Pia Oppel

Die Grenzen der Datenschutz-Guerilla

Kann die eigene Privatsphäre im digitalen Zeitalter noch geschützt werden? Die Journalistin Julia Angwin, der Netzaktivist Max Schrems und der Datenschutzexperte Peter Schaar antworten darauf mit einem vorsichtigen „Ja, aber".

Leute, die keine „Nerds, Hacker oder Kryptographen" sind und sich trotzdem der digitalen Ausbeutung und Überwachung widersetzen wollen, können ein paar einfache Regeln befolgen, meinte der Schriftsteller Hans-Magnus Enzensberger einige Monate nach Beginn der Snowden-Enthüllungen.[1] Das Mobiltelefon wegwerfen wäre ein guter Anfang und Online-Dienste meiden ein sinnvoller nächster Schritt. Das war kein Aufruf zum analogen Einsiedlerdasein, sondern eine ironische Replik auf die von Enzensberger kritisierte „Passivität" der Politik. Denn letztlich sei das Individuum auf politische Lösungen angewiesen, da es der Datensammelwut von Staat und Wirtschaft wenig entgegen setzen könne.

Die US-amerikanische Journalistin Julia Angwin hat versucht diese These mit einem Selbstexperiment zu widerlegen – was ihr teilweise gelungen ist. In *Dragnet Nation* beschreibt sie ihren Versuch, den Schleppnetzen *(dragnets)* der Internetkonzerne, Datenhändler und Geheimdienste mit technologischen Mitteln zu entkommen. In deren Netzen bleiben die Zeugnisse unseres Alltags haufenweise hängen. Zum Beispiel spuckt Angwins Google-Account auf Nachfrage folgende Informationen aus: Seit 2006 hatte sie mit 2 192 Kontakten einen E-Mail-Austausch und pro Monat gab sie im Schnitt 26 000 Suchanfragen ein. Am 30. November 2010 hat sie zum Beispiel morgens Nachrichten gelesen, dann nach einem Geschenk für ihre Tochter gesucht, im Online-Thesaurus nach einem Begriff für einen Artikel gestöbert, am Nachmittag ein Restaurant reserviert und sich schließlich noch auf der Webseite des Kongresses mit Datenschutzgesetzen dokumentiert. Intimer als ihr Tagebuch seien diese Informationen, „a window into my thoughts each day".

Digitale Enthaltsamkeit, die schnell in Paranoia umschlagen kann, hält die US-amerikanische Journalistin Julia Angwin für keine realistische Option.

Zusätzlich versucht Angwin in Erfahrung zu bringen, was staatliche Stellen, Kreditrating-Agenturen, Facebook, Twitter und Scharen von Datenhändlern über sie gesammelt haben – die NSA gibt natürlich keine solchen Auskünfte. In den meisten Fällen durfte sie nur einen Bruchteil der gesammelten Informationen einsehen „and even this tiny amount was disturbingly comprehensive". Die Informationen umfassten alle ihre bisherigen Adressen und Telefonnummern, die Namen von nahezu allen Familienmitgliedern und ihre Kaufgewohnheiten: „I couldn't help but compare my data to the Stasi files I had reviewed, with their rudimentary surveillance and limited windows into people's lives. Even in their wildest dreams, the Stasi could only fantasize about obtaining this amount of data about citizens with so little effort."

In wenigen Jahren hat die Datenwirtschaft Fakten geschaffen, die nur schwer mit den etablierten Prinzipien des demokratischen Rechtsstaats vereinbar sind. Angwin erinnert daran, dass der Supreme Court beispielsweise 1958 entschieden hat, dass der Bundesstaat Alabama kein Recht auf Einsicht in die Mitgliederlisten der Bürgerrechtsbewegung National Association for the Advancement of Colored People hat, „because it could chill members' First Amendment right to freedom of association". Heute kann keiner mehr davon ausgehen, dass solche Informationen geschützt werden, so Angwin.

Wer sich dieser Gegebenheit entziehen und trotzdem, wie Angwin, „in the modern world" leben will, kann sich keinen

Pia Oppel arbeitet als Journalistin in der Nachrichtenredaktion des Radio 100,7.

In ihrem Dokumentarfilm *Citizen Four* zeigt Laura Poitras die aufwändigen Prozeduren, die Edward Snowden ihr erklärte, um eine abhörsichere Kommunikation zu garantieren. (© Laura Poitras, *Citizen Four,* 2014)

Purismus leisten. Digitale Enthaltsamkeit („surveillance veganism"), die schnell in Paranoia umschlagen kann, hält sie für keine realistische Option. Aber auch ihr pragmatischer Ansatz („surveillance flexitarianism") stellt sich als Herkules-Aufgabe heraus. Sie experimentiert mit Dutzenden Programmen, um ihre Kommunikation zu verschlüsseln und Online-Tracking zu vermeiden. Sie lässt sich eine Kreditkarte mit dem Pseudonym Ida Tarbell erstellen und nutzt keine öffentlichen Wifi-Netzwerke mehr (Detail: siehe Kasten S. 18). Angwin lässt sich dabei von einer Armada befreundeter Hacker und Datenschutzexperten beraten. Die praktische Unterstützung von Informatikern stellt sich angesichts der häufig geringen Nutzerfreundlichkeit von Datenschutzsoftware als unabdingbar heraus (obwohl die studierte Mathematikerin durchaus technikaffin ist).

Alles in allem habe ihr Experiment sie „surprisingly hopeful" gestimmt: „I had avoided the vast majority of online ad tracking. My passwords – made by my daughter by rolling dice and picking words out of a dictionary – were pretty good. My fake identity Ida Tarbell had allowed me to disassociate my true identity from sensitive purchases and some phone calls and in-person meetings. And I had convinced some of my friends and sources to exchange encrypted texts, instant messages, and e-mails."

Weniger Erfolg hatte Angwin mit den Datenhändlern, die ihre Daten nicht löschen wollen. Vor Google und Facebook gibt es kein Entkommen: sie sammeln auch Daten über Nicht-Nutzer. Und verschlüsselte Kommunikation speichert die NSA (Snowden-Dokumenten zufolge) vorsorglich „for later analysis". Gleichzeitig hat Angwin ein mulmiges Gefühl, dass der Rechtsstaat sich auch mit richterlichem Beschluss keinen Zugang zu verschlüsselten Inhalten verschaffen kann: „The deeper I looked at anonymous digital transactions, the less I liked them. They seemed to be havens for criminals." Anonymität dürfe keine Immunität für Geldwäsche und Kinderpornographie bedeuten – auch das Recht auf Verschlüsselung könne kein absolutes sein.

Den Mehrwert ihres Experiments sieht Angwin hauptsächlich in seiner politischen Dimension: „My opt-outs were one more bit of evidence to undermine the [...] argument that few people care enough about privacy." Ihr Erfahrungsbericht zeigt, dass der Einzelne beim Datenschutz ähnlich wie beim Umweltschutz früher oder später an Grenzen stößt. Veganer allein retten uns nicht vor dem Klimawandel.[2] Genauso wenig stellen verschlüsselte E-Mails einen effektiven Grundrechtschutz im digitalen Zeitalter her. Die individuellen Anstrengungen (so wertvoll sie auch sein mögen) laufen ab einem gewissen Punkt ins Leere. Zur politischen Dimension der Datenschutzdebatte macht Angwin zwar einige Vorschläge,[3] die interessanteren Antworten findet man jedoch bei Peter Schaar und Max Schrems (falls man sich nicht von den unsäglichen Buchtiteln *Überwachung total* und *Kämpf um deine Daten* abschrecken lässt). Beide betonen, dass es ein Recht auf Datenschutz geben muss, auch für jene, die nicht am technologischen „Wettrüsten" teilnehmen, sei es gegen die NSA oder Google.

Geheimdienste vs. Menschenrechte

Die Snowden-Enthüllungen fielen in Peter Schaars zehntes und letztes Amtsjahr als deutscher Bundesbeauftragter für Datenschutz. Seine Behörde sei damals machtlos gewesen, hat der heutige Vorsitzende der Europäischen Akademie für Informationsfreiheit und Datenschutz im Januar vor dem BND-Untersuchungsausschuss erklärt.[4] Zum Beispiel konnte er nicht überprüfen, ob Internetknotenpunkte in Deutschland von Geheimdiensten angezapft wurden. Von dieser Ohnmachtserfahrung ist in

Schaars Buch über die staatlichen Überwachungsmethoden im digitalen Zeitalter wenig zu spüren. Er ist überzeugt, dass die EU einen anderen Weg einschlagen und dem von den USA ausgehenden Überwachungswahn zumindest auf dem eigenen Territorium ein Ende setzen könnte.

Schaar erklärt ausführlich, was mittlerweile über die Aktivitäten der NSA, des britischen GCHQ und des deutschen Bundesnachrichtendienstes bekannt ist: von „Prism" (Zugang zu großen Datenzentren, Auswertung der Daten großer US-Internetkonzerne), über „Tempora" (Überwachung der Unterseekabel, die Europa mit den USA verbinden), bis „XKeyscore" (Überwachung, Auswertung und Verknüpfung weltweiter Kommunikationsdaten) oder „Socialist" (Infiltration des belgischen Telekommunikationsunternehmens Belgacom – zu dessen Kunden zahlreiche europäische Institutionen mit Sitz in Brüssel gehören).

In Luxemburg haben die sukzessiven Regierungen übrigens bestritten, dass der eigene Geheimdienst zu PRISM beigetragen habe,[5] dass der Satellitenbetreiber SES Spionage im Auftrag ausländischer Geheimdienste tätige,[6] oder dass Skype von Luxemburg aus zur NSA-Spionage beigetragen habe.[7] Politisches Interesse an einem neuen Geheimdienst-Untersuchungsausschuss gab es nach dem Sturz der CSV-LSAP-Regierung im Juli 2013 offensichtlich nicht mehr. Und obwohl der damalige Premier Jean-Claude Juncker 2013 in der SREL-Enquetekommission unter Eid ausgesagt hat, er habe die Nutzung eines Staatstrojaners untersagt, ist seit dem „Leak" beim Software-Entwickler HackingTeam bekannt, dass der SREL über ein solches Spähprogramm verfügt. Die umstrittene Investigationsfirma Sandstone des früheren Geheimdienstmitarbeiters Frank Schneider stand auch in Kontakt mit HackingTeam.[8] Die Beurteilung, ob Internetüberwachung auch in Luxemburg Grundrechte verletzt, überlässt das Parlament also bis auf Weiteres der Exekutive.

Die Europäische Union beteiligt sich an der (womöglich grundrechtswidrigen) Massenüberwachung übrigens auch auf offiziellem Weg. Abkommen mit den USA regeln die Übermittlung von Flugpassagierdaten (PNR), von Informationen zu Finanztransaktionen (SWIFT) ebenso wie die Datentransfers von Firmen aus der EU in die USA (Safe Harbor). Peter Schaar meint, diese Abkommen sollten ausgesetzt werden, bis sie tatsächlich den Datenschutzanforderungen der EU entsprechen. Auch die Verhandlung über das Freihandelsabkommen TTIP sollten die Europäer an die Bedingung knüpfen, dass ihr Datenschutzrecht respektiert wird.

Dann gelte es die eigenen Hausaufgaben zu machen, und Länder wie Großbritannien und Deutschland daran zu „erinnern", dass sie gegen EU-Verträge verstoßen, da ihre Überwachungstätigkeiten europäische Interessen verletzen. Die EU müsse auch als Wirtschaftsakteur aktiv werden und mit Datenschutzsiegeln und Investitionsprogrammen zur Entwicklung von europäischen Software-Alternativen beitragen. Die Meinungen über die „Sinnhaftigkeit eines regional begrenzten Routings" gingen zwar auseinander, so Schaar, aber „technisch ist es heute ohne weiteres möglich, Datenverbindungen, bei denen beide Kommunikationspartner sich in Europa befinden, nur über europäische Netzknoten zu leiten".

Das Fehlen territorialer Grenzen im Netz bliebe aber auch dann eine Herausforderung für den Grundrechtsschutz. Deshalb hält Schaar ein internationales Abkommen für notwendig. Juristisch gesehen, seien zwar heute schon „Auslandstaten, die sich gegen inländische Rechtsgüter richten" (z. B. Spionage, die das Geschäfts- oder Fernmeldegeheimnis verletzt, oder gegen Datenschutzgesetze verstößt) durchaus strafbar und könnten verfolgt werden. Man sieht jedoch, dass die europäischen

Aufrüsten und Daten schützen

Anonymes Web-Browsen: TOR („The Onion Router"), JonDo, JAP (AN.ON-Projekt)

Verschlüsselte Verbindung zu Webseiten: HTTPS Everywhere

E-Mail-Verschlüsselung: GnuPG, CounterMail, Riseup, Enigmail

Verschlüsselung für das Mobiltelefon (Audio und Nachrichten): RedPhone, TextSecure, Off-the-Record Messaging, SilentPhone, SilentText

Datenschutzfreundlicher Cloud-Dienst mit Verschlüsselung: SpiderOak

Keine unverschlüsselten, öffentlichen Wifi-Netzwerke nutzen

Pseudonyme nutzen und wenn möglich falsche Angaben machen

Tracken blockieren: Adblock, NoScript, Ghostery, Disconnect

Software, die es erlaubt wahre E-Mail-Adressen dank „Wegwerf-Adressen" zu maskieren: MaskMe, Blur

Datenschutzfreundliche Suchmaschinen: DuckDuckGo, ixquick, Metgarer

Online-Dienste in Anspruch nehmen, deren Geschäftsmodell nicht auf der Auswertung und dem Verkauf von Daten beruht, und stattdessen lieber etwas für die Leistung zahlen

Nutzung eines Passwort-Managers (z. B. 1Password), der komplizierte Passwörter generiert und verwaltet

Staaten bisher darauf verzichten, ernsthafte Ermittlungen anzustoßen. Im Fall des abgehörten Merkel-Handys hat die deutsche Bundesanwaltschaft die Ermittlungen mangels Beweisen eingestellt. In der offiziellen Mitteilung heißt es „die mögliche massenhafte Erhebung von Telekommunikationsdaten der Bevölkerung in Deutschland durch britische und US-amerikanische Nachrichtendienste bleibt weiter unter Beobachtung".

Der ehemalige Datenschutzbeauftragte plädiert daher dafür, die völkerrechtliche Verankerung des Datenschutzes zu verbessern. Das könne über ein Zusatzprotokoll zum UN-Zivilrechtspakt erfolgen. Eine entsprechende Initiative von Deutschland und Brasilien ist 2013 gescheitert – auch aufgrund der mangelnden Unterstützung durch andere EU-Mitgliedstaaten. Mittlerweile liegt zu dieser Problematik ein Bericht des UN-Menschenrechtskommissars vor, in dem es heißt, dass die „internationalen Menschenrechtsnormen […] einen klaren und universellen Rahmen für die Förderung und den Schutz des Rechts auf Privatheit [bieten], auch im Zusammenhang mit innerstaatlicher und extraterritorialer Überwachung, dem Abfangen digitaler Kommunikation und der Erhebung personenbezogener Daten. [...] Als Sofortmaßnahme sollten die Staaten ihre eigenen nationalen Rechtsvorschriften, Politiken und Praktiken überprüfen, um ihre volle Übereinstimmung mit den internationalen Menschenrechtsnormen sicherzustellen."[9] Die USA haben zwar mittlerweile einige Änderungen an der NSA-Gesetzgebung vorgenommen, Menschenrechtsnormen haben dabei aber keine Rolle gespielt.

Ob es Gerichten gelingt, gegen die internationalen Abhör- und Spionagepraktiken vorzugehen, bleibt noch abzuwarten. Unter anderem der Europäische Gerichtshof für Menschenrechte muss noch über eine Klage gegen die Überwachungstechniken des GCHQ befinden.[10] Und der Europäische Gerichtshof könnte „Safe Harbor" kippen. Die Richter müssen darüber befinden, ob das nach EU-Recht erforderte „angemessene Datenschutzniveau" noch gegeben ist, wenn US-Firmen die Daten ihrer europäischen Nutzer auf Servern in den USA speichern und diese Daten dann dank „Prism" oder ähnlichen Programmen systematisch bei der NSA landen können. Der Kläger in dieser Sache heißt: Max Schrems.

Standortpolitik statt Datenschutz

Der österreichische Jura-Doktorand und Gründer der Initiative „Europe versus Facebook" sieht in der Einforderung des Grundrechtsschutzes vor Gericht den „wichtigsten Schlüssel für echten Datenschutz". Denn momentan seien EU-Bürger gegen die Exzesse der Datenwirtschaft auf dem Papier zwar gut geschützt, jedoch verstießen die Konzerne systematisch und ungestraft gegen geltendes Recht. Zum Beispiel hat Facebook eine sogenannte „Zustimmung durch Dritte" eingeführt, um damit Zugriff auf Daten von Nicht-Nutzern zu legitimieren: „Facebook fragt einfach alle anderen Nutzer nach Ihren Daten: ‚Lade dein Adressbuch hoch', ‚Synchronisiere dein Handy mit Facebook' […] oder ‚Lade deine Freunde zu Facebook ein'." Facebook hat seinen europäischen Sitz in Dublin. Die somit für die Firma zuständige irische Datenschutzbehörde hält diese „irrwitzige" Praxis jedoch für legal.

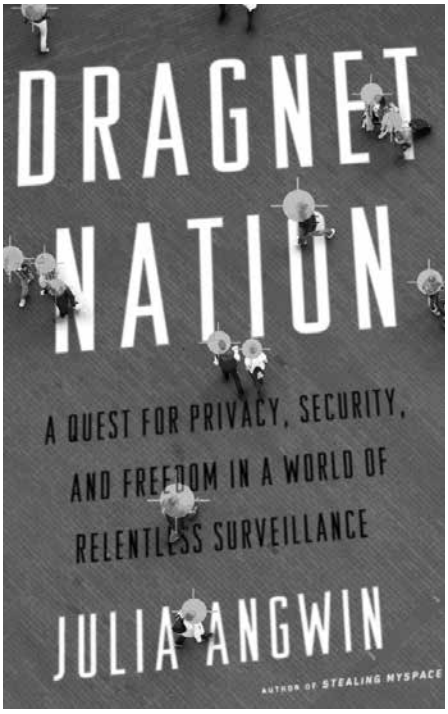
Einige Datenschutzbehörden stehen aktivem Grundrechtsschutz im Weg, da sie zuerst die wirtschaftlichen Interessen ihres Landes im Blick haben

Einige Datenschutzbehörden stehen aktivem Grundrechtsschutz im Weg, da sie zuerst die wirtschaftlichen Interessen ihres Landes im Blick haben: Schrems hält es für symptomatisch, dass der Vize-Chef der Behörde Garry Davis mittlerweile bei Apple als „Head of Privacy Europe" arbeitet. Auch der luxemburgischen Datenschutzkommission (CNPD) wirft Schrems vor, „im Zweifel" für die Firmen Stellung zu beziehen. Auf seine Beschwerde hat die CNPD geantwortet, sie könne keinerlei Datenschutzprobleme bei Skype in Folge der NSA-Affäre erkennen.[11] Seither sah die kleine Behörde aus der Avenue du Rock'n'Roll in Esch-Belval sich häufiger mit dem Vorwurf konfrontiert, Internetkonzerne in Schutz zu nehmen.[12]

Abgesehen von solchen „Extremfällen" fehlt es Schrems zufolge „in allen Staaten an Personal, ausreichenden Kompetenzen und scharfen Untersuchungsrechten. Mancherorts kommt dann noch fehlender Wille und fehlender politischer Rückhalt hinzu." Das Problem ist den Brüsseler Gesetzgebern bekannt und die neue EU-Datenschutzgrundordnung verspricht hier Besserung: Der Druck auf die nationalen Behörden, EU-Recht effektiv durchzusetzen, wird erhöht. Zur Glaubwürdigkeit des europäischen Datenschutzes trägt sicher auch bei, dass in Zukunft empfindliche Geldstrafen bei Missachtung der Gesetze möglich sind.

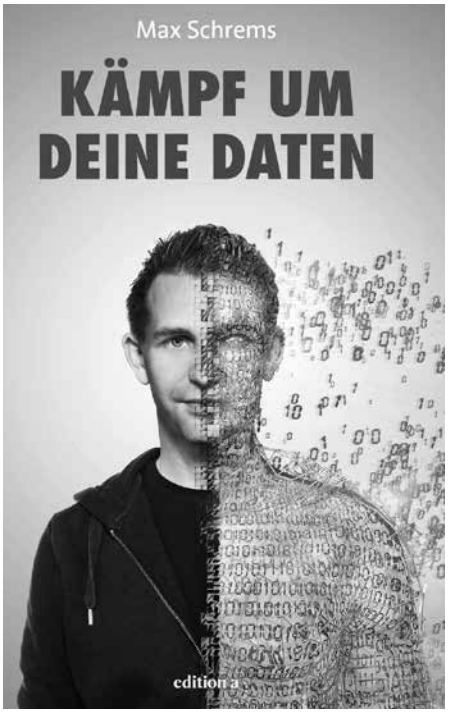
Handlungsbedarf sieht Max Schrems auch bei der Regulierung der Datenwirtschaft. Er plädiert dafür, in den digitalen Markt einzugreifen, um datenschutzfreundlichen Anbietern eine Chance im Konkurrenzkampf gegen Quasi-Monopolisten zu geben. Die Monopolstellung von Firmen wie Google oder Facebook erschwere es, Rechte durchzusetzen. Kritik pralle einfach ab: „Es ist vollkommen egal, ob die Leute einen mögen, ob sie freiwillig dabei sind, ob das Unternehmen einen guten Dienst anbietet, innovativ und kundenorientiert arbeitet, wenn es erst einmal ein Monopol hat."

Zu diesem Marktversagen tragen seiner Meinung nach „geschlossene Netzwerke" bei, mit denen Online-Anbieter ihre Nutzer an sich binden. Sie lassen beispielsweise nicht zu, dass ihre Nutzer mit Kunden anderer Dienste kommunizieren: „Ich kann heute meinen Handybetreiber wechseln und morgen noch mit allen Freunden telefonieren, auch wenn diese bei meinem alten Betreiber sind. Ich kann selbstverständlich von einem E-Mail-Provider zum anderen schreiben. [...] Wenn ich aber nun von Facebook auf ein anderes Netzwerk wechsle, kann ich nicht mehr mit meinen Freunden auf Facebook schreiben." Wäre „Interoperabilität" garantiert, würde Marktdruck entstehen: „Kein Mensch geht in ein Geschäft und sagt: ‚Bitte, ich will das Handy von dem Hersteller, der am meisten Daten von mir absaugt.' [...] Wenn die Unter-



Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance,* New York, Times Books, 2014, 304 S.

Peter Schaar, *Überwachung total. Wie wir in Zukunft unsere Daten schützen,* Aufbau Verlag, 2014, 301 S.



Max Schrems, *Kämpf um deine Daten,* Wien, edition a, 2014, 221 S.

nehmen nun so tun, als ob die Nutzer die Freiheit hätten, nicht überwacht zu werden, dann ist das blanker Hohn."

Schrems nimmt die Internetnutzer auch vor gängigen Einwänden in Schutz. Auch wenn „einige alles ins Netz stellen, haben nicht andere ihr Recht auf Privatheit aufgegeben. Nach der gleichen Logik würde eine große Spendenbereitschaft der Bevölkerung eine Erosion des Eigentumsrechts bedingen. Nur weil viele Leute ihr Geld verschenken, ist das keine Rechtfertigung für Diebstahl."

Auch die im Argumentationsarsenal der IT-Lobbyisten beliebte Gleichung „mehr Daten bedeutet mehr Innovation" hält Schrems in ihrer Einfachheit für „inhärent falsch". Innovativ sei, was größeren gesellschaftlichen Nutzen habe. Beim Autobau zählen dazu höhere Effizienz und Umweltverträglichkeit. In der digitalen Wirtschaft könne „eine maßvolle Pflicht zum Datenschutz" Innovationen provozieren, die es den Nutzern ermöglichen würden, ihre Privatsphäre dem eigenen Bedürfnis entsprechend zu schützen. Julia Angwin argumentiert ähnlich: „We didn't shut down the industrial economy to stop pollution. We simply asked the polluters to be more accountable for their actions. We passed laws and created a new governmental agency [...]. Similarly, we don't need to shut down the data economy." Peter Schaar schlägt in dieselbe Kerbe: „Das Recht und die Technik stehen nicht außerhalb der Gesellschaft, sie sind Resultate und zugleich Triebfedern der Entwicklung." Das von IT-Gurus gerne beschworene „Ende der Privatsphäre" ist eine Kapitulation vor imaginierten Sachzwängen, diese Erkenntnis verbindet die drei Autoren. Mit ihren Büchern legen sie nicht nur die Asymmetrie des technologischen Guerillakriegs offen – sie rüsten ihre Leser mit politischen Argumenten, die in der Datenschutzdebatte häufig zu kurz kommen. ◆

1 Enzensberger, Hans Magnus: Wehrt Euch! Enzensbergers Regeln für die digitale Welt, in: *Frankfurter Allgemeine Zeitung,* 28.2.2014.

2 Für einen Vergleich mit Klimaschutz-Selbstexperimenten siehe: Oppel, Pia: Lesen gegen den Klimawandel, Rezension von Colin Beavan „No Impact Man" und Peter Unfried „Öko. Al Gore, der neue Kühlschrank und ich", in: *forum* 296, Mai 2010, S. 53-54.

3 Angwin entwickelt einen Kriterienkatalog für besseren Datenschutz, der sich an sechs Fragen orientiert. Darunter: „Does the dragnet provide individuals with legal right to access, correct, and dispute the data? Are the dragnet operators held accountable fort he way the data are used? Is the dragnet too intrusive for its purpose?" usw.

4 Biermann, Kai: BND hielt sich Datenschützer mit allen Tricks vom Leib, in: *Die Zeit,* 16.1.2015.

5 Rapport d'activités de la Commission de Contrôle parlementaire du Service de Renseignement de l'Etat 2013.

6 Réponse de Monsieur le Premier ministre, ministre des Communications et des Médias à la question parlementaire N° 1149 de Monsieur Claude Adam concernant Espionnage des lignes de communications par satellite et des „data centers".

7 Rapport de la Commission d'enquête sur le Service de Renseignement de l'État (Document Parlementaire N° 6565), 5. Juli 2013.

8 https://wikileaks.org/hackingteam/emails/emailid/610771

9 Das Recht auf Privatheit im digitalen Zeitalter. Bericht des Amtes des Hohen Kommissars der Vereinten Nationen für Menschenrechte, http://www.un.org/depts/german/menschenrechte/a-hrc-27-37.pdf

10 Gerichtsverfahren nach Snowden: https://netzpolitik.org/2015/gerichtsverfahren-nach-snowden/

11 http://www.cnpd.public.lu/fr/actualites/national/2013/11/skype-microsoft/lettre-skype.pdf, http://www.europe-v-facebook.org/CNPD_Skype.pdf

12 Kürzlich in Zusammenhang mit den gespeicherten Einkaufsdaten bei Amazon: http://www.heise.de/newsticker/meldung/Unbefristete-Amazon-Speicherpraxis-Kritik-an-Luxemburger-Datenschutz-Behoerde-2765721.html