung offen. Durch unsere Leserfinanzierung sind wir unabhängig von großen Unternehmen und Institutionen. Wir können uns auf die Themen konzentrieren, die wir für wichtig und richtig halten, weil wir nicht abhängig von Reichweite und Klicks sind. Bei uns haben auch Themen eine Chance, die bei anderen unter den Tisch fallen.

7. Wir haben schon über den NSA-Skandal berichtet, als Edward Snowden noch gar nicht für den Geheimdienst gearbeitet hat. Wir werden weiter darüber berichten, wenn die Medienaufmerksamkeit schon längst weitergezogen ist.

8. Wir bloggen auch, wenn der Staat uns Polizisten in den Nacken setzt. netzpolitik.org hat Rückgrat und lässt sich nicht einschüchtern. Weder von Abmahnungen noch von staatlichen Stellen. Wir haben das Informationsfreiheitsgesetz fast durchgespielt und werden vermehrt unsere Transparenzrechte einklagen.

9. Wir sagen nicht, dass wir neutral sind. Wir haben Haltung, berichten journalistisch und faktentreu. Immer mit Blick auf digitale Grundrechte, ein offenes Netz und das Gemeinwohl.

10. Wir machen Open Journalism. Unsere Wurzeln liegen im Netz: Wir sind offen, wir verlinken unsere Quellen, wir kommunizieren auf Augenhöhe. Wir experimentieren, reflektieren transparent und stehen im ständigen Dialog mit unserer Community. Uns liegen Dokumente nicht nur vor, wir veröffentlichen sie in der Regel auch. Denn die Leserinnen und Leser haben ein Recht darauf, sich selbst ein Bild zu machen. Dafür stehen wir ein. Unsere Inhalte stehen unter einer Creative Commons Lizenz und können zu nichtkommerziellen Zwecken weiterverwendet werden.

    One more thing …

11. Günther Oettinger ist jetzt der neue EU-Kommissar für Netzpolitik. Deswegen braucht es noch mehr netzpolitik.org!

Abkürzungen

30C3 30. Chaos Communication Congress
A1 Telekom Austria
ACTA Anti-Counterfeiting Trade Agreement – Anti-Produktpiraterie-Handelsabkommen
ADL Anti-Defamation League
AfD Alternative für Deutschland
AIVD Allgemeiner Auskunfts- und Sicherheitsdienst – Geheimdienst der Niederlande
APA Austria Presse Agentur
ARD Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland
ARM Mikroprozessor-Architektur
BBC British Broadcasting Corporation
BfV Bundesamt für Verfassungsschutz
BKA Bundeskriminalamt
BMI Bundesministerium des Innern
BND Bundesnachrichtendienst
BRD Bundesrepublik Deutschland
BSD Berkely Software Distribution
BSI Bundesamt für Sicherheit in der Informationstechnik
CALEA Communications Assistance for Law Enforcement Act – US-amerikanisches Gesetz (1994), das Justizbehörden in ihrem Recht stärkt, elektronische Kommunikation zu überwachen und Hersteller von Endgeräten verpflichtet, ihre Produkte so auszustatten, dass dies möglich ist
CCC Chaos Computer Club
CC Creative Commons
CCTV Closed-Circuit Television
CDC Centre for Digital Cultures
CDU Christlich-Demokratische Union
CEO Corporate Executive Officer
CETA Comprehensive Economic and Trade Agreement - Freihandelsabkommen zwischen Kanada und der EU
CIA Central Intelligence Agency
CIO Chief Information Officer – Dt.: IT-Leiter
CMS Content Management System
CNE Computer Network Exploitation – Militärischer Begriff, der das Sammeln von Informationen von gegnerischen Computern und Computernetzwerken beschreibt
COINTELPRO COunter INTELligence PROgram – Ehemals geheimes Programm des FBI, das politische Organisationen und AktivistInnen in den USA systematisch überwachte, unterwanderte und störte
CSI Crime Scene Investigation
CTIRU Counter Terrorism Internet Referral Unit – Gruppe der Metropolitan Police, die Inhalte mit 'terroristischen' Inhalten aus dem Internet entfernen soll
CTIVD Intelligence and Security Services Review Committee – Kontrollgremium der niederl. Geheimdienste
(D)DoS (Distributed) Denial of Service – Nichtverfügbarkeit eines Internet-Dienstes durch Überlastung von Servern und anderer Infrastruktur
DE-CIX Deutscher Commercial Internet Exchange – Internet-Knoten in Frankfurt am Main
DIN Deutsche Industrienorm
DMCA Digital Millennium Copyright Act – US-amerikanisches Gesetz (1996) zur Verfolgung von Urheberrechtsverletzungen im Internet
DNSCurve Protokoll zur sicheren Auflösung von Domain-Namen in IP-Adressen
DNS Domain Name Service
DNSSec Domain Name System Security Extensions
DRIP Data Retention and Investigatory Powers Act – Britisches Gesetz zur Vorratsdatenspeicherung

DRM Digital Rights Management – Prozesse der Rechteverwaltung von digitalen Immaterialgütern

DVB-T Digital Video Broadcasting — Terrestrial

EAD Europäischer Auswärtiger Dienst – de facto das Außenministerium der EU

EDRi European Digital Rights

ENLETS European Network of Law Enforcement Technology Services

ePub Electronic Publication E-Book-Format

EU Europäische Union

EuGH Europäischer Gerichtshof

FAZ Frankfurter Allgemeine Zeitung

FBI Federal Bureau of Investigation

FIfF Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

FISA Foreign Intelligence Surveillance Act – Dt.: „Gesetz zum Abhören in der Auslandsaufklärung", regelt die Auslandsaufklärung und Spionageabwehr der USA (1978)

FPÖ Freiheitliche Partei Österreichs

FSFE Free Software Foundation Europe

FTP File Transfer Protocol

G10 Artikel 10 des Grundgesetzes; Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses

GAR Gemeinsames Abwehrzentrum Rechtsextremismus

GASIM Gemeinsames Analyse- und Strategiezentrum Illegale Migration

GCHQ Government Communications Headquarters

GDS Government Digital Service – Regierungsorganisation in GB, die mit dem Transfer der Regierungstätigkeiten ins digitale Zeitalter betraut ist

GEMA Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte

GG Grundgesetz

GNU GNU's Not Unix! – Unixähnliches Betriebssystem

GOBT Geschäftsordnung des Deutschen Bundestages

GPS Global Positioning System

GPU Graphics Processing Unit – Dt.: Grafikprozessor

GSM Global System for Mobile Communications

GTAZ Gemeinsames Terrorabwehrzentrum

HEFCE Higher Education Funding Council for England – Der HEFCE fördert Forschung und Bildung im Spitzenbereich an Universitäten und Colleges in England

HKW Haus der Kulturen der Welt

HoGeSa Hooligans gegen Salafisten

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

IATI International Aid Transparency Initiative – Weltweite Initiative mit dem Ziel, die Finanzflüsse in der Entwicklungszusammenarbeit transparenter und vergleichbar zu machen

ICANN Internet Corporation for Assigned Names and Numbers

IFG Informationsfreiheitsgesetz

IMAP Internet Message Access Protocol

IMK Innenministerkonferenz

IMSI International Mobile Subscriber Identity – Nummer zur eindeutigen Identifizierung von Netzteilnehmern in Mobilfunknetzen

IMS Interception Management System – Programme zur Überwachung von Telekommunikationsdiensten

IP Internet Protocol

IPRED Intellectual Property Rights Enforcement Directive – Richtlinie (2004) des Europäischen Parlaments und des Rates zur Durchsetzung der Rechte des geistigen Eigentums

IPv6 IP Version 6

ISC Internet Software Consortium

ISDS Investor-state dispute settlement – Instrument des internationalen Rechts, das es Investoren erlaubt, gegen eine ausländische Regierung, in deren Land investiert wurde, ein Streitbeilegungsverfahren anzustoßen

IS Islamischer Staat – dschihadistisch-salafistische, terroristische Organisation

IT Informationstechnologie

IVW Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V.

IWG Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen

IZD Internationales Zentrum Donaustadt – Bürogebäude in Wien, in dem u.a. die

US-Vertretung bei den Vereinten Nationen untergebracht ist

KDP Kindle Direct Publishing

KfW Kreditanstalt für Wiederaufbau

LDAP Lightweight Directory Access Protocol – Anwendungsprotokoll, das die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes erlaubt

LIMS Lawful Interception Management System – Programme zur gesetzlich geforderten Überwachung von Telekommunikationsdiensten; wird von Regierungen eingesetzt

LiMux Projektname der Umstellung der gesamten öffentlichen Verwaltung Münchens auf Open-Source Lösungen

MD4 Message Digest Algorithm 4

MD5 Message Digest Algorithm 5

MdB Mitglied des Bundestags

MdEP Mitglied des Europäischen Parlaments

MIT Massachusetts Institute of Technology

MIVD Militärischer Geheimdienst der Niederlande

Mobi Mobipocket E-Book-Format

MPAA Motion Picture Association of America

NASA National Aeronautics and Space Administration

NATO North Atlantic Treaty Organization

NDR Norddeutscher Rundfunk

NFS Network File System

NGO Nichtregierungsorganisation

nmap Network Mapper

NPD Nationaldemokratische Partei Deutschlands

NRW Nordrhein-Westfalen

NSA National Security Agency

NSU Nationalsozialistischer Untergrund

OA Open Access

OCaml Objective Caml – Programmiersprache

ODP Open Document Presentation

ODT Open Document Text

OGP Open Government Partnership – Internationale Open-Government-Initiative zur Förderung von Transparenz, Bürgerbeteiligung und Verwaltungsmodernisierung in Regierungen

OKF (DE) Open Knowledge Foundation (Deutschland)

OpSec Operations Security

ORF Österreichischer Rundfunk

ÖVP Österreichische Volkspartei

PCLOB Privacy and Civil Liberties Oversight Board – vom US-Kongress eingesetzes Gremium zur Beratung der Regierung in Bürgerrechtsfragen

PEGIDA Patriotische Europäer gegen die Islamisierung des Abendlandes

PGP Pretty Good Privacy – Programm zur Verschlüsselung von Daten

PHP Skriptsprache

PHW Personenbezogene Hinweise

PIN Persönliche Identifizierungsnummer

PLoS Public Library of Science – Nichtkommerzielles Open-Access-Bibliotheksprojekt, das wissenschaftliche Texte frei zur Verfügung stellt

PNR Passenger Name Records – Dt.: Fluggastdatensatz, Sammlung aller Daten rund um eine Flugbuchung, die über einen gewissen Zeitraum in Computerreservierungssystemen gespeichert werden

PSI-Richtlinie EU-Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors

RCUK Research Council Großbritannien

RSA Rivest, Shamir, Adleman – Asymmetrisches Kryptosystem

SHA Secure Hash Algoritm

SIGINT Signals Intelligence – Dt.: Signalerfassende Aufklärung, Oberbegriff für die Gewinnung von Informationen durch Funksignale und elektronische Signale

SNMP Simple Network Management Protocol – Netzwerkprotokoll, das Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer, etc.) von einer zentralen Station aus überwachen und steuern kann

SQL Structured Query Language – Datenbankabfragesprache

SSL Secure Sockets Layer

StGB Strafgesetzbuch

SVP Schweizer Volkspartei

TAFTA Transatlantic Free Trade Area – Überbegriff für transatlantische Freihandelsabkommen

TC Trusted Computing

TED Konferenz „Technology, Entertainment, Design“
Telko Telekommunikationsanbieter
TLS Transport Layer Security
Tor The Onion Router – Netzwerk zur Anonymisierung von Verbindungsdaten
TPM Trusted Platform Module
TTIP Transatlantic Trade and Investment Partnership – Transatlantische Handels- und Investitionspartnerschaft zwischen der EU, den USA und weiteren Staaten
UMTS Universal Mobile Telecommunications System
UN(O) United Nations (Organization)
UPC United Philips Cable – europäisches Telekommunikationsunternehmen
UrhG Urheberrechtsgesetz
URL Uniform Resource Locator
USA United States of America
VK VKontakte – Russisches soziales Netzwerk
V-Mann Verbindungsmann
VOIP Voice over IP – Internet-Telefonie
VPN Virtual Private Network
VPS Virtual Private Server
VS Verfassungsschutz
WAM Women, Action & the Media
WCIII Computerkriminalitätsgesetz in den Niederlanden
WDR Westdeutscher Rundfunk
WWW World Wide Web
XMPP Extensible Messaging and Presence Protocol
ZDF Zweites Deutsches Fernsehen
ZKM Zentrum für Kunst und Medientechnologie Karlsruhe