NETZPOLITIK.ORG

Netzpolitik betrifft alle, jede und jeden. Was im Jahr 2012 wichtig war, was vielleicht auch zu kurz kam, darauf blickt dieses Jahrbuch zurück. Die Autorinnen und Autoren waren Beobachter und Akteur zugleich.

Ihre Berichte in diesem Buch fassen die wichtigsten Themen des Jahres zusammen, ordnen ein und reflektieren.

Von A wie ACTA und Anonymous über Open-Data und Überwachung bis zu Urheberrecht und Z wie Zensur: komprimiert, informiert und frei lizensiert.

ISBN: 978-3-8442-4234-8

Markus Beckedahl,
Andre Meister

Jahrbuch Netzpolitik 2012
Von A wie ACTA bis Z wie Zensur.

NETZPOLITIK.ORG

Hrsg. Markus Beckedahl und Andre Meister

Jahrbuch Netzpolitik 2012

Von A wie ACTA bis Z wie Zensur.

Hrsg. Markus Beckedahl, Andre Meister

Jahrbuch Netzpolitik 2012

Von A wie ACTA bis Z wie Zensur

netzpolitik.org

Jahrbuch Netzpolitik 2012
1. Auflage, Dezember 2012
Herausgeber & Redaktion: Markus Beckedahl, Andre Meister
Gestaltung: Andrea Jonjic (Lektorat & Königin der Fußnoten), Andreas Müller (Dr. strg.c. strg.v.) , Matthias „wetterfrosch" Mehldau (Umschlag & Satz)
Titelbild: CC BY 2.0 optikfluffel
ISBN: 978-3-8442-4234-8
Druck und Verlag: epubli GmbH, Berlin, www.epubli.de

Buch kaufen: https://netzpolitik.org/jahrbuch-2012/

Inhalt

Vorwort 7

Wissen 9

Urheberrechtspolitik jenseits des Urheberrechts....11
Interview mit Lawrence Lessig: 10 Jahre Creative Commons....18
Urheberrechtsverletzungen: Das ist doch verboten!....27
Crowdfunding vs. Gratismentalität....30
2012: Das Jahr, in dem Open Education in Deutschland ankam....32
Ohne Gleichberechtigung und sozialen Ausgleich bleibt Open dicht....38
Zur netzpolitischen Dimension von Gangnam Style....41
Interview mit Joi Ito: „Das Internet hat mein Leben gerettet“....43

Daten 47

Datenjournalismus 2012: Mühen der Ebene....49
Informationsfreiheitsgesetz: Das Jahr, in dem wir Kontakt aufnahmen....53
FragDenStaat.de: der Informationsfreiheitsverstärker....59
Deutschland, deine Datenschätze! Open Data Jahresrückblick 2012....62
Das Unbehagen im Datenhaufen: Big Data und Datenschutz....70
Die Versuchungen von Big Data....74

Demokratie 79

Die Reform des europäischen Datenschutzrechts....81
Petitionen 2012: Zwischen Stimmungsbild und Willensbekundung....88
Eine Chronik zum Thema Elektronische Demokratie....95

Ist Open Source demokratisch?.....108
Hilfe, meine Tochter ist auf Facebook: Ein digitaler Elternabend.....114
Zur Zukunft der öffentlich-rechtlichen Medien.....117
Blowing the whistle: Heldinnen oder Kriminelle?.....122

Kontrolle *127*

Wer kontrolliert das Netz?.....129
Die Politik der Internet Governance.....132
Von Selbstregulierung zur Zensur durch private Unternehmen.....142
Die neuen Hilfssheriffs des Internets.....146
Schönes neues Internet-Protokoll: IPv6 & Privacy.....149
Secure-Boot: Wer kontrolliert Ihren nächsten Computer?.....153
Das Meldegesetz: Erst durchgewinkt, dann durchgefallen.....161
Krieg mit Drohnen: Das Gesicht unserer Gegner von morgen.....165

Überwachung *171*

Funkzellenabfrage: Die millionenfache Handyüberwachung Unschuldiger. 173
Interview mit Ulf Buermeyer: „Auf Vorratsdatenspeicherung verzichten“....179
Passenger Name Records: Absturz der Privatsphäre.....183
Regierungen sind noch immer die größte Gefahr für ein freies Netz.....187
Clean IT: Der geheime Plan der EU, der keiner war.....192
Nach INDECT: Ein Plädoyer für eine fundiertere Überwachungskritik.....196

Aktivismus *203*

ACTA und die Folgen.....205
25.000-Euro-Kampagne: Der Waffenindustrie das Fürchten gelehrt.....214
Anonymous: Leuchtfeuer der digitalen Freiheit.....220

Big Picture 229

Digitale Solidarität. Perspektiven der Netzpolitik.....231
Netzpolitik in Österreich.....241
EU-Strategie zur Cybersicherheitspolitik im internationalen Umfeld.....246
Das Jahr, in dem die Netzpolitik Emotionsbingo spielte.....259

AutorInnenverzeichnis 265

Vorwort

Liebe Leserinnen und Leser,

warum ein Buch, werden sich viele vielleicht fragen, wenn wir den Rest des Jahres ohnehin ein Blog vollschreiben? Die Antwort ist ganz einfach: Wir lieben Bücher. Uns ist es aber mittlerweile egal, auf welchem Trägermedium sie zu uns kommen. Hauptsache kein Kopierschutz. Während das Blog uns ermöglicht, tagesaktuell und vor allem schnell über Ereignisse und Entwicklungen zu berichten, bietet ein Buch Zeit zum Reflektieren.

Die Idee für dieses Buch hatten wir schon lange: Aus verschiedenen Perspektiven das vergangene Jahr reflektieren und zusammenfassen. Immer passiert so viel, aber viel verschwindet auch aus der Erinnerung. Aus dem üblichen „müsste man mal …“ wurde in den letzten Jahren eine andere Idee: Warum nicht die besten Artikel aus netzpolitik.org am Ende des Jahres zu einer Kollektion zusammen stellen? Aber es fehlte die Zeit. In diesem Jahr gaben wir uns einen Tritt und fragten herum, wer mitmachen will. Wir waren selbst überrascht, wie viele bereit waren, einen Artikel beizutragen, damit aus der Idee eine konkrete Umsetzung wird.

Statt den interessantesten und beliebtesten Artikeln auf netzpolitik.org gibt es in diesem Buch jetzt viele neue und bisher unveröffentlichte Beiträge. Für die Unterstützung möchten wir uns bei allen Autorinnen und Autoren herzlich bedanken. Ganz herzlich danken wollen wir auch allen Beteiligten im Hintergrund: Christian Heise hat uns in vielen Fragen bezüglich der Vertriebswege und Möglichkeiten beraten. Matthias „wetterfrosch“ Mehldau hat das Cover-Design entworfen und das Layout gemacht. Andreas Müller und

Andrea Jonjic haben unermüdlich übersetzt und Korrektur gelesen. Christian Wöhrl steuerte die Übersetzung des Interviews mit Lawrence Lessig bei. Zuletzt darf natürlich der Dank an epubli nicht fehlen, für die unkomplizierte Zusammenarbeit und 1000 Freiexemplare unseres Jahrbuchs.

Dieses Buch ist auch ein Experiment für uns. Wir wissen bereits, wie aufwändig es sein kann, Texte zu schreiben. Auf unserem Blog netzpolitik.org publizieren wir seit über acht Jahren fast täglich Artikel, von kurzen Hinweisen bis hin zu halben Büchern. Einige von uns haben auch bereits Erfahrungen mit dem Publizieren von Büchern in Kooperation mit Verlagen gemacht. Erst in diesem Jahr ist beispielsweise das Buch „Die digitale Gesellschaft – Netzpolitik, Bürgerrechte und die Machtfrage“ im dtv-Verlag erschienen, das Markus Beckedahl zusammen mit Falk Lüke geschrieben hat.

Was wir jetzt gerne ausprobieren wollen: Wieviel Aufwand ist es in heutigen Zeiten, selbst zum Verleger zu werden und ein Buch zu veröffentlichen? Wie funktionieren die dafür notwendigen Vertriebswege, von Print-on-Demand bis zu den unterschiedlichen eBook-Infrastrukturen? Und: Kauft das auch wer? Wenn ja, über welchen Weg? Das wollen wir austesten und darüber wiederum im Blog berichten.

Apropos kaufen: Dieses Buch steht unter der Lizenz Creative Commons Namensnennung – Weitergabe unter gleichen Bedingungen. Es darf zu den Bedingungen der CC BY-SA 3.0 Lizenz beliebig genutzt und weiter verteilt werden. Das ist zugleich unser Beitrag zum zehnten Geburtstag von Creative Commons. Wir freuen uns natürlich trotzdem, wenn das Buch als eBook oder in gedruckter Form erworben wird, weil das netzpolitik.org finanziell zugute kommt. Für alle, die es auf anderen Wegen erhalten: Wenn Euch unsere Arbeit gefällt, freuen wir uns über Unterstützung. netzpolitik.org wird im Jahr 2013 mit Crowdfunding experimentieren, um die Redaktion ausbauen zu können.

Kann sein, dass das Buch niemanden außer unsere Familien interessiert. Sollte dieser Fall eintreten, haben wir wenigstens an Erfahrung gewonnen. Verlieren kann man dabei nicht.

In diesem Jahr ist viel passiert. Wir waren Beobachter und Akteur zugleich. Davon berichtet dieses Buch. Viel Spaß beim Lesen.

Markus Beckedahl und Andre Meister

Wissen

Urheberrechtspolitik jenseits des Urheberrechts

Leonard Dobusch

Wer bei Urheberrechtsproblemen nur auf eine Reform des Urheberrechts setzt, hat fast schon verloren. Kreative Lösungen setzen auch jenseits einer Reform des Urheberrechts an – und zwar mit Hilfe von Creative Commons, das im Dezember 2012 seinen 10. Geburtstag gefeiert hat.

Der Reformbedarf im Urheberrecht ist groß, die Liste an Reformvorschlägen lang. Wer sich heute medienkompetent im Internet bewegt, verletzt regelmäßig und fast schon automatisch Urheberrechte. Sei es der geteilte Link auf Facebook, bei dem der Algorithmus ein Foto der Webseite einbindet oder sei es das Video der letzten Geburtstagsparty auf dem privaten Blog: oft werden dabei urheberrechtlich geschützte Werke eingebettet, ohne die Rechte geklärt zu haben. Auch Lehrer, Archivare und Künstler kämpfen vielfach mit einem komplizierten und unzeitgemäßen Urheberrecht.

Viele Reformvorschläge sind aber sehr umstritten, unrealistisch oder beides, wie das Beispiel der Forderung nach Verkürzung langer urheberrechtlicher Schutzfristen beweist. Eine automatische Schutzdauer von über 70 Jahren nach dem Tod des Urhebers mag für eine winzige Minderheit besonders gut verwertbarer Werke – Mickey Mouse Comics und Musik von Elvis Presley zum Beispiel – noch irgendwie nachvollziehbar sein. Für die große Mehrheit an Werken, die bereits nach wenigen Jahren kaum mehr kommerziell genutzt wird, führt diese Schutzfrist aber mit der Zeit zur Verwaisung. Das Abklären von Rechten wird schwerer und teurer, die Nutzung komplizierter und bleibt schließlich völlig aus. Weil das besonders viele Werke des vergangenen Jahrhunderts betrifft, sprechen Archivare in diesem Zusammenhang von der „Lücke des 20. Jahrhunderts“: ein großer Teil unseres kulturellen Erbes verrottet in Archiven, anstatt in Remix-Kunst, Schulen oder Online-Plattformen wie Wikipedia verwendet zu werden.

Eine Verkürzung urheberrechtlicher Schutzfristen scheitert aber nicht nur am heftigen Widerstand großer Rechteinhaber, die an Longsellern wie den Beatles besonders gut verdienen, sondern auch an internationalen Verträgen wie der Revidierten Berner Übereinkunft oder dem TRIPS-Abkommen im Rahmen der Welthandelsorganisation. Weil die langen urheberrechtlichen

Schutzfristen in diesen von über 100 Staaten ratifizierten Abkommen nur einvernehmlich geändert werden könnten, sind sie quasi in Stein gemeißelt. Ähnliches gilt für den Bereich von Ausnahmeregelungen, den sogenannten „Schranken" des Urheberrechts. Auch ihnen werden in denselben internationalen Verträgen enge Grenzen gesetzt.

Eine Urheberrechtspolitik, die bloß auf die Reform des Urheberrechts setzt, ist also von vornherein dazu gezwungen entweder am ganz großen Rad internationaler Verträge zu drehen oder kleine, nationale Reformbrötchen zu backen. Aber selbst wer sich damit abgefunden hat, der kämpft noch mit den vielfältigen Anwendungsbereichen des Urheberrechts. Was Softwarefirmen recht ist, muss Filmschaffenden noch lange nicht billig sein. Während Autoren und Musiker mit dem Verkauf ihrer Werke Geld verdienen wollen, ist diese Frage für Forschung und Lehre von untergeordneter Bedeutung: sie sind größtenteils öffentlich finanziert. Die einen profitieren von langen Schutzfristen, den anderen sind sie ein Dorn im Auge.

Glücklicherweise aber muss sich Urheberrechtspolitik nicht auf Veränderungen des Urheberrechts beschränken. In vielen Bereichen lässt sich Urheberrechtspolitik sogar völlig ohne Änderung von Gesetzen betreiben. Der Schlüssel für eine Versöhnung des Urheberrechts mit der digitalen Revolution sind alternative Urheberrechtslizenzen wie Creative Commons. Sie basieren zwar auf dem Urheberrecht, räumen Dritten allerdings bestimmte Nutzungsweisen ein, die mehr und mehr zum Internet-Alltag gehören: öffentliches Zugänglichmachen, digitale Weitergabe und, je nach Lizenzmodul, auch Remix und kommerzielle Verwertung.

Der bekannteste Nutzer von Creative Commons ist die Online-Enzyklopädie Wikipedia. Erst die Creative-Commons-Lizenz ermöglicht, dass aus Millionen von Einzelbeiträgen Hunderttausender Autoren ein gemeinsames Werk wird. Weil alle Beitragenden die Lizenzbedingungen akzeptieren, müssen zwischen den vielen Autoren keine Rechte geklärt werden – und auch Dritte können ohne nachzufragen Teile der Wikipedia wie zum Beispiel Fotos oder Kartenmaterial in ihre Werke einbinden.

Creative Commons bietet sich aber nicht nur für digitale Gemeinschaften wie die Wikipedia-Community an. Die Lizenzen sind Dank ihres modularen Aufbaus (siehe Tabelle) genauso flexibel einsetzbar, wie es die vielfältigen Anwendungsbereiche des Urheberrechts erfordern. Fotografen, die nichts dage-

gen haben, wenn ihre Werke in privaten Blogs und auf Facebook auftauchen, können sich mit dem Non-Commercial-Modul eine kommerzielle Nutzung vorbehalten. Eine Tageszeitung müsste also weiterhin für einen Abdruck des Fotos zahlen. Ähnlich im Musikbereich: Filesharing und Verwendung in privaten Videos können erlaubt und gleichzeitig für den Einsatz in Werbespots oder Spielfilmen eine Vergütung verlangt werden.

Vor allem im öffentlichen Bereich ist das Potential von Creative Commons besonders groß. Wo Verwertungsinteressen nicht im Vordergrund stehen, bietet Creative Commons eine einfache und etablierte Lösung, um digitale Verbreitung und Weiternutzung von Werken zu ermöglichen, ja zu fördern. Umso erstaunlicher, dass es in diesem Bereich bislang noch kaum zum Einsatz kommt. Drei Felder eignen sich besonders für Urheberrechtspolitik jenseits von Urheberrechtsreform mit Hilfe von Creative Commons: die Vergabe öffentlicher Kulturförderungen, der öffentliche Rundfunk sowie Bildung und Wissenschaft.

Die eingefahrenen Bahnen der staatlichen Kulturförderpolitik sind spätestens seit der Forderung nach radikaler Umverteilung von Fördermitteln in der Streitschrift „Kulturinfarkt" Thema. Unabhängig davon lohnt es aber jedenfalls, bei der Vergabe öffentlicher Kulturfördermittel die Frage der Lizenzierung geförderter Werke überhaupt einmal zum Thema zu machen. Denn mit der Verwendung einer freien Lizenz ist ein Zusatznutzen für die Allgemeinheit verbunden. Bibliotheken und Schulen können frei lizenzierte Werke kostenlos zugänglich machen und andere Kreative können solche Werke unkompliziert in neue Schöpfungen einbauen. Bislang jedoch spielt die Lizenzfrage bei der Vergabe von Förderungen keine Rolle.

Wie es gehen könnte, zeigt die österreichische Stadt Linz. Seit sie 2009 Kulturhauptstadt Europas war, erhalten geförderte Künstler, die ihre Werke unter einer freien Lizenz veröffentlichen, einen Förderbonus in Höhe von zehn Prozent. Wichtiger noch als diese Vergütung und die damit verbundene Anerkennung für den gesellschaftlichen Mehrwert offener Lizenzierung ist aber der Aufklärungseffekt der Maßnahme: Antragssteller setzen sich dadurch oft erstmals mit der Option Creative Commons auseinander. Auf diese Weise wird mit der Berücksichtigung von Creative Commons in der Kulturförderung auf kommunaler Ebene Urheberrechtspolitik gemacht.

Der größte öffentliche Produzent urheberrechtlich geschützter Inhalte ist aber wohl der öffentlich-rechtliche Rundfunk. Wie im Bereich der Kulturförderung ist allerdings Creative Commons dort fast unbekannt. Wieder gibt es nur ein gallisches Dorf von Creative-Commons-Nutzern, konkret das Medienmagazin ZAPP des NDR. Dessen Beiträge stehen unter einer Creative-Commons-Lizenz. Angenehmer Nebeneffekt: auf diese Weise bleiben die Sendungen trotz Pflicht zum Depublizieren dauerhaft online verfügbar.

In beiden Fällen, Kulturförderung und öffentlicher Rundfunk, sind es vor allem zwei Hürden, die einer Verwendung von Creative Commons derzeit noch im Wege stehen. Erstens sind an Film- und Tonwerken meistens eine größere Zahl an Urhebern beteiligt, die alle einer freien Lizenz zustimmen müssten. Da eine solche Option in den Standardverträgen derzeit aber weder vorgesehen ist noch entsprechend vergütet wird – schließlich könnten Wiederholungshonorare wegfallen – sind die Werke trotz öffentlicher Finanzierung nicht frei verfügbar. Zweitens sind die allermeisten beteiligten Kunstschaffenden Mitglieder in Verwertungsgesellschaften. Diese verbieten aber meistens, wie im Musikbereich die GEMA, die Verwendung von Creative Commons für ausgewählte Werke. Die Adressierung beider Probleme, Vertragsgestaltung genauso wie Verwertungsgesellschaften, bedarf keiner Änderung des Urheberrechts. Urheberrechtspolitik bedeutet hier vielmehr, Geschäftspraktiken und Verwertungsgesellschaften mit freien Lizenzen wie Creative Commons kompatibel zu machen – und auch Vergütungen entsprechend anzupassen.

Noch offensichtlicher ist das Potential für Urheberrechtspolitik jenseits von Urheberrechtsreformen im dritten Feld, dem Bereich von Bildung und Wissenschaft. Wieder werden urheberrechtlich geschützte Werke öffentlich finanziert, wieder sind sie deshalb aber noch lange nicht auch öffentlich zugänglich. Im Bereich der Wissenschaft ist die Situation besonders bizarr: öffentlich finanzierte Forscher schreiben Aufsätze, die von anderen öffentlich finanzierten Forschern begutachtet und schließlich von öffentlich finanzierten Universitätsbibliotheken zu exorbitanten Preisen von Wissenschaftsverlagen zurückgekauft werden. Obwohl weder für das Verfassen noch für die Begutachtung von Artikeln Geld fließt, kosten Abos wissenschaftlicher Zeitschriften bis zu 20.000 Euro pro Jahr – und werden nur in teuren Paketen verkauft. Angesichts dieser Situation setzen die großen Wissenschaftsorganisationen wie Max-Planck-Gesellschaft und Deutsche Forschungsgemein-

schaft auf die Förderung von Open-Access-Zeitschriften, die ihre Inhalte unter Verwendung von Creative-Commons-Lizenzen frei zugänglich machen. Auch im nächsten EU-Rahmenprogramm wird die Vergabe von Forschungsförderung an öffentlichen Zugang zu den solcherart finanzierten Ergebnissen gekoppelt sein.

Während also in der Wissenschaft einiges in Bewegung ist, lässt sich Ähnliches für den Bildungsbereich nicht behaupten. Schulbücher werden nicht nur immer noch auf tote Bäume gedruckt und in überdimensionierten Rucksäcken durch die Gegend geschleppt, sondern sie sind trotz Finanzierung über öffentliche Gelder oder Elternbeiträge nicht frei online verfügbar. Mehr noch, nirgends bewegt man sich so schnell in der Illegalität, wie im Bereich von Lehr- und Lernunterlagen. Zwar gibt es im Urheberrecht Ausnahmen für den Bildungsbereich – ausgenommen von dieser Ausnahme sind aber just jene Materialien, die speziell für den Bildungsbereich hergestellt werden.

Was wie ein Schildbürgerstreich klingt, hat in Deutschland erst mit 1. Januar 2008 nach heftigem Lobbying der Schulbuchverlage als §53 Abs. 3 Eingang ins Urheberrechtsgesetz gefunden. Er untersagt die digitale Verwendung auch nur kleinster Teile, also zum Beispiel einer einzelnen Grafik oder Übung, eines anderen als des verwendeten Lehrbuchs. Hauptprofiteure dieser Regelung sind die drei Großverlage Klett, Cornelsen und Westermann, die 90 Prozent des deutschen Schulbuchmarktes unter sich aufteilen. Auf der Strecke bleiben didaktische Vielfalt, Kreativität und letztlich Qualität des Unterrichts.

In anderen Ländern wie den USA, Kanada oder Polen investieren öffentliche und private Bildungsträger deshalb in offene Lernunterlagen unter Creative-Commons-Lizenz, sogenannte Open Educational Ressources. Ziel ist nicht unbedingt Kostensenkung sondern ein Systemwechsel. Offene Ausschreibung der Erstellung frei lizenzierter Lernunterlagen sorgt für mehr Wettbewerb und gleichzeitig dafür, dass der digitalen Nutzung der Lernunterlagen durch Lehrer und Schüler kaum Grenzen gesetzt sind. Unternehmen wie Flatworld Knowledge wiederum beweisen, dass sich auch mit offenen Lernunterlagen Geld verdienen lässt. Der US-amerikanische Lehrbuchverlag verdient Geld mit Printausgaben und Dienstleistungen rund um die Erstellung digitaler Lernmaterialien.

In Deutschland braucht es für die Förderung offener Lernunterlagen vor allem eine Umstellung von Ausschreibungsregelungen und Qualitätssicherungsverfahren für Schul- und Lehrbücher. Bis vor kurzem war das reine Zukunftsmusik, doch mittlerweile haben Bildungsministerium und Kultusministerkonferenz 25 Experten zu einer Anhörung zu offenen Lernunterlagen geladen. Bei aller gebotener Skepsis was die Dynamik deutscher Bildungspolitik betrifft scheint also auch hierzulande etwas in Bewegung zu geraten. Es gilt aber auch in diesem Fall: Urheberrechtspolitik ist jenseits von Urheberrechtsreform möglich. Mehr noch, wie die angeführten Beispiele zeigen, erlauben Lizenzen wie Creative Commons gezielt Schwerpunkte in jenen Bereichen zu setzen, wo die herrschende Urheberrechtssituation besonders unzufriedenstellend ist. Jenseits der Einheitsgröße Urheberrechtsgesetz erlauben sie in verschiedenen Feldern eine Annäherung an ein Urheberrecht nach Maß.

Creative Commons: Lizenzbausteine

Creative Commons bietet auf seiner Homepage ein System urheberrechtlicher Lizenzverträge kostenfrei an, die es Kreativen möglichst einfach machen sollen, Dritten bestimmte Rechte an ihren Werken einzuräumen. Der jeweilige Lizenzvertrag wird dabei aus den folgenden vorformulierten Lizenzbausteinen frei zusammengestellt:

Namensnennung („Attribution", BY): Erlaubt anderen, unter der Voraussetzung, dass die Rechtsinhaberschaft durch Nennung des Namens anerkannt wird, den Inhalt und darauf aufbauende Bearbeitungen zu vervielfältigen, zu verbreiten, aufzuführen und öffentlich zugänglich zu machen.

Nicht-Kommerzielle Nutzung („Noncommercial Use", NC): Erlaubt anderen, den Inhalt und darauf aufbauende Bearbeitungen zu nicht-kommerziellen Zwecken zu vervielfältigen, zu verbreiten, aufzuführen und öffentlich zugänglich zu machen. Kommerzielle Nutzung erfordert eine gesonderte Vereinbarung.

Keine Bearbeitungen („No Derivatives", ND): Erlaubt anderen, nur unveränderte Kopien des Inhalts zu vervielfältigen, zu verbreiten, aufzuführen und öffentlich zugänglich zu machen, dagegen sind keine Bearbeitungen erlaubt, die auf dem Inhalt basieren.

Weitergabe unter gleichen Bedingungen („ShareAlike", SA): Erlaubt anderen, Bearbeitungen des Inhalts nur unter einem Lizenzvertrag zu verbreiten, der demjenigen entspricht, unter dem der Inhalt lizenziert worden ist.

Interview mit Lawrence Lessig: 10 Jahre Creative Commons

netzpolitik.org: Sicher hast du diese Frage schon viel zu oft beantwortet, aber warum habt ihr Creative Commons gegründet?

Lawrence Lessig: Der konkrete Anlass war, dass wir damals den Fall Eldred vs. Ashcroft verhandelten, und Eric Eldred war skeptisch, ob wir den Fall gewinnen könnten. Und er sagte, er wolle sicherstellen, dass bei der Verhandlung nicht bloß ein verlorener Fall vor dem Obersten Gerichtshof der Vereinigten Staaten heraus käme, sondern dass daraus ein tragfähiges Fundament entstehen würde für das, was wir heute Freie Kultur nennen.

Ich fand das richtig; und ich erkannte (was noch wichtiger war), dass wir, um jemals echte Veränderungen zu bewirken, bei den Menschen selbst auf Verständnis hinwirken müssten. Das hier würde sich nicht von oben verordnen lassen, es würde von unten wachsen müssen. Also begannen einige von uns darüber zu sprechen, wie man so eine Bewegung schaffen könnte, um diese Idee umzusetzen: Wie man Menschen in die Lage versetzen könnte, zu zeigen, dass sie an keines der beiden Extreme glauben – weder an perfekte Kontrolle noch an den Verzicht auf sämtliche Rechte. Und das war die Initialzündung für Creative Commons.

netzpolitik.org: Es gab doch schon mehrere Open-Content-Lizenzen. Warum habt ihr eigene CC-Lizenzen entwickelt, statt zum Beispiel die bestehenden Lizenzen der Free Software Foundation zu unterstützen?

Lawrence Lessig: Das hatte zwei Gründe. Erstens dachten wir, dass wir einen größeren und flexibleren Bereich von Lizenzen bräuchten. Die GNU-Lizenz für freie Dokumentation ist zum Beispiel so ein Fall einer freien Lizenz, die sich nicht unbedingt auf alle Arten von Material anwenden lässt. Aber zweitens fanden wir es wirklich wichtig, dass man seine eigenen Lizenzen verstehen kann; es war sehr wichtig, endlich eine Architektur einzubetten, die (A) menschenlesbar, verständlich wäre, (B) maschinenlesbar und (C), ganz wesentlich, auf dem Rechtsweg durchsetzbar. Und keine der anderen Lizenzierungsstrukturen da draußen hatte diese Anforderungen berücksichtigt, drei Sprachen zugleich sprechen zu können. Das gab uns den Anstoß zu diesem Konstrukt.

Von Anfang an hatten wir es uns auf die Fahne geschrieben, zwischen den freien Lizenzen Portabilität zu ermöglichen; mit der GNU-Lizenz für freie Dokumentation ist uns das gelungen, und bei der Lizenz Freie Kunst sind wir da noch in Gesprächen. Unsere Idee war, dass es irgendwann egal sein soll, in welchem Bereich freier Lizenzen man sich bewegt, Hauptsache, es findet sich eine äquivalente freie Lizenz, die kompatibel mit CC ist.

netzpolitik.org: Du hast gesagt, CC sei ein Werkzeug gewesen, mit dem Leute dokumentieren können, dass sie an der Urheberrechts-Grundeinstellung, „alle Rechte vorbehalten", nicht interessiert sind. Inwieweit ist es für dich ein Werkzeug, und inwieweit ist es eine Bewegung?

Lawrence Lessig: Ich denke, es muss beides verbinden. Es muss echten Wert erzeugen, also kann es nicht nur eine Bewegung sein – echten Wert meine ich im Hinblick auf Leute, die schöpferisch tätig sein wollen. Sehr wichtig dabei war der Aspekt eines Innovations-Ökosystems, das auf der Grundlage freier Inhalte aufbaut. Es gibt da zum Beispiel ein paar ganz tolle Android- und iPhone-Apps, die auf dem freien flickr-Archiv CC-lizenzierter Bilder aufsetzen. Nehmen wir Haikudeck: Damit lassen sich Bildersammlungen erstellen, indem die Software, sobald man anfängt, ein Wort zu tippen, die Bedeutung analysiert und dazu passende Fotos von flickr zieht, CC-lizenzierte Fotos. Und damit es hochwertige Bilder werden, schaut die App nach, aus welcher Kamera sie kommen, und wenn es eine super Kamera war, dann wird sie wohl auch super Fotos gemacht haben (lacht). Die Bilder, die man damit bekommt, sind echt erstaunlich; diese App, diese ganze Art und Weise, Kreativität verfügbar zu machen, das wäre alles gar nicht möglich ohne das grundlegende Ökosystem frei lizenzierter Werke.

Insofern erfüllt es eine Funktion; wie ja auch diese Remix-Musik und Remix-Websites sich nicht bloß auf CC stützen, sondern CC in ihrem Erbgut haben: Es ist schlicht unmöglich, ohne solch eine Struktur ein Werk zu lizenzieren. Auf diese Weise liefert es einen echten Mehrwert beim Erledigen deiner Arbeit. Aber eine Stufe darüber ist eine Bewegung, Leute, die zu Universitäten sagen, „eure Arbeit sollte nicht weggeschlossen bleiben", worauf kommt „aber was sollen wir sonst machen?", und darauf antworten sie, „ihr könntet ja zum Beispiel unter einer beliebigen CC-Lizenz veröffentlichen". Und hier müssen wir beide Seiten ermutigen, weil es noch ein weiter Weg ist bis dahin, dass die Leute begreifen, dass das Urheberrecht in seiner herkömmlichen Form keinen Sinn ergibt.

netzpolitik.org: Als du CC mitbegründet hast, war es euch da schon klar, dass es so bald eine internationale, eng vernetzte Organisation werden würde, oder habt ihr euch am Anfang nur auf die USA konzentriert und erst später um den Rest der Welt gekümmert?

Lawrence Lessig: Ich habe von Anfang an daran geglaubt, dass wir einen internationalen Fokus brauchen. Und wir hatten das große Glück, Christiane Asschenfeld, heute von Donnersmarck, zu finden, die sich um die internationale Seite kümmern wollte. Sie eröffnete das Büro in Berlin und ruck-zuck hatten wir ein System für die vereinfachte Vergabe und die Portierung von Lizenzen, und dann hatten wir auch schon ein internationales Netzwerk. Und das war sehr wichtig, denn der Erfolg hing davon ab, dass man das Projekt als eine Idee der Freiheit auffassen würde – nicht als eine originär amerikanische Idee. Und indem wir das internationale Projekt unter unsere Fittiche nahmen, konnten wir viele Leute zur Mitarbeit hier bewegen: Sie portierten Lizenzen und wurden so ein Teil der Community. Ihr beide, ihr wart ja schon von Anfang an bei uns und wisst, wie dieser Prozess abgelaufen ist; aber in vielen Ländern wird das Ganze so wahrgenommen, dass einige zentrale Leute auf kreative, progressive Art über das Problem nachdenken, und das gibt den Anstoß für diverse andere Aktivitäten, die darauf aufbauen.

netzpolitik.org: Reden wir mal über die Zukunft: Immer mal wieder kommen Leute zu uns, die ein Projekt zu Open Access planen; oder eins darüber, wie man Open Access zertifiziert; oder die einen Open-Access-Standard für Wissenschaft und Forschung etablieren wollen. Und die sagen, „hey, es gibt da diesen Standard für Freie Software, der von der Free Software Foundation zertifiziert ist"; da weiß jeder, klar, das hier ist Freie Software und das hier nicht. Aber bei Open Access ist das nicht so klar. Ist etwas Open Access oder wird es bloß so gelabelt? Kannst du dir also vorstellen, dass irgendwer, ein Komitee, eine Institution, einen weltweit verbindlichen Standard für Open Access definiert, wie das die Free Software Foundation für Freie Software getan hat?

Lawrence Lessig: Nun, es gibt da ja schon eine Körperschaft, die sich in Verbindung mit der Wikipedia ergeben hat und deren Aufgabe es ist, Werke freier Kultur als solche zu kennzeichnen. Und einige der CC-Lizenzen sind mit diesem Free-Cultural-Works-Label vereinbar, und einige andere sind es nicht. Ich halte das für wertvoll insofern, als da Leute sind, die diese Unterscheidung treffen mögen und die eben lieber auf Material aufbauen wollen, das als

Werk freier Kultur definiert ist. Das ist schon sehr nützlich. Aber wovon ich noch nicht überzeugt bin, das ist diese Sitte, die Lizenzstruktur als Waffe gegen Leute einzusetzen, die ihr Material nicht genau so lizenzieren, wie gewisse andere Leute das erwarten würden. Es gibt da draußen eine unglaubliche Vielfalt von Kreativen, die aus den unterschiedlichsten Motiven Dinge erschaffen – und unter den verschiedensten Zwängen.

Ein Beispiel: Einer der ersten Filme, die wir bekamen, war ein Film von Davis Guggenheim, der auch „Eine unbequeme Wahrheit" und „Waiting for ‚Superman'" gemacht hat. Darin geht es um Erziehung, und er wurde teilweise in öffentlichen Schulen gedreht. Dementsprechend sieht man in dem Film ziemlich viele Kinder. Und Davis wollte den Film unter CC lizenzieren, um den Zugang möglichst einfach zu machen. Aber er fühlte auch eine moralische Verantwortung den Kindern gegenüber: Ihre Aufnahmen sollten nicht in einem anderen Kontext verwendet werden als demjenigen, in dem er die Kinder dargestellt hatte. Also verwendete er eine Lizenz, die keine Bearbeitung erlaubt (Anm.: CC-Lizenzelement ND), weil es ihm wichtig war, die Menschen zu schützen, die er zeigte. Das finde ich völlig in Ordnung, obwohl es ja streng genommen keine freie Lizenz mehr ist. Nein, ich finde, wir sollten aufhören, davon zu träumen, dass die ganze Welt so funktioniert wie freie Software, und lieber akzeptieren, dass es diese Unterschiede gibt. Und dann sollten wir die Leute in Richtung dieser Freiheit stupsen, damit sie Dinge tun können, die ihren eigenen Werten entsprechen und den jeweiligen Absichten ihres Kulturschaffens.

netzpolitik.org: Kommen wir zur nächsten Frage: Wir haben ständig diese Diskussion mit den Wikipedianern, dass nur die Lizenzen, die kommerzielle Nutzung erlauben, freie Kultur seien – den Rest könne man vergessen. Außerdem haben wir ein Definitionsproblem für „nichtkommerziell" (Anm.: CC-Lizenzelement NC). Wie würdest du nichtkommerziell definieren? Und würdest du es im Rückblick aus heutiger Perspektive noch mal genauso machen?

Lawrence Lessig: Meiner Ansicht nach war „nichtkommerziell" (weniger im geschriebenen Sinn der Lizenz als im umgangssprachlichen Verständnis) ein Platzhalter für eine bestimmte kulturelle Übereinkunft, die besagt: Ich stelle dir etwas zur Verfügung und es ist völlig okay, wenn du dich daran bedienst. Aber es ist absolut nicht okay, wenn du die Früchte meiner Arbeit nimmst, um sie sonst jemandem zu verkaufen. Okay, so würde das niemand ausdrücken; es gibt einfach kein simples Wort dafür, um diese Grenzlinie zu beschreiben,

zumal die Linie je nach Kontext ja auch immer anders verlaufen kann. Jedenfalls finde ich es völlig nachvollziehbar, dass du zum Beispiel eine CD mit einer Menge frei lizenzierter Musik unter nichtkommerzieller Lizenz und mit Weitergabe unter gleichen Bedingungen (Anm. CC-Lizenzelemente NC, SA) herausbringen würdest. Denn die Idee, dass Sony daraus einen Filmsoundtrack machen und damit Geld scheffeln könnte – klar, ich verstehe vollkommen, wenn jemand sagt, er will das nicht.

Ich selbst lizenziere meine Arbeiten ja komplett frei; ich wäre happy, wenn jemand meinen Kram nehmen und daraus einen Film machen würde (lacht). Aber ich denke nicht, dass jemand die schlechtere Kreative ist oder weniger der Idee Freier Kultur verpflichtet, wenn sie sagt, „wenn jemand von meiner Arbeit profitieren will, sollte er zuerst mit mir darüber reden". Ich wünschte, wir könnten die Grenze zwischen dieser kulturellen Übereinkunft und der jeweils angemessenen kommerziellen Interaktion klarer bestimmen. Und wir grübeln ja immer noch über Methoden, wie wir die Grenzbestimmung vereinfachen können. Aber ich bleibe bei meiner Überzeugung, dass es diese Trennung gibt und dass sich Menschen ausgenutzt fühlen würden, wenn sie ihre Arbeit verfügbar machen und daraus Dritten die Möglichkeit erwächst, Geld zu verdienen, ohne dass davon etwas beim ursprünglichen Urheber ankommt.

netzpolitik.org: CC feiert ja gerade zehnten Geburtstag. Welche Entwicklungen haben wir in Zukunft zu erwarten. Welche strategischen Ziele habt ihr für die Organisation und die Lizenzen? Soll es noch mehr Lizenzen geben, oder kümmert ihr euch um noch mal andere Sachen?

Lawrence Lessig: Ich hoffe – aber ich bin nicht mehr im Management, also kann ich nichts versprechen – auf einen sehr spannenden neuen Ansatz, den wir zurzeit diskutieren. Das ist der Ansatz, mehr Leute an die Lizenzierungsstrukturen heranzuführen, indem wir ihnen eine effektivere Methode an die Hand geben, ihre Rechte durchzusetzen. Dann könnte auch, sagen wir, ein Profifotograf ein Interesse haben, so eine Lizenz zu verwenden. Er könnte dann guten Gewissens die nichtkommerziellen Rechte an seiner Arbeit freigeben, wenn er im Gegenzug weiß, er bewegt sich innerhalb eines Rechtsrahmens, in dem die Durchsetzbarkeit seiner Rechte viel effizienter ist als im bestehenden System. Daran arbeiten wir jedenfalls momentan. Und darin sehe

ich eine riesige Chance, denn damit würde man ja nicht nur mehr Werke frei unter CC-Lizenzen zugänglich machen, sondern man würde im Prinzip die Urheberrechts-Gesetze ganz allgemein vereinfachen.

Ich glaube auch, dass wir (hoffentlich gemeinsam mit der Wikipedia) neue Anreize schaffen müssen, um die Commons (Anm. Im Deutschen manchmal auch Allmende genannt), den Pool freier Werke, zu bereichern. Dafür brauchen wir Spiele und andere Apps, mit denen Leute eigene Beiträge leisten können oder mit denen sie sich im Pool bedienen können; es muss einfacher werden, die Commons zu füttern, damit man wiederum besser Material finden und darauf aufbauen kann. Dieser Aspekt, die Commons leichter als bisher anzureichern und zu kuratieren, wird meines Erachtens sehr entscheidend sein. Ich hoffe, das sind die beiden Wege, die CC einschlagen wird.

netzpolitik.org: Magst du uns drei CC-Projekte nennen, die du besonders toll fandest und bei denen du dachtest, wow, fantastisch, wie man auf freien Lizenzen neue, unglaubliche Dinge aufbauen kann?

Lawrence Lessig: Puh, nur drei neue, unglaubliche Projekte?

netzpolitik.org: Du darfst gern auch zehn aufzählen!

Lawrence Lessig: Es gibt da einige Remix-Projekte, die im CC-lizenzierten Bereich für Wettbewerb gesorgt haben. Und was ich immer extrem ermutigend finde, sind diese Geschäftsmodelle, die auf der Basis kreativen Ausdrucks etwas Neues obendrauf setzen, weil das für mich die Idee eines Ökosystems stützt. Über Haikudeck hatte ich ja schon gesprochen; oder nehmen wir ein Projekt wie al-Dschasira. Dort werden alle palästinensischen Filme unter der freiesten Lizenz, CC-BY, veröffentlicht, damit das Material möglichst leicht zugänglich ist und Dokumentarfilme und TV-Nachrichten Zugriff darauf haben, was wirklich in Palästina passiert. Das fand ich sehr spannend. Aber nichts ist so wesentlich wie die Entscheidung der Wikipedia-Community, dass dies die Infrastruktur-Plattform sein soll, auf der sie weiter aufgebaut werden soll. Es dauerte etliche Jahre, bis dieser Übergang ausgehandelt war, und es war viel Bescheidenheit und Weisheit gefragt, bevor Richard Stallman der Migration zustimmte. Aber ich denke, das macht nochmals deutlicher, dass CC eine Dachmarke für freie Kultur ist, und damit sollte die Prominenz und der Erfolg des Projekts auf Dauer gewährleistet sein.

netzpolitik.org: Wie entscheidend ist Netzneutralität für die Weiterentwicklung dieser neuen Bewegung und für die Kreativkultur allgemein?

Lawrence Lessig: In meinen Augen ist Netzneutralität sehr entscheidend, und zwar nicht nur für freie Kultur. Freie Kultur hängt davon ab, vielleicht sogar mehr als andere Dinge (darüber wäre mal nachzudenken), aber es betrifft eben mehr als nur die freie Kultur. Ich halte sie für einen eigenen, unabhängigen Wert, um den wir uns kümmern müssen, zusätzlich zu dem Problem, wie wir die Kontrolle von Inhalten ausbalancieren. Von Benkler habe ich für mein Buch „The Future of Ideas" (Die Zukunft der Ideen) das Konzept einer in Schichten aufgebauten Architektur geklaut. Ich habe das Konzept auf drei Ebenen eingedampft und stelle mir vor, dass es auf jeder Ebene eine freie und eine proprietäre Komponente gibt. Der Kerngedanke ist, dass man auf jeder einzelnen Ebene zumindest eine Balance zwischen frei und proprietär herstellen muss, und im Idealfall würde man den freien Anteil maximieren. In diesem Schema bewegt sich Netzneutralität auf einer anderen Ebene als freie Kultur, aber die beiden Aspekte greifen ineinander und bedingen einander.

netzpolitik.org: Wie würdest du Netzneutralität definieren? Darunter stellt sich ja jeder was anderes vor.

Lawrence Lessig: Netzneutralität entstand aus dem, was Netzwerkarchitekten das Ende-zu-Ende-Prinzip nennen. In Stanford hatten wir um 2001 eine Konferenz zum Thema „Architektur des Ende-zu-Ende-Prinzips". Dort trafen sich Tim Wu, Barbara van Schewick, Yochai Benkler und eine Menge anderer Leute, um darüber zu sprechen, inwieweit dieses konstruktive Prinzip wirtschaftliche und soziale Folgen hatte und warum es so wichtig war, es aufrecht zu erhalten. Dort begann Tim die Arbeit am Projekt, dann mussten wir dem Kind einen Namen geben, und im Oktober 2002 wurde die Netzneutralität geboren. Und egal aus welcher Richtung man es betrachtet, darf man es nicht nur technisch sehen – es ist immer entscheidend, die politische Ausrichtung und den Wettbewerbsaspekt dieses Prinzips im Auge zu behalten. Es ist zwar ein technisches Prinzip, aber es hat uns ein wettbewerbsfreundliches Ökosystem gebracht, und es liegt an uns, das Wesentliche dieses Prinzips zu bewahren, um damit zugleich das Wettbewerbs-System erhalten zu können.

Für mich ist dabei wichtig, dass in diesem Ökosystem keine rechtliche Möglichkeit vorgesehen ist (die technische Möglichkeit gibt es immer), dass das Netzwerk zu Diskriminierungszwecken eingesetzt wird. Denn das wäre Gift

für jeglichen Anreiz, Innovationen bei Apps und Inhalten voranzutreiben, die in diesem Netzwerk zum Einsatz kommen. Vielleicht sollten wir das Prinzip durchsetzen, indem wir den im Netz involvierten Firmen bestimmte Arten von Verträgen gesetzlich verbieten – das wäre sicher besser, als einen Regulierer darauf anzusetzen, wie man die Kanäle sauber und offen hält, damit die Daten fließen können. Aber das ist nur eine Detailfrage.

Im Kern geht es darum, sicherzustellen, dass niemand seine Macht über die Infrastruktur dazu missbrauchen kann, zerstörerische Macht im Wettbewerb zu erlangen. Das muss man besonders für die USA betonen, weil wir die Idee, die damals Open Access hieß, schon aufgegeben haben – es ging damals um den Letzte Meile-Zugang konkurrierender Infrastruktur-Anbieter im Netzwerk. Dazu war im 1996er Kommunikationsgesetz der USA etwas festgeschrieben, aber das war unzureichend, weil es sich nur auf Telefonleitungen bezog, nicht aber auf Datenkabel.

Aber als 2000 die Bush-Regierung an die Macht kam, war das Prinzip nicht mal mehr für Telefonleitungen gültig. Es gab damit auf der physikalischen Ebene keinen verbindlichen Wettbewerb mehr, nun ging es also darum, ein Modell für funktionierenden Wettbewerb auf der logischen Ebene zu etablieren. Dazu sollte das Ende-zu-Ende-Prinzip beitragen. Daraus erklärt sich auch, warum es in unterschiedlichen Teilen der Welt unterschiedlich wichtig ist. In Barbara van Schewicks Worten: Selbst bei optimalen Wettbewerbsvoraussetzungen auf der physikalischen Ebene müssen wir uns immer noch Sorgen um die Netzneutralität machen. Trotzdem denke ich, dass die Netzneutralität unter weniger Druck steht, je stärker der Wettbewerb auf der physikalischen Ebene stattfindet.

Andere Länder überall auf der Welt bleiben dem Ideal von Open Access auf der physikalischen Ebene übrigens immer noch treu, lange nachdem die USA sich davon verabschiedet haben. Und wie man rückblickend feststellen muss: Eine Studie von Yochai Benkler bei Berkman hat gezeigt, dass Länder, die am Open-Access-Prinzip festhielten, viel schnelleres, preisgünstigeres und besseres Internet anbieten konnten als Länder wie die Vereinigten Staaten, die Open Access aufgegeben hatten. Solche Länder mögen sich vielleicht weniger Sorgen um Open Access und Netzneutralität machen müssen als wir; aber ich denke, man kann überall beobachten, besonders hier in Deutschland, wie der

Wettbewerb auf der physikalischen Ebene allmählich verkrustet und verkalkt. Und deshalb ist es so wichtig, darauf zu achten, dass zumindest auf der logischen Ebene hinreichender Wettbewerb erhalten bleibt.

Das Interview mit Lawrence Lessig führten John Weitzmann und Markus Beckedahl im September in Berlin. Das Transkript wurde freundlicherweise von Christian Wöhrl erstellt und übersetzt.

Urheberrechtsverletzungen: Das ist doch verboten!

Johnny Häusler

Alle drehen am Urheber-Rad, seit sich Sven Regener von vermeintlichen „Künstler-scheiße-Findern" ins Gesicht gepisst fühlte und neue YouTube-Rekorde mit der Ankündigung versprach, dass uns Kim Schmitz demnächst Lieder vorsingen würde. Vernunft und Ausgewogenheit drohen in der Debatte ebenso verloren zu gehen wie die ursprünglichen Punk-Ideale einiger Protagonisten. Eine Bestandsaufnahme.

Plötzlich stand der ehemals mit künstlerischer Anarchie verknüpfte Name Xaõ Seffcheque unter einem inhaltlich durchaus ins Sonntagabend-Programm der ARD passenden „Offenen Brief von 51 Tatort-Autoren". Dann tauchte unter dem Titel „Wir sind die Urheber! Gegen den Diebstahl geistigen Eigentums" ein weiterer offener Brief auf, den diesmal über 1500 Nicht-Tatort-Autoren unterzeichnet hatten, der zynischerweise aber nicht von Urhebern, sondern vom Literaturagenten Matthias Landwehr initiiert worden war. Und vermutlich formieren sich im Internet gerade mehrere Dutzend weiterer offener Briefe von „Wir sind die Urheberrechtsabschaffungsbefürworter!" bis „Ihr seid die Raubkopierer-Schweine!".

Man ahnt, wie offene Briefe funktionieren und wie die Unterschriften darunter zustande kommen. Da ruft der eine die andere an, weil „der Martin eine tolle Aktion vorhat, und Sigrid hat einen super Text geschrieben, ich mail dir den mal rüber, und Daniela macht auch mit und die Agentur von Achim verbreitet das über alle Kanäle und das wird fett und willst du nicht auch?" – „Na klar, wenn Sigrid das geschrieben hat und Daniela dabei ist, logisch, mach mal. Thorsten macht auch mit? Super, dann erst recht, liebe Grüße, wir müssen uns unbedingt mal wieder sehen, ja, ich melde mich, Tschüss!"

So passiert es wahrscheinlich, dass eine Oberflächenweisheit wie „Das Urheberrecht ermöglicht, dass wir Künstler und Autoren von unserer Arbeit leben können" von sonst so klugen Menschen wie Rocko Schamoni unterzeichnet wird, womit suggeriert wird, das Urheberrecht sei von ein paar Mitgliedern der Piratenpartei bedroht, die nicht einmal eine Chance hätten, dieses Recht abzuschaffen, wenn sie Regierungspartei wären. Und ungeachtet der Tatsache, dass sich ihr letztes Buch trotz (oder etwa wegen?) des Internets über

zwei Millionen Mal verkauft hat, betrachtet auch Charlotte Roche ihr Publikum offenbar in erster Linie als mögliche Parasiten: „Die alltägliche Präsenz und der Nutzen des Internets in unserem Leben können keinen Diebstahl rechtfertigen und sind keine Entschuldigung für Gier oder Geiz." Immerhin sind Roches Werke tatsächlich in Online-Tauschbörsen erhältlich, was in Anbetracht ihrer Rekordverkäufe die aktuelle Botschaft der vorgeblich vereinten Urheber noch absurder macht, ganz im Gegensatz übrigens zur Musik von Sven Regeners Band Element Of Crime, die man vergeblich illegal zu laden versucht, wenn man weniger als drei Wochen Zeit dafür hat.

Keinerlei empörte offene Briefe findet man von diesen Autoren oder ihren Agenten übrigens als Reaktion auf die Tatsache, dass ihre Vertreter und Verwerter seit vielen Jahren versuchen, Bürgerrechte brutal einzuschränken, um ihre wirtschaftlichen Interessen durchzusetzen. Der Künstler als politischer Mensch, der Gedanken und den Diskurs über gesellschaftliche Veränderungen nicht nur zulässt, sondern sogar fordert, und der sich dabei mit seinem Publikum verbündet oder es wenigstens herausfordert: Er ist schwer zu finden in diesen Tagen. Stattdessen lassen sich Tausende von Urhebern, denen kein halbwegs klar denkender Mensch ihre Rechte oder Einkommensmöglichkeiten absprechen will, gegen ihr Publikum aufhetzen, lassen sich von der Verwertungsindustrie Gefahren einreden, die keine sind, und vor den Karren einer Anwaltsmaschinerie spannen, die konstant die Unmöglichkeit der Rechtsdurchsetzung im Internet behauptet und dabei mit Hilfe technischer und juristischer Möglichkeiten jedes Jahr hunderttausende von Abmahnungen an Privatpersonen verschickt.

Niemand bestreitet, dass das Internet Veränderungen mit sich bringt, mit denen wir uns beschäftigen müssen, weshalb dies auch an allen Ecken getan wird. Wenn auch äußerst selten von Künstlern. Diese fabulieren stattdessen im Jahr 14 nN (nach Napster) den drohenden Untergang ihrer Kunst herbei, in einer Zeit also, in der die legalen Angebote im Netz massiv zunehmen und für wieder steigende Umsätze in der Unterhaltungsbranche sorgen. Man kann nur hoffen, dass Urheber weiterhin 90 % ihrer Einnahmen an Verwerter und Anwälte abgeben, damit sie sich allein auf ihre Kunst konzentrieren können und nicht auf die Idee kommen, noch mehr offene Briefe zu schreiben. Ansonsten müssten wir nämlich weiterhin dabei zusehen, wie ehemalige Punkrocker mit erhobenem Zeigefinger vor jungen Menschen stehen und et-

was von Recht und Ordnung faseln, als hätten sie sich in ihrer Blütezeit erst einmal eine Arbeitsgenehmigung für ihre Gigs geholt und nicht gesoffen und gekifft, weil es in ihrem damaligen Alter schließlich verboten war.

Menschen nutzen illegale Angebote nicht, um den Künstlern zu schaden. Das Internet bietet den geradezu grenzenlosen Zugriff auf die Kultur und Kunst dieser Welt, und diesen nicht zu nutzen, wäre dämlich. Wenn dieser Zugriff nun an einigen Stellen nicht ganz legal ist, dann scheißen speziell junge Leute mit begrenzten Budgets auch mal darauf, was in gewisser Hinsicht eine digitale Version von Rock'n'Roll ist. Denn jeder Jugendkultur war es im überschaubaren Rahmen schon immer herzlich egal, wie erlaubt oder verboten ihre Handlungen waren. Ein Stück weit muss man als Urheber und Verwerter mit dieser Tatsache leben, ein anderes Stück weit wird sich die Industrie weiter darum kümmern müssen, legale Angebote reizvoller zu machen als die illegalen (die, wenn sie im großen Stil passieren, schließlich auch dauernd geschlossen werden), und am Ende wird sich alles einpendeln. Dass dieser Prozess durch offene Urheber-Briefe der bisherigen Art beschleunigt wird, darf jedoch stark bezweifelt werden.

Dieser Beitrag erschien zuerst in Spex 340, der September/Oktober-Ausgabe 2012.

Crowdfunding vs. Gratismentalität

Jörg Braun

Es tobt ein Kampf um das bestehende Urheberrecht. Die eine Seite will es nicht nur erhalten sondern zementieren – die andere hält es für nicht zeitgemäß und fordert Reformen. Ein beliebtes Argument der Verteidiger analoger Geschäftsmodelle in der Diskussion um Digitalisierung und Urheberrecht lautet: „Dafür muss man zahlen, kostenloses Kopieren und Downloaden ist Diebstahl." Implizit klingt da immer noch ein Schlagwort mit, das mittlerweile so nur noch selten ausgesprochen wird: Eine „Umsonstmentalität" im Internet mache Kultur und Kreativwirtschaft kaputt. Wem man erklären muss, dass sie oder er für Content zahlen müsse, der oder die will offensichtlich kein Geld ausgeben. Am lautesten heulen hier Film- und Musikbranche und übertönen so regelmäßig die Realität.

Die für Content, ob analog oder digital, verfügbare Geldsumme fließt heute nicht mehr nur in den Kauf von Büchern, Konzert-, Theater- oder Kinokarten sondern auch schon seit einigen Jahrzehnten in Tonträger diverser Art und damit in Videokassetten, DVDs, BluRays und mittlerweile Downloads. Neben den klassischen Kulturformen vor allem auch in Spiele, Apps etc.

Es gibt zudem die ein oder andere Studie[1], die nahelegt, dass diejenigen, die downloaden, auch viel kaufen. Vollkommen ad absurdum geführt wird das Argument der Umsonstmentalität schließlich durch Crowdfunding. Hierzu zwei einschlägige Beispiele.

Nachdem vor einiger Zeit schon das durch Fans finanzierte Erotikfilmchen „Hotel Desire" Premiere feiern durfte, erlebte im Februar diesen Jahres der Sci-Fi-Nazi-Trash-Film „Iron Sky" seine Uraufführung auf der Berlinale. Ein Teil der Produktionskosten wurde von Fans aufgebracht, die dafür Einblicke in die Produktion erhielten. Gesammelt wurde das Geld im Netz.

Die Menschen wollen also nicht nur Geld für Content ausgeben, sie tun es sogar noch vor der Erstellung der Werke. Besonders eindrücklich zeigt dies ein zweites Beispiel: Der in seiner Branche zu den Berühmtheiten zählende Com-

1 Zum Beispiel: http://www.neunetz.com/urheberrecht/#toc-entwicklung-der-musikbranche-im-filesharing-zeitalter; 3.12.2012.

puterspielprogrammierer Tim Schafer wollte ein eher altmodisch anmutendes Klick-and-Point-Game produzieren, wie es vor 20 Jahren populär war. Er fand zunächst keine Investoren. Dann fragte er das Netz um Geld und hatte die angefragten 400.000 Dollar binnen acht Stunden zusammen. Am Ende der Geldeinwerbephase waren es dann 1,6 Millionen.

Natürlich löst diese Zahlungsbereitschaft nicht alle Probleme, die rund ums kreative Schaffen derzeit bestehen. Wie finden Neulinge Unterstützung? Funktioniert Crowdfunding in allen kreativen Bereichen? Es ist beispielsweise auch nicht klar, ob Crowdfunding am Ende wieder nur Megastars beim Verdienen hilft, während kleinere Fische, wie heute auch schon, darben (Wobei Iron Sky und das Projekt von Tim Schafer solche Nischenprodukte sind, die es im Mainstream-Markt so nicht geben würde). Es besteht auch die Gefahr, dass Crowdfunding nicht zusätzlich zu anderen bestehenden Kulturförderinstrumenten und Bezahlsystemen etabliert wird, sondern diese ersetzt. Solange Staatsaufgaben immer mehr auf zivilgesellschaftliches Engagement abgewälzt werden, ist so etwas immer zu befürchten.

Dennoch: Die Menschen zahlen nicht nur für den bequemen Zugang zu Inhalten wie im Falle der sogenannten „Premium-Kunden" beim brisanten Beispiel Megaupload. Sie zahlen auch gern, prompt und viel für angekündigte Werke. Im Voraus.

Allerdings, und das ist etwas, was in der Debatte um ein Urheberrecht für die digitale Gesellschaft vielleicht stärker mitbedacht werden muss, findet hier ein weiterer Strukturwandel statt. Nicht nur Produktionstechnik und die Werkträger haben sich massiv verändert, nicht nur die Distribution wurde revolutioniert und damit die Macht der Verwerter geschwächt. Die Nutzerinnen und Nutzer lassen sich offenbar von den alten Playern in Kultur und Entertainment auch nicht mehr sagen, für was sie Geld ausgeben sollen.

Es sind heute weniger als früher PR-Abteilungen und Feuilleton-Redakteure, sondern die Nutzerinnen und Nutzer, die Hits produzieren. Dabei erscheint Crowdfunding auch bei kommerziellen Großprojekten als eine spezielle Variante des User generated Content, die zunächst die althergebrachte Top-Down-Kultur in Frage stellt. Damit einher geht womöglich auch, dass das tradierte Verständnis davon, was Kultur ist, aktualisiert werden muss. Hit and Run und Thomas Mann.

2012: Das Jahr, in dem Open Education in Deutschland ankam

Leonard Dobusch

Arbeitsblätter gestalten. Foliensätze zusammenstellen. Syllabi entwerfen. Kreative Übungen erfinden. Material aus verschiedenen Lehrbüchern miteinander kombinieren. Mit diesen und ähnlichen Tätigkeiten verbringen Lehrende an Schulen und Universitäten gleichermaßen einen guten Teil ihrer Arbeitszeit. Internet und digitale Technologien wiederum erleichtern diese Arbeiten mehr und mehr. Viele Inhalte sind bereits digital verfügbar. „Copy&Paste" ist zwar als Kulturtechnik durch Plagiate in Verruf geraten, als Basis für den Remix von Lernunterlagen hilft es aber auch dabei, Unterricht interessanter und abwechslungsreicher zu gestalten.

Technisch wäre es ein leichtes, diese täglich tausendfach erarbeiteten Lernunterlagen im Internet zugänglich zu machen – um Doppelarbeit zu vermeiden und die Qualität von Schule und Universität insgesamt zu verbessern. Der Grund, warum dieses Teilen von Lernunterlagen bislang trotzdem in der Regel unterbleibt, ist das Urheberrecht. Weil dasselbe Recht, mit dem Rihanna CDs und Steven Spielberg Filme verkaufen auch für Lernunterlagen gilt, sind deren Remix und Weitergabe enge Grenzen gesetzt. Mehr noch, im Bildungsbereich ist das Urheberrecht sogar besonders restriktiv. Der erst 2008 nach Lobbying der Bildungsmedienverlage ins Urheberrechtsgesetz eingefügte §53 Abs. 3 verbietet auch nur „kleinste Teile" von Unterrichtsmaterialien elektronisch, und sei es nur im schulinternen Intranet, zugänglich zu machen. Hinsichtlich digitaler Lernunterlagen gilt deshalb: die Technik ist vorhanden, das Recht ist im Weg.

An diesem Punkt setzt Open Education an. Mit Hilfe alternativen Urheberrechtslizenzen wie Creative Commons sollen die Potentiale des Internets für bessere Bildung trotz einer veralteten Rechtslage realisiert werden. Ziel ist mehr als „nur" kostenloser Zugang zu digitalen Lernunterlagen und mehr als bloß digitale Multimedia-Schulbücher. Mit Open Education verbunden ist die Vision von „Rip, Mix & Share" im Bildungsbereich: Lernunterlagen selektiv nutzen, rekombinieren und mit anderen teilen.

Bereits 2001 hatte das Massachusetts Institute of Technology (MIT) als erste große Bildungseinrichtung damit begonnen, komplette Kursunterlagen kostenlos online verfügbar zu machen. Ein Beispiel, das Schule machen sollte: Universitäten auf der ganzen Welt stellten ebenfalls Kursunterlagen ins Netz und schlossen sich im Open Courseware Consortium zusammen, um Erfahrungen damit auszutauschen. Mittlerweile sind knapp 200 Bildungseinrichtungen Mitglied in dem Verband – deutsche Universitäten sind allerdings keine darunter.

Ein Jahr nach der MIT-Initiative einigte sich ein UNESCO-Forum offiziell auf den Begriff „Open Educational Resources" (OER) zur Bezeichnung offener – im Sinne von offen lizenzierter – Lehr- und Lernunterlagen. In Deutschland sollte es aber noch zehn weitere Jahre dauern, bis sich 2012 Bildungsministerium und Kultursministerkonferenz erstmals offiziell mit dem Thema in Form einer Expertenanhörung[1] beschäftigen. Mit ein Auslöser dafür war die Verabschiedung der „Pariser Deklaration" im Rahmen des „World Open Educational Resources Congress" der UNESCO anlässlich des zehnjährigen OER-Jubiläums.

Nach einer Präambel, die Bildung als Menschenrecht ausweist und eine Reihe vorhergehender Erklärungen anführt, geht es im Kern der Deklaration um einen zehn Punkte umfassenden Forderungskatalog an die UNSECO-Mitgliedsländer[2]:

- Bekanntheit und Nutzung von OER fördern: Die Verwendung von OER soll zur Verbesserung des Zugangs zu Bildung auf allen Ebenen, sowohl formal als informal, aus einer Perspektive des lebenslangen Lernens vorangetrieben werden und damit zu sozialer Inklusion, Gleichheit der Geschlechter und besonderen Bedürfnissen in der Bildung beitragen. Sowohl Kosteneffizienz als auch Lernerfolg werden durch die vermehrte Nutzung von OER verbessert.

1 Werkstatt.bpb.de: Angehört: Fachgespräch zu Open Education des Bildungsministeriums, in: http://werkstatt.bpb.de/2012/11/angehort-fachgesprach-zu-open-education-des-bildungsministeriums/; 6.12.2012.

2 Eigene, gekürzte Übersetzung des Forderungskatalogs, übernommen von https://netzpolitik.org/2012/10-jahre-open-educational-resources-kongress-und-deklaration/; 6.12.2012.

- Rahmenbedingungen für ermöglichenden Einsatz von Informations- und Kommunikationstechnologie schaffen: Die digitale Spaltung durch Entwicklung angemessener Infrastruktur, insbesondere leistbarer Breitbandverbindungen, breit zugänglicher Mobilfunktechnologie und verlässlicher Stromversorgung. Medienkompetenz verbessern und die Entwicklung von OER in offenen Standarddatenformaten anregen.
- Entwicklung von OER-Strategien und -Policies verstärken: Spezifische Handlungsleitfäden für die Erstellung und Verwendung von OER im Rahmen allgemeiner Bildungsstrategien entwerfen.
- Offene Lizenzen verbreiten und verwenden: Mittels offener Urheberrechtslizenzen Wiederverwendung, Überarbeitung, Remix und Weiterverbreitung von Bildungsmaterialien auf der ganzen Welt fördern.
- Aufbau von Institutionen für eine nachhaltige Entwicklung qualitativ hochwertiger Lernmaterialien fördern: Einrichtungen sowie Lehrkräfte und andere Akteure unter Berücksichtigung lokaler Anforderungen bei Erstellung und Teilen hochwertiger Lernmaterialien unterstützen. Qualitätssicherung von OER vorantreiben.
- Strategische Allianzen für OER knüpfen: Strategische Partnerschaften zwischen Akteuren innerhalb und außerhalb des Bildungssektors für mehr Nachhaltigkeit eingehen.
- Erstellung und Anpassung von OER in einer Vielfalt an Sprachen und kulturellen Kontexten anregen: OER in lokalen Sprachen und diversen kulturellen Kontexten sichert deren Bedeutung. Internationale Organisationen sollten das Teilen von OER über Sprach- und Kulturgrenzen hinweg unter Wahrung indigenen Wissens bzw. indigener Rechte befördern.
- Forschung zu OER unterstützen: Forschung zu Entwicklung, Nutzung und Re-Kontextualisierung von OER sowie hinsichtlich ihrer Folgen für Qualität und Kosteneffizienz von Lehren und Lernen liefert die Datenbasis für öffentliche Investitionen.

- Suche, Bereitstellung und Teilen von OER fördern: Entwicklung nutzerfreundlicher Werkzeuge zum Auffinden und Abrufen von OER mit Bezug auf spezifische Bedürfnisse. Dabei angemessen offene Standards zur Sicherstellung von Interoperabilität und Verwendung in verschiedenen Medienkontexten einsetzen.
- Öffentlich finanzierte Lernunterlagen offen lizenzieren: Regierungen und andere zuständige Stellen sollten sicherstellen, dass Lernunterlagen, die mit öffentlichen Geldern entwickelt wurden, unter offenen Lizenzen zugänglich gemacht werden.

Vor allem der letzte Punkt, eine Art OER-Klausel bei der Vergabe öffentlicher Mittel zur Erstellung von Lehr- und Lernunterlagen, würde in Deutschland tiefgreifende Änderungen in den bisherigen Finanzierungspraktiken und -strukturen, zum Beispiel im Schulbuchbereich erfordern. Dass solche Reformen aber keineswegs unmöglich sind, beweisen andere Länder. Zum Beispiel startete in Polen 2012 ein Pilotprojekt zur Erstellung offener Lernunterlagen im Schulbereich. In den USA gab es, nachdem OER lange vor allem von privaten Stiftungen wie der Hewlett-Foundation vorangetrieben worden war, gleich eine ganze Reihe von öffentlichen Initiativen.

Im Bundesstaat Washington wurde eine „Open Course Library" ins Leben gerufen, in der staatliche Colleges offene Kursunterlagen gemeinsam zum Download anbieten. Kalifornien beschloss ebenfalls ein Gesetz zum Aufbau einer digitalen Lehrbuchbibliothek und auf Bundesebene verkündete Arbeitsministerin Hilda L. Solis die bislang größte OER-Initiative. Binnen vier Jahren werden zwei Milliarden Dollar in Community Colleges investiert (500 Millionen sind bereits ausgeschüttet), wobei sämtliche damit finanzierten Lernunterlagen unter einer Creative-Commons-Lizenz stehen. Parallel dazu veranstaltete das US-Bildungsministerium gemeinsam mit Creative Commons und der Open Society Foundation einen Wettbewerb zur Gestaltung von Videos zum Thema „Why Open Education Matters".

Von derartigem politischen Engagement ist Deutschland noch vergleichsweise weit entfernt. Die im Vorfeld der oben erwähnten Expertenanhörung versandten Fragen[3] beschäftigten sich denn auch prinzipiell mit Potentialen, Ri-

3 Vgl. https://netzpolitik.org/wp-upload/Anlage2_Fragenliste_OER.docx

siken und Hürden im Bereich von OER. Während die größten Risiken im Verpassen bildungspolitischer Chancen liegen, sind die Potentiale beträchtlich. Ohne Anspruch auf Vollständigkeit zählen dazu:

- besserer Zugang zu digitalen Lernunterlagen für sämtliche Akteure, inklusive die Möglichkeit zum Selbststudium und neuen Lernformen wie großzahligen und zertifizierten Online-Lernangeboten (MOOC).
- bessere digitale Nutzbarkeit von Lernunterlagen, weil die Klärung von Rechten durch die Verwendung von offenen Lizenzen (z. B. Creative Commons) radikal vereinfacht wird.
- bessere Vergleichbarkeit digitaler Lernunterlagen für Lehrende, Lernende, Eltern und Politik.
- Einfachere Kombinierbarkeit verschiedener Lernunterlagen und damit verbunden die Verbesserung der Lernerfahrung.
- Verbesserung der Qualität von Lernunterlagen durch mehr Möglichkeiten zu Feedback und Remix verschiedener Lernunterlagen. Damit verbunden ist das Potential für vermehrte didaktische Innovation.
- Mehr qualitätsorientierter Wettbewerb, vor allem im derzeit oligopolistischen Markt für Schulbücher.

Wie steinig der Weg zum Ausschöpfen dieser Potentiale sein wird, machte die Anhörung selbst deutlich: Einigkeit bestand vor allem darin, dass in sämtlichen Bereichen – von Qualitätssicherung über rechtliche und ökonomische bis hin zu technologischen Fragen – noch großer Forschungsbedarf besteht.

Umso erfreulicher angesichts dieser nur sehr kleinen Fortschritte auf politischer Ebene waren dafür die steigende Zahl an Bottom-up-Intiativen im Bereich von OER. Neben zwei White Papers zum Thema[4], Informationsaustausch in Veranstaltungen wie dem ersten #OER-Camp in Bremen und Platt-

4 *Bretschneider, M./Muuß-Merholz, J./Schaumburg, F.* (2012: Open Educational Resources (OER) für Schulen in Deutschland: Whitepaper zu Grundlagen, Akteuren und Entwicklungsstand im März 2012, online: PDF; *Dobusch, L.* 2012: Digitale Lehrmittelfreiheit: Mehr als digitale Schulbücher, online: PDF.

formen wie werkstatt.bpb.de, die sich der Praxis digital-offener Bildung widmen, gab es auch den Versuch mit Hilfe von Crowdfunding eine Plattform für offene Schulbücher („Schulbuch-O-Mat") zu finanzieren.

Angesichts dieser und vieler anderer Aktivitäten besteht kein Zweifel, dass OER 2012 zumindest in der bildungspolitischen Debatte auch in Deutschland angekommen ist. Es war allerdings auch höchst an der Zeit, denn längst sind im Kontext von OER bereits neue Entwicklungen wie der Boom an Massive Open Online Courses (MOOCs).[5] Einher mit diesen offen zugänglichen, zertifizierten Online-Kursen geht ein noch größeres, transformatives Potential: Die Auslagerung der bloßen Wissensvermittlung ins Netz, auf dass Bildungseinrichtungen sich gänzlich auf ihre eigentliche Aufgabe konzentrieren können: Lernen.

5 Für einen Überblick vgl. https://netzpolitik.org/2012/ct-schwerpunkt-zu-lernplattformen-im-netz/.

Ohne Gleichberechtigung und sozialen Ausgleich bleibt Open dicht

Jörg Braun

Open Access, der freie und offene (Online-)Zugang zu wissenschaftlichen Ergebnissen, meist in Form von Aufsätzen oder Diskussionspapers, gewinnt stetig an Bedeutung. Dabei gibt es weiterhin im Prinzip zwei Wege, etwas Open Access zu veröffentlichen: Die Green Road und die Golden Road. Im Gegensatz zur Green Road, der freien und offenen Zweitveröffentlichung nach einer exklusiven Vermarktung der Beiträge durch privatwirtschaftliche Verlage, bedeutet die Golden Road, eine wissenschaftliche Publikation gleich bei der Erstveröffentlichung frei und offen zur Verfügung zu stellen. Daraus haben einige privatwirtschaftliche Verlage mittlerweile ein neues Geschäftsmodell entwickelt. Das hat Vorteile, überall dort, wo Wissenschaft stark durch diese Verlage dominiert ist. Der Nachteil aber ist, dass so nur diejenigen von der neuen Offenheit profitieren, die sich die Verlagskosten auch bisher schon leisten konnten. Hier zeigt sich ein Problem, das auch andere „Open"-Bewegungen haben: Je nach Ausgestaltung sind sie nur für wenige Menschen wirklich offen.

Anfang Mai erschien im Universitätsverlag des Saarlands der von Ulrich Herb herausgegebene Sammelband „Open Initiatives: Offenheit in der digitalen Welt und Wissenschaft".[1] Darin findet sich ein lesenswerter Beitrag von Jutta Haider, „Open Access hinter verschlossenen Türen oder wie sich Open Access im und mit dem Entwicklungsdiskurs arrangiert".[2]

Haider zeigt dort anschaulich, wie die ideologische Begründung für Open Access letztlich im imperialistischen Diskurs einer Entwicklungshilfe verortet ist, die „armen" oder „unterentwickelten" Gesellschaften die angeblichen und

1 *Herb, Ulrich* (Hrsg.) 2012: Open Initiatives: Offenheit in der digitalen Welt und Wissenschaft, in: http://universaar.uni-saarland.de/monographien/volltexte/2012/87/; 6.12.2012.

2 *Haider, Jutta* 2012: Open Access hinter verschlossenen Türen oder wie sich Open Access im und mit dem Entwicklungsdiskurs arrangiert, in: http://eprints.rclis.org/handle/10760/17229#.UMB3WBKiI4C; 6.12.2012.

realen Segnungen der kapitalistischen Industrieländer des globalen Nordens überhelfen soll. Besser noch, es soll die Hoffnung auf diese Segnungen dauerhaft aufrecht erhalten, kann diese aber de facto nicht erfüllen.

Haider ist dabei nicht im Geringsten daran gelegen, den offenen Zugang zu wissenschaftlicher Arbeit an sich zu kritisieren. Sie kritisiert, mit welchen Argumenten die Archive und Publikationsprozesse geöffnet werden sollen. Sie kritisiert, das eine rein technische Lösung (übers Netz zugängliche Datenbanken) als Allheilmittel gegen Ungleichheit (hier: in der Wissenschaft) gepriesen wird und dabei die flankierende PR die Ungleichheit dauerhaft zementiert.

Dem ließe sich entgegnen, dass es in Open Access-Zeitschriften einen messbar höheren Anteil an Publikationen von WissenschaftlerInnen gibt, die aus den sogenannten Entwicklungsländern stammen und dort arbeiten.[3]

Andererseits zeigt die aktuelle Definition der Golden Road des Open Access, dass es gerade die großen Wissenschaftsverlage sind, die es sehr genau verstanden haben, Open Access für sich und damit für eine weitergehende Vormachtstellung zu nutzen. War mit der Golden Road ursprünglich nur gemeint, Wissenschaftliche Beiträge offen und frei erstzuveröffentlichen wird „golden" mittlerweile mehrheitlich so verstanden, dass privatwirtschaftliche Verlage nach Zahlung einer Publikationsgebühr die offene und freie Erstveröffentlichung der wissenschaftlichen Beiträge organisieren.

Dies hat, v.a. Für die „westliche" Wissenschaft, den Vorteil, dass Open Access so kompatibel wird zur gängigen wissenschaftlichen Veröffentlichungspraxis [vgl. 1] sowie den dazugehörigen Methoden der Qualitätssicherung und der Verleihung von Reputation für die AutorInnen.

Dabei spielen namhafte Verlage eine wichtige Rolle für die Reputation der WissenschaftlerInnen. Die möglichst objektiv zu bemessende Reputation wiederum ist wichtig bei Bewerbungen innerhalb des Wissenschaftsbetriebs, wie wir ihn derzeit kennen. Gerade in Naturwissenschaften und der Medizin ist hierbei der Journal Impact Factor (JIF) von Bedeutung, der misst, welcher Artikel wie oft in welchen namhaften Zeitschriften erwähnt wird. Es ist unnötig zu erwähnen, dass der JIF von einem us-amerikanischen Medienkonzern gemessen wird und die wichtigsten Wissenschaftsverlage aus Europa und Nordamerika stammen.

3 *Evans, James/Reimer, Jacob* 2009: Open Acces and Global Participation, in: Science, 323:5917; 1025.

Einerseits hat die Kompatibilität mit tradierten Systemen dazu geführt, dass Open Access binnen weniger Jahre eine immens wichtige Stellung in einigen Disziplinen eingenommen hat, was im offenen Kampf gegen die Traditionen wohl nicht möglich gewesen wäre.

Anderseits zeigt sich hier, dass es passend zu Jutta Haiders Diskursanalyse auch statistische und ökonomische Indizien dafür gibt, dass Open Access so kaum etwas an herrschenden Ungleichheiten in der globalen Wissensvermittlung ändert.

Ulrich Herb hat, ebenfalls vor zwei Monaten, in einem Artikel über Open Science bei Telepolis in eine ähnliche Kerbe gehauen[4]. Zunächst zeigt er knapp und gut auf, was Open Science, also die transparente und öffentlich zugängliche (Online-)Dokumentation aller Teile des wissenschaftlichen Erkenntnisprozesses, ausmacht. Dann aber folgt ebenso knapp und gut der Hinweis darauf, dass Open Science nichts daran ändert, dass Wissenschaft weiterhin vor allem ein Geschäft der sozialen Eliten ist und die gläserne Decke auch in der Wissenschaft Frauen massiv benachteiligt. Sein Fazit lautet daher: „Der Offenheit fehlt es noch an Partizipation."

Letztlich ist dies ein Problem aller Open-Bewegungen, die im Zuge der Digitalisierung entstanden sind.

Open Innovation soll externes Wissen und somit eine Bedürfnisorientierung in die Produktentwicklung tragen, läuft aber Gefahr, eine Privatisierung von crowdgesourctem Know-How zu werden, wenn es nicht mit einer fairen Teilhabe der FabrikbelegschaftenInnen, KonsumentInnen oder anderen IdeengeberInnen an den Ergebnissen einhergeht.

Open Data und Open Government sind Spielzeug oder gar Machtinstrumente für digitale Eliten, solange die Internetnutzung selbst in Deutschland eine Frage von formal hoher Bildung und hohem Einkommen ist[5]. Dennoch, die netzaffinen Open-Bewegungen haben alle großes emanzipatorisches Potential. Sie können es aber nur entfalten, wenn technische Lösungen begleitet werden durch konkrete globale wie lokale Maßnahmen für Gleichberechtigung und sozialen Ausgleich.

---

4 *Herb, Ulrich* 2012: Wie offen ist die Open Science?, in: http://www.heise.de/tp/artikel/36/36891/1.html; 3.12.2012.

5 Initiative D21 2012: (N)Onliner-Atlas, in: http://www.nonliner-atlas.de/; 3.12.2012.

Zur netzpolitischen Dimension von Gangnam Style

Leonard Dobusch

Das Video „Gangnam Style" des südkoreanischen Rappers Psy avancierte im Jahr 2012 zum meistgesehenen YouTube-Video aller Zeiten mit über 900 Millionen Views und man braucht kein Prophet sein um zu prognostizieren, dass es die 1-Milliarde-Marke knacken wird. Die Originalversion ist in Deutschland geblockt, es finden sich aber Kopien auf YouTube, die nicht gesperrt sind und mit Hilfe von Browser-Extensions wie zum Beispiel dem YouTube Unblocker lässt sich auch das Originalvideo ansehen.

Der virale Erfolg machte nicht nur Psy von einem südkoreanischen zu einem Weltstar, sondern hatte, wenn man der Wikipedia-Seite über Gangnam Style glauben darf, noch viel weiter reichende Konsequenzen:

> *Nach dem Erfolg des Musikvideos pocht Südkorea auf ein Anziehen der Nachfrage von Touristen aus aller Welt. Jayne Clark von der USA Today schrieb, dass Gangnam Style Seoul „auf der Reisekarte platziert hatte". Die Fluggesellschaft British Airways kündigte an, ab 2. Dezember 2012 Flüge nach Seoul sechs mal die Woche anzubieten. Wegen des Gangnam-Style-Phänomens ist die Nachfrage nach Flugtickets „enorm" angestiegen.*

Auch die Musikindustrie profitiert, mit Gangnam Style hat sich das ganze Genre K-Pop am US-Markt etabliert und der Song selbst schaffte es auf Platz 1 in zahlreichen Verkaufscharts (auch in Deutschland).

In netzpolitischer Hinsicht ist Gangnam Style gleich in mehrfacher Hinsicht instruktiv. Klar ist, dass der Erfolg von Gangnam Style nicht mit der Durchsetzung von Urheberrechten zusammenhängt, eher im Gegenteil. Maßgeblichen Anteil am Erfolg hat der Verzicht auf die Durchsetzung von Urheberrechten, und zwar nicht nur was die Weitergabe der Originaldatei betrifft, sondern auch hinsichtlich der Erstellung von Remixes und Parodien. Dass ein Verzicht auf Durchsetzung durch den Rechteinhaber nicht gleichbedeutend mit Zugänglichkeit ist, beweisen allerdings die zahlreichen geblockten Parodien auf YouTube. Witzigerweise ist Gangnam Style Hitler in Deutschland nicht gesperrt.

Ein offizieller Copyright-Verzicht Psys ist übrigens nicht belegt, nur der faktische Verzicht auf Rechtsdurchsetzung. Das ist deshalb entscheidend, weil viele der Remixes auch nach US-Fair-Use eine Urheberrechtsverletzung darstellen (vgl. dazu „Parodies Of Rap Artist Psy's Gangnam Style Are Fun. But Are They Legal?"). Die Verwendung einer Creative-Commons-Lizenz hätte hier für mehr Rechtssicherheit gesorgt.

Klarerweise ist Gangnam Style *kein* Beweis dafür, dass ein Verzicht auf die Durchsetzung von Urheberrechten Erfolg garantiert – im konkreten und in anderen Fällen (z. B. Chris Brown's Forever) handelt es sich um eine notwendige, keineswegs aber um eine hinreichende Bedingung für viralen Erfolg. Gleichzeitig illustriert das Beispiel Gangnam Style, dass Kulturmärkte auch jenseits von Urheberrechten nach dem Starprinzip funktionieren: Aufmerksamkeit zählt bzw. zahlt sich aus – und zwar auf verschiedenste Weise und auch für viele, die selbst keine Aufwände hatten.

Wenn die südkoreanische Nationalbank verkündet, dass die Außenhandelsbilanz des Landes auf Grund der gestiegenen K-Pop-Umsätze ins Plus gedreht hat, dann dokumentiert das, wie sehr (gerade auch: Kreativ-)Wirtschaft ein Nicht-Nullsummenspiel sein kann. Von dem Erfolg von Psy profitieren auch zahlreiche andere koreanische Künstler, ohne dass diese ihre Einkünfte deshalb mit ihm teilen müssen. Und das ist wohl in Ordnung so: denn auch Psy knüpft mit seinem Werk ja an zahlreiche K-Pop-Traditionen an und bedient sich dabei am gemeinsamen kulturellen Erbe.

So lässt sich zum Abschluss auch ein Argument zum Thema Leistungsschutzrecht für Presseverleger machen, ohne den Bogen damit zu überspannen. Alleine der Umstand, dass Suchmaschinen mit Links auf Verlagsangebote Geld verdienen, begründet eben nicht automatisch einen Vergütungsanspruch für Verlage. Mehr noch, mit so einem Vergütungsanspruch entstehen Transaktionskosten, die am Ende alle Beteiligten schlechter dastehen lassen könnten. Zum Beispiel, weil dadurch die Entstehung innovativer News-Dienstleistungen wie z. B. Rivva behindert wird, die Probleme der Presseverlage (Stichwort: Entbündelung) aber völlig unberührt bleiben. Wenn Gangnam Style ein Beispiel für Win-Win ist, dann ist das Leistungsschutzrecht ein Beispiel für Lose-Lose.

Interview mit Joi Ito: „Das Internet hat mein Leben gerettet“

netzpolitik.org: In deiner Keynote auf dem Mozilla Drumbeat Festival sprachst du über „Das Internet hat mein Leben gerettet“ – Was hast Du damit gemeint?

Joi Ito: Das Internet hat mein Leben gerettet, weil ich sehr frustriert war: Ich ging in Japan zur High School und war nicht besonders gut, aber durch das Internet lernte ich viele tolle Menschen kennen, von denen ich etwas lernen konnte und war in der Lage, mich in Communities zu organisieren. Das bestärkte erst mal meine Zuversicht, dass ich etwas beitragen konnte und dass ich andere Menschen wie mich finden konnte. Ich konnte durch das Internet lernen und meine eigenen Methoden der Vernetzung und des Lernens entwickeln. Ursprünglich rettete es also mein Leben dadurch, dass es mich lehrte und es mir erlaubte, zu lernen. Ich mag es nicht, unterrichtet zu werden, ich mag es zu lernen. Später befasste ich mich mit Medien. Ich begann als erster CEO beim ersten ISP in Japan und arbeitete im Netz. Als junger Mensch war ich in der Lage, Geld zu verdienen, ohne einen College-Abschluss und ohne um Erlaubnis bitten zu müssen. Ich war Unternehmer und jedes meiner erfolgreichen Geschäfte kam wegen dem Internet zustande. Ich hätte niemals in einer anderen Umgebung arbeiten können. Also versuche ich der Community etwas zurückzugeben, dadurch dass ich beim ICANN-Board war, Creative Commons mache und einzelne Pfeiler der Offenheit mit aufbaue.

Menschen haben verschiedene Persönlichkeiten, manche kommen sehr gut mit dem Bildungssystem klar, meine Schwester zum Beispiel – aber wenn es das Internet nicht gegeben hätte, wäre es für mich wohl nie möglich gewesen zu lernen, erfolgreiche Unternehmen aufzubauen und einen Lebensunterhalt zu verdienen. Alles was ich weiß oder alles, was ich zu erreichen fähig bin, das alles existiert aufgrund des Internets, bzw. der Architektur des Internets: Die Möglichkeit zur Partizipation ohne um Erlaubnis zu fragen und eine weltweite Vernetzung. Nachdem ich fünf oder zehn Jahre lang im Medienbusiness arbeitete, treffe ich nun als Vertreter von Creative Commons viele meine alten Kameraden aus den Fernseh-, Musik- und Spielfilm-Tagen wieder. Aber es ist jetzt eine völlig neue Welt: Ich denke und handle auf eine vollkommen andere Art und Weise als wenn ich eine herkömmliche Ausbildung gehabt,

Mainstream-Medien konsumiert und in normalen Strukturen gearbeitet hätte … mein grundlegendes Ethos ist es, Autoritäten zu hinterfragen und selbst zu denken. Du kannst so etwas nicht in einem geschlossenen System tun. Hacker-Philosophie.

netzpolitik.org: Hier bei Mozilla Drumbeat geht es um das offene Netz. Wie definierst du diesen Begriff?

Joi Ito: Es gibt viele Definitionen für „open". Für mich bedeutet es offene Standards, dass sich jeder im Prozess beteiligen kann. Ein offenes Netzwerk ermöglicht es, dass sich jeder vernetzen kann ohne um Erlaubnis zu fragen. Offen in der Art und Weise, dass es nicht zentral kontrolliert oder geplant wird, und es gehört auch zu Open Source: Es beginnt mit der Software, aber ich denke es führt zu offenen Inhalten. Zurück zum Punkt: Als es eine Welt gab, die auf Knappheit basierte, mussten Dinge verschlossen werden, um die Ressourcen zu schonen, damit es funktionierte. Man konnte nicht alles öffnen, sonst wäre nichts mehr verfügbar. Aber jetzt, wo wir Überfluss haben, denke ich ist es die Idee, Dinge zu öffnen und zu versuchen, aus dem Chaos eine Struktur zu erschaffen, die nicht geplant und nicht kontrolliert ist. Also denke ich, dass das andere Element von „Offenheit" die Frage ist, wie man neuartige Führungsstrukturen schafft.

In offenen Systemen gibt es eine völlig andere Art von Herrschaft, denn in geschlossenen Systemen gibt es die Möglichkeit zu bestrafen, zu kontrollieren und zu verteilen. In einem geschlossenen System hast Du das Steuer in der Hand. Das unterscheidet sich stark von der Verwaltung einer Freiwilligen-Organisation, wo Menschen ausschließlich deshalb sind, weil sie da sein wollen und du motivierst Menschen mit der Ausgestaltung einer richtigen Umgebung. Wenn man sich anschaut, wie erfolgreiche offene Organisationen funktionieren: Sie funktionieren durch einen ganz anderen Führungsstil der Peer-to-Peer-Partizipation. Mich interessiert das sehr. Und wenn wir über ein offenes Netz reden, reden wir über all diese Dinge. Man lenkt durch das Schaffen der richtigen Umgebung, die richtige soziale Atmosphäre und solche Faktoren. Das haben wir erfahren als das Internet aufkam. Aber jetzt versuchen wir das auf andere Gebiete zu übertragen. Das fasziniert mich. Wir müssen das offene Netz schützen, aber wir müssen ebenso viele neue offene Dinge erschaffen.

netzpolitik.org: Was sind die Gefahren für ein offenes Netz? *Joi Ito:* NGOs sind nun zum Beispiel mächtiger durch ein offenes Netz – und sie gefährden Autoritäten. Wenn eine Autorität gefährdet wird, versucht sie sich zu schützen. Wenn sie also sehen, dass das offene Netz der treibende Motor dafür ist – und egal ob es sich um eine repressive Regierung handelt, ein hoch-profitables Telefonunternehmen oder eine Software-Firma die auf proprietären Code angewiesen ist – dann können all diese offenen Dinge als Gefahr gesehen werden. Und wenn du dann all die gefährdeten Autoritäten zusammen bringst, bekommst du Dinge wie das ACTA-Abkommen. Menschen versuchen ihre „Rechte“ dadurch zu schützen, indem sie versuchen, das Netz zu schließen. Offenheit ist eine Gefahr für geschlossene Dinge.

Die Gefahren für ein offenes Netz kommen aus verschiedenen Richtungen. Und ein Weg um es zu schützen sollte sein, dass man nicht geschlossene Systeme bekämpft, sondern für Offenheit eintritt. Nimm Linux: Linus Torvalds ist nicht Anti-Microsoft, er ist Pro-Linux. Ich denke daher, der beste Weg, das offene Netz zu schützen, ist, es erfolgreich zu machen. Es geht nicht um einen Kampf, es geht darum ein System zu erschaffen, dass widerstandsfähig gegen Attacken ist.

netzpolitik.org: Du erwähntest Netzneutralität nicht, das derzeit vielleicht größte Problem zusammen mit einem reformbedürftigem Urheberrecht.

Joi Ito: Diese Gefahr gibt es seit einer Weile und existiert in vielen Formen. Es ist unklar, wie das geschafft werden soll. Wir müssen Lobbyarbeit machen bei Regierungen und politischen Entscheidungsträgern. Es gibt verschiedene Ebenen, auf denen man für Netzneutralität kämpfen kann und ich unterstütze die Menschen, die es tun. Manchmal schafft man Korrekturen auch durch das Erstellen von Technologie oder Unternehmen, die diese Dinge umgehen: Wir waren immer erfolgreich darin, Schäden zu kompensieren. Es ist aber eine sehr komplizierte Debatte. Ich glaube nicht, dass es einen Königsweg gibt. Genauso wie es keinen Königsweg gab bei Spam. Es brauchte viele schlaue Menschen und verschiedene Zugänge. Aber: Wir lösten Spam ohne mit dem Netzwerk kämpfen zu müssen – mein Gefühl ist daher, dass die Bedenken vieler Menschen, die gegen Netzneutralität argumentieren, dadurch verringert werden, dass einfach mehr Bandbreite zur Verfügung gestellt wird und ihre Argumente dann obsolet werden. Ich neige dazu, technisch innovative Lösungen zu mögen. Aber ich unterstütze ebenfalls die Menschen, die in Washington oder anderen Hauptstädten kämpfen. Manchmal braucht man

Menschen, die sehr stark nach außen streiten, damit mehr Potential vorhanden ist, damit Menschen sich innerlich verändern. Aber ich denke, das ist eine enorm wichtige Debatte.

Dieses Interview mit Joi Ito entstand auf dem Mozilla Drumbeat Festival 2010 in Barcelona. Es lag dann aus nicht mehr nachvollziehbaren Gründen zwei Jahre auf einer Festplatte herum, bis wir uns erinnerten und es für dieses Buch transkribierten und übersetzten.

Daten

Datenjournalismus 2012: Mühen der Ebene

Lorenz Matzat

Als Genre hat sich im Jahr 2012 Datenjournalismus weiter etabliert: So kamen dieses Jahr eine Reihen neuer Tools, Methoden, Visualisierungsformen und Akteure hinzu. Vier Aspekte halte ich dieses Jahr für besonders bemerkenswert:

1.

Die hierzulande erste Datenjournalismuskonferenz zeigte, dass auch im deutschsprachigen Raum eine Community zum Thema herangewachsen ist.[1] Zwei Tage lang ging es im März beim Gastgeber Gruner & Jahr in Hamburg um „Daten & Recherche". Die Fachkonferenz, ausgerichtet vom Netzwerk Recherche, drehte sich um Austausch, Ansätze und Werkzeuge. Der Effekt solch eines Zusammentreffens von über hundert Personen ist schwer zu messen. Meinem Eindruck nach trug es dazu bei, dass Thema Datenjournalismus in hiesigen Redaktionen mehr zu verankern. Und die Haltung ihm gegenüber zu ändern: Gefragt wird nicht mehr „warum sollte man datenjournalistisch arbeiten", sondern „wie macht man das".

2.

International war auch einiges los. So wurde Ende Mai der erste internationale Datenjournalismuspreis[2] verliehen. Und vor allem erschien das Data Journalism Handbook. Die Idee dafür war Ende 2011 entstanden; Mitte 2012 lag nun die fertige Onlinefassung vor; mehr als 30 Autoren aus verschiedenen Ländern brachten Analysen, Herangehensweisen und Tutorials dafür ein. Das Buch, organisiert vom European Journalism Center, steht kostenfrei im Netz; ebenfalls gibt es eine gedruckte Version[3]. Mittlerweile wurde das Buch in mehrere Sprachen übersetzt. Es zeugt von einer lebendigen internationalen

1 Berichterstattung in einem offenen Pad: http://okfnpad.org/drg12; 5.12.2012.

2 2012 Data Journalism Awards winners announced, in: http://datajournalismawards.org/; 5.12.2012.

3 The Data Journalism Handbook, in: http://datajournalismhandbook.org/; 5.12.2012.

data driven journalism-Szene, die sich derzeit vor allem aus Personen aus Nordamerika und Westeuropa zusammensetzt – mit einer deutlichen Männerlastigkeit.

Doch gibt es auch auf dem afrikanischen Kontinent Bewegung: Eine erste African News Challenge[4] fand im Herbst statt. Die scheint bislang eher im Sinne von Entwicklungszusammenarbeit zu funktionieren und wurde von außen hereingetragen. In Südamerika läuft es mit Datenjournalismus in manchen Ländern anders: In Buenos Aires stieg im Spätsommer eine Hacks/Hackers „Media Party" mit 400 Teilnehmern[5].

3.

Es gab dieses Jahr einige Großereignissen, die zum Austoben in Sachen Daten einluden: Im Guardian wurde hinsichtlich der Olympischen Sommerspiele gefragt: „London 2012: is this the first open data Olympics?"[6] Und es gab eine Reihe von bahnbrechenden Ideen und Visualisierungen zu sehen. Um nur eine zu nennen: Der Lauf aller männlichen 100-Meter Medaillengewinner aller olympischen Spieler gegeneinander in der NYT[7].

Das Naturereignis des Hurrikans Sandy, das mit der Endphase des US-Präsidentschaftswahlkampfs zusammentraf, schlug sich nicht zuletzt in diversen Kartenvisualisierungen nieder. Großartig war dabei (als nicht unmittelbar Betroffener) die bereits einige Monate zuvor erschiene „Wind Map"[8] im Auge zu behalten. Die kann auch als Beispiel dafür herhalten, wie Visualisierungsideen weitergedacht werden: Eine interaktive Grafik zur Wählerwanderung der NYT zeigte sich eindeutig von der Wind Map inspiriert.[9]

4 African News Innovation Challenge, in: http://africannewschallenge.org/; 5.12.2012.

5 Wölfle, Maria 2012: Hacks / Hackers Buenos Aires: Erfolgreiche Media Party, in: http://blog.zdf.de/hyperland/2012/09/hacks-hackers-buenos-aires-erfolgreiche-media-party/; 5.12.2012.

6 Rogers, Simon 2012: London 2012: is this the first open data Olympics?, in: http://www.guardian.co.uk/commentisfree/2012/aug/03/london-2012-olympics-open-data; 5.12.2012.

7 Quealy, Kevin/ Roberts, Graham 2012: All the Medalists: Men's 100-Meter Sprint, in: http://www.nytimes.com/interactive/2012/08/05/sports/olympics/the-100-meter-dash-one-race-every-medalist-ever.html: 5.12.2012.

8 Wind Map, in: http://hint.fm/wind/gallery/oct-30.js.html; 5.12.2012.

9 The New York Times 2012: How Obama Won Re-election, in: http://www.nytimes.com/interactive/2012/11/07/us/politics/obamas-diverse-base-of-support.html; 5.12.2012.

4.

Die Wortschöpfung „Big Data" hat 2012 endgültig Einzug in das Hype-Wörterbuch gehalten. Wie so oft sind solche Begriffe zweischneidiger Natur: Sie sind nützlich, weil sie einen offensichtlich Trend markieren. Gleichzeitig tragen sie dazu bei, eben diesen aufzubauschen und zu verwässern. Große Datenmengen spielten im US-Wahlkampf jedenfalls eine große Rolle. Einmal brachten sie den ersten Datenjournalismus-Star hervor: Den Statistiker und Journalisten Nate Silver; der mit nüchternen Methoden in seinem Blog Fivethirthyeight bei der NYT sehr exakt den Wahlausgang voraussagte.[10]

Aber auch die Techniker des Wahlkampfteams von US-Präsident Barack Obama wurden mit Lob überschüttet. Vom „Triumph der Nerds" war die Rede. Neben dem Aufbau einer gewaltigen Online-Infrastruktur gelang es ihnen nicht zuletzt durch schlaue Datenanalyse, Helfer und Wähler zu aktivieren.[11]

Es gab allerdings auch Stimmen, die der ganzen Aufregung etwa Erdung verschaffte: Tom Steinberg, Leiter der britischen NGO MySociety, erinnerte an den „Unterschied zwischen der Entscheidung, sein technologisches Können anzuwenden, um einen bestimmten Kampf zu gewinnen. Und dem Versuch, die Arbeitsweise des demokratischen Systems zu verbessern oder Menschen zu helfen sich selbst zu organisieren, damit sie mehr Kontrolle über ihr eigenes Lebens übernehmen können„[12].

10 Beaujon, Andrew 2012: Nate Silver wins, and data is vindicated, in: http://www.poynter.org/latest-news/mediawire/194661/nate-silver-wins-and-data-is-vindicated/; 5.12.2012.

11 Madrigal, Alexis 2012: When the Nerds Go Marching In, in: http://www.theatlantic.com/technology/archive/2012/11/when-the-nerds-go-marching-in/265325/?single_page=true; 5.12.2012.

12 Steinberg, Tom 2012: Dear Ninja Campaigner Geek: Why I work on non-partisan tech, and why I encourage you to take a look, in: http://www.mysociety.org/2012/11/21/dear-ninja-campaigner-geek-why-i-work-on-non-partisan-tech-and-why-i-encourage-you-to-take-a-look/; 5.12.2012.

Fazit

Selbstredend hantierten zahllose Medien dieses Jahr mit Daten und es gab einiges mehr zu sehen; hier allen gerecht zu werden, würde den Rahmen sprengen. Wen das Thema interessiert, der lese das Hashtag #ddj (data-driven-journalism) auf Twitter mit[13]. Oder schaue sich diese Übersicht an [14] – sie macht deutlich, wie Guardian und NYT dieses Jahr zur Höchstform aufliefen. Meiner Beobachtung nach steht Datenjournalismus hierzulande vor den Mühen der Ebene: Das Konzept ist bekannt, es wird Austausch gepflegt und Methoden sowie Tools werden sich von mehr und mehr Journalisten angeeignet. Auch erwärmen sich mehr Programmierer für das Thema.

Allerdings herrscht Mangel: Weder gibt es wie in den USA Datenwerkzeuge und -plattformen à la Document Cloud[15], Overwiew[16] oder dem Pandaproject[17], die zeitungsübergreifend genutzt und weiterentwickelt werden. Was sich zumindest ändern soll: Eine „Arbeitsgruppe Pandaprojekt" will beim internationalen Open Data Hackathon im Februar 2013 das Open Source-Tool Pandaproject[18] für den deutschsprachigen Raum anpassen.

Doch bleibt unklar, ob viele Medienhäusern bereit sind, Datenjournalismus bei sich zu integrieren; sprich Mittel und Personal dafür aufzubringen, In diesen Zeiten anhaltender Verunsicherung der Zeitungsbranche ist längst noch nicht ausgemacht, dass das Format als Chance für den digitalen Journalismus erkannt und genutzt wird.

13 Hashtag #ddj auf Twitter: http://twitter.com/search?q= %23ddj&src=typd
14 http://marijerooze.nl/thesis/graphics/
15 http://www.documentcloud.org/
16 http://overview.ap.org/
17 http://pandaproject.net/
18 http://pandaprojekt.tumblr.com/

Informationsfreiheitsgesetz: Das Jahr, in dem wir Kontakt aufnahmen.

Markus Beckedahl

Das Informationsfreiheitsgesetz ist eigentlich eine gute Sache. Bürger erhalten vom Staat ein Werkzeug in die Hand, um die Verwaltung und den Staat kontrollieren und transparenter machen zu können. Soweit zur Theorie. Die Umsetzung bietet aber noch einiges an Verbesserungspotential, wie wir vor allem in diesem Jahr feststellen konnten.

Im August 2011 gab es eine kleine Revolution: Die Plattform *Frag den Staat* wurde von der Open Knowledge Foundation Deutschland e. V. Gestartet, um die Barriere für die Nutzung des Informationsfreiheitsgesetzes zu senken. Seitdem kann man mit wenigen Klicks wie in einem Sozialen Netzwerk eine Anfrage an die jeweilige Behörde zusammenstellen und auf eine Antwort warten. Wenn denn eine kommt.

Das Informationsfreiheitsgesetz schreibt eigentlich vor, dass Behörden innerhalb eines Monats antworten müssen, aber die Frist gilt eher als Wunschterminierung denn als verbindlicher Termin. Oftmals müssen Bürger nach Ablauf der Frist pro-aktiv nachforschen, wann denn mit einer Antwort zu rechnen ist. Beamte hoffen wohl darauf, dass eine Anfrage in Vergessenheit gerät. Und wenn tatsächlich eine Antwort kommt, ruft diese des öfteren Erstaunen hervor. So ging es uns in der Netzpolitik-Redaktion in diesem Jahr zumindest.

ACTA und die größtmögliche Transparenz

Im Februar, kurz vor den Massenprotesten gegen ACTA, erklärte unsere Bundesjustizministerin Sabine Leutheusser-Schnarrenberger, dass sie eine kritische Haltung zu ACTA eingenommen hätte und Deutschland deshalb das Abkommen erst einmal nicht ratifizieren würde. Der schwarze Peter wurde an das EU-Parlament abgeschoben. Die EU-Kommission reagierte verwundert und erklärte, dass die Bundesregierung doch an allen Verhandlungen teilgenommen habe und es vorher keinerlei Einwände gegeben hätte. Daraufhin stellte Mathias Schindler eine Anfrage an das Bundesjustizministerium: er

wollte wissen, welche Mitarbeiter aus welchen Abteilungen an den Verhandlungen für die Bundesregierung teilgenommen haben und wünschte alle Dokumente über die Verhandlungen zu sehen.

Die erste Antwort kam mit der Auskunft, dass das nicht billig sein würde: „Es wird wahrscheinlich ein Arbeitsaufwand entstehen, der den Rahmen einer einfachen Auskunft übersteigt, wofür Gebühren bis zu 500 € erhoben werden können (siehe nähere Einzelheiten in der Informationsgebührenverordnung)". Das ist eine Standardformulierung bei größeren Auskunftsersuchen, allerdings lassen sich viele unbedarfte Bürger wahrscheinlich von den Kosten abschrecken, trotz des „bis zu" vor den 500 Euro.

Mathias Schindler wählte eine Alternative und antwortete, dass er auf die umfangreichen Akten verzichte und erst einmal nur die Namen wünsche. Das sei sicherlich günstig zu machen. Die nächste Antwort verblüffte – Mathias Ansinnen wurde mit einer Gefährdung der Öffentlichen Sicherheit abgewiesen: „Das Bekanntwerden der Informationen zu den Personen, die für die Bundesregierung bei den Verhandlungsrunden zu ACTA anwesend waren, kann die öffentliche Sicherheit, zu der auch die Rechtsgüter der betroffenen Mitarbeiter gehören, gefährden." Wir entschieden uns daraufhin an einem Freitag Abend dafür aufzurufen, über den gemeinnützigen Digitale Gesellschaft e. V. Spendengelder zu sammeln, um Mathias bei einer Klage unterstützen zu können. Zu unserer Verwunderung kamen bis Montag Morgen rund 10.000 Euro zusammen. Mathias Schindler legte Widerspruch ein und forderte dazu wieder alle Dokumente an. Ausreichend Kopiergeld war ja jetzt vorhanden. Zum Zeitpunkt des Erscheinens dieses Artikels läuft das Widerspruchsverfahren noch, denn Mathias Schindler hat nach vielen Monaten immer noch keine offizielle Antwort erhalten, um endlich vor Gericht gehen zu können. ACTA hingegen ist seit einem halben Jahr bereits Geschichte.

Ackermann Geburtstagsliste

Im Jahre 2008 fand im Bundeskanzleramt ein Ereignis statt, welches nicht nur die Medien in den darauffolgenden Jahren beschäftigen sollte: Der damalige Bundesbank-Chef Josef Ackermann wurde von Bundeskanzlerin Angela Merkel zu seinem 60. Geburtstag mit einer exklusiven Geburtstagsparty beschenkt. Wer dabei war und warum die Party ausgerichtet wurde, blieb aber vorerst geheim. Der Verbraucherschützer Thilo Bode wollte die Gästeliste der illustren Runde sowie die Rechnung für das Essen einsehen und stellte eine

Anfrage nach Informationsfreiheitsgesetz. Das lehnte das Kanzleramt ab. Also klagte Bode vor dem Verwaltungsgericht Berlin und gewann. Das Kanzleramt legte Berufung ein und verlor erneut. Das Oberverwaltungsgericht Berlin-Brandenburg urteilte im März diesen Jahres:

> *Die Berufung der Beklagten ist unbegründet. Zu Recht hat das Verwaltungsgericht die Beklagte verpflichtet, den Klägern Zugang zu den unkenntlich gemachten Passagen in der Redevorlage vom 17. April 2008, dem Adressverteiler, den beiden Gästelisten und der Tisch- und Sitzordnung zu gewähren. […] Die Revision ist nicht zuzulassen.*

Nach diesem rechtskräftigen Urteil hat auch Stefan Wehrmeyer auf FragDenStaat.de die Dokumente angefordert. Die hat er zwar erhalten, doch die Bundesregierung wollte eine Veröffentlichung verhindern. Im Begleitschreiben stand: „Ich weise darauf hin, dass das Bundeskanzleramt einer Weiterverbreitung der übersandten Kopien, namentlich einer Veröffentlichung der darin enthaltenen personenbezogenen Daten durch Sie nicht zustimmt."

Das wunderte doppelt. Einerseits waren alle Namen der Teilnehmer bereits von Medien publiziert worden. Andererseits wurde die Information bereits erfolgreich „rausgeklagt".

Da es nicht unserer Rechtsauffassung des Informationsfreiheitsgesetzes entspricht, eine Information zwar zu erteilen, aber die Veröffentlichung zu verbieten, haben wir die Dokumente im Juli publiziert. Im Bonuspaket zu den Namen fand sich noch die Sammelrechnung der Küche, die transparent darlegte, dass auch die Köche der Kanzlerin im Supermarkt einkaufen, sowie eine Redevorlage samt Abwägung, ob man überhaupt für Josef Ackermann eine Party schmeißen dürfe, weil er doch in der öffentlichen Kritik stand.

Eignet sich auch zur Unterdrückung von Informationen: Das Urheberrecht

Aber diese beiden Erfahrungen mit dem Informationsfreiheitsgesetz sollten noch getoppt werden. Im Jahre 2008 wurde der Wissenschaftliche Dienst des Deutschen Bundestages beauftragt, doch mal den aktuellen Stand der Abgeordnetenkorruption in Deutschland zusammenzufassen und Handlungsempfehlungen zu geben. Dabei kam u. a. Heraus, dass Deutschland noch nicht mal die UN-Konvention gegen Korruption unterzeichnet hat. Dieser

völkerrechtlich bindende Vertrag enthält Präventionsmaßnahmen gegen Korruption sowie die Pflicht der Staaten, verschiedene Sachverhalte rund um Korruption unter Strafe zu stellen. Bisher haben 161 Staaten das Übereinkommen ratifiziert. Deutschland nicht, zusammen mit Myanmar, Sudan, Saudi-Arabien, Nordkorea und Syrien. Das macht Deutschland hier zur Bananenrepublik – weit weg vom internationalen Standard. Ebenso erklärte das Gutachten, dass unsere Gesetze zur Abgeordnetenbestechung „praktisch bedeutungslose symbolische Gesetzgebung" seien und dringend verschärft werden müssen. Passiert ist seitdem aber wenig, was vielleicht auch damit zu tun haben könnte, dass niemand das Gutachten zu sehen bekam. Es kursierte zwar im politischen Berlin, aber außerhalb von Politiker- und Journalistenkreisen bekamen es Bürger nicht zu sehen.

Im Januar wurde über FragdenStaat.de die Anfrage gestellt, das Gutachten durch das Informationsfreiheitsgesetzes zu erhalten. Im Februar wurde es verschickt, allerdings mit dem Vermerk: „Ich weise deshalb darauf hin, dass das Ihnen übersandte Gutachten für Sie persönlich bestimmt ist. Die Übersendung beinhaltet *nicht* die Befugnis der Verbreitung oder Veröffentlichung. Die unerlaubte Veröffentlichung oder Verbreitung von Arbeiten des Wissenschaftlichen Dienstes stellt einen Verstoß gegen das Urheberrecht dar und hat sowohl zivilrechtliche als auch strafrechtliche Folgen." Mehr als 600 Bürger klickten ebenfalls über FragdenStaat.de eine IFG-Anfrage und erhielten das Dokument mit dem Verbot, es zu publizieren.

Als die Debatte um Abgeordnetenkorruption im September wieder an Fahrt gewann, entschlossen wir uns, das Gutachten bewusst trotz der Gefahren von „zivilrechtlichen als auch strafrechtlichen Folgen" zu publizieren. Anfang Oktober ging das Gutachten online. Mitte Oktober erhielten wir einen freundlichen Brief der Bundestagsverwaltung mit Frist, doch bitte das Gutachten wieder aus dem Netz zu nehmen. Diesem Wunsch verweigerten wir uns allerdings und warten seitdem, ob etwas passiert. Das Gutachten ist bereits an etlichen Stellen im Netz verfügbar, so dass eine gerichtliche Auseinandersetzung an einer Verbreitung nichts mehr ändern würde. Sollte es zu einer gerichtlichen Auseinandersetzung kommen, werden wir diese selbstverständlich führen. Uns ging es bei der Aktion darum, mehr Aufmerksamkeit auf die bizarre Situation der ungelösten Abgeordnetenkorruption zu werfen, bei der wir uns dafür schämen, dass Deutschland in einer Liste mit Bananenstaaten und Diktaturen genannt wird. Und unsere Hauptmotivation ist es weiterhin

zu klären, ob es im Informationsfreiheitsgesetz ein Recht auf Publizieren gibt – und falls nicht, Aufmerksamkeit dafür zu schaffen, dass dort eine Lücke vorherrscht. Wenn Bürger ihre Kontrollfunktion durch das IFG wahrnehmen können und sollen, dann müssen sie auch das Recht haben, befreite Dokumente im Original zu publizieren, um anderen Bürger darüber berichten zu können.

Es gibt aber auch Positivbeispiele: Die EU macht vor, wie es geht.

Urheberrecht, Gefährdung der Öffentlichen Sicherheit und Datenschutz. Wenn es Ausreden bedarf, um Anfragen mit Hilfe des Informationsfreiheitsgesetzes ablehnen zu können, sind deutsche Beamte sehr kreativ. Das IFG lässt ihnen dazu leider zu viele Lücken. Dass es auch anders geht, zeigte uns die EU-Kommission. Ende letzten Jahres überraschte EU-Kommissarin Neelie Kroes die Öffentlichkeit mit der Ernennung von Karl-Theodor zu Guttenberg zum EU-Beauftragten für Internetfreiheit. Nun war zu Guttenberg hierzulande bisher nur durch zahlreiche andere Themen aufgefallen, aber nicht durch Positionen zur Internetfreiheit, doch die EU-Kommissarin hatte sicherlich Gründe für ihre Entscheidung. Das wollten wir näher wissen und fragten über ein Portal der EU-Kommission direkt an, welche schriftlichen Kommunikationsunterlagen zu der Entscheidung vorhanden sind. Innerhalb von 14 Tagen muss die EU-Kommission darauf antworten und wir waren positiv überrascht, als tatsächlich innerhalb der Frist eine umfangreiche Antwort kam. Darin enthalten waren Kopien der Protokolle und vom Mailkontakt mit zu Guttenberg.

Wir freuten uns, lachten über einzelne Formulierungen und nahmen uns vor, darüber zu bloggen. Leider waren wir nicht die einzigen, die diese Anfrage gestellt hatten. Und Telepolis berichtete früher darüber. Was blieb war aber die Erkenntnis, dass die EU in Sachen Informationsfreiheit und Transparenz unseren nationalen Rahmenbedingungen einiges voraus hat. Und wir dringend unser Informationsfreiheitsgesetz verbessern müssen.

Unsere Forderungen an ein zeitgenössisches Informationsfreiheitsgesetz

Das Prinzip umdrehen: Die Ausnahmen zur Regel machen!

Ausnahmeregeln für die Auskunftspflicht müssen auf ein Mindestmaß reduziert werden (also Datenschutz ja, aber Wahrung von Geschäftsgeheimnissen, Urheber-, Markenrechten einschränken, um eine zeitgemäße Abwägung von öffentlichem Interesse auf Zugang zu Informationen und privatem Interesse auf Wahrung von Schutzrechten herzustellen)

Abschaffung (oder deutliche Einschränkung) der Möglichkeit, Entgelte für IFG-Auskünfte zu fordern

Natürlich gibt es bei IFG-Anfragen Trolle, die ganze Verwaltungen nerven. Aber das sind Einzelfälle und deswegen sollte man nicht allen Bürgern hohe Hürden auferlegen, die von Beamten zudem recht willkürlich genutzt werden können, um Anfragen teuer zu machen.

Recht auf Zugang = Recht auf Publikation

Wenn Bürger die Verwaltung durch ein IFG kontrollieren sollen so müssen sie selbstverständlich das Recht haben, Dokumente und Daten der öffentlichen Verwaltung auch weiterverarbeiten und weiterverbreiten zu können. Also ein Right to Data im IFG verankern oder durch ein Transparenzgesetz regeln.

FragDenStaat.de: der Informationsfreiheitsverstärker

Ein Interview mit Stefan Wehrmeyer

netzpolitik.org: Was ist die Idee hinter FragDenStaat.de?

Stefan Wehrmeyer: FragDenStaat.de hilft Bürgern ihr Recht auf staatliche Informationen zu nutzen und dokumentiert deutsche Informationsfreiheit in der Praxis. Was steht in den Verträgen mit meinem lokalen Energieversorger und wie viel hat das neue Open-Government-Portal der Bundesregierung gekostet? Solche Anfragen kann man über ein einfaches Formular auf FragDenStaat.de an Behörden auf Bundesebene, in NRW, Berlin, Brandenburg und Hamburg stellen. Die Anfragen werden zusammen mit den Antworten der Behörden veröffentlicht. Dadurch wird die Bearbeitung der Informationsfreiheitsanfragen durch die Behörden öffentlich dokumentiert.

netzpolitik.org: Die Plattform ist jetzt 1,5 Jahre live. Habt Ihr ein paar Zahlen zur Nutzung?

Stefan Wehrmeyer: Einer der großen Vorteile von FragDenStaat.de: die Zivilgesellschaft kann jetzt ihre eigenen quantitativen und qualitativen Statistiken zur Informationsfreiheit in Deutschland erfassen. Seitdem FragDenStaat.de im August 2011 an den Start gegangen ist haben wir über 2500 Informationsfreiheitsanfragen versendet. 70 Prozent dieser Anfragen sind allerdings aus unseren Ein-Klick-Aktionen entstanden: wenn wir Antworten nicht veröffentlichen dürfen, dann geben wir unseren Nutzern die Möglichkeit mit einem Klick die gleiche Anfrage im eigenen Namen zu stellen. Wir zählen diese Ein-Klick-Anfragen nicht zu unseren normalen Anfragen dazu, sie landen aber tatsächlich als echte Informationsfreiheitsanfragen bei den Behörden. Dort verursachen sie Bearbeitungsaufwand, deswegen empfehlen wir auch die Veröffentlichung von Antworten nicht zu verbieten. Es bleiben 741 einzigartige Anfragen übrig, von denen 624 öffentlich sind.

Während das Bundesinnenministerium nur Zahlen sammelt, baut FragDenStaat.de ein öffentliches Informationsfreiheits-Archiv auf. Dadurch wird eine qualitative Analyse der Anfrage-Bearbeitung möglich. Wir hoffen, dass dies im kommenden Jahr von akademischer Seite geschieht.

netzpolitik.org: Was sind Probleme?

Stefan Wehrmeyer: Die Ausweitung von FragDenStaat.de auf mehr Bundesländer gestaltet sich schwierig: Listen von Behörden mit Kontaktinformationen sind nur kaum strukturiert aufzutreiben, die Gesetzeslage ist überall ein bisschen unterschiedlich und der Kontakt zu regionalen Verfechtern der Informationsfreiheit fehlt. Dennoch wollen wir es 2013 schaffen, die restlichen sieben Bundesländer mit Informationsfreiheitsgesetzen aufzunehmen.

Die Zusammenarbeit mit den Behörden ist spürbar besser geworden, es besteht aber gerade bezüglich digitaler Kommunikation noch Aufholbedarf. Es kommt regelmäßig vor, dass Antworten noch ausgedruckt, eingescannt und dann an die falsch abgetippte E-Mailadresse verschickt werden. Das wird sich hoffentlich mit dem kommenden E-Government-Gesetz ändern.

Das größte Problem, das leider auch nicht technisch lösbar ist, ist natürlich die durchwachsene und teilweise sehr rückständige Gesetzeslage in Deutschland oder auch deren Auslegung seitens mancher Behörden. Neben den altbekannten Geschäfts- und Betriebsgeheimnissen, die so manchem Informationsbegehren unabwägbar im Weg stehen, gesellen sich auf FragDenStaat.de auch viele andere Ausnahmen und Ausreden wie die öffentliche Sicherheit, Urheberrechte oder – ganz klassisch – die Nicht-Anwendbarkeit des Gesetzes. Wir beobachten aber auch neue, sehr beunruhigende Ablehnungs-Auswüchse: ist die angefragte Information nicht exakt wie beschrieben vorhanden, kam es schon vor, dass sie abgelehnt wurde. Dies ist besonders bedenklich, da die eigentlich nach Gesetz zu veröffentlichenden Aktenpläne der Behörden meist nicht vorliegen und der Bürger somit gar nicht wissen kann, welche Art von Information genau vorhanden ist.

Durch die Öffentlichkeit der Ablehnung erfahren diese immerhin eine genauere Prüfung. Doch oftmals hilft nur sich den Informationszugang zu erklagen, was wir unseren Nutzern in Zukunft noch erleichtern wollen. Denn diese Klagen sind in vielen Fällen erfolgreich und bringen somit die Informationsfreiheit in der Praxis voran.

netzpolitik.org: Wie kommt die Plattform bei den Behörden an?

Stefan Wehrmeyer: Die Akzeptanz von FragDenStaat.de bei Behörden variiert. Einigen Behörden muss man erklären, dass der oder die AnfragestellerIn FragDenStaat.de als E-Mailanbieter gewählt hat und daher nicht noch eine andere, private E-Mailadresse oder eine Postadresse benötigt wird. Doch mittlerweile haben sich die häufiger angefragten Behörden an das Portal gewöhnt.

netzpolitik.org: Wie häufig kommt es vor, dass Bürger keine Antwort erhalten, obwohl innerhalb eines Monats eine Antwort erfolgen soll?

Stefan Wehrmeyer: Da wir bei Postantworten auf die Gewissenhaftigkeit unsere Nutzer angewiesen sind, können wir für den Bereich nur Schätzungen vornehmen. Danach erfolgen ungefähr ein Viertel aller Antworten nicht in der gesetzlichen Frist. Wir empfehlen und erinnern unsere Nutzer daran, nicht locker zu lassen, auf die Verspätung hinzuweisen und nachzufragen, bis sie eine Antwort erhalten.

netzpolitik.org: Was wollt Ihr noch an der Plattform verbessern?

Stefan Wehrmeyer: Wir wollen die vielen, befreiten Verwaltungsdokumente besser zugänglich machen. Außerdem überlegen wir uns, es Nutzern zu ermöglichen anfallende Gebühren für Anfragen über die Plattform zu crowdfunden.

netzpolitik.org: Ihr habt jetzt etwas Erfahrung mit dem IFG gesammelt. Welche Änderungswünsche habt Ihr an die Politik?

Stefan Wehrmeyer: Bisher werden immer einzelne Verbesserungen an die Informationsgesetze herangetragen. Das Beispiel des Hamburger Transparenzgesetzes hat jedoch gezeigt, dass sich die Informationspolitik grundlegend ändern lässt. Verwaltungsdokumente aus verschiedenen Kategorien müssen ohne Anfrage direkt öffentlich zugänglich gemacht werden und zwar elektronisch und möglichst maschinenlesbar. Eine Anfrage über FragDenStaat.de muss der selten nötige Spezialfall werden.

Deutschland, deine Datenschätze! Open Data Jahresrückblick 2012

Julia Kloiber

Daten – Bits und Bytes oder besser Gigabits und Gigabytes – sind der virtuelle Rohstoff des Informationszeitalters. Egal ob Wirtschaft, Politik oder Wissenschaft, Daten sind wesentliche Ressourcen und spielen in allen gesellschaftlichen Bereichen eine wichtige Rolle. Auf Basis von Daten werden Entscheidungen getroffen und Produkte verkauft. Etliche Geschäftsmodelle basieren mittlerweile auf der Erzeugung, Interpretation, Verwertung und dem Verkauf von digitalen Daten und den daraus abgeleiteten Informationen.

Auch Staat und Verwaltung sammeln und erzeugen eine Vielzahl an Daten. Behörden, Gerichte, Ämter und andere staatliche Stellen häufen große Mengen an Informationen an – diese reichen von Wetterdaten über Haushaltsstatistiken bis hin zu Informationen zur Parteienfinanzierung. Primär dienen diese Daten der Erfüllung staatlicher Aufgaben. Ähnlich wie in den Datensammlungen großer Unternehmen, steckt auch in Verwaltungsdaten großes Potenzial für Wirtschaft und Gesellschaft. Aus diesem Grund sind Verwaltungs- und Regierungsdaten von großem öffentlichen Interesse. Doch obwohl die Datenbestände von Behörden und staatlichen Einrichtungen mit Hilfe von Steuergeldern erhoben und gepflegt werden, haben BürgerInnen auf viele Datensätze gar keinen oder nur sehr eingeschränkt Zugriff.

Anders als in Ländern wie Großbritannien und den USA – die Vorreiter im Bereich Open Government und Open Data sind und seit mehreren Jahren die Strategie eines offenen und partizipativen Staates verfolgen – ist man in Deutschland eher zögerlich, was die Öffnung von behördlichen Daten und die Beteiligung von BürgerInnen angeht. Zwar gab es 2012 in Deutschland einige positive Entwicklungen im Bereich Open Data/Open Government, doch von einem Paradigmenwechsel hin zu einem offenen Staat mit aktiver Einbindung der BürgerInnen ist man noch weit entfernt.

Was sich in Deutschland im letzten Jahr im Bereich Open Data getan hat, in welchen Bereichen es Schwierigkeiten gibt, oder Verbesserungen dringend notwendig sind und wie weit der Weg in Richtung eines Open Government noch ist, zeigt ein kurzer Open Data Jahresrückblick.

Apps für Deutschland

Mit einem bundesweiten „App-Wettbewerb“[1] startete Deutschland vielversprechend in das Jahr 2012. Unter der Schirmherrschaft des Bundesministeriums des Inneren und der Trägerschaft der drei NGOs Open Knowledge Foundation Deutschland, Open Data Network und dem Government 2.0 Netzwerk Deutschland wurde bereits im November 2011 zur Entwicklung kreativer Anwendungen und Ideen auf Basis von offenen Daten aufgerufen. Ziele des Wettbewerbs waren: mehr offene Daten, politische Transparenz, Wirtschaftsförderung und mehr nützliche Anwendungen sowie die Ansprache von Entwicklern, Ideengebern und Kreativen. Das Ergebnis war jedoch wenig nachhaltig, was auf mehrere Umstände zurückzuführen ist. So stellten nur wenige Behörden interessante Datensätze zur Verfügung. Anstatt von Daten mit politischer Relevanz, wie Daten aus dem Unternehmensregister oder dem Bundeshaushalt, standen den Teilnehmern überwiegend statistische Daten oder etwa die Pegel deutscher Wasserstraßen zur Verfügung.

Einen weiteren Anlass zu Kritik bietet die mangelnde Nachhaltigkeit des Wettbewerbs. Nach der Preisverleihung auf der Cebit wurde es still um die Preisträger. Ob die Projekte erfolgreich umgesetzt wurden oder auf Festplatten verstauben, ist nicht bekannt.

2013 geht der Wettbewerb unter dem Titel „Gov Apps“[2] in die zweite Runde. Diesmal ohne die drei NGOs und ohne in der Ankündigung das Wort „open“ zu erwähnen. Damit ist die Neuauflage des Wettbewerbs im nächsten Jahr vielleicht weniger Feigenblatt-Aktion für Open Data und Open Government und mehr ehrliche Wirtschaftsförderung.

Als Gegenmodell zu „App-Wettbewerben“ versteht sich das im Herbst 2012 gestartete Projekt „Stadt Land <Code>“[3] der Open Knowledge Foundation Deutschland. Unter dem Motto „Gesellschaft hacken“ waren Entwicklerinnen und Coder dazu aufgerufen, Apps und Anwendungen umzusetzen, die den

1 S.: http://apps4deutschland.de/

2 https://www.govapps.de/wettbewerb

3 http://stadtlandcode.de/

Alltag von Bürgern vereinfachen und Bürger untereinander und mit dem Staat besser vernetzen. Neben der Entstehung neuer Anwendungen ist es Ziel des Projektes, die Civic Apps Community in Deutschland besser miteinander zu vernetzen und zu fördern.

Datenkataloge und Portale

Nachdem 2011 mit daten.berlin.de[4] der erste Datenkatalog Deutschlands in Berlin online gegangen ist, haben sich 2012 weitere Städte und Bundesländer der Open Data Initiative angeschlossen und Datenportale gestartet. Darunter sind Bremen, Köln und Baden Württemberg. Diese Entwicklungen sind positiv, zeigen sie doch, dass einzelne Kommunen und Städte das Potenzial von offenen Daten verstanden haben. Ohne politischen Druck und gesetzliche Regelungen verkommen die Portale jedoch zu langweiligen Archiven für statistische Datensätze, anstatt zur Quelle für Innovation und politische Transparenz zu werden.

Ein Großteil der Datenkataloge ist eher spärlich befüllt und viele der vorhandenen Daten sind weder wirtschaftlich noch politisch von Relevanz. Zwar befinden sich alle Portale noch im Beta-Stadium und damit im Aufbau, solange es jedoch kein breites Angebot an Datensätzen gibt, kann sich das volle Potenzial von Open Data nicht entfalten. In vielen Katalogen reihen sich Standortkoordinaten von Altglascontainern an Übersichten von Badestellen und Weihnachtsmärkten und nur vereinzelt finden sich für Open Government relevante Datensätze – Haushaltsdaten, Parteispenden, Firmenregister. Deutsche Behörden sind zurückhaltend, wenn es um die Öffnung ihrer Datenschätze geht. Eine Ursache dafür ist das Fehlen einer gesetzlichen Verpflichtung, Daten „proaktiv" zur Verfügung zu stellen. Das führt dazu, dass Behörden ohne gesetzliche Rückendeckung, lieber auf Nummer sicher gehen und häufig nur politisch neutrale Datensätze veröffentlichen.

Auch mit der uneingeschränkten Offenheit von Daten im Sinne von Open Data hat man vielerorts Probleme. So sind Kosten und Geldleistungsmodelle für Daten ein häufig diskutiertes Thema in Kommunen. Für viele Gemeinden und Städte ist dabei besonders die kostenlose Bereitstellung für kommerzielle Zwecke ein schwieriges Thema. Denn der Verkauf von Daten wie Geodaten ist ein lukratives Geschäft, auf das viele nicht verzichten wollen bzw. können.

4 http://daten.berlin.de/

Viele befürchten hohe Umsatzeinbußen, wenn zuvor kostenpflichtige Datensätze plötzlich offen zur Verfügung stehen. Diese Befürchtung wird zwar von einigen internationalen Beispielen widerlegt, doch die Skepsis bleibt.

Um Open Data in Deutschland zu stärken und weiter voranzutreiben, ist die gesetzliche Verankerung eines Rechtsanspruchs auf die „proaktive" Veröffentlichung von Daten unumgänglich. Ernüchternd in dieser Hinsicht ist die Tatsache, dass fünf deutsche Bundesländer bis dato nicht einmal über einfache Informationsfreiheitsgesetze verfügen. Einen Meilenstein hingegen stellt das im Juni 2012 in Hamburg erlassene Transparenzgesetz dar, das die weitgehende Veröffentlichung von behördlichen Daten vorschreibt. Eine ähnlich fortschrittliche Regelung gibt es sonst lediglich in Bremen.

Die Plattform „Open Data in Kommunen"

Während einzelne Städte bereits Datenkataloge haben, sind viele Kommunalpolitiker noch eher ratlos was das Thema Open Data betrifft. Um dies zu ändern, hat der Digitale Gesellschaft e. V. Die Plattform „Open Data in Kommunen"[5] ins Leben gerufen. Ziel des Portals ist es, das Konzept von Open Data klar und einfach zu erklären und Politikern Beispiele und Argumente an die Hand zu geben. Zusätzlich sollen auf der Plattform Antragsvorlagen für kommunale Anträge zur Umsetzung von Open Data zur Verfügung gestellt werden. Mithilfe dieser Vorlagen soll der erste Schritt in Richtung einer Öffnung von Daten, das Einreichen eines Antrages, vereinfacht werden.

Do:Index

Um in weiterer Folge einen Überblick über die Vielzahl an kommunalen Initiativen zum Thema Open Data zu behalten, hat der Digitale Gesellschaft e. V. In Zusammenarbeit mit dem österreichischen Verein Freie Netze. Freies Wissen. Und dem Schweizer Verein Digitale Allmend das Projekt Do:Index[6], kurz für Digital Openness Index, gestartet. Mithilfe dieses Index will man für mehr Transparenz und Übersicht im Bereich von digitalen Allgemeingütern sorgen und Rankings erstellen. Durch Rankings und Vergleiche sollen Kommunen für Open Data sensibilisiert und wechselseitiges Lernen gefördert werden.

5 http://opendata-kommunen.de/

6 http://www.do-index.org/

Open Government Data auf Bundesebene

Auch auf Bundesebene gab es 2012 Bewegung im Bereich von Open Data. So hat man im Bundesministerium des Inneren mit der Entwicklung einer zentralen Open Government Data Plattform für Deutschland[7] begonnen. Bis 2013 will man damit alle Open-Data-Angebote der Kommunen auf einem Portal bündeln. Im Vorfeld wurde eine Open Government Data Studie[8] in Auftrag gegeben, in der es neben einer Problemanalyse zu den föderalen Strukturen von Kommunen, Ländern und Bund auch mehrere Handlungsempfehlungen für die Umsetzung von Open Government Data in Deutschland gibt. Einige dieser Empfehlungen – wie die zu eigenen deutschen Nutzungsbedingungen und Geldleistungsmodelle – gelten als umstritten in der Open Data Community. Es wird befürchtet, dass eigene Nutzungsbedingungen dazu führen, dass Datenaustausch und Nutzung auf europäischer und internationaler Ebene erschwert werden und sich Deutschland damit vom Ausland abschottet. Geldleistungsmodelle sind aus einem ähnlichen Grund umstritten, denn sie behindern die hürdenfreie Weiterverwendung von Daten.

Mit dem Open Government Portal des Bundes werden sich deutschlandweite Standards etablieren. Deshalb ist es besonders wichtig, darauf zu achten, dass es zu keiner Verwässerung des Begriffs Open Data kommt und „offen" auch wirklich „offen" bleibt. Im Dezember wird es für Entwickler, Open Data Experten und alle anderen Interessierten die Möglichkeit geben, den Prototypen des Open Government Portals unter die Lupe zu nehmen und Feedback zu geben. Diese Offenheit bei der Entwicklung einer bundesweiten Plattform ist ein Meilenstein für deutsche Verhältnisse. Bleibt zu hoffen, dass das Feedback aus der Community auch angenommen und umgesetzt wird.

Der offene Bundeshaushalt

Ein weiterer wichtiger Schritt in Richtung Open Data und Open Government war die längst überfällige Öffnung der Haushaltsdaten des Bundes. Im Sommer dieses Jahres hat das Bundesfinanzministerium die Seite „bundeshaushalt-info.de"[9] gestartet. Ein Datencenter, in dem sich Bürger darüber infor-

7 http://www.daten-deutschland.de/

8 BMI: Bundesinnenministerium veröffentlicht Studie „Open Government Data Deutschland", in: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2012/mitMarginalspalte/07/opengovernment.html; 6.12.2012.

9 http://www.bundeshaushalt-info.de/startseite/

mieren können, wie der Bund seine Einnahmen und Ausgaben plant. Dieser Schritt in Richtung Transparenz kann als Erfolg der Open Data Bewegung gewertet werden. Denn seit geraumer Zeit gibt es von der Open Knowledge Foundation Deutschland ein ähnliches Projekt zu den Haushaltsdaten des Bundes, das dem Finanzministerium als Inspiration gedient haben dürfte. Auf der Seite „Offener Haushalt“[10] stellt der gemeinnützige Verein seit 2010 die inoffiziellen Haushaltsdaten des Bundes als Open Data zur Verfügung. Warum das Bundesministerium sein Vorbild „Offener Haushalt“ beim Start der eigenen Seite in keinem Wort erwähnt hat, bleibt eben so unverständlich wie die Tatsache, dass man anstatt auf die auf Open Source basierte Plattform „Open Spending“[11] aufzusetzen, eine Agentur mit der Entwicklung einer eigenen Plattform beauftragt hat. Doch was am Ende zählt, ist der Erfolg: Deutschland hat offene Haushaltsdaten.

Apps and the City: Offene Nahverkehrsdaten – die Deutschlandpremiere in Berlin

Kurz vor Jahresende gab es auch im Bereich der Nahverkehrsdaten einen Erfolg zu verbuchen. Seit der letzten Novemberwoche stellt der Verkehrsverbund Berlin Brandenburg (VBB) als erster Nahverkehrsverbund Deutschlands seine Fahrplandaten offen zur Verfügung. Ein Erfolg, an dem die Open Data Community maßgeblich beteiligt war. Monatelang haben Open Data Experten u. a. Aus der Open Knowledge Foundation und Vertreter aus der Senatsverwaltung für Wirtschaft, Technologie und Forschung mit dem VBB diskutiert und versucht Vorurteile auszuräumen. Und als wäre die Bereitstellung der Daten nicht schon Revolution genug, war der VBB auch noch Mitveranstalter eines Hackdays[12] auf dem sich mehr als 150 Entwickler mit den Daten der Verkehrsunternehmen auseinandersetzten. Besonders vor dem Hintergrund der Open Data-Blockadehaltung der Deutschen Bahn ist die Herausgabe der Nahverkehrsdaten Berlins ein großer Erfolg, der hoffentlich viele Nachahmer findet.

10 http://bund.offenerhaushalt.de/
11 http://openspending.org/
12 http://appsandthecity.net/

Inoffizielle Innovation – Projekte jenseits der staatlichen Offenheit

Offenes Köln

Neben staatlichen Projekten im Bereich Open Data starteten 2012 auch zahlreiche Projekte aus der Zivilgesellschaft. Eines von ihnen ist die Plattform „Offenes Köln" von Marian Steinbach. „Offenes Köln"[13] ist eine interaktive Stadtkarte und Schnittstelle, über die politische Vorgänge aus der Kölner Kommunalpolitik, sowie Informationen aus dem Ratsinformationssystem der Stadt Köln zugänglich gemacht werden. Da es im Vorfeld des Projektes keine offizielle Genehmigung der Stadt für die Nutzung der Daten gab, stieß die Plattform zunächst auf wenig Gegenliebe von offizieller Seite. Skepsis und Sorge haben sich mittlerweile aber ins Gegenteil verkehrt und die Stadt Köln ist stolz auf ihre Informationsplattform aus der Zivilgesellschaft. „Offenes Köln" ist ein gutes Beispiel dafür, wie Innovation auch ohne offizielle Erlaubnis Prozesse beschleunigen kann.

openPlanB

Ein weiteres Beispiel für inoffizielle Innovation – oder wie Michael Kreil es nennt „Innovation without Permission" – ist das Projekt „openPlanB".[14] Unter diesem Titel hat Kreil im Herbst 2012 die Daten zu über 300.000 Bahnhöfen der Deutschen Bahn eigenmächtig veröffentlicht. Offizielle Unterstützung fand er dabei keine, ganz im Gegenteil, die Deutsche Bahn sperrt sich seit Jahren dagegen, ihre Daten im Sinne von Open Data allen zur Verfügung zu stellen. Ganz anders verhält es sich, wenn ein Großkonzern wie Google anklopft. Dann stellt man – wie im Herbst geschehen – gerne alle Datensätze kostenlos und exklusiv zur Verfügung. Die Datenbefreiungs-Aktion von Michael Kreil hingegen ist weniger gut angekommen. Die Bahn bezichtigte ihn der vorsätzlichen Verletzung von Rechten und will ihn im Wiederholungsfall strafrechtlich zur Verantwortung ziehen. Der Fall hat für Aufsehen gesorgt und wird sein Ziel trotz vorzeitiger Niederlage vielleicht doch noch erreichen. Denn offene Bahndaten sind nun Thema in Deutschland.

13 http://offeneskoeln.de/

14 http://openplanb.tumblr.com/

Mehr Schein als Sein

Trotz mehrerer erfolgreich umgesetzter Projekte und Initiativen im Bereich von offenen Daten fällt das Open Data Fazit 2012 ernüchternd aus. Neben positiven Entwicklungen gab es leider auch mindestens genauso viele verpasste Chancen für Wirtschaft und Demokratie. Gemessen an internationalen und europäischen Entwicklungen geht der Fortschritt hierzulande nach wie vor nur langsam voran. Deutschland ist weder Mitglied der Open Government Partnership[15] noch gibt es ein parteienübergreifenden politisches Bekenntnis zu Open Data und mehr Transparenz.

Als zaghaft und halbherzig kann man die deutschen Entwicklungen im Bereich Open Data und Open Government beschreiben. Der Schwerpunkte liegt dabei oft nicht auf Transparenz, sondern auf der Förderung von Wirtschaft und Verwaltungseffizienz. Zwar gibt es vereinzelt positive Ausreißer, im größeren Zusammenhang fehlt es aber an einer klaren Strategie und Vision für die Öffnung von Staat und Verwaltung. Umso wichtiger ist es, dass zivilgesellschaftliche Organisationen und Initiativen sich weiterhin für offene Daten einsetzen, Aufklärung betreiben und die Datenschätze Deutschlands nach und nach heben.

15 http://www.opengovpartnership.org/

Das Unbehagen im Datenhaufen: Big Data und Datenschutz

Andre Meister

Große Datensätze sind toll für die Forschung, doch der Rückschluss auf Personen wird immer einfacher. Unser Umgang mit persönlichen Daten muss sich ändern.

Im Jahr 2012 gab es einen Hype um das Buzzword „Big Data", die taz sprach gleich vom „nächsten großen Ding."[1] Tatsächlich sind große Datenmengen nur die logische Konsequenz der fortschreitenden Digitalisierung unserer Gesellschaft. Kaum ein Lebensbereich wird nicht durch vernetzte Computersysteme durchdrungen, und dabei fallen immer mehr Daten an, die natürlich auch verarbeitet werden.

Geheimdienste und Großkonzerne machen das schon länger. Banken wenden statistische Verfahren auf die Finanztransaktionen ihrer Kunden an, um Unregelmäßigkeiten zu entdecken. Die amerikanische Einzelhandels-Kette Walmart verarbeitete schon vor zwei Jahren eine Million Kunden-Transaktionen, pro Stunde.[2] Facebook speichert mehr als 200 Milliarden Fotos seiner Nutzer, täglich kommen zehn Millionen neue dazu.[3] Die scannt es nach Gesichtern – und trainiert damit seinen Algorithmus zur Gesichtserkennung. Und der amerikanische Geheimdienst NSA baut gerade im abgelegenen Utah das größte Spionage-Rechenzentrum der Welt, zum Sammeln und Rastern von Datenmengen in unvorstellbaren Ausmaßen.[4]

Das neue ist nur, dass große Datensätze auch immer mehr Forschern und sogar Endanwendern zur Verfügung stehen. Teilweise lassen sich daraus tolle Erkenntnisse ziehen. Forscher der Elite-Uni Harvard haben die Handydaten

1 *Paletta, Giuseppe* 2012: „Es wird größer als das Internet", in: http://www.taz.de/!105303/; 5.12.2012.

2 The Economist 2010: Data, data everywhere, in: http://www.economist.com/node/15557443; 5.12.2012.

3 *Kiss, Jeremia* 2012: Facebook hits 1 billion users a month, in: http://www.guardian.co.uk/technology/2012/oct/04/facebook-hits-billion-users-a-month; 5.12.2012.

4 *Bamford, James* 2012: The NSA Is Building the Country's Biggest Spy Center (Watch What You Say), in: http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/; 5.12.2012.

von 15 Millionen Kenianern über den Zeitraum von einem Jahr ausgewertet und mit Karten über die Ausbreitung von Malaria verglichen.[5] Damit konnten sie den Ursprung der Tropenkrankheit sowie ihren Ausbreitungsweg nachvollziehen[6] – und dass Menschen ebenso zur Verbreitung beitragen wie Moskitos.

Auch Polio soll mit Big Data bekämpft werden. Eine private Datenanalyse-Firma will mit Handydaten Impfpläne verbessern und bisher nicht verzeichnete Dörfer einbeziehen.[7] In Großbritannien sollen die Krankenakten aller Einwohner zentral gesammelt und mit anderen Datenbanken verknüpft werden.[8] Das wird als Revolution der medizinischen Forschung gefeiert.

Drei Daten, eine Identität

Dabei wird immer versprochen, dass die Datensätze natürlich anonymisiert sind. Doch die Kehrseite von Big Data ist auch, dass eine herkömmliche Anonymisierung, also das Entfernen von eindeutig identifizierbaren Informationen wie Name und Anschrift, nicht ausreichend ist und immer leichter rückgängig gemacht werden kann. Bereits in den Neunziger Jahren versicherte der Gouverneur von Massachusetts, dass die veröffentlichten Krankendaten seines Staates datenschutzrechtlich unbedenklich sind, weil personenbezogene Informationen entfernt wurden.

Die Forscherin Latanya Sweeney machte diese Anonymisierung rückgängig, in dem sie nicht anonymisierte, scheinbar harmlose Informationen des Datenbergs mit weiteren Datensätzen verknüpfte. So war sie in der Lage, die persönliche Krankenakte des Gouverneurs herauszufinden und ihm zuzuschicken.

---

5 *Wesolowski, Amy/ Eagle, Nathan/ Tatem, Andrew J.* et al.2012: Quantifying the Impact of Human Mobility on Malaria, in: Science 338:6104; 267-270, in: http://www.sciencemag.org/content/338/6104/267; 5.12.2012.

6 Pressemitteilung Harvard 2012: Using Cell Phone Data to Curb the Spread of Malaria, in: http://www.hsph.harvard.edu/news/press-releases/2012-releases/cell-phone-data-malaria.html; 5.12.2012.

7 *Stepanek, Martin* 2012: Big Data soll Malaria und Polio ausrotten, in: http://futurezone.at/future/11714-big-data-soll-malaria-und-polio-ausrotten.php; 5.12.2012.

8 *Sample, Ian* 2012: NHS patient records to revolutionise medical research in Britain, in: http://www.guardian.co.uk/science/2012/aug/28/nhs-patient-records-medical-research-revolution; 5.12.2012.

Im Jahr 2000 fand Sweeney heraus, dass 87 Prozent aller Amerikaner mit nur drei kleinen Daten eindeutig identifiziert werden können: Geschlecht, Geburtsdatum und Postleitzahl. Seitdem haben immer mehr Studien gezeigt, dass man aus scheinbar anonymisierten Datensätzen Einzelpersonen „re-identifizieren" oder „de-anonymisieren" kann, oft mit erstaunlicher Leichtigkeit. Die Königliche Gesellschaft Großbritanniens kam kürzlich in einem Bericht zu dem Fazit, „dass die Sicherheit von persönlichen Daten in Datenbanken durch Anonymisierung nicht garantiert werden kann, wenn aktiv nach Identitäten gesucht wird."[9]

Der Chaos Computer Club erweiterte schon in den Achtziger Jahren die Hackerethik um den Grundsatz: „Öffentliche Daten nützen, private Daten schützen". Auch bei diesem Thema stellt sich also erneut die Frage Was ist privat, was ist öffentlich? Die Sozialforscherin Danah Boyd beschäftigte sich vor zwei Jahren mit der Frage nach Datenschutz im Zeitalter von Big Data.[10] Eine ihrer fünf Überzeugungen ist: „Nur weil man Zugriff auf Daten hat, ist es noch nicht ethisch vertretbar, diese auch zu verwenden."

Mobilfunk-Anbieter speichern Verbindungs- und Ortsdaten ihrer Kunden zu Abrechnungszwecken. Als der Telefónica-Konzern mit seiner deutschen Tochter O2 aus diesen Daten Bewegungsprofile erstellen zu Werbezwecken erstellen wollte, musste sich erst das Wirtschaftsministerium einmischen, bis der Konzern die Pläne für Deutschland zurückzog. Im deutschen Recht existiert das Konzept der Zweckbindung, nach der Daten nur für vor der Erhebung definierte Zwecke verwendet werden dürfen.

Datenbriefe sind dringender denn je

Ein großes Problem dabei ist jedoch, dass wir in der digitalen Gesellschaft gar nicht mehr überblicken können, wer welche Daten über uns erhebt, verarbeitet und weitergibt. Die Grundvoraussetzung für eine bewusste Entscheidung ist jedoch genau dieses Wissen. Verbraucher sollten regelmäßig von Firmen, Behörden und Institutionen informiert werden, welche personenbezogenen Daten über sie dort gespeichert sind. Dieses Konzept des so genannten Datenbriefs ist nicht neu – aber dringender denn je.

---

9 The Royal Society 2012: Science as an open enterprise. Final report, in: http://royalsociety.org/policy/projects/science-public-enterprise/report/; 5.12.2012.

10 *Boyd, Danah* 2010: „Privacy and Publicity in the Context of Big Data", in: http://www.danah.org/papers/talks/2010/WWW2010.html; 5.12.2012.

Zudem sollten Verbraucher frei und selbstbestimmt entscheiden dürfen, für welche Zwecke sie welche Daten zur Verfügung stellen. Die derzeit gängige Praxis, alle möglichen Verwendungszwecke in undurchsichtigen und ellenlangen Geschäftsbedingungen zu verstecken und absegnen zu lassen muss durch einfache und offene Fragen ersetzt werden. Dienste müssen auch nutzbar sein, wenn man der unbestimmten Verarbeitung und Weitergabe meiner Daten widerspricht. Das schafft einen fairen Ausgleich zwischen dem Erkenntnisinteresse der Datenforscher und dem Selbstbestimmungsrecht des Einzelnen.

Dieser Text erschien zuerst auf taz.de, am 21. November 2012.

Die Versuchungen von Big Data

Jeanette Hofmann

Die Inwertsetzung und Vermarktung von Daten erweist sich als Kehrseite der digitalen Gesellschaft. Ein grundlegendes Merkmal der sich digitalisierenden Gesellschaft besteht darin, dass die vor wenigen Jahren noch selbstverständliche Unterscheidung zwischen Online- und Offline-Dasein für immer mehr Menschen ihre Relevanz verliert. Smartphones, Flatrate Verträge und neue ortsbezogene Informationsdienste sorgen dafür, dass wir immer und überall auf das Netz zugreifen und sich Internet und Gesellschaft zunehmend wechselseitig durchdringen. In dem Maße, in dem das Internet als eigenständiger Kommunikationsraum, in den man sich bewusst hineinbegibt – „ich bin drinnen" verkündete einst ein gar nicht so alter Werbespot – verschwindet und das Netz mobil wird, schwellen auch die Datenströme, die wir konsumieren und produzieren, kontinuierlich an. Unsere Datenspuren wiederum bilden den Rohstoff für einen neuen Wirtschaftsbereich, die Datenökonomie. Bereits vor zwei Jahren prophezeite der Economist, dass wir uns am Anfang der Entwicklung zu einer datenzentrierten Ökonomie befinden, die sich auf das Sammeln, Aufbereiten und Verkaufen von Information spezialisiert.[1]

Wichtige Quellen für das Geschäft mit den Daten bilden neben dem mobilen Internet die sogenannten sozialen Medien wie Facebook oder Twitter, die darauf ausgelegt sind, dass Nutzerinnen selbst Inhalte produzieren und mit anderen teilen. Einem Bericht von McKinsey[2] zufolge veröffentlichen die 900 Millionen aktiven Mitglieder bei Facebook monatlich derzeit rund 90 Informationsobjekte wie Notizen, Fotos, Videos oder Links. Alles in allem summiert sich der Austausch auf Facebook zu eindrücklichen 30 Mrd. Informationsobjekten, über die das Unternehmen Verfügungsrechte beansprucht. Die 490 Mio. individuellen Nutzerinnen von Youtube laden ca. 24 Stunden neues Videomaterial pro Minute auf die Plattform.

1 Economist 2010: Data, data everywhere, in: http://www.economist.com/node/15557443; 5.12.2012.

2 McKinsey 2011: Big data: The next frontier for innovation, competition, and productivity, in: http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation; 5.12.2012.

Eine große Rolle für die anwachsenden Datenströme spielt weiterhin das Cloud Computing, die Entstehung virtueller Infrastrukturen, die Speicherkapazität, Programme oder Arbeitsumgebungen bereitstellen. Die Cloud wird zum Beispiel als externer Speicher oder für das Teilen von Informationen mit Dritten verwendet. Eine weitere wichtige Quelle von Big Data schließlich könnte das Internet der Dinge werden, das heißt die zunehmende digitale Vernetzung der materiellen Welt. Beispiele dafür sind „smart meters" zur Messung des Stromverbrauchs, die Kennzeichnung und Ortung von Warenströmen, Verkehrsmitteln oder Sehenswürdigkeiten. Die sich abzeichnende Digitalisierung der Städte wird die Datenproduktion und -konsumtion weiter anheizen.

Glaubt man den allgemeinen Schätzungen, dann bewegt sich das jährlich hinzukommende Datenaufkommen inzwischen im Exabyte Bereich und wächst um rund 40 % pro Jahr.[3] Um eine Vorstellung vom Umfang der weltweit gespeicherten Daten zu vermitteln, hat International Data Corporation (IDC) das 2009 gespeicherte Datenvolumen mit einem Stapel DVDs bis zum Mond und wieder zurück verglichen.[4] Entgegen dem ehernen Grundsatz der Zweckgebundenheit von Datenerhebung und -speicherung besteht der Anreiz der neuen Informationswirtschaft gerade darin, so viele Datenquellen wie möglich zu erschließen, um aus diesem Rohstoff verwertbare Informationen und Dienste zu gewinnen. In den USA hat sich für dieses Phänomen der Begriff Big Data durchgesetzt.

Der Begriff Big Data ist allerdings etwas irreführend. Das Neue und Besondere dieses Phänomens besteht eben nicht allein in der schieren Masse der Daten, sondern in der Art und Weise, wie diese Daten aggregiert, korreliert, bewertet und genutzt werden, kurz: wie aus diesem Informationsrohstoff handelbare Produkte werden. Die Autorinnen Boyd & Crawford schlagen deshalb vor, Big Data als ein kulturelles, technisches und wissenschaftliches Phänomen zu verstehen, das die Maximierung von Algorithmen und Rechenkapazität, aber eben auch den Glauben an gesellschaftliche Erkenntnisfortschritte durch große Datensätze, die „Aura von Wahrheit, Objektivität und Genauig-

3 Die jüngste Studie des Unternehmens IDC (2011) geht von einer Verdopplung aller gespeicherten Daten alle zwei Jahre aus, in: http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf.

4 IDC 2010 „Digital Universe Study", in: http://gigaom.files.wordpress.com/2010/05/2010-digital-universe-iview_5-4-10.pdf.

keit" umfasst[5]. Big Data, so die Autorinnen, evoziert utopische wie auch dystopische Rhetorik, löst gleichermaßen Hoffnungen auf gesellschaftlichen Fortschritt als auch Ängste vor Überwachung aus.

Die Definition von Big Data als Amalgam aus Rechenverfahren, Rechnerleistung und der – positiven wie negativen – Beschwörung von Informationsmacht ist deshalb so treffend, weil sie mit dem Finger auf die gesellschaftliche Dimension zeigt: Der Erfolg von Big Data beruht darauf, dass die digitale Gesellschaft nicht nur in wachsendem Umfang Daten produziert, konsumiert und Dritten zur Verfügung stellt, sondern den daraus generierten Informationen auch traut und einen Wert zuschreibt. Immerhin 75 % der Daten des „digital universe" werden von Individuen erzeugt. Big Data muss somit als ein ko-produziertes Phänomen verstanden werden. Das heißt, die individuellen Nutzerinnern sind aktive Kollaborateure der Datenökonomie.

Ein gutes Beispiel für das Zusammenspiel zwischen Nutzern und Unternehmen in der Produktion von Big Data ist die Arbeitsweise von Siri. Bei Siri handelt es sich, iPhone Nutzerinnen wissen das, um einen sogenannten persönlichen Assistenten, mit dem man in natürlicher Sprache kommunizieren kann. Zumindest in der Theorie beantwortet Siri alltägliche Fragen wie etwa die, ob es heute noch regnet, wo die nächste Bushaltestelle ist oder ob das Essen beim Italiener um die Ecke empfehlenswert ist. Siri soll aber auch auf komplexere Anforderungen bewältigen wie etwa auf Zuruf zu Hause anzurufen, wenn ich gelandet bin oder das Büro verlasse. Wie bewerkstelligt Siri solche Aufgaben?

Es wird niemanden überraschen, dass Siris Kompetenz mit dem Detailwissen über unsere Lebensumstände steigt. Um uns kennenzulernen, kopiert Siri zunächst einmal unserer Onlinekonten und Kontaktlisten, um unsere individuellen Beziehungsnetzwerke zu erschließen. Zusätzlich ermittelt Siri Standortdaten und verfügbare Informationen über unseren Musik-, Film- und Literaturgeschmack. Diese Kontextinformationen wandern in die Cloud, in der die eigentliche Spracherkennung stattfindet. Auch die Aufzeichnungen unsere Verständigung mit Siri werden auf Apples Servern abgelegt und unter anderem zur Verbesserung seiner Algorithmen genutzt. Ähnlich wie die Bild- bzw. Gesichtserkennung von Facebook erzeugt auch Siri biometrische Daten, die eine Identifizierung der Nutzer ermöglichen und somit zur Profilbildung bei-

5 *Boyd, Danah/Crawford, Kate* 2012: Critical Questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon, in: Information, Communication & Society; 1-18

tragen. Experten zufolge ist in der kommenden Zeit mit einer Ausbreitung von Spracherkennungsverfahren und folglich einer Zunahme von biometrischen Daten in privaten Händen zu rechnen.[6]

In den USA hat sich um das Phänomen Big Data herum eine innovative Start-Up Szene gebildet, die, begünstigt durch ein schwaches Datenschutzrecht, mit der Kommerzialisierung der Datenflut experimentiert. So sind neben Facebook inzwischen viele weitere Plattformen entstanden, die ihre Mitglieder dazu animieren, persönliche Informationen mit Dritten teilen – wohlwissend, dass diese kommerziell verwendet werden. Augenfällig ist dieser Trend ausgerechnet im Gesundheitsbereich wo besonders sensible Daten anfallen. In Foren wie patientslikeme.com oder curetogether.com teilen Nutzer ihre Krankengeschichten, tauschen ihre Erfahrungen mit Therapieformen aus und beteiligen sich an Wirkungsstudien über neue Medikamente. Sie tun dies in dem Wissen, dass ihre Daten an die Pharmaindustrie weitergegeben werden. Big Data verbindet sich hier offenbar mit einem Trend zur partizipatorischen Gesundheitsversorgung, der eine stärkere Selbstbestimmung des wohl informierten Individuums und womöglich eine größere Kontrolle über die eigene Zukunft verheißt.[7] Auch die teils öffentlich betriebene Selbstoptimierung unter dem Begriff „quantified self" geht in diese Richtung.[8]

Über weitere Motive für diese selbst-entblößende Vergemeinschaftung kann man nur spekulieren. In jedem Fall haftet der Nutzung von Informationsdiensten und der damit verbundenen Preisgabe persönlicher Daten etwas Verführerisches an, weshalb Datenschutzbedenken häufig in den Wind geschlagen werden. Auffällig ist die große Bereitschaft, persönliche Daten als „Währung" einzusetzen – und das selbst in Ländern wie Deutschland, die über eine vergleichsweise ausgeprägte Datenschutztradition verfügen. Aus diesem Grunde greift es womöglich zu kurz, Internetnutzerinnen bloß als Opfer von Big Data anzusehen. In vielen Situationen, in denen Daten preisgegeben werden, kann man sich auch dagegen entscheiden, das heißt die Mitgliedschaft bei Facebook beenden, den Ortungsdienst des Smartphones deaktivieren oder auf mobile Anwendungen ganz verzichten. Insofern erscheint es angemessener, von einer Doppelrolle der Nutzerinnen auszugehen: Wir sind Opfer, aber zugleich auch Koproduzentinnen der neuen Datenökonomie; wir

6 *Talbot, David* 2012: Siris großer Bruder, Technology Review, in: http://www.heise.de/tr/artikel/Siris-grosser-Bruder-1635042.html; 5.12.2012.

7 *Bollier, D.* 2010: The Promise and Peril of Big Data. A. Institute. Washington D.C., Aspen; 26.

8 *Dahm, Georg* 2012: Ich möchte Zahlen, Business Punk, 1.

sind zwar im Prinzip für einen strengen Datenschutz, aber in der Praxis finden wir ihn dann doch oft lästig. Es steht zu wünschen, dass die künftigen Datenschutzregelungen dieser widersprüchlichen Situation Rechnung tragen, indem sie die Rechte der Bürger an ihren Daten stärken und ein (allerdings schwer umzusetzendes) Recht auf Vergessen schaffen.

Dieser Beitrag erschien zuerst im Heft Böll, Thema 2/2012: Digitale Demokratie am 12. September 2012.

Demokratie

Die Reform des europäischen Datenschutzrechts

Jan Philipp Albrecht, MdEP

Im Januar 2012 hat die EU-Kommissarin für Grundrechte und Justiz die lang erwartete Reform des Datenschutzrechts in Europa auf den Tisch gelegt. Das gesamte Jahr über wurde lebhaft über die Reformvorschläge – insbesondere die neue EU-Datenschutzgrundverordnung – diskutiert. Der zuständige Berichterstatter des Europäischen Parlaments ist der Grünen-Europaabgeordnete Jan Philipp Albrecht. Am 10. Januar 2013 wird er dem Innenausschuss seine Änderungen vorlegen und im Frühjahr mit dem Ministerrat verhandeln. Vor den Wahlen zum Europäischen Parlament 2014 sollen die neuen Datenschutzregeln unter Dach und Fach sein.

Datenschutz wird wichtiger, nicht unwichtiger

Eine Reform des EU-Datenschutzrechts: Das klingt nach Paragrafenreiten grauer Männer aus einer anderen Zeit. Bunt und einfach umarmt uns dagegen unsere digitalisierte Welt: „Ah, der Zug hat Verspätung, gut zu wissen.“, „Cool, Anna hat ein Bild aus New York gepostet.“, „Wow, ich kann hier einfach mit meinem Smartphone bezahlen.“ Datenschutz allein den grauen Männern zu überlassen, ist allerdings naiv. So wie wir versuchen, den CO2-Ausstoß von Kraftwerken und gefährliche Spekulationen an den Finanzmärkten einzudämmen, müssen wir für eine lebenswertere Welt auch die Verbreitung unserer Daten kontrollieren. Die derzeit diskutierte Reform des EU-Datenschutzrechts bietet die Chance dazu.

Unsere digitale Umwelt funktioniert weitestgehend privatisiert – mit allen dazugehörigen Vor- und Nachteilen. Mit den vielen hilfreichen Innovationen geht eine schwer durchschaubare und risikoreiche Ansammlung von Daten einher. Daten sind dabei nicht nur das Abfallprodukt nützlicher Anwendungen, die wir in Anspruch nehmen. Im Gegenteil: Ihr Weiterverkauf bildet immer öfter die Gewinnmarge der Unternehmen. Der Marktlogik folgend, braucht es für mehr Gewinn also immer mehr Daten. Jüngst erregte der Mobilfunkanbieter O2 Aufsehen mit dem Vorstoß, die Standortdaten seiner KundInnen in Verbindung mit persönlichen Daten an Gewerbetreibende zu verkaufen, etwa um feststellen, wie lange und wie oft Kunde X vor welchen

Schaufenstern verweilt. Das bedeutet nichts anderes als eine private Vorratsdatenspeicherung. Doch solche Datensammlungen wecken nicht nur kommerzielle Begehrlichkeiten: Noch nie wurde Google aufgefordert, so viele NutzerInnendaten an staatliche Behörden auszuhändigen wie im Jahr 2012. Das größere Problem hinter all diesen Phänomen: Auf Basis unserer persönlichen Informationen wird definiert, wer wir sind. So kann sich ohne unser Wissen entscheiden, ob wir kreditwürdig sind, wie viel wir für unsere Versicherung bezahlen, welche Nachrichten wir zu lesen kriegen oder ob wir einen Job bekommen. Zudem ist Datenschutz Grundlage demokratischen Zusammenlebens. Wie das Bundesverfassungsgericht im berühmten Volkszählungsurteil hervorhob, werden Menschen, die sich beobachtet fühlen, ihr Verhalten anpassen. Die freie Meinungsäußerung, elementare Grundlage demokratischen Miteinanders, wird so beeinträchtigt. Wegen dieser vielfach schon Realität gewordenen Gefahren auf die Vorteile der Digitalisierung zu verzichten, wäre dumm. Der einzige Weg aus diesem Dilemma: Wir müssen wieder Souverän über unsere Daten werden. Der Schutz personenbezogener Daten wurde nicht umsonst in der EU-Grundrechtecharta verankert.

Die bestehenden Gesetze zum Datenschutz sind unzureichend. Unternehmen müssen sich kaum für ihren Umgang mit persönlichen Daten verantworten, geschweige denn Konsequenzen befürchten. Sie preschen selbstbewusst mit neuen Funktionen ihrer Produkte, die noch mehr Daten in neuen Kontexten verarbeiten, auf den Markt. Wer sowieso NutzerIn ihrer Angebote ist, hat oft keine Wahl. Wer will schon seinen jahrelang genutzten Google Mail-Account aufgeben, weil er oder sie nicht mit einem neuen „Feature“, wie der Verknüpfung von Sucheingaben und E-Mail-Nutzungsdaten zur „Optimierung der Suchergebnisse“, einverstanden ist?

Die derzeit geltende Rechtsgrundlage in Europa ist die europäische Datenschutzrichtlinie von 1995. Ein Update ist also mehr als überfällig. Im Januar 2012 hat die Europäische Kommission einen Vorschlag für ein solches Update vorgelegt. Dem Gesetzgebungsverfahren der EU folgend, wird der Entwurf für die EU-Datenschutz-Grundverordnung derzeit im Europäischen Parlament und im Rat der Europäischen Union diskutiert, überarbeitet und erweitert. Als Berichterstatter für das Europäischen Parlaments bin ich einer der Abgeordneten mit dem größten Einfluss auf die Verordnung. Der Vorschlag der Kommission ist für mich grundsätzlich eine gute Grundlage. Er zielt auf hohe, stärker harmonisierte und dem Internetzeitalter angemessene Daten-

schutzstandards unter Beibehaltung der an sich sinnvollen Prinzipien der 1995er-Richtlinie: Datensparsamkeit, Einwilligung durch die NutzerInnen, die Zweckbindung der erhobenen Daten und ein Recht auf Auskunft. Aus bürgerrechtlicher Perspektive geht es jetzt vor allem darum, Ausnahmeregeln zu begrenzen und die guten Ideen zu konkretisieren.

Es lohnt, die EU-Datenschutzreform mitzugestalten

An erster Stelle ist die Änderung der Rechtsform im Kommissions-Vorschlag hervorzuheben: Von der Richtlinie zur Verordnung. Das bedeutet praktisch, dass nach der Reform in jedem EU-Mitgliedstaat die gleichen Datenschutzstandards gelten müssen. Derzeit erlassen die 27 Mitgliedstaaten ihre eigenen Gesetze anhand der Datenschutz-Richtlinie von 1995. Die unterschiedliche Umsetzung dessen hat zu einem ungleichmäßigen Datenschutzniveau in der EU geführt. Vorteil der geplanten Verordnung: Unternehmen können sich nicht mehr das Land mit den niedrigsten Datenschutzstandards als Firmensitz aussuchen. Nicht umsonst hat Facebook seinen europäischen Firmensitz in Irland, wo ein vergleichsweise schwaches Datenschutzniveau vorherrscht. Doch auch der Rückzug aus Europa hilft den Firmen nicht: Der Reformvorschlag sieht vor, dass europäische Datenschutzstandards gelten, sobald Daten von EuropäerInnen verarbeitet werden – unabhängig vom Sitz des Unternehmens. Umso wichtiger ist es daher für uns, möglichst hohe und klar definierte Datenschutzstandards im Reformvorschlag festzuschreiben.

Datenschutz beginnt vor der Nutzung eines Dienstes. NutzerInnen müssen laut Reformvorschlag eindeutig darüber informiert werden, was mit ihren Daten geschieht, um dann bewusst einzuwilligen. Aber Hand aufs Herz: Wer hat die seitenlangen allgemeinen Geschäftsbedingungen der von ihm oder ihr genutzten Internetdienste wirklich gelesen? Es braucht daher einfach und schnell verständliche Nutzungsbedingungen in Form von standardisierten Symbolen, wie wir sie etwa bei Lebensmitteln kennen. Das Prinzip der expliziten Einwilligung sollte zudem technisch gestärkt werden: Wenn ich durch die Privatsphäre-Einstellungen meines Internetbrowsers signalisiere, dass ich dem Erstellen von Nutzungsprofilen anhand meines Surfverhaltens nicht zustimme, sollen Diensteanbieter das respektieren. Eine Möglichkeit hierfür böte die sogenannte Do Not Track-Funktion, die in gängigen Browsern bereits installiert ist. Der Gesetzesvorschlag sollte ein Anreiz für Internetdienstleister sein, bei solchen Maßnahmen mitzuwirken.

Auch auf Unternehmensseite beginnt Datenschutz vor dem Anbieten eines Dienstes. Der Reform-Vorschlag verpflichtet Unternehmen, ihre Angebote möglichst datensparsam zu konzipieren und mit den datenschutzfreundlichsten Voreinstellungen anzubieten. Facebook verfährt beispielsweise derzeit genau anders herum: Wenn ich einen Account eröffne, sind die Privatsphäre-Einstellungen am niedrigsten. Beim datenschutzfreundlichen Design wollen wir das Prinzip der Zweckbindung stärken. Das heißt: Welche Daten sind für die Nutzung des Dienstes wirklich nötig? Und: Braucht es immer meine eindeutige Identifizierung? Diese Fragen sollen sich Diensteanbieter im Vorfeld stellen. Viele Angebote funktionieren auch mit anonymer oder pseudonymer Nutzung. Ob meine Freundin unter vollem Namen oder als „spacecommander86" mit mir chattet, beeinträchtigt unsere Kommunikation in keinster Weise.

Sind unsere Daten einmal in der Welt, gilt es, die Kontrolle über sie zu behalten. Daher müssen Speicherfristen klar definiert werden und Daten, wenn der Zweck der Verarbeitung erfüllt wurde, auch wieder gelöscht werden. Das im Reformvorschlag gestärkte Recht auf Löschung und Korrektur meiner Daten muss einfach wahrnehmbar sein. Dazu sollten mit der Verordnung Auskunftsrechte gegenüber den Anbietern gestärkt werden. In verständlicher Sprache, kostenfrei und möglichst schnell soll mir mitgeteilt werden, wer was mit welchen Daten von mir macht. Neu ist dabei das Recht auf Datenportabilität: Auf Anfrage sollen mir Diensteanbieter meine bei ihnen gespeicherten Daten in einem maschinenlesbaren Format, das heißt digital und nicht auf hunderten Seiten Papier, aushändigen. Damit könnte ich dann zum datenschutzfreundlicheren Konkurrenzanbieter wechseln oder meine Daten visualisieren lassen, wie es der Grüne Malte Spitz jüngst vorgemacht und damit die Ausmaße der über ihn gespeicherten Daten veranschaulicht hat. Was Malte Spitz nur als Mammutprojekt mit professioneller Hilfe realisieren konnte, sollte für uns alle möglich werden. So können wir in Zukunft besser vergleichen, wo unsere Daten wirklich gut aufgehoben sind.

Eine weitere Neuerung im Reformvorschlag ist das „Recht auf Vergessenwerden". Dieses Recht kann ein weiterer Schutzmechanismus gegen den Missbrauch persönlicher Informationen sein, wenn es richtig ausgestaltet ist. Es geht nicht um technische Verfallsdaten, sondern um einen rechtlichen Anspruch auf Durchsetzung des Löschungsersuchens. Der Anbieter, der ohne meine Einwilligung Daten von mir erhoben, weitergegeben oder veröffent-

licht hat, soll sich auch bemühen, dass Dritte einem Korrektur- oder Löschungsanspruch meinerseits nachkommen. Wessen persönliche Informationen im Jugendalter unrechtmäßig durch ein soziales Netzwerk an Dritte gegeben wurden, ist zehn Jahre später mit Recht daran interessiert, dass davon nicht mehr ihre oder seine Chancen auf einen Hauskredit oder Job abhängen. Dies gilt natürlich nicht im Kontext öffentlichen Interesses oder der Informations- und Meinungsfreiheit. PolitikerInnen etwa soll damit keine Hintertür zur Verhinderung unliebsamer Berichterstattung geöffnet werden. Das sollte im Reformvorschlag noch einmal klargestellt werden. Es geht darum, die Folgen unrechtmäßiger Daten(weiter)verarbeitung abzumildern und nicht darum, die Meinungsfreiheit einzuschränken.

Damit die Datenschutz-Grundverordnung kein zahnloser Tiger bleibt, zielt der Verordnungsvorschlag vor allem auf eine verbesserte Durchsetzung des Datenschutzrechts. Dazu sollen zunächst die Datenschutzbehörden gestärkt werden. Datenschutzwer? Nur ein Drittel der EuropäerInnen kennt die eigenen nationalen Datenschutzbehörden. Sie sind normalerweise zur Kontrolle und Durchführung der Datenschutzstandards zuständig. Bislang endet ihr Tätigkeitsbereich an den Ländergrenzen der Mitgliedstaaten. Der Jurastudent Max Schrems, der Facebook wegen seiner unzulässigen Datenschutzpraktiken verklagt hat, musste dies über den Umweg der irischen Datenschutzbehörde tun. Der Reformvorschlag soll deshalb die Zusammenarbeit zwischen den nationalen Datenschutzbehörden verbessern, so dass immer meine nationale Datenschutzbehörde, die meine Landessprache spricht, auch meine Ansprechpartnerin ist. Dazu müssen die Datenschutzbehörden vor allem besser ausgestattet werden. Zudem fordert der Reformvorschlag finanzielle Sanktionen in Höhe von 2 % des Jahresumsatzes der Unternehmen. Sanktionen in dieser Größenordnung können wehtun. Zum Vergleich: Der Lebensmittelkonzern musste wegen Datenschutzvergehen zuletzt 1,5 Millionen Euro Strafe zahlen. Lidl hat einen Jahresumsatz von 30,85 Milliarden Euro. Bei Anwendung des Verordnungsvorschlags müssten sie nun 617 Millionen Euro zahlen. Das wäre der 411fache Strafbetrag.

Die neue EU-Datenschutz-Grundverordnung bringt vor allem ein Mehr an Transparenz und Kontrolle. Das Ungleichgewicht zwischen multinationalen Konzernen und uns als NutzerInnen kann damit wieder in die Waage gebracht werden.

Das Jahr 2013 wird das Datenschutzjahr in der EU

Nachdem die Europäische Kommission den Vorschlag für eine Datenschutz-Grundverordnung im Januar 2012 vorgestellt hat, wird dieser nun im Europäischen Parlament sowie im Rat der Europäischen Union diskutiert und überarbeitet. Danach diskutieren die drei Institutionen miteinander und versuchen zu einer Einigung und damit zu einem fertigen Gesetz zu kommen, mit dem alle Beteiligten leben können. Voraussetzung dafür ist, dass die Institutionen jeweils eine Meinung samt Änderungsvorschlägen zum Gesetzesvorschlag haben. Für das Europäische Parlament mit seinen über 700 Abgeordneten ist das naturgemäß am schwierigsten.

Im Parlament ist der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) federführend. Diesem Ausschuss lege ich als Berichterstatter meinen Bericht vor, der meine gesammelten Änderungswünsche am Kommissionsvorschlag enthält. Dieser Bericht soll nun am 10. Januar 2013 vorgestellt werden. Danach können andere Abgeordnete des LIBE-Ausschusses ihre Änderungswünsche am Kommissionsvorschlag anbringen. Doch nicht nur der LIBE-Ausschuss diskutiert die Datenschutz-Grundverordnung. Auch andere Ausschüsse wie der Ausschuss für Beschäftigung und soziale Angelegenheiten (EMPL) befassen sich mit dem Entwurf, etwa in Fragen des ArbeitnehmerInnen-Datenschutzes. Die Meinungen der beteiligten Ausschüsse werden im federführenden LIBE-Ausschuss berücksichtigt. Es folgt die finale Abstimmung im LIBE-Ausschuss. Hier werden alle vorgebrachten Änderungsvorschläge am Kommissions-Vorschlag abgestimmt. Als Berichterstatter kommt mir im Vorfeld der Abstimmung die Rolle der Kompromissfindung zu. Fraktionsübergreifend muss der Ausschuss, stellvertretend für das gesamte Parlament, hier zu seiner Position zum Kommissions-Entwurf kommen. Das Ergebnis der abschließenden Abstimmung im LIBE-Ausschuss ist dann das Verhandlungsmandat, mit dem das Parlament in die Verhandlungen mit dem Ministerrat tritt.

Das Europäische Parlament ist sich in Sachen Datenschutz-Grundverordnung relativ einig. Es begrüßt den Kommissions-Vorschlag und drängt zusammen mit der Kommission auf eine schnelle Verabschiedung des Vorschlags mit einigen Konkretisierungen. Ziel ist eine Einigung noch innerhalb der Legislaturperiode, also bis 2014. Anders verhält es sich im Rat. Einige Mitgliedstaaten sind dem Kommissions-Vorschlag zur Datenschutz-Grundverordnung abgeneigt und versuchen das Verfahren zu verzögern. Besonders

das deutsche Innenministerium erregte jüngst Aufsehen mit seiner Kritik am Verordnungsvorschlag. Die Kritik des Innenministeriums wirkt dabei eher wirtschaftsfreundlich. Immer öfter ist das Wort „Selbstregulierung" aus Berlin zu hören. Das bedeutet im Klartext, dass Firmen sich unverbindlichen Regeln verschreiben und der Gesetzgeber sich weitestgehend heraushält. An der Fähigkeit zur Selbstregulierung von Firmen wie Facebook ist zu zweifeln. Ausgerechnet der deutsche Innenminister Hans Peter Friedrich (CSU) versprach im Jahr 2011 „mittelfristig einen allgemeinen Kodex für soziale Netzwerke zu schaffen". Das Ergebnis bleibt er uns bis heute schuldig.

Das Stichwort Wirtschaft ist schon gefallen. Nicht nur das deutsche Innenministerium, auch die Abgeordneten des Europäischen Parlaments stehen derzeit unter massivem Lobbydruck. Viele Unternehmen fürchten um ihre Geschäftsgrundlage. Eine bürgerrechtsfreundliche Datenschutz-Grundverordnung beeinträchtigt fragwürdige Geschäftsmodelle, die persönliche Informationen aus unterschiedlichen Kontexten zusammenführen, Personenprofile erstellen und diese weiterverkaufen. In Unternehmenskreisen wird dabei wird oft vergessen, dass die Reform für die Unternehmen auch Erleichterungen mit sich bringt. Gerade multinational agierende Firmen müssen sich nicht mehr auf 27 unterschiedliche Datenschutzgesetze, sondern nur noch ein europäisches Datenschutzgesetz einstellen. Die liberale Forderung nach weniger Bürokratie wird so Wirklichkeit. Zudem bietet eine Reform des europäischen Datenschutzes auch die Chance, eine neue digitale Ökonomie zu schaffen, die nachhaltig mit persönlichen Daten umgeht und genau dies zu ihrem Gütesiegel macht. Doch um einen hohen Datenschutzstandard auf europäischer Ebene in diesem Sinne zur Realität werden zu lassen, gilt es, im Jahr 2013 mit breiter Front für eine möglichst gute und starke EU-Verordnung einzutreten. Dafür braucht es die Unterstützung all jener, die den Datenschutz als Grundrecht und grundlegendes Verbraucherrecht bewahren wollen.

Petitionen 2012: Zwischen Stimmungsbild und Willensbekundung

Kilian Froitzhuber

In der Einführung in das Petitionsrecht auf den Seiten des Bundestags wird die Geschichte der Petition mit der Untertanenbitte unter Caesar begonnen und mit der Einführung der ePetition im Jahr 2005 abgeschlossen.[1] Doch auch 2012 wurde sie fortgeschrieben. Ein Rückblick auf Verbesserungen, Enttäuschungen und Erfolge.

1. Veränderungen im Petitionsrecht des deutschen Bundestags

War 2012 für das Partizipationsinstrument Petition ein gutes Jahr? Schwer zu sagen. Es begann auf jeden Fall gut: Die Regelungen für ePetionenen beim Deutschen Bundestag wurden zum 1. Januar 2012 übersichtlicher. Zuvor hatten zwei unterschiedliche Fristen für Verwirrung gesorgt: Eine Drei-Wochen-Frist, die bei Erreichen von 50.000 Signaturen verbindlich zu einer öffentlichen Sitzung mit der Petentin führte, und eine Sechs-Wochen-Frist, bei der man in der zweiten Hälfte die Möglichkeit hatte, den Zähler zu erhöhen ohne dass damit irgendein Mechanismus verbunden gewesen wäre. Ersetzt wurde diese Regelung von einer Vier-Wochen-Frist. Innerhalb dieser Zeit sammelt man im besten Fall mindestens 50.000 Stimmen und bekommt dafür wie gehabt eine öffentliche Sitzung im Petitionsausschuss. Die zweite größere Neuerung wurde im September des Jahres eingeführt: Die Möglichkeit, pseudonym gegenüber der Öffentlichkeit zu zeichnen.

2. Netzpolitik-Petitionen

Jede Menge Petitionsverfahren mit Netzpolitik-Bezug wurden im Verlauf des Jahres beendet. Das ist jedes mal schön, weil dabei eine mal mehr, mal weniger ausführliche Begründung für die Bestätigung oder Ablehnung des Anliegens gegeben wird.

1 Vgl.: http://www.bundestag.de/bundestag/ausschuesse17/a02/petitionsrecht_einfuehrung.html

Der Abschluss des Verfahrens ist allerdings keine sonderlich öffentlichkeitswirksame Aktion. So wurde beispielsweise am 8. November 2012 Franziska Heines Internetsperren-Petition abschließend beraten, mit dem Ergebnis, dass der Petentin zuzustimmen sei. Zweieinhalb Jahre nach der öffentlichen Anhörung und ein Jahr nach Aufhebung des Zugangserschwerungsgesetzes heißt es in der Begründung des Petitionsausschusses:

> *Dem Anliegen der Petition ist damit entsprochen wurden [sic!]. Der Petitionsausschuss empfiehlt daher, das Petitionsverfahren abzuschließen, weil dem Anliegen entsprochen werden konnte.*[2]

Dass das niemanden mehr interessiert hat ist also durchaus verständlich, der politische Prozess und der öffentliche Diskurs waren zu diesem Zeitpunkt schon längst abgeschlossen.

Diverse weitere Petitionsverfahren, die teilweise schon vor mehreren Jahren begonnen worden waren, fanden in den letzten 12 Monaten ihren offiziellen Abschluss, ohne dass ihnen während der Zeichnungsfrist oder anschließend besondere mediale Aufmerksamkeit zuteil geworden wäre und ohne dass sie jemals in die Nähe von 50.000 Unterschriften gekommen wären. Unter den für den netzpolitischen Diskurs interessanten Fällen findet man unter anderem diese:

Einer Petition, die den Verkauf von E-Mail-Adressen verbieten lassen wollte, wurde teilweise entsprochen, weil die geltende Rechtslage ohnehin schon sachgerecht sei.[3]

Einem Petenten, der forderte, dass zum Schutz vor Trojanern und Keyloggern nur Personalausweis-Lesegeräte mit Tastatur zum Einsatz kommen sollten, wurde nicht entsprochen, weil das Bundesamt für Sicherheit in der Informationstechnik (BSI) anderer Meinung war.[4]

Ein Transparenzgebot im Grundgesetz wurde als überflüssig angesehen, da der bestehende Rechtsrahmen ohnehin schon für Transparenz sorge.[5]

---

2 Abschlussbegründung, in: https://epetitionen.bundestag.de/petitionen/_2009/_04/_22/Petition_3860.abschlussbegruendungpdf.pdf.

3 Vgl.: https://epetitionen.bundestag.de/petitionen/_2010/_03/_28/Petition_11083.abschlussbegruendungpdf.pdf.

4 Vgl.: https://epetitionen.bundestag.de/petitionen/_2010/_08/_24/Petition_13675.abschlussbegruendungpdf.pdf.

Eben sowenig braucht es laut Petitionsausschuss im Grundgesetz ein ausdrückliches Grundrecht auf Datenschutz und informationelle Selbstbestimmung, da das Grundgesetz „darunter leiden könnte, wenn bereits geltendes materielles Verfassungsrecht nochmals ausdrücklich in den Verfassungstext aufgenommen wird. Zudem würde mit der Schaffung eines Grundrechts auf Datenschutz nur ein Teilbereich des allgemeinen Persönlichkeitsrechts ausdrücklich hervorgehoben, während andere ähnlich gewichtige Inhalte unerwähnt blieben."[6]

Eine verbindliche Kennzeichnung urheberrechtlich geschützter Inhalte im Internet wurde abgelehnt, da das Fehlen einer verbindlichen Kennzeichnung sachgerecht sei. Ebenso brauche es keinen Copyleft-Vermerk, da es dafür bereits Creative Commons gebe.[7]

Netzneutralität sei tatsächlich ein wichtiges Thema, und dank Breitbandausbau, einem funktionierenden Markt und bereits bestehender Interventionsmöglichkeiten der Bundesregierung bei Verstößen auf einem guten Weg.[8]

Der Vorschlag einer gesetzlichen Pflicht zur Verschlüsselung von Passwörtern und Mindeststandards bezüglich erlaubter Maximalpasswortlänge und Erlaubnis der Sonderzeichenverwendung wurde als nicht zielführend bewertet, da das Internet schnelllebig sei und die vorgeschlagene Lösung nicht für alle Anwendungsbeispiele sinnvoll sei.[9]

Die Einführung von Regelungen zur Löschung von Benutzerdaten im Todesfall wurde abgelehnt, da das Prinzip der Gesamtrechtsnachfolge aus dem Erbrecht auch hier gelte.[10]

---

5 Vgl.: https://epetitionen.bundestag.de/petitionen/_2010/_10/_30/Petition_14787.abschlussbegruendungpdf.pdf.

6 https://epetitionen.bundestag.de/petitionen/_2010/_02/_05/Petition_9889.abschlussbegruendungpdf.pdf.

7 Vgl.: https://epetitionen.bundestag.de/petitionen/_2011/_02/_07/Petition_16438.abschlussbegruendungpdf.pdf

8 Vgl.: https://epetitionen.bundestag.de/petitionen/_2010/_08/_11/Petition_13511.abschlussbegruendungpdf.pdf

9 https://epetitionen.bundestag.de/petitionen/_2011/_04/_29/Petition_17870.abschlussbegruendungpdf.pdf

10 https://epetitionen.bundestag.de/petitionen/_2010/_12/_27/Petition_15914.abschlussbegruendungpdf.pdf

RFID-Chips müssen laut Petitionsausschuss nicht verboten werden, weil sie laut BSI und „Wissenschaftlern aus Hochschulen" sicher seien.[11]

Man erkennt ein Muster: Es handelt sich in der Regel um die Feststellung, dass der Status quo ganz in Ordnung sei. Sogar die Weiterleitung des Anliegens an zuständige Stellen zwecks Kenntnisnahme und weiterer Beschäftigung wird, obwohl (oder auch weil) von Oppositionsparteien des Öfteren vorgeschlagen, nur in absoluten Ausnahmefällen durchgeführt.

Bei einigen anderen, deutlich häufiger signierten Petitionen wird es noch ein bisschen dauern, bis das Abschlussdokument den Weg in das Parlamentsdokumentensystem finden wird. So wurde, mehr als ein Jahr nach Erreichen des Quorums, die öffentliche Anhörung zur von über 60.000 Personen unterstützten Petition gegen die anlasslose Vorratsdatenspeicherung, im Oktober abgehalten.[12] Zu diesem Thema wurde das Mittel der Petition auch in anderen Ländern genutzt und fand breiten Anklang: Auch in Großbritannien und Österreich können viele Menschen nicht nachvollziehen, warum sie unter Generalverdacht stehen, entsprechende Petitionen hatten extreme Signaturzahlen. Während die Ausschuss-Sitzungen im deutschen Bundestag vergleichsweise ausführlich sind, ist das in Österreich eher nicht der Fall, wie Andreas Krisch, Obmann des AK Vorrat ausführte: „Im Schnitt stehen dem Ausschuss dafür durchschnittlich 4,6 Minuten zur Verfügung."[13] Da kann man in Deutschland ja froh sein, im Petitionsausschuss auch mal ausreden zu können.

Schneller als bei der Vorratsdatenspeicherung ging der Prozess zur ACTA-Petition: Im März gestartet, über 60.000 Unterschriften gesammelt und im Mai schon verhandelt. Der überzeugende Auftritt von Petent Herbert Bredthauer vor dem Petitionsausschuss war ein weiterer Sargnagel für den Versuch, mit ACTA das in der bestehenden Form nicht mehr zeitgemäße Urheberrecht durch ein internationales Handelsabkommen zu zementieren. Insgesamt ist das bestehende Urheberrecht kein Freund der direkten Bürgermit-

11 https://epetitionen.bundestag.de/petitionen/_2010/_09/_15/Petition_13968.abschlussbegruendungpdf.pdf

12 *Meister, Andre* 2012: Vorratsdatenspeicherung im Petitionsausschuss: 60.000 Menschen fordern Anschaffung der Datenspeicherung, auch auf EU-Ebene, in: https://netzpolitik.org/2012/vorratsdatenspeicherung-im-petitionsausschuss-60-000-menschen-fordern-abschaffung-der-datenspeicherung-auch-auf-eu-ebene/; 6.12.2012.

13 *Lohninger, Thomas* 2012: Themenverfehlung, setzen! Direkte Demokratie in Österreich, in: https://netzpolitik.org/2012/themenverfehlung-setzten-direkte-demokratie-in-osterreich/; 6.12.2012.

sprache: Auch die GEMA bekam auf diesem Weg einen mit; die erfolgreiche Petition zur Abschaffung der GEMA-Vermutung befindet sich seit Oktober in der Prüfung. Dabei hatte die Verwertungsgesellschaft noch Glück: Die rapide Zuwachsrate in der Verlaufskurve der Mitzeichnungszahl gegen Ende der Zeichnungsfrist hätte hochgerechnet bei einer Verlängerung der Frist um einige weitere Tage einige Millionen Stimmen bedeutet.[14] Aber die 62.842 reichen ja auch.

Nicht gereicht hat den meisten BeobachterInnen dagegen bekanntlich die Zahl 21.366. So viele Stimmen kamen gegen das Leistungsschutzrecht zusammen. Größere Teile der deutschen Blogosphäre beschimpften daraufhin das Mittel der Petition an sich als gestrig und abgenutzt. Andere wandten ein, dass die Petition vielleicht gar nicht die Ablehnung gegenüber einem Leistungsschutzrecht für Presseverlage gemessen habe, da viele potentielle UnterzeichnerInnen entweder den Text dumm fanden, mit der Nase des Petenten wenig anfangen konnten oder aus Baumschutzgründen ein Leistungsschutzrecht so lange ertragen wollten, bis die treibenden Kräfte dahinter sich tot geschützt hätten. Andre Meister schrieb damals: „Das eigentliche Ziel ist die Öffentlichkeit. Das Sichtbarmachen, dass zehntausende Menschen mit ihrem Namen für (oder gegen) ein Anliegen einstehen. Und das hat die Petition geschafft. Auch wenn noch mehr Unterschriften natürlich noch besser gewesen [wären].“[15]

3. Abseits des Bundestags

Für dieses Ziel, das Sichtbarmachen, ist es logischerweise nicht relevant, ob die Petition auf dem Server eines Parlaments gestartet wird oder auf einer unabhängigen Plattform. Einige Initiativen waren so bei der Herstellung von Öffentlichkeit überaus erfolgreich.

Die meisten und seltsamsten Petitionen dieser Art dürfte es rund um Warlord Joseph Kony gegeben haben. Wir erinnern uns: Die Organisation Invisible Children produzierte einen Film, der sich rasend schnell verbreitete und zur Folge hatte, dass Justin Bieber, Kim Kardashian und die Bewohner von Face-

14 Vgl.: https://epetitionen.bundestag.de/petitionen/_2012/_08/_28/Petition_35441.mitzeichnen.html.

15 Meister, Andre 2012: Leistungsschutzrecht: Nur weil „nur“ 20.000 Menschen dagegen unterschrieben haben, ist es immer noch nicht akzeptabel, in: https://netzpolitik.org/2012/leistungsschutzrecht-nur-weil-nur-20-000-menschen-dagegen-unterschrieben-haben-ist-es-immer-noch-nicht-akzeptabel/; 6.12.2012.

book eine militärische Intervention irgendwo in Afrika forderten, um den bösesten Menschen der Welt zu fangen. Von 3,7 Millionen gesammelten großen Indianerehrenwörtern[16] abgesehen wurde auf Plattformen wie change.org, gopetition.com, ipetitions.com, thepetitionsite.com und SignOn.org unter anderem gefordert, dass Invisible Children Joseph Kony fangen[17] und das People Magazine ihn als Coverboy verwenden[18] solle. Kanadas Premierminister Harper wurde von 4413 Personen aufgefordert, sich den Film anzuschauen[19], und auch Barack Obama wurde nochmals per Petition informiert (auch wenn diese, von Fehlinformationen abgesehen, für ihn nichts Neues geboten haben dürfte, wenn man sich beispielsweise sein Schreiben aus dem Oktober 2011 zum Thema ansieht.[20] Ärgerlicherweise macht das Petitionssystem des Weißen Hauses ältere Petitionen sowie die Reaktionen darauf übrigens unzugänglich).

Auch Facebook wurde in diesem Zusammenhang als Petitionsplattform verwendet. Die Seite „facebook.com/MakeJosephKonyFamouse" beispielsweise „is a petition demanding the goverment to do somthing about Joseph Kony [...] *each „like" counts for 1 signature so please share because you cann make a diffrence*". Immerhin 157 Personen machten mit.

Das Anliegen, Joseph Kony per Petition berühmt zu machen, war insgesamt das häufigste Motiv hinter den unzähligen Petitionen. Zumindest das hat alles in allem ja auch ganz gut geklappt, auch wenn die Halbwertzeit in der Social-Media-Bilderflut nicht allzu hoch sein dürfte.

Dass ein geschickt gemachtes Video wie im Fall Kony sich extrem auf die Aufmerksamkeit für Petitionen auswirken kann, bestätigt auch Jörg Mitzlaff, Geschäftsführer von openPetition.de: Einige der erfolgreichsten Petitionen des Portals hätten viel Zulauf von YouTube aus bekommen. Nicht immer wird auf diese Weise Sinnvolles unterstützt, wie das Anonymous-Video gegen die Hetz-Seite kreuz.net zeigte, das zur Unterzeichnung einer eher skurrilen Pe-

16 Video: 3.7 Million KONY 2012 Pledges Delivered, in: http://www.causes.com/causes/227-invisible-children/actions/1667877; 6.12.2012.

17 Vgl.: http://www.gopetition.com/petitions/capture-joseph-kony-2012.html

18 Vgl.: http://www.change.org/petitions/put-joseph-kony-on-the-cover-of-people-magazine

19 Vgl.: http://www.change.org/en-CA/petitions/canadian-prime-minister-stephen-harper-global-leaders-watch-the-kony-2012-film-created-by-invisible-children-and-say-enough

20 The White House 2011: Letter from the President, in: http://www.whitehouse.gov/the-press-office/2011/10/14/letter-president-speaker-house-representatives-and-president-pro-tempore; 6.12.2012.

tition aufrief: „Offenbar war eine starke emotionale Aufladung der Petition ein wichtiger Faktor für die vielen Unterschriften: Die Kommentare und die Debatte war extrem emotional, auch das YouTube-Video nutzte dramatische Musik und Optik. Ins Bild passt in dem Zusammenhang, dass die UnterzeichnerInnen sich offenbar nicht daran störten, dass es keine Forderung gab und die Adressaten „Regierungen Europaweit" ungeeignet waren, denn die Seite ist deutschsprachig, die Server stehen anscheinend außerhalb Europas – darauf wurde in der Debatte auch mehrfach hingewiesen. Damit ist die Petition mehr ein Stimmungsbild als eine Willensbekundung – und damit recht unpolitisch," so Mitzlaff.[21]

OpenPetition ist neben change.org die wohl wichtigste nichtstaatliche Petitionsplattform im deutschsprachigen Raum und konnte mit der Unterschriftenaktion gegen die GEMA-Tarifreform die meist-gezeichnete Petition des Jahres in Deutschland verzeichnen: Über 300.000 Personen beteiligten sich. Doch nicht nur für die großen bundesweiten, sondern auch und gerade lokale und regionale Anliegen sollen durch das Mittel der Petition vorangebracht werden. Fast 5000 BürgerInnen unterschrieben beispielsweise gegen die Abschiebung von Kenesa Guluma – der Petitionsausschuss des Bayrischen Landtags setzte daraufhin die Abschiebung aus.[22]

Die Einsatzmöglichkeiten von Petitionen sind vielschichtig. Von einzelnen enttäuschten Erwartungen sollte man sich auch 2013 nicht entmutigen lassen, wenn es darum geht, wichtigen Anliegen aus der Zivilgesellschaft heraus mehr Gewicht zu geben. Dass man sich dabei im besten Fall zusammen mit Gleichgesinnten abspricht und einen geeigneten Zeitpunkt für das Anliegen abpasst, sollte sich von selbst verstehen.

21 Andererseits: kreuz.net ist weg, mission accomplished.

22 Vgl.: https://www.openpetition.de/petition/online/bleiberecht-fuer-kenesa-abschiebung-nach-aethiopien-verhindern

Eine Chronik zum Thema Elektronische Demokratie

Christian Heise

Das Jahr 2012 ist fast vorbei und da für mich auch 2012 nur sehr wenig Zeit zum Bloggen blieb, will ich die wichtigsten Themen aus meiner Sicht mit dem Schwerpunkt auf elektronische Demokratie und elektronische Partizipation an dieser Stelle noch einmal Revue passieren lassen. Das ich mit dem Dezember 2011 beginne ist einzig und allein dem Umstand geschuldet, dass dieser Text Ende November 2012 verfasst wurde. Der Rückblick erhebt dabei weder den Anspruch auf Vollständigkeit noch auf eine rein objektive Sichtweise.

Starten wir mit dem Rückblick: Im Dezember 2011 wurde mit der Gründung des Vereins „D64" ein Think Tank für das digitale Zeitalter der Öffentlichkeit vorgestellt. Unter dem Dach vereinen sich „Menschen, die täglich mit den Möglichkeiten und Herausforderungen des Internets für die Transformation unserer Gesellschaft arbeiten".[1] Andere sehen darin eher eine „Plattform für frustrierten SPD-Nachwuchs".[2] Ähnlich wie bei der Gründung von Digitale Gesellschaft gab es zum Start einige Diskussionen rund um Lobby-/Parteiarbeit (SPD) und privates Engagement bei D64.[3]

Ebenfalls im Dezember verkündete die EU-Kommission, dass in der Öffnung und elektronischen Bereitstellung von Verwaltungsdaten in Europa ein wirtschaftliches Potenzial von 40 Milliarden Euro jährlich steckt. Außerdem kündigte die Vizepräsidentin der Europäischen Kommission und Zuständige für die digitale Agenda, Neelie Kroes, für das Frühjahr 2012 ein offenes Open Daten-Portal der EU an. Später im Jahr 2012 stellt sich heraus, dass die Plattform wohl erst Anfang 2013 bereitstehen wird.

Am 12. Dezember 2011 hat die Internet-Enquete ihren Zwischenbericht zum Thema Datenschutz beraten und beschlossen. Der Datenschutz-Zwischenbericht ist somit der fünfte Zwischenbericht der Enquete. Eine Übersicht über

1 http://d-64.org/

2 *Biermann, Kai* 2011: Die SPD bekommt netzpolitische Nachhilfe, in: http://www.zeit.de/digital/internet/2011-12/spd-thinktank-d64; 6.12.2012.

3 D64 2011: Lobbyarbeit, privates Engagement und D64, in: http://d-64.org/lobbyarbeit-privates-engagement-und-d64/; 6.12.2012.

die Berichte der Enquete findet man findet man auf der Webseite des Bundestags.[4] Mit dem fünften Bericht ging auch die Bürger-Beteiligungsplattform der Internet-Enquete online.[5]

In den USA ist die Debatte um „Stop Online Piracy Act" (SOPA) und Protect IP Act (PIPA) im Dezember 2011 voll im Gange. SOPA sollte die juristische Grundlage dafür liefern, dass Rechteinhaber „problematische" Seiten umstandslos aus dem Netz hätten filtern und entfernen können. Mit den beiden Gesetzen sollten in erster Linie die Rechte der Medienunternehmen geschützt werden. Zum Ende des Jahres verlor die Initiative jedoch viele öffentliche Befürworter und wurde zu Beginn des Jahres 2012 eingestellt. Zum Glück!

Zum Unglück beschloss daraufhin der Rat der Europäischen Union im selben Monat das zwar reichlich entschärfte, doch weiterhin sehr umstrittene Anti-Counterfeiting-Trade-Agreement (ACTA). Zu dem Zeitpunkt war dem Rat und den Initiatoren noch nicht klar, dass das Anti-Produktpiraterie-Handelsabkommen auch im darauffolgenden Jahr noch aus vielerlei Hinsicht zu einem Meilenstein der öffentlichen Debatte um Netzpolitik werden würde.

Zum Abschluss des Jahres 2011 müssen auch nochmal explizit die arabischen Revolutionen erwähnt werden, die sich wie ein roter Faden durch 2011 gezogen haben und ihre Strahlkraft auch weit in das Jahr 2012 haben werden. Über den direkten Einfluss des Internets auf die Entwicklungen kann man streiten, dennoch hat es Gero von Randow in einem kurzen Text geschafft[6], darauf angemessen einzugehen. Weitere interessante Beiträge[7][8] zum Einfluss des Internets auf die arabische Revolution werden in 2012 folgen.

Kurz vor dem Jahreswechsel verkündete der Bundestag in einer Pressmitteilung eine Änderung für die Zeichnungsfrist für Online-Petitionen beim Petitionsausschuss.[9] Mit dem 1. Januar 2012 läuft die Zeichnungsfrist nur noch vier statt bisher sechs Wochen und auch die Zeit zum Erreichen der 50.000-

4 S.: http://www.bundestag.de/internetenquete/Zwischenberichte/index.jsp

5 Enquete Beteiligung, in: https://enquetebeteiligung.de/.

6 *Von Randow, Gero* 2011: Revolution online, in: http://www.zeit.de/2011/07/P-Widerspruch; 6.12.2012.

7 Zeiton, Moez 2012: Connected Conflict, in: http://www.technologyreview.com/notebook/427707/connected-conflict/; 6.12.2012.

8 Gayo-Avello, Daniel 2012: A Balanced Survey on Election Prediction usinf Twitter Data, in: http://arxiv.org/pdf/1204.6441v1.pdf; 6.12.2012.

9 Pressemitteilung des Deutschen Bundestags, in: http://www.bundestag.de/presse/pressemitteilungen/2011/pm_1111161.html; 6.12.2012.

Mitzeichnungs-Grenze wird auf vier Wochen angepasst. Im Rahmen dieser Änderung ist ebenfalls geplant, ab Mitte des Jahres automatisch generierte Pseudonyme einzuführen.

Am 9. Januar 2012 wurde das Open Data-Portal des Bundes daten-deutschland.de gelauncht. Auf dieser Seite erfährt man, dass „Open Government als Modernisierungsprojekt" aufgenommen wurde und ein Teil der im Regierungsprogramm „Vernetzte und transparente Verwaltung" verankerten Maßnahmen ist. Eine Zeitleiste informiert den Besucher über „Statusinformationen" zur Beauftragung einer Open-Data Plattform von Bund und Ländern im Jahr 2013. Beauftragt durch das Bundesministerium des Innern und realisiert durch die Beratungsgesellschaft Capgemini, macht die Seite aber nicht viel Hoffnung auf Besserung in dem Bereich.

Über die Weihnachtsfeiertage hat Andreas Berthold vom österreichischen Umweltbundesamt aus dem Open Government Data Weißbuch eine sehr anschauliche und leicht verständliche Mindmap zum Thema Open Government und Open Data erstellt.[10]

Ein Wahlcomputer, der abstürzt und Abstimmungen falsch interpretiert ist trotz besseren Wissens für die kommende Präsidentschaftswahl in den USA zugelassen. Gleichzeitig verschrotten Irland[11] und die Stadt Dortmund[12] die Wahlcomputer der Pilotphasen. Der Ausstieg aus dem E-Voting wurde jeweils schon 2009 beschlossen.

„Umstrittenes US-Zensurgesetz wird auf Eis gelegt", betitelt heise.de Mitte Januar 2012 die Entwicklungen rund um die Debatte des Stop Online Piracy Acts (SOPA). Andere sind vorsichtiger und titeln: „#SOPA scheint erstmal tot – Gefahr bleibt".[13] Die Enzyklopädie Wikipedia und einige andere Seiten waren darauf hin aus Protest gegen SOPA und ähnliche Vorhaben am 18. Januar von 8 bis 20 Uhr nicht erreichbar. Netzpolitik.org hat dazu umfangreiche Blackout-Gallery veröffentlicht.[14]

---

10 http://cdn.open3.at/wp-content/uploads/2012/01/Mindmap_OGD_20110112.pdf

11 *Müller, Andreas* 2012: Island verschrottet seine Wahlcomputer, in: https://netzpolitik.org/2012/irland-verschrottet-seine-wahlcomputer/; 6.12.2012.

12 Volmerich, Oliver 2012: Dortmunds Wahlcomputer sind verschrottet, in: http://www.ruhrnachrichten.de/lokales/dortmund/Dortmunds-Wahlautomaten-sind-verschrottet;art930,1514838; 6.12.2012.

13 Beckedahl, Markus 2012: #SOPA scheint erstmal tot – Gefahr bleibt, in: https://netzpolitik.org/2012/sopa-scheint-erstmal-tot-gefahr-bleibt/; 6.12.2012.

14 S.: https://netzpolitik.org/2012/sopa-blackout-gallery/

Am 31.01.2012 startete die britische Regierung mit Gov.uk eine One-Stop-Lösung für Online-Informationen und Dienste rund um Staat und Verwaltung. Diese Beta-Version ist der erste Schritt hin zu einer zentralen Regierungswebseite als Anlaufpunkt für Bürger. Ziel der Nachfolgeplattform von direct.gov.uk ist es Einsparungen bei den ca. 150 Millionen Anrufen durch Briten bei öffentlichen Einrichtungen pro Jahr zu erzielen und (natürlich) dem Bürger einen besseren Service zu bieten.

Anfang Februar 2012 kündigte die Deutsche Bahn die Unterstützung des deutschen Equivalents zu FixMyStreet, Maerker Brandenburg[15], an. Die Plattform ermöglicht es Bürgern, den teilnehmenden Kommunen lokale Infrastrukturprobleme, wie zum Beispiel Schlaglöcher zu melden. Die Bahn bietet „Bürgern die Möglichkeit, über diesen direkten Draht für Probleme der Infrastruktur vor Ort auch Hinweise mit Bahn-Bezug anzumelden".[16]

Mit Offenes Köln startet ein weiteres vorbildliches Projekt, das Informationen des Kölner Ratsinformationssystems einfach und filterbar abrufbar macht. Ziel von Offenes Köln ist es, Informationen, Dokumente und Daten aus der Kölner Lokalpolitik für jedermann offen und einfach zugänglich zu machen.

Auch wenn Deutschland das Anti-Produktpiraterie-Handelsabkommen (ACTA) vorerst nicht unterschreibt, kam es Mitte Februar zu Anti-ACTA-Protesten in Deutschland: Vor allem in München, Berlin und Köln demonstrieren Zehntausende gegen das Handelsabkommen aber auch in anderen europäischen Städten gingen die Menschen gegen ACTA auf die Straße.

Am 16. Februar veröffentlichte die Berliner Senatsverwaltung für Wirtschaft, Technologie und Forschung eine Studie zur „Berliner Open Data-Strategie".[17] In den Handlungsempfehlungen werden unter anderem ein Gesamtverantwortlicher für offene Daten für Berlin sowie die Fortführung und der Ausbau des im Herbst 2011 gestarteten Datenportals daten.berlin.de gefordert.

„Würde sich die EU bei uns um Beitritt bewerben, müssten wir sagen: demokratisch ungenügend", so beschrieb der ehemalige EU-Kommissar Günther Verheugen das Thema Demokratiedefizit in der EU. Dass sich daran auch di-

15 S.: http://maerker.brandenburg.de/lis/list.php?page=maerker

16 MI Brandenburg 2012: Deutsche Bahn AG unterstützt kommunales Service-Portal „Maerker", in: http://www.mi.brandenburg.de/cms/detail.php/bb1.c.278988.de; 6.12.2012.

17 *Both, Wolfgang/Schieferdecker, Ina* (Hrsg.) 2012: Berliner Open Data Strategie, in: http://www.berlin.de/projektzukunft/fileadmin/user_upload/pdf/sonstiges/Berliner_Open_Data-Strategie_2012.pdf; 6.12.2012.

gital nichts ändert, verdeutlicht ein sehr lesenswerter Beitrag des neue Debattenportals Diskurs@Deutschlandfunk: „Von eDemocracy keine Spur. Digitale Bürgerbeteiligung ist auf europäischer Ebene nahezu unmöglich!“.[18]

Mit „Linked Open Data: The Essentials – A Quick Start Guide for Decision Makers“ ist ein sehr gutes Buch über Open Data unter Creative Commons Lizenz (CC-BY) erschienen, das Entscheidungsträgern in Unternehmen und in der Politik das Thema Linked Open Data und all seine Vorzüge näher bringen will.[19]

Ende Februar launchte die Britische Regierung den Government Cloudstore mit 1.700 öffentlichen Apps, die kleinen Unternehmen helfen sollen Software an den öffentlichen Sektor heranzutragen – ein guter erster Schritt.[20]

Laut einer im Februar veröffentlichten repräsentativen Umfrage des Arbeitskreises Open Government Partnership Deutschland (bei dem ich Mitglied bin) und TNS Emnid fordern 96 Prozent der Bürger eine weitere Öffnung von Politik und Verwaltung.[21] Die Bürger sehen dabei vor allem in allen Open Government-Bereichen (politische Transparenz, Amtsmissbrauch, Partizipation, Rechenschaftslegung und Korruptionsbekämpfung) großen Handlungsbedarf.

Als „Ersatz für die gescheiterte E-Signatur“ veröffentlichte im März 2012 das Bundesinnenministerium des Inneren einen Referentenentwurf des Gesetzes zur „Förderung der elektronischen Verwaltung“ sowie zur Änderung weiterer Vorschriften im Rahmen der Bürgerdienste.[22] So sollen Bürger und Unternehmen zukünftig einfacher und schneller mit der Verwaltung kommunizieren können. Eine persönliche oder telefonische Abwicklung soll aber weiterhin möglich bleiben.

---

18 *Fiedler, Kirsten/McNamee, Joe* 2012: Von eDemocracy keine Spur. Digitale Bürgerbeteiligung ist auf europäischer Ebene nahezu unmöglich!, in: http://diskurs.dradio.de/2012/02/17/digitale-partizipation-ist-auf-europaischer-ebene-fast-unmoglich/; 6.12.2012.

19 http://www.semantic-web.at/LOD-TheEssentials.pdf

20 gcloud.civilservice.gov.uk/cloudstore

21 Studie des Arbeitskreises Open Government Partnership Deutschland, in: http://opengovpartnership.de/2012/02/studie-des-arbeitskreises-open-government-partnership-deutschland/; 6.12.2012.

22 Klostermeier, Johannes 2012: Ersatz für gescheiterte E-Signatur, in: http://www.cio.de/public-ict/2304470/; 6.12.2012.

Nach dem Wahlsieg der Grünen im „Ländle“ versprach man im Passus „Open Data“ des Koalitionsvertrags, das „Regierungshandeln daran (zu) orientieren (und) die zugrunde liegenden Daten und Dokumente weitestmöglich öffentlich zugänglich zu machen“. Im Rahmen der CeBIT wurde daraufhin am 7. März der Prototyp des Open Data Portals Baden-Württemberg mit rund ursprünglich 73 Datensätzen gelauncht.[23]

Im Rahmen des Wettbewerbs Apps für Deutschland wurden auf der CeBIT die Preisträger ausgezeichnet. Insgesamt wurden 320 Datensätze, 112 Ideen und 77 Apps bei dem Wettbewerb eingereicht. Fazit: Die meisten der eingereichten Ideen waren auf Grund der fehlenden Bereitstellung von öffentlichen Daten noch nicht realisierbar.

Ebenfalls wurde auf der CeBIT das Geoportal.DE freigeschaltet. Dabei handelt es sich um ein Portal, auf der Geodaten der öffentlichen Hand einsehbar sind und einfach mit öffentlichen Informationen angereichert werden können. Darüber hinaus können die Daten auch direkt bestellt werden. Als Rechercheplattform ist das interessant, mehr aber auch nicht, denn um offene Geo-Daten handelt es sich hier nicht.

Trotz aller E-Government Euphorie auf der CeBIT 2012 landete Deutschland im internationalen Vergleich abgeschlagen auf dem 17. Platz (2010: Platz 15, 2008: Platz 22) in der ebenfalls im März 2012 veröffentlichten Ausgabe der „UN E-Government Survey 2012: E-Government for the People“. Ein Schelm, wer das schlechte Abschneiden Deutschlands auf den neuen Studienansatz mit Fokussierung auf den Bürger schieben möchte.

Nach der Internetkampagne der Organisation Invisible Children „Kony 2012“, die zu einer großen Mobilisierung führte, stellten sich einige die Frage, ob die Kampagne zum (Klick-)„Muster für Interessen geleitete Netzgemeinden wird, die Agenda des Politbetriebes zu diktieren“.[24] Passend dazu greift Rafael Behr das Thema in seinem im März erschienen Essay „The real opposition„[25] auf, beleuchtet aber die Frage, ob Social Media Politik beeinflusst aus einem etwas anderem Blickwinkel.

---

23 http://opendata.service-bw.de

24 Pauli, Ralf 2012: „Stop Kony“: Globale Hetzjagd oder geniales Marketing?, in: http://politik-digital.de/stop-kony-globale-netzjagd-oder-geniales-marketing/; 6.12.2012.

25 Behr, Rafael 2012: 38 Degrees – the real opposition?, in: http://www.newstatesman.com/uk-politics/2012/03/essay-digital-online-degrees; 6.12.2012.

Wieder ACTA, diesmal aber im April 2012: Die Demonstrationen der vergangenen Monate zeigen Wirkung und es war endlich eine öffentliche Debatte über Urheberrecht abzusehen. Wenn sich im Juli eine Mehrheit des Europaparlaments gegen ACTA ausspricht, ist das Abkommen endgültig vom Tisch.

Am 17. April wurde das Digital Engagement Cookbook[26] veröffentlicht. Im Gegensatz zu anderen Datenbanken über digitales Engagement geht es hierbei mehr um die Methoden als um konkrete Fallbeispiele. Über die Webseite können Methoden auf Grundlage bestimmter eigener Eingaben evaluiert, geprüft und verglichen werden.

Die niedersächsische Gemeinde Wennigsen/Deister und die Stadt Dresden wurden im April im Rahmen der Veranstaltung 15. Effizienter Staat mit dem ersten Preis für Online-Partizipation unter Verwaltungsbehörden ausgezeichnet. Der Gemeinde Wennigsen/Deister war es gelungen, 60 Prozent der Haushalte in die geplante Neugestaltung öffentlicher Bereiche eines maroden Wohnquartiers mit einzubinden. Dresden bekam den Preis für die „Dresdner Debatte" bei der sowohl Offline- als auch Online-Beteiligungsverfahren für die Umgestaltung der inneren Neustadt sowie des Neumarktes eingesetzt wurden.

„Im vergangenen Jahr wurden 3.280 Anträge auf Informationszugang gestellt. Das ist im Vergleich zum Vorjahr eine Steigerung von 110 Prozent. Noch im ersten Berichtszeitjahr 2010 verzeichneten die Bundesbehörden nur 1.557 Anträge nach dem Informationsfreiheitsgesetz", so heißt es im Tätigkeitsbericht zur Informationsfreiheit für die Jahre 2010 und 2011, der am 24.4.2012 veröffentlicht wurde.

Im Rahmen der anstehenden Landtagswahl in Niedersachsen Anfang Mai wird nicht nur der Wahl-o-Mat der Bundeszentrale für politische Bildung wiederbelebt, sondern die Landeszentrale veröffentlichte auch einen mehrteiligen und sehr sehenswerten Video-Podcast mit dem Titel „E-Demokratie: Elektronisch. Demokratisch. Gut".[27]

Der Monat Mai 2012 brachte gleich zu Beginn mit dem Handbuch Bürgerbeteiligung einen Beitrag zur Versachlichung der Partizipationsdebatte.[28]

26 http://www.digitalengagement.org

27 Landeszentrale für Politische Bildung Nordrhein-Westfalen: E-Demokratie, in: http://www.politische-bildung.nrw.de/multimedia/podcasts/00167/index.html; 6.12.2012.

28 http://demos-monitor.de/index.php/gerade-rechtzeitig-handbuch-burgerbeteiligung-erschienen/

In einer sehr prägnanten Zusammenfassung erläutert edemocracyblog.com, wie elektronische Petitionen die Zusammenarbeit von Bürgern mit dem Parlament fördern können.[29]

Vom 2. Bis 4. Mai fand in Berlin die re:publica statt. Im Rahmen der Session „Deliberation 3.0. – Das Gespenst der digitalen Demokratie geht um" und des Workshops „#Partizipation #wtf" gab es interessante Debatten über die Frage, wie „gelingende Partizipation" aussehen könnte und welche beziehungsweise wie viel Vision und Utopie in den Konzepten digitaler Demokratie steckt.

An der Donau Universität in Krems fand im Mai CeDEM 12 (International Conference for E-Democracy and Open Government) statt. In acht Tracks diskutierten E-Demokratie-Spezialisten aus Wissenschaft, Regierungen und Wirtschaft über alles rund um elektronische Demokratie und offenes Regieren.

Der Online-Wahlkampf in Frankreich war im Mai im vollen Gange, dennoch dominierte weiterhin das Fernsehen. Laut einer Studie nutzten 74 Prozent der Franzosen das Fernsehen als primäre Informationsquelle über den Wahlkampf. Mit immerhin 40 Prozent trug das Internet zwar zum Informationsfluss bei, war aber nicht „wahlentscheidend".

Am 11. Mai wird der mit 10.000 Euro dotierte Wolfgang-Heilmann Preis für humane Nutzung der Informationstechnologie 2012 an abgeordnetenwatch.de verliehen.[30] Ich finde zu recht!

Vom 22. bis 23. Mai fand in Leipzig der Kongress neue Verwaltung mit dem „Generalthema eGovernment" (http://www.neue-verwaltung.de/) statt. Bei der Veranstaltung erfolgte auch der Startschuss für die Beteiligungsplattform höchst-spannend.de von DEMOS auf der Bürger, Netzbetreiber, Naturschutzverbände, Bürgerinitiativen und Behörden zum Thema Energiewende in einen ständigen Austausch treten sollen.

---

29 http://www.edemocracyblog.com/edemocracy-blog/how-epetitions-could-improve-public-engagement-with-parliament

30 *Reyher, Martin* 2012: abgeordnetenwatch.de gewinnt Wolfgang-Heilmann-Preis für „Mehr Demokratie durch IT", in: http://blog.abgeordnetenwatch.de/2012/02/16/abgeordnetenwatch-de-gewinnt-wolfgang-heilmann-preis-2012-fur-mehr-demokratie-durch-it/; 6.12.2012.

Das britische Petitionssystem bekommt eine API43, über die umfangreiche Analysen der Daten im Petitionssystem gemacht werde können. Zum Vergleich: In Deutschland gibt es gerade einmal einen RSS-Feed der neusten Petitionen, sowie Feeds für den täglichen und wöchentlichen Mitzeichnungsstatus einer jeweiligen Petition.

Anfang Juni 2012 wurde in Berlin der 2. Berlin Open Dataday veranstaltet. Vertreter aus der Berliner Stadtverwaltung, Netzaktivisten und Bürger debattierten im Roten Rathaus über die Zukunft von Offenen Daten in Berlin. Fazit: Der Beginn eines Kulturwandels hin zu einer offenen Verwaltung ist absehbar, dennoch fehlen Konzepte Möglichkeiten und Wege den Bürger zu erreichen.

Mit leichter Verzögerung startete am 5. Juni unter e-konsultation.de/opengov die Onlinekonsultation zum Thema „Eckpunktepapier für Offenes Regierungs- und Verwaltungshandeln (Open Government)" des IT-Planungsrates.

Am 13. Juni beschloss die Hamburger Bürgerschaft überraschend das Transparenzgesetz. Damit ist Hamburg das erste Bundesland, das in Deutschland ein modernes Transparenzgesetz bekommt. Das Gesetz sieht vor, dass Politik und Verwaltung Dokumente von öffentlichem Interesse unaufgefordert und kostenfrei im Internet zugänglich machen müssen. Der Entwurf wurde vorab unter Einbeziehung von Bürgerinnen und Bürgern in einem Wiki erarbeitet. Darüber hinaus wird es binnen 2 Jahren ein Informationsregister geben.

Die britische Regierung veröffentlichte Ende Juni das „Open Data White Paper: Unleashing the Potential" und legt damit offen, welche Strategien und Bemühungen es gibt, steuerfinanzierte Daten offen zu legen.[31] Daran könnte sich die deutsche Regierung mal ein Beispiel nehmen.

Ebenfalls Ende Juni wurde mit dem (N)ONLINER Atlas 2012 die jährliche Ausgabe der größten Studie zur Internetnutzung in Deutschland vorgestellt. Kurzzusammenfassung: 75,6 Prozent aller Deutschen sind online (+0,9 Prozent zum Vorjahr). Internetnutzung hängt immer noch eng mit dem Einkommensniveau und dem Alter (95 Prozent der 14-39-Jährigen sind online) zusammen. Senioren bleiben offline.

31 CabinetOffice: Open Data White Paper: Unleashing the Potential, in: http://www.cabinetoffice.gov.uk/resource-library/open-data-white-paper-unleashing-potential; 6.12.2012.

Mit „MapIt Global„[32] veröffentlichte die britische NGO mySociety Anfang Juli 2012 eine globale API für das Auslesen von Staats- und Verwaltungsgrenzen auf der Basis von GEO-Koordinaten und OpenStreetMap.

In der im Juli veröffentlichten Studie „Europäische Cybersicherheitspolitik[33]“ der Stiftung Wissenschaft und Politik (SWP) kritisieren die Forscher, dass die „EU ihren demokratischen Ansprüchen nicht Rechnung trägt“ und Transparenz und Rechenschaftspflicht in fast allen betrachteten Bereichen sehr zu wünschen übrig lassen.

Nicht nur die UN beurteilte die eGovernment-Entwicklungen in Deutschland als unbefriedigend, auch die dritte Ausgabe des „eGovernment Monitor[34] „gab keinen Anlass zur Euphorie. Die Initiative D21 und das Institute for Public Information Management (ipima) der TU München attestieren vor allem bei der Entwicklung von durchgängig digitalisierten Services zur Vereinfachung von Verwaltungsvorgängen viel Nachholbedarf.

Im Blog der Weltbank erschien ein Beitrag mit dem Titel „Opening Government Data. But Why?“[35]. Die Autorin, Governance Spezialistin der Weltbank, bezog sich dabei auf die rhetorische Blase um den Begriff „Open Government“ und kommt zu dem Schluss, dass eine vernünftige und ehrliche Öffnung von Daten ein hervorragender Katalysator für den politischen Wandel darstellt, alles andere sei nur ein künstlicher Nebelschleier rund um Politiker und Bürokraten.

Am 1. August 2012 veröffentlichte das Bundesministerium des Innern die Studie „Open Government Data Deutschland“.[36] Die Studie befasst sich mit den rechtlichen, technischen und organisatorischen Herausforderungen bei der Offenlegung von Datenbeständen der öffentlichen Verwaltung. Leider wurde die Studie ohne die tiefere Einbeziehung zivilgesellschaftlicher Gruppen er-

32 http://global.mapit.mysociety.org/

33 Stiftung Wissenschaft und Politik 2012: Europäische Cybersicherheitspolitik, in: http://www.swp-berlin.org/de/publikationen/swp-studien-de/swp-studien-detail/article/europaeische_cybersicherheitspolitik.html; 6.12.2012.

34 http://www.egovernment-monitor.de/

35 *Dokeniya, Anupama* 2012: Opening Government Data. But why?, in: http://blogs.worldbank.org/publicsphere/opening-government-data-why; 6.12.2012.

36 BMI 2012: Bundesinnenministerium veröffentlicht Studie „Open Government Data Deutschland“, in: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2012/mitMarginalspalte/07/opengovernment.html; 6.12.2012.

stellt und Lorenz Matzat fasste das Ergebnis auf netzpolitik.org wie folgt zusammen: „Es bleiben ganze zwei Seiten der über 500 Seiten-Studie für die Rolle des Bürgers, also des Souveräns, beim offenen Regierungshandeln übrig (S. 56f). Für neue Partizipationsmodelle, etwa Liquid Democracy, ist da kein Platz."

Mit OffeneKommune.de startete Anfang August 2012 eine freie Internetplattform auf Basis der Open Source-Software Adhocracy, auf der Bürger, Kommunen und Initiativen lokale und regionale Themen diskutieren können. Betrieben wird die Plattform vom Liquid Democracy e. V.

Anfang September 2012 wurde das elektronische Petitionssystem des Bundestags überarbeitet. Neu dabei: die Nutzung eines Pseudonyms ist endlich möglich. Bei den weiteren Änderungen, wie „Hierarchische Forenlogik", „Informationen zum Petitionsverlauf" und die „Kontextbezogene Hilfe" handelt es sich eher um Schönheitskorrekturen.

Laut einer repräsentativen Umfrage der Bertelsmann-Stiftung und TNS Emnid51 fordern 89 Prozent der Bürger mehr Mitsprache bei Infrastrukturprojekten wie beispielsweise neuen Straßen, Kraftwerken oder Stromtrassen. Jeder zweite befragte Bürger kann sich sogar vorstellen, sich intensiv mit dem Projekt zu beschäftigen – jedoch nur ein Drittel würde sich längerfristig engagieren.

Seit 2009 findet einmal jährlich das *PolitCamp* statt. So auch am 22. und 23. September 2012: Wie in jedem Jahr war es Ziel, Netzgemeinde, Politiker, Webaktivisten, parlamentarische Mitarbeiter, Unternehmen und Journalisten zu aktuellen netzpolitischen Themen zusammen zu bringen. Neben interessanten Debatten und Diskussionen hat der Berliner Pirat Christopher Lauer für einen kleinen Eklat gesorgt: Als ihn ein Sozialdemokrat kritisierte, verließ Christopher Lauer beleidigt das Podium – schöne neue politische Welt.

Clay Shirky sprach bei einer TED-Konferenz über „How the Internet will (one day) transform government"[37] und forderte Regierungen auf, von der Open Source Welt zu lernen wie man mit vielen divergierenden Ideen umgehen und sie für ein besseres Gemeinwohl nutzbar machen kann.

37 Video bei YouTube, in: http://www.youtube.com/watch?v=CEN4XNth610.

Am 19. September beschloss die Bundesregierung den im März 2012 erstmals vorgelegten Gesetzentwurf zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften.[38]

Im Oktober 2012 ist der Wahlkampf in den USA in vollem Gange und weil Barack Obamas Erfolg bei den Präsidentschaftswahlen 2008 nicht zuletzt auch das Ergebnis einer bis dato einzigartigen Online Wahlkampf-Strategie war, wird der Online-Wahlkampf auch hierzulande aufmerksam beobachtet.

Mitglieder verschiedener Fachgruppen der Gesellschaft für Informatik (GI) haben ein sehr gelungenes Memorandum zur Öffnung von Staat und Verwaltung erarbeitet und am 17. Oktober der Öffentlichkeit vorgestellt.[39] Das fünfseitige Positionspapier der GI beschäftigt sich mit den nötigen Voraussetzungen des 21. Jahrhunderts für ein offenes Regierungs- und Verwaltungshandeln und gibt vier konkrete Handlungsempfehlungen.

Die Plattform fragdenstaat.de, über die Bürgerinnen und Bürger ursprünglich Anfragen auf Grundlage der Informationsfreiheitsgesetze an die öffentliche Verwaltung auf Bundesebene stellen konnten, wurde für Anfragen aus dem seit Anfang Oktober geltenden Hamburger Transparenzgesetz angepasst. Im Laufe des Jahres 2012 wurde die Plattform schon auf Anfragen an die Landes- und Kommunalbehörden von Berlin, Brandenburg und Nordrhein-Westfalen optimiert.

Eparticipation.eu wurde komplett überarbeitet und fokussiert sich nun stärker auf die Hilfe zur Selbsthilfe bei der Erarbeitung und Umsetzung von elektronischen Beteiligungsmöglichkeiten innerhalb der EU. An Fallstudien wird erläutert, welchen Einfluss elektronische Medien auf politische Verfahren haben kann.

Am 25.10 hat der IT-Planungsrat in seiner 9. Sitzung das Eckpunktepapier „Offenes Regierungs- und Verwaltungshandeln (Open Government)“ behandelt. Im Ergebnis spricht sich der IT-Planungsrat dafür aus, das Eckpunktepapier „als eine wesentliche Grundlage für die weitere Arbeit im Steuerungsprojekt heranzuziehen“. Leider ist es nach der Online-Konsultation im Juni

38 BMI 2012: „E-Government-Gesetz“: bürgernahe elektronische Verwaltung, in: http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2012/09/egovernmentgesetz.html; 6.12.2012.

39 Positionspapier zu Open Government, in: http://fb-rvi.gi.de/fileadmin/gliederungen/fg-vi/FGVI-121016-GI-PositionspapierOpenGovernment.pdf.

2012 weder technisch noch inhaltlich gelungen, die Einbeziehung der Experten in angemessener Form zu kommunizieren, noch den Entscheidungsprozess transparent zu gestalten. Unter e-konsultation.de/opengov/ kann das entstandene Eckpunktepapier eingesehen und halbwegs nachvollzogen werden, welche Anregungen aus der Konsultationsphase aufgegriffen wurden.

Aufgrund des Hurrikans „Sandy" im November 2012 beschloss man kurzerhand im US-Staat in New Jersey die Möglichkeit einzuführen, via Email, Fax oder Brief an der Präsidentschaftswahl teilzunehmen. Die „Directive Regarding Email Voting and Mail-in Ballots for Displaced Voters" führte zu Chaos in den Wahlbüros, zu berechtigter Kritik und massiven Sicherheitsbedenken.

Im November 2012 wird eine Infografik veröffentlicht, die die Online-Wahlkämpfe von Obama und Romney im Jahr 2012 vergleicht[40] und später im Monat erschien ein interessanter Beitrag über die Technik hinter der Spenden-Plattform von Obama.[41]

Mit dem Projekt „Stadt Land <Code>" will die Open Knowledge Foundation Deutschland (Disclaimer: Der Autor ist im Vorstand der OKFN) zeigen, mit welchen digitalen Werkzeugen das politische sowie alltägliche Zusammenleben vereinfacht und weiterentwickelt werden kann. Aus den eingereichten Ideen werden vier Ideen im Zeitraum zwischen Dezember 2012 und März 2013 mit einem Stipendium gefördert.

Mit *Govapps* startete die Beauftragte der Bundesregierung für Informationstechnik einen App-Katalog. Leider verwendet das Portal weder offene Schnittstellen zur maschinenlesbaren Abfrage des govapps-Katalogs noch stehen die Texte unter einer offenen Lizenz. Letztendlich hätte man mit den Kosten die für Erstellung und Betrieb des Portals entstehen, sicher auch sinnvollere Projekte wie „Stadt Land <Code>" unterstützen können und den Katalog dann später im Rahmen der Open-Data-Strategie des BMI einbinden können.

Ende November veröffentlichte das Entwicklungshilfeprogramm der Vereinten Nationen die Plattform open.undp.org inklusive einer Schnittstelle. Die Seite öffnet umfangreiche Information über die mehr als 6.000 Projekte der Organisation in 177 Länder.

---

40 http://callersmart.com/blog/2012-11-02-dialing-for-dollars-and-votes-infographic/

41 Rush, Kyle 2012: Meet the Obama campaign's$250 million fundraising platform, in: http://kylerush.net/blog/meet-the-obama-campaigns-250-million-fundraising-platform/; 6.12.2012.

Ist Open Source demokratisch?

Mirko Boehm

„Kann Open Source demokratisch sein?“ fragte Glyn Moody, und beförderte das Thema umgehend zu einer der zentralen Diskussionen zur Internetkultur im Jahr 2012. Er beschreibt seine Erfahrung, wie Open Source als verteiltes, von der Basis entwickeltes System der Programmierung entstanden ist, und wie sich dieses System im Laufe der Zeit verändert hat. Diese Kultur war geprägt von einem sehr umfassend partizipativen Prozess nicht nur der technischen Aspekte der Softwareentwicklung, sondern auch von deren Organisation, sowie einer engen wechselseitigen Beziehung zwischen Programmierern und Benutzern. Benutzer als auch Programmierer trugen zum Fortschritt der Projekte bei, sie arbeiteten gemeinsam daran. Dieser Prozess veränderte sich über die Zeit, er wurde institutionalisiert, kommerzialisiert und zunehmend langweiliger – „ein ‘Firefox Affiliate’ zu werden führt bei kaum jemandem zu einem beschleunigten Puls.“[1] Üblicherweise spielen Benutzer inzwischen keine bedeutende Rolle mehr in Open-Source-Projekten.

Wenn diese Entwicklung bedauert wird, liegt dem die Annahme zu Grunde, das Open Source grundsätzlich demokratisch sei, und diese Annahme gilt es zu hinterfragen. Open-Source-Communities gelten als selbstgesteuert, meritokratisch et cetera, aber ein besonderer demokratischer Charakter ihres Funktionierens steht selten im Vordergrund. Einzelne investieren oft großen Aufwand in ihr Lieblingsprojekt, um zu einem größeren Ganzen beizutragen, und Demokratie gilt ebenfalls oft als höheres Gut. Es ist daher verlockend, vom einen aufs andere zu schließen und Open-Source-Communities ebenfalls als grundsätzlich demokratisch anzunehmen. Aber ist das wirklich der Fall? Was bedeutet Demokratie im Kontext von Open Source eigentlich? Wie würde eine demokratische Open-Source-Community aussehen?

Man könnte vermuten, dass sich politische Begriffe wie Demokratie nicht leicht auf die Funktionsweise von Open-Source-Communities übertragen lassen. Auch wenn es nicht leicht ist, kann es sich trotzdem lohnen – Demokratien hatten ähnliche Probleme der Teilhabe und der Verteilung von Macht und

1 Moody, Glyn 2012: Can open source be democratic?, in: http://www.h-online.com/open/features/Can-open-source-be-democratic-1663702.html; 5.12.2012.

Verantwortung zu lösen wie Communities. So wie demokratische Staaten sind Communities freiwillige Zusammenschlüsse für die Herstellung von öffentlichen Gütern. So wie Bürger stehen Mitglieder in Communities vor der Entscheidung zwischen Mitmachen und Aufhören, die sie auf Grund des erwarteten Einflusses ihres Beitrags treffen. Es lassen sich genügend Parallelen konstruieren, um das Lernen vom Beispiel demokratischer Staaten zu rechtfertigen.

Mitwirkende als Elemente von Communities

Demokratie bedeutet „Herrschaft des Volkes" und fordert unter anderem für jeden einzelnen Bürger Gleichheit vor dem Gesetz und eine Stimme im Prozess der politischen Willensbildung und bei der Wahl der regierenden Repräsentanten. Diese Anforderungen führen sofort zur zentralen Yin-Yang-Frage, wer denn Bürger sei und wer nicht. Sind Benutzer integrative Bestandteile (Bürger) von Open-Source-Communities? Wie sieht es mit weiter Außenstehenden aus, die gelegentlich Feedback geben? Und sollten diese dann den Entwicklern gleichgestellt sein? Wie in Staaten stellt sich die Frage nach Gleichheit. Während Gleichheit, also Nicht-Diskriminierung nach Alter, Geschlecht, Hautfarbe und so weiter, heute weitgehend als gegeben hingenommen wird, ist sie in Wirklichkeit ein dynamisches Konzept, dessen kulturelle Bedeutung sich über die Zeit wandelt. Der Voting Rights Act in den USA hob 1965 die Diskriminierung von Wählern nach Hautfarbe aus. In Saudi Arabien werden Frauen voraussichtlich im Jahr 2015 das Wahlrecht erhalten. Die beschriebene Veränderung des Open-Source-Prozesses bedeutet in diesem Kontext, dass Benutzer sich von gleichberechtigten Mitgliedern der Community gewandelt haben zu Randgruppen, als hätten sie keine Stimme.

Eignung und Akzeptanz unterscheiden den Bürger von Barbaren und Sklaven. Eignung fragt danach, welche Individuen potentiell Bürger werden können. Die Akzeptanz bestimmt die Anforderungen, die ein geeignetes Individuum erfüllen muss, um die uneingeschränkten Bürgerrechte zu erhalten. Zum Beispiel kann ein im Inland lebender Ausländer geeignet sein, die Bürgerrechte zu erhalten, muss aber eine Anzahl Jahre Steuern gezahlt oder im Land gelebt haben, um aufgenommen zu werden. Wendet man die selben Kriterien auf Open-Source-Communities an, werden sie zu „Wer ist ein Mitwirkender und damit geeignet, Mitglied der Community zu werden, welche Kriterien muss man im einzelnen erfüllen, um zum Teil der Community zu

werden?“ (Eignung) und „Was muss ein Neueinsteiger tun, um als Mitwirkender betrachtet zu werden?“ (Akzeptanz). Für Open-Source-Erfahrene lässt sich die Frage einfacher formulieren – „Wie werde ich ein Committer?“. Während in den meisten Communities grundsätzlich alle geeignet sind, Mitglied zu werden, muss man, um akzeptiert und aufgenommen zu werden, am Programmcode des Projekts arbeiten. Schon die zentrale Rolle der Funktion „Committer“ (jemand, der den Code ändern darf) deutet darauf hin.

Damit also Benutzer wieder integraler Bestandteil einer Open-Source-Community werden, müssen diejenigen Nicht-Programmierer, die sich in den entsprechenden Projekten engagieren, sich als Gleiche unter Gleichen einbringen können. Dies ist bei weitem nicht der Standard und entspricht im allgemeinen nicht der Einstellung der Contributoren. Üblicherweise betrachten Communities direkte Beiträge zur Entwicklung der eigentlichen Software als wertvoller als zum Beispiel Feedback von Benutzern. Zumindest unterbewusst behandeln sie Benutzer als Außenstehende und verweisen diese darauf, sich mit dem Bugtracker zu unterhalten – ein bewährter Weg um sicherzustellen, dass sie nicht noch einmal mit Feedback wiederkommen. Um wieder zum Wunschzustand der kollaborativ arbeitenden Community zu kommen, müssen also zum einen Benutzer wieder als potentielle, vollwertige Mitwirkende betrachtet werden. Zum anderen müssen sie sich mit ihren im Zweifel nichttechnischen Beiträgen wie etwa Feedback zur Aufnahme als gleicher unter gleichen Mitwirkenden qualifizieren.

Über Open Governance

Aber nicht alle Mitwirkenden sind notwendigerweise vor dem Projekt gleich. Wenn bewertet werden soll, wie demokratisch eine Open-Source-Community ist, ist es darüber hinaus notwendig, sich mit ihrer Entstehung auseinanderzusetzen. Nicht alle Open-Source-Projekte werden von Entwicklern und Benutzern gemeinsam begonnen, und die Verteilung von Macht und Verantwortung folgt üblicherweise dem vorher gesetzten Ziel, ihrer Doktrin. Wenn ein Projekt von einer Gruppe Freiwilliger mit einem gemeinsamen Ziel begonnen wird und organisch zu einer offen und transparent gelenkten Community wächst (wie etwa die KDE-Community), zeigt sie im allgemeinen eher demokratische Züge. Ein Projekt dagegen, welches zum Beispiel als Investition eines Unternehmens gestartet wird, wie etwa Mozilla Firefox oder Qt, und vielleicht externe Mitwirkende zulässt, solange sie sich an die Contributor Li-

cense Agreements des Projekteigentümers halten, ähnelt eher einer Aristokratie. Nicht alle Mitwirkenden sind Gleiche unter Gleichen, und die Führung des Projekts kann von der Basis nicht ersetzt werden.

Die Debatte darüber, was die wesentliche Eigenschaft einer Demokratie ausmacht ist nicht neu. Es gibt unterschiedliche Meinungen, aber es gibt eine einem Lackmustest ähnelnde Frage – können die Bürger in schöner Regelmäßigkeit die im Amt befindliche Regierung in einem geregelten Prozess abwählen und ersetzen, ohne dabei auf eine Revolution zurückgreifen zu müssen? In diesem Licht betrachtet wird deutlich, dass tatsächlich nicht alle Open-Source-Communities von demokratischer Natur sind. KDE zum Beispiel ist es, die Community hat einen relativ schwachen Vorstand und wählt regelmäßig neue Repräsentanten, wobei jedes aktive Mitglied genau eine Stimme hat (und andere, etwa Unternehmen, keine). Man stelle sich einen Versuch der Community vor, die Führung des Android-Projekts abzuwählen und zu ersetzen, und der Unterschied wird nahezu plastisch deutlich. Nach diesem Kriterium sind die wenigsten populären Open-Source-Projekte demokratisch.

Zurück zur Frage, wie der in den letzten Jahren gewachsene Abstand zwischen Benutzern und Entwicklern wieder überwunden werden kann, wie wieder Communities mit lebhafter Kollaboration entstehen können. Engagierte Benutzer, wie jeder andere Mitwirkende, werden für sich bewerten, welchen Effekt ihr Einbringen von Zeit und Aufwand in das Projekt bewirken wird. Wenn der gefühlte Nutzen, zum Beispiel durch das warme Gefühl, an etwas mitzuwirken, dass der Allgemeinheit zu Gute kommt, oder auch durch die Pflege der persönlichen Reputation, höher ist als der gefühlte Aufwand, werden sie gewillt sein, sich der Community anzuschließen und bei der Fortentwicklung des Projekts zu helfen. Dieser gefühlte Nutzen hängt eng damit zusammen, wie offen Strukturen und Prozesse der Gemeinschaft für die Mitwirkenden sind – man spricht von Open Governance. Der gefühlte Nutzen wird niedriger ausfallen, wenn der Einzelne nur bei unbedeutenden Details ein Mitspracherecht bekommt, und höher, wenn sie zum Beispiel durch ihre Beiträge zum nächsten Vorstand des KDE e. V. Aufsteigen kann. Dieser Umstand betont die Wichtigkeit von Open Governance für die Langlebigkeit und den Zusammenhalt von Open-Source-Communities. Nur wenn der Open Source Way kombiniert wird mit einer Kultur der Open Governance, wird für

den einzelnen die Freiheit des Mitwirkens so deutlich, dass sie ihn überzeugt, dem Projekt beizutreten und seine Zeit einzubringen. Demokratie in Communities bedeutet die Kombination von Open Source und Open Governance.

Gleiche unter Gleichen

Aus dem Status, Mitwirkender – Bürger – in einer Community zu sein, ergeben sich wie in Staaten eine Reihe von Rechten und Pflichten, an den Aktivitäten der Gemeinschaft teilzunehmen. Open Source kann demokratisch sein, wenn Communities alle Mitwirkenden mit den gleichen Rechten und Pflichten ausstatten. Drei Anforderungen lassen sich aus dem bisher gesagten ableiten, wenn Open-Source-Communities als demokratisch gelten wollen:

- Als demokratisch zu gelten erfordert, keine Diskriminierung zwischen den Mitwirkenden zuzulassen. Benutzer sind Mitwirkende, genauso wie Programmierer. Da diese Haltung in den letzten Jahren nicht weit verbreitet war, müssen insbesondere Benutzer ermutigt werden, der Community beizutreten, Feedback zu geben und auf verschiedene andere Weise dem Projekt zu helfen.
- Demokratie in Communities bedeutet die Kombination von Open Source und Open Governance. Die Verfügbarkeit des Projektquellcodes unter einer Freie-Software-Lizenz ist nicht ausreichend als Grundlage für eine demokratisch arbeitende Gemeinschaft. Ohne Gleichheit, ohne die vollständige Kontrolle der Mitwirkenden über das gesamte Projekt, mag dieses vielleicht ein Open-Source-Projekt sein, aber es ist nicht demokratisch.
- Eine Gemeinschaft exerziert Open Governance, wenn alle Mitwirkenden die gleichen Rechte und Pflichten haben, und gemeinsam die Führung und Repräsentanz der Community bestimmen. Definiert man Open Governance als eine Situation, in der die Mitwirkenden die Kontrolle über ihr Projekt auf allen Ebenen innehaben, dann kann Demokratie in Communities nur erreicht werden, wenn alle Mitwirkenden gleiche Mitspracherechte in allen Aspekten des Projekts haben.

Ob Mitwirkende wirklich Gleiche unter Gleichen sind oder nicht lässt sich nur anhand von Taten, nicht von Worten nachweisen. In der Realität ist es oft nicht der Fall, weit verbreitet sind zum Beispiel unterschiedliche Wertungen

verschiedener Arten von Beiträgen (Entwicklung, Qualitätssicherung/Feedback, Design, Benutzbarkeit, …), aber auch die Unantastbarkeit der Inhaber bestimmter Funktionen („Benevolent Dictator for Life"). Der ethischen Frage, ob Demokratie wünschenswert oder gar notwendig ist für den Erfolg von Open-Source-Communities, wurde weitgehend ausgewichen, aber eins ist deutlich: Es ist kein Zufall, dass mit zunehmender Ungleichheit ein Rückgang der Beiträge von Benutzern zu verzeichnen war. Um die Erfolgsgeschichte von Open Source fortzusetzen ist es nötig, alle direkt und indirekt Mitwirkenden wieder gleichberechtigt zur Zusammenarbeit zu bewegen, und das bedeutet mehr Open Governance und weniger Kontrolle der Gründer, ob Individuen oder Unternehmen, über die Projekte.

Mit der weiter zunehmenden Komplexität von Open-Source-Software ist es nur natürlich, dass die Entwickler immer erfahrener und der computerfachliche Abstand zum Benutzer weiter wachsen wird. Dieser Trend wird sich mit der wachsenden Benutzerbasis wahrscheinlich fortsetzen. Da sich diese zunehmende Spezialisierung nicht vermeiden lässt, sind Open-Source-Communities gut beraten, Benutzer mehr und gleichberechtigter einzubinden und durch Open Governance mehr Demokratie zu wagen.

Hilfe, meine Tochter ist auf Facebook: Ein digitaler Elternabend

Karina Fissguss

Was tun, großer Schock. Es gibt Eltern, denen ist Facebook von Grund auf suspekt. Sie halten es für gefährlich und wollen möglichst ungewollte Facebook Partys für ihre Teenage Kinder vermeiden. Diese Eltern sind zutiefst verunsichert. Schließlich geht es um das Wohlergehen ihres wohlgehüteten Nachwuchses. Der beste Kinderwagen, die beste Kita, die beste Schule und nun kommt dieses unberechenbare Internet daher. Was tun? Medienpädagogen sind mittlerweile damit beschäftigt, Eltern aufzuklären. Aufzuklären über den Computer, der die Zeit ihrer Kinder sehr beansprucht. Was machen die Kids so lange vor dem Ding? Bekommen die etwa Dinge zu sehen, die sie definitiv nicht sehen sollten? Und außerdem heißt es doch immer 30 Min Medienkonsum unter 6 Jahren und 1 Stunde über 6 Jahren sollte reichen. Hilfe. Hilfe! Ein digitaler Elternabend muss her.

Also teilen wir mal die Elternschaft in zwei Gruppen, die Holzspielzeugfraktion, die nicht möchten, dass Kinder zu viel Fernsehen und vor dem Computer sitzen und die andere Holzspielzeugfraktion, die versucht den Kindern, den Umgang mit dem Computer beizubringen. Zwar sind das meist die Väter. Aber das würde an dieser Stelle zu weit führen. Also hält Fraktion 1 das Internet für Kinder für Teufelszeug und möchte sie so lange es geht davor bewahren. In dieser Gruppe wird vom Programm Paint als pädagogischem Ziel gesprochen. In der anderen Gruppe sagen die Kinder schon mit zwei Jahren, dass sie an den „Puter“ wollen, können mit der Maus schon auf YouTube Baggerfilmchen oder die Teletubbies anklicken. Manche Eltern haben dort schon feststellen müssen, dass es auf YouTube nicht nur Teletubbies für Kinder gibt, sondern auch Teletubbies Filmchen, die damit enden, dass urplötzlich ein Erschießungskommando auftaucht und diese nervigen Wesen niedermacht – zum eigentlich inneren Vergnügen der Eltern – aber wohl weniger des Nachwuchses.

Da wäre, „oh Gott, wir machen das Ding aus" eine Lösung. Eine bessere wäre, sich gleich nach guten Seiten für Kindern umzusehen. Da gibt es auch genügend. Nur ein Beispiel die Seite der Münchener Staatsoper.[1] In der ein Flash animierter Maestro Margarini sein Orchester, die Instrumente und die Oper erklärt. Eindeutig pädagogisch wertvoll und vor allem den Kindern macht es auch Spaß mit der Maus die verschiedenen Instrumente anzuklicken.

„Hier, nimmt das iPad und gib Ruhe" mag ja manchmal ein richtiger Segen sein, um kleine Kinder ruhig zu stellen, aber hier fängt der Streit zwischen den Elternteilen meistens an. Zuviel Computer und stillsitzen überfordert die Kleinen, danach würden sie erst recht unausstehlich – meist die Argumentation der Mütter im Übrigen. Das Kind müsse doch den Umgang mit dem Computer genauso lernen wie alles andere auch, so der andere Elternteil. Dann wird gezankt. Medienpädagogen behaupteten doch, zu viel Computer schade der kindlichen Gehirnentwicklung[2], auf der anderen Seite gibt das Bundesfamilienministerium Broschüren mit Klicktipps für Kinder heraus[3] und auch der Kinderkanal KiKa versucht Eltern im Umgang mit Kind und Computer Hilfeseiten anzubieten[4] – sogar die Redaktion der Sendung mit der Maus tut das.[5]

Ernst wird es dann, wenn die Kinder in die Schule kommen und lesen lernen und sich ein weniger selbstständiger um das Netz bemühen. Was heißt schon das Netz? Sie wollen halt alleine mit Oma und Opa, Onkel und Tante skypen, mit ihren Freunden chatten und warum nicht auch auf Facebook. Doch, oh Weh!

Da warten die Abgründe. Wie stellt man die Privatsphäre-Einstellungen richtig ein? Was darf man posten und was besser nicht, um nicht Opfer von Cybermobbing zu werden? Sollte man überhaupt Fotos einstellen, wenn man sie

1 http://www.bayerische.staatsoper.de/data/kinder_flash/index.html

2 Isfort, Volker 2012: Hirnforscher Manfred Spitzer: Computer macht dumm, in: http://www.abendzeitung-muenchen.de/inhalt.mediennutzung-hirnforscher-manfred-spitzer-computer-machen-dumm.c7abe68a-d1eb-4e0e-9200-bb7c87e40e13.html; 6.12.2012.

3 Bundesministerium für Familie, Senioren, Frauen und Jugend: Ein Netz für Kinder. Surfen ohne Risiko?, in: http://www.bmfsfj.de/RedaktionBMFSFJ/Broschuerenstelle/Pdf-Anlagen/Netz-fuer-Kinder-Elternteil,property=pdf,bereich=bmfsfj,sprache=de,rwb=true.pdf; 6.12.2012.

4 Kikaninchen: Fernsehen und Internet, in: http://www.kikaninchen.de/eltern/tippszummedienumgang/fernsehenundinternet/index.html.

5 WDR: 10 goldene Regeln für Die Seite mit dem Elefanten, in: http://www.wdrmaus.de/elefantenseite/eltern/pdf/goldene_regeln_internet.pdf

je wieder aus dem Internet wegbekommt? Aus den vielen Fragen beim Elternabend kristallisiert sich ein deutliches Bild heraus. Eltern sollte mal der Umgang mit Facebook beigebracht werden, damit ihre Kinder auch einen vernünftigen Umgang mit sozialen Medien von ihnen lernen können. Am besten sie überwinden sich, melden sich selbst da an, wo ihre Kinder unterwegs sind. Befreunden sich mit ihnen und staunen meinetwegen wie offen jede Beziehung über Facebook geführt wird, was man da alles von und über seine Kinder erfährt, was man möglicherweise auch gar nicht wissen will. Aber wenn dann zu Hause beim Abendessen ein Satz fällt wie „Mama, ich hab jetzt einen Freund. Ich wollte es Dir gleich sagen, bevor Du es über Facebook erfährst" ist das doch genau das, worum es hier geht. Das Zurückübertragen der digitalen Welt ins Familienleben. Und davon sollten sich Eltern doch nicht selber ausschließen.

Zur Zukunft der öffentlich-rechtlichen Medien

Volker Grassmuck

Die Informationsflut wird täglich größer, der Aufwand für Sichtung und Auswahl steigt, die Zeit für die Auseinandersetzung mit dem, was uns wichtig ist, wird immer knapper. Ist also weniger mehr?

Schreiben

Disintermediation war ein Zauberwort der Boom-Phase des Internet in den 1990ern. Cutting out the middleman. Wer etwas zu sagen hat, kann es sagen, in Schrift, Bild und Ton, einem potentiellen Publikum von heute zweieinhalb Milliarden Menschen oder 34,3 % der Weltbevölkerung. Ohne erst das Nadelöhr der Verlage, genauer ihrer Zerberusse, der Lektoren, Redakteure, A&Rs usw., passieren zu müssen, also derjenigen, die meinen zu wissen was gut ist und wer es verdient, aus der Unterwelt der Unsichtbarkeit ans Licht der Öffentlichkeit gehievt zu werden. Ohne die Intermediäre der Massenmedien und dank dessen, was die neuere Medienwissenschaft als Medium erkannt hat: des Computers. Nach Reichweite ist das Universalmedium längst zu dem Massenmedium geworden, dass alle anderen übertrifft, doch mit den Nadelöhren der alten Zentrum-an-alle-Medien hat es nur noch unter anderem zu tun.

Jede und jeder unter den zweieinhalb Milliarden Menschen mit Internetzugang (von den Hunden und anderen Haustieren ganz zu schweigen) kann eigene Artikel, Fotos, Videos, Musik, Apps veröffentlichen. Sie kann das tun, wo alle es tun: auf Youtube, Facebook, iTunes, Flickr, Twitter, Amazon. Will sie Geld verdienen, kann sie auf die Selbstverlagsangebote von YouTube („Revenue Sharing" oder deutsch „Monetarisierung": 55 % der Werbeeinnahmen gehen an die Autorin, nur verrät Google nicht, wie hoch die sind), iTunes (für Apps: 70 % der Verkaufserlöse, für Musik eingepflegt über Tunecore o.ä. ca. 70 %), Amazon (70 %) setzen. Oder, wenn ihr die neuen Gatekeeper (ihre Monopolstellung, ihr Profit aus der Aktivität der Vielen, ihre Datenschutzregeln usw.) nicht behagen, kann sie auf dem Internet Archive, Jamendo oder per BitTorrent veröffentlichen. Wer mit dieser Haltung Geld verdienen möchte, kann auf Vodo.net, Magnatune oder Peer-Funding setzen.

Die neuen Intermediäre mögen neue Probleme mit sich bringen, (deren Lösungen im Prinzip bekannt sind: gegen Konzentration Verteilung (Diaspora statt Facebook), gegen Überwachung Kryptographie, gegen Monopolprofite alternative Ökonomien) – eines sind sie nicht: selektiv (abgesehen von Inhalten, die ihnen Klagen einbringen können: Volksverhetzung, Verstöße gegen Persönlichkeitsrechte, Urheber-, Markenrechte usw.). Es gibt neue Gatekeeper, aber die Tore stehen weit offen, meist in beide Richtungen.

Lesen

Der Segen ist zugleich ein Fluch. Ich kann potentiell zweieinhalb Milliarden Menschen erreichen, sie aber auch mich. Das wirft die Frage auf: Wie kann ich in diesen Fluten navigieren? Wie finde ich, was mich interessiert? Wer filtert das alles für mich? „Alle, natürlich", wird die geneigte Leserin des Netzpolitik-Jahrbuchs spontan antworten, wohl wissend, das „Suchmaschinen" keine zielführende Antwort ist.

Was gut ist, setzt sich durch. Wo könnte die alte Weisheit, die uns aus der Bierwerbung entgegenschallt, wahrer sein als im Internet? Sicher: Gutheit liegt im Auge des Betrachters. Aber: Viele Augen sehen mehr. Metriken für Qualitäten fallen ganz von selbst aus dem Internet und täglich werden neue hinzu implementiert.

Was viele verlinken, steht in den Suchmaschinen oben. Ebenso, was viele Views auf Youtube bekommt, Pins auf Pinterest usw. Aber ist tatsächlich gut, was viele sehen, oder sehen es vielmehr viele, weil viele es sehen? Und wie viele von den Vielen sind Bots oder SEO- und social marketing-Dienstleister?

Die Aktivitäten der Vielen erlauben durch Analyse von großen Datenmengen, z. B. Suchanfragen, interessante Erkenntnisse. So lassen uns Google Trends & Zeitgeist Aufkommen und Umlaufgeltung eines Begriffs, z. B. „Leistungsschutzrecht", das rasche Abklingen des Interesses an Fukushima nach März 2011 und das stetig abnehmenden Interesse am Thema „geistiges Eigentum" sehen. Doch diese Erkenntnisse gibt es immer nur im Rückspiegel. Für meinen Tagesbedarf helfen sie wenig.

Schauen wir, wie sich der auf Youtube decken lässt. Unter der „Kategorie" „Nachrichten" finden sich auf den drei Bildschirmen „Top-News" fast nur arabische und einige türkische Beiträge und eine drei Wochen alte Tagesthemen-Sendung. Nun sind Ägypten und Palästina ohne Frage wichtige Themen,

aber spiegelt das tatsächlich die Popularität unter den in Deutschland geklickten Nachrichten-Clips wieder? Die aus meiner Klickgeschichte algorithmisch bestückten „Empfehlungen für dich" zeigen meist mehr vom gleichen, was mich, wie bei Amazon-Empfehlungen, in aller Regel nicht interessiert. Zielführender sind da schon die abonnierbaren Kanäle. Aber selbst mit einer gut gemixten Filterblase (ARD, Euronews, Al Jazeera, Netzpolitik usw.) lässt sich so schwerlich ein informativer TV-Abend zusammen klicken. Die Weiterzapprate ist beim konventionellen TV deutlich geringer und die Öffentlichen-Rechtlichen stellen nur einen Bruchteil ihres Programms auf Youtube. Direkte Suche nach geeigneten Wörtern (z. B. „Leistungsschutzrecht") dagegen liefert einen recht informativen Überblick. Fazit: Für die Deckung des täglichen Informationsbedarfs oder ein unterhaltsames Abendprogramm unbrauchbar.

Dann doch lieber meine Freunde auf Facebook & Co als Filter. Die meisten von ihnen teilen mindestens eines meiner Interessengebiete. Die Wahrscheinlichkeit, dass, was sie interessant finden, auch mich interessiert, ist also ziemlich hoch.

Eine willkürliche Stichprobe auf Facebook ergibt vor allem Persönliches: Musik, Fotos vom Nachwuchs, Essen, Reisen, Meldungen in mir auch mit Übersetzungen nicht verständlichen Sprachen und Fonts, die nicht dargestellt werden (Sanskrit?). Bonmots aus dem täglichen Leben und zeitlose Spruchweisheiten („Videos schauen verstärkt das Aufmerksamkeitsdefizit. Was wollte ich hier gleich wieder machen?"). Und dazwischen Neuigkeiten über Bradley Manning, die WCIT in Dubai und über den Papst, der seinen offiziellen Twitter-Account @pontifex gestartet hat. Und nicht zu vergessen: Markus Beckedahl, der ein Netzpolitik Jahrbuch 2012 ankündigt. Fazit: Eine deutlich höhere Trefferquote bei für mich relevanten Tagesereignissen und Kommentaren. Und dennoch bleibt eine Zufälligkeit in dem, was durch diesen Filter aufscheint. Umfassend informiert fühle ich mich danach nicht.

Oder doch der Markt? Der ist schließlich auch ein Filter in dem alle an der Kasse abstimmen. Aber da geht es mir wie mit den meistgeklickten Videos auf Youtube: Auf den Bestsellerlisten finden ich selten etwas, das mich interessiert.

Oder die Profis? Die meinungsmachenden Journalisten, Großkritiker, Alpha-Blogger? In meine Blogroll tauche ich regelmäßig ein. Doch auch hier bin ich mir bewusst, dass ich mich in einer selbstgewählten Filterblase bewege.

Rundfunken

In der digitalen Gesellschaft stapft der öffentlich-rechtliche Rundfunk wie ein Dinosaurier herum, noch dazu mit Fußfesseln. Wie könnte man ihn auf Trab bringen, damit er uns bei unserem täglichen Bedarf nach Information, Bildung, Beratung und Unterhaltung das Leben leichter macht?

Das Programmschema einer Station linear durchzuschauen, ist es sicher nicht. Serendipity, also Zappen bringt mehr Vielfalt, aber in die letzten drei Minuten einer spannenden Reportage zu geraten, bringt mehr Frust als Freude. Immerhin kann ich dann Mediathek.app darauf ansetzen. Im EPG kann ich mir wieder meine persönliche Filterblase bauen, doch auch hier im Bewusstsein der Beschränkung auf einige Suchwörter und selbst dann noch mit Streuverlusten.

Anstalten und Geräteindustrie wollen uns als Lösung neue, „interaktive" hbbTVs und SmartTVs verkaufen. Danke, nein danke, ich habe schon vier Computer.

Alles nicht befriedigend. Unsere Navigationswerkzeuge sind noch unterentwickelt. Algorithmen bringen interessante kollektive Muster zu tage, aber solange wir nicht einschätzen können, was sie alles nicht sehen und nicht gezielt Einfluss nehmen können auf ihre Auswahl, sind sie keine Lösung für die private und öffentliche Meinungsbildung.

Menschliche Intelligenz mit einem Einschlag Personalisierung und das in einem kompakten Mikroformat – das wär's.

Für die private und öffentliche Meinungsbildung sind traditionell die öffentlich-rechtlichen Medien zuständig. Und sie gelten als „Garant für Qualität".

Wie wär's also mit einem öffentlich-rechtlichen Twitter- (besser: Status.net-) Angebot? Eine Redaktion stellt Feeds in verschiedenen Rubriken zusammen, über die ich mir jederzeit, ob auf dem Handy unterwegs oder auf dem heimischen Beamer, einen Überblick verschaffen kann über Politik, Kultur, Medien, Sport. Die Tweets enthalten aussagekräftige Kurztexte und Links auf nach journalistischen Kriterien ausgewählte Beiträge, natürlich aus der laufenden Produktion der Anstalten selbst und ihrer öffentlich-rechtlichen Partner im Ausland, auf Beiträge aus ihren Archiven, die für aktuelle Entwicklungen relevant sind – der vollständigen Archive, nicht der künstlich auf sieben Tage verkürzten – und ebenso auf gründlich recherchierte, vertrauenswürdige und

qualitätvolle Internet-native Beiträge auf Blogs, Vlogs und Podcasts. Deren Urheber würden, da sie nun zum öffentlich-rechtlichen Informationsangebot beitragen, auch an den öffentlich-rechtlichen Beiträgen partizipieren. Eine „Stiftung Internet", die mit einem Prozent der Rundfunkabgabe, also rund 80 Millionen Euro ausgestattet ist, würde dem freien Journalismus, der Bildberichterstattung und anderen Kreativen im Internet einen gewaltigen Aufschwung verschaffen, und damit der Vielfalt in der Meinungsbildung.

Schließlich filtert mein Client die Feeds und lernt, dass mir bestimmte Sendungen oder Formate nicht gefallen und ich zu diesem Thema gern mehr, zu jenem weniger hätte. Was mir angezeigt wird, kann ich auch runterladen, in offenen Standards und unter einer Freilizenz, die Remixing erlaubt.

Wenn zu alledem nicht nur mein lokaler Filter, sondern auch die Redaktionen „interaktiv" werden, also nicht nur auf meine Klicks, sondern auch auf meine Vorschläge hören und dazu lernen, so dass wir alle besser informiert und klüger werden, dann wäre das eine Grundversorgung, die ich mir gefallen ließe.

Ob die Zukunft der öffentlich-rechtlichen Medien in diese oder eine ganz andere Richtung gehen wird, ist die Millionen-Euro-Frage. Aber auch ohne Kristallkugel lässt sich voraussagen, das 2013 das Jahr des öffentlich-rechtlichen Rundfunks wird. Mit dem ersten Tag des Jahres tritt die Haushaltsabgabe in kraft. Voraussichtlich ebenfalls Anfang des Jahres wird „Germany's Gold" starten. Unter dem Arbeitstitel wollen ARD und ZDF „das Beste aus 60 Jahren deutscher Fernsehgeschichte" anbieten, gegen Pay-per-view, Abo und Werbung. Schließlich wird das Bundesverfassungsgericht sein Urteil über die Staatsferne des ZDF sprechen, dessen CDU-dominierter Verwaltungsrat 2010 den langjährigen Chefredakteur des ZDF Nikolaus Brender abserviert hatte.

Ebenfalls 2010 hat die Netzgemeinschaft sich erstmals in der Rundfunkpolitik engagiert und den 14. Rundfunkänderungsstaatsvertrag zum Jugendmedienschutz abserviert. Drei Jahre in der Offline-Welt, – wenn die alte Regel noch stimmt, 21 Jahre in der Internet-Welt – werden dann vergangen sein, also die Reifezeit vom Krabbeln bis zum Studium. Man darf auf das Jahr der öffentlich-rechtlichen Medien gespannt sein.

Blowing the whistle: Heldinnen oder Kriminelle?

Andrea Jonjic

Bradley Manning zwischen Friedensnobelpreis und Todesstrafe

Bradley Manning ist der derzeit wohl bekannteste Whistleblower der Welt. Der 25-Jährige sitzt seit Mai 2010 in Haft, im Februar 2011 wurden 22 Anklagepunkte publik, unter anderem „Kooperation mit dem Feind". Für diesen Anklagepunkt könnte die Todesstrafe gefordert werden, was unter anderem die Politiker Michael Rogers, Mitglied des Repräsentantenhauses, und Mike Huckabee, ehemaliger Gouverneur, öffentlich begrüßten.[1] Die Anklage sah jedoch davon ab, es bleiben bis zu 52 Jahre Haft – lebenslang.

Bradley Manning wurde im Sommer 2009 im Irak stationiert, als Nachrichtenanalyst mit Zulassung zur Geheimhaltungsstufe „Top Secret". Im Mai 2010 kontaktierte er Adrian Lamo, einen bekannten Hacker und Sicherheitsanalysten. Einsam, sei er und fühle sich so hilflos, schreibt Manning a.k.a. „bradass87" im Chat.[2] Und vertraut Lamo an, dass er vertrauliche Dokumente an WikiLeaks weitergegeben hat, eine anonyme Whistleblowing-Plattform. Adrian Lamo sah darin eine Gefahr für „Diplomatie, operative Sicherheit und menschliches Leben"[3] und informierte die amerikanischen Polizeibehörden, die Bradley Manning wenig später festnahmen. Manning hatte gehofft, dass, wenn die Öffentlichkeit erfährt was im Irak geschieht, wie Zivilisten getötet werden, sie dann das Unrecht erkennt und dagegen protestiert. Das wahrscheinlich von ihm weitergegebene „Collateral Murder" Video war ein solcher, erschreckender Ausschnitt einer Realität, die der Öffentlichkeit so nicht zugängig ist.

---

1 *Levey-Baker, Cooper* 2010: Huckabee calls for execution of person who leaked diplomatic documents to WikiLeaks, in: http://floridaindependent.com/15935/mike-huckabee-calls-for-execution-of-person-who-leaked-diplomatic-documents-to-wikileaks; 3.12.2012.

2 *Hansen, Evan* 2011: Manning-Lamo Chat Logs Revealed, in: http://www.wired.com/threatlevel/2011/07/manning-lamo-logs/; 3.12.2012.

3 Tweet von Adrian Lamo am 26. August 2011, in: http://www.twitlonger.com/show/clkgck; 3.12.2012.

Ein verzweifelter, einsamer junger Mann, der das von ihm empfundene Unrecht öffentlich machen wollte. In diesem Jahr war er nominiert für den Friedensnobelpreis. Im November sagte er zum ersten Mal aus, berichtete von den schlimmen Bedingungen in der monatelangen Isolationshaft in Quantico und von folter-ähnlichem Umgang. Manning hat im November angeboten, sich in acht der 22 Anklagepunkte schuldig zu sprechen. Dadurch drohten ihm bis zu 16 Jahre Haft – die US-Regierung hat sich jedoch noch nicht dazu geäußert, ob sie das Angebot annehmen wird.

Whistleblower belastet Nationalbankchef – und wird selbst angeklagt

Ein Schweizer Nationalbankchef tätigt im Januar diesen Jahres private Devisentransaktionen. Er, der die Geldmenge, den Wechselkurs, maßgeblich beeinflusst, scheint sich damit des Insiderhandels strafbar zu machen. Der IT-Mitarbeiter einer Bank leakte diese Informationen und zeigte sich danach selbst an. Daraufhin wurde er angeklagt, gegen das Bankgeheimnis verstoßen zu haben.

Der Schweizer Nationalbankchef Philipp Hildebrand spekulierte privat mit Millionenbeträgen, kaufte wenige Wochen vor Festsetzung der Euro-Untergrenze von CHF 1.20 eine halbe Millionen US-Dollar bei einem Kurs von 0,7929 und verkaufte diese nach Festsetzung des neuen Frankenkurses mit einem Gewinn von 75000 Franken. Ist ein Nationalbankpräsident, der private Devisentransaktionen tätigt, vertrauenswürdig? Handelt er im Sinne seines Amtes und somit der Schweiz, oder trifft er seine Entscheidungen aufgrund persönlicher Interessen?

Ein IT-Experte der Bank Sarasin & Cie hatte Bankdaten über die Devisengeschäfte des Nationalbankchefs und seiner Frau an eine externe Person weitergegeben, und sich angezeigt. Er warf Hildebrand vor, den Insider-Tatbestand verletzt zu haben. Dann wurde er selbst angeklagt – wegen Verletzung des Bankengesetzes. Er sei kein Whistleblower, sagte Jean-Pierre Méan,[4] Präsident von Transparency International Schweiz. Denn der Hinweisgeber hätte sich an eine zuständige Instanz wenden müssen, an die Compliance-Stelle seines Arbeitgebers oder die Revisionsstelle der Nationalbank. Er gab die geleakten Informationen jedoch an einen politisch engagierten Anwalt weiter, der sie einem Schweizer Rechtspopulisten zuspielte – und verlor laut Méan

4 Schweizer Fernsehen, 2012: Datenklauer: Gauner oder Held?, in: http://www.videoportal.sf.tv/video?id=c1710330-1347-43a6-b62f-ffadf0d2f331; 3.12.2012.

damit seinen Status als zu schützender Whistleblower. Weiterhin wurde der IT-Angestellte wenige Tage nach seiner Selbstanzeige fristlos entlassen. Hildebrand dementierte währenddessen, die Transaktionen selbst getätigt zu haben, es seien Devisengeschäfte seiner Frau, von denen er erst ihm Nachhinein erfahren habe. Über die Glaubwürdigkeit dieser Aussage und die moralische Verwerflichkeit seiner Tat oder der seiner Frau wurde ausführlich diskutiert in der Schweiz. Der Nationalbankchef trat infolgedessen zurück, bei Prüfungen seiner Finanztransaktionen wurden jedoch keine Regelverletzungen festgestellt.

Die Schuld des Hinweisgebers wurde kaum angezweifelt.

In kleinen Schritten zum Whistleblowerinnen-Schutz

Whistleblowerinnen seien in Deutschland (wie auch in der Schweiz) völlig unzureichend geschützt, so das Whistleblower Netzwerk e. V. 2011.[5] Und das, obwohl bereits im November 2008 beim G20-Gipfel in Seoul formuliert wurde, dass Deutschland bis Ende 2012 gesetzliche Regelungen zum Whistleblowerinnenschutz einführen würde. Am 21. Juli 2011 folgte zusätzlich das Urteil des Europäischen Gerichtshofs für Menschenrechte, der im Fall der Berliner Altenpflegerin Brigitte Heinisch entschied, dass Whistleblowing durchaus von der Freiheit auf Meinungsäußerung gedeckt werden kann. Doch was ist seitdem passiert, wie steht es um den gesetzlichen Whistleblowerschutz in Deutschland kurz vor Ende des Jahres 2012?

Auf eine Kleine Anfrage der Fraktion Bündnis 90 /Die Grünen zum gesetzlichen Whistleblowerschutz antwortete die Bundesregierung am 21. September 2011, dass Hinweisgeberinnen, „die den zuständigen Behörden echte oder vermeintliche Missstände in den Betrieben melden", durch das bestehende Arbeitsrecht bereits ausreichend geschützt seien.[6] Der grünen Bundestagsfraktion reichte das nicht – sie legten als erste Fraktion einen Gesetzentwurf vor, um Whistleblowerinnen arbeits- bzw. dienstrechtlichen Diskriminie-

5 Whistlebloer Netzwerk e. V. 2011: Stellungnahme zum Entwurf der Grünen für ein Gesetz zum Whistleblowerschutz, in: http://www.whistleblower-net.de/blog/2011/11/22/stellungnahme-zum-entwurf-der-grunen-fur-ein-gesetz-zum-whistleblowerschutz/; 3.12.2012.

6 Antwort der Bundesregierung, in: http://dipbt.bundestag.de/dip21/btd/17/070/1707053.pdf; 3.12.2012.

rungsschutz zu gewährleisten und zu regeln, unter welchen Voraussetzungen sie sich an eine außerbetriebliche Stelle oder direkt an die Öffentlichkeit wenden dürfen. Was ist seitdem passiert?

Im Februar diesen Jahres legte die SPD einen Entwurf für ein Whistleblowerinnen-Schutzgesetz vor, die Linkspartei brachte Mitte 2011 bereits einen „Antrag zur Bekenntnis zum Whistleblowerschutz“[7] ein und die Piratenpartei hat sich den Schutz von Hinweisgeberinnen in ihr Grundsatzprogramm geschrieben.[8] Als im Juni ein Gesetzentwurf der Fraktion Bündnis 90/Die Grünen im Bundestag diskutiert wurde, zeigte sich, dass die sowohl CDU/CSU als auch FDP noch immer keinen Regelungsbedarf sehen. Sie sind der Meinung, es gebe bereits genügend Normen zum Schutz von Hinweisgeberinnen, etwa im Arbeitsrecht. „Interne Hinweisgebersysteme“ seien jedoch nötig. Die Verantwortung für die Schaffung solcher Systeme wird den Unternehmen überlassen. Und während in den USA der Senat Mitte November ein Gesetz zum Whistleblower-Schutz verabschiedet hat, rückte ein solches in Deutschland Ende September in vorerst unerreichbare Entfernung. In der Bundestagsdebatte über einen Antrag der Linkspartei zur Erstellungen eines Whistleblowerinnen-Schutzgesetzes Ende September wiederholten die Koalitionsparteien, dass die bestehenden Regelungen völlig ausreichend seien und dass die Vorgaben von G20 unverbindlich seien.

Damit bleibt der Umgang mit Whistleblowerinnen vorerst weiterhin unsicher und ungeklärt – sie werden häufig entlassen, gemobbt oder landen selbst vor Gericht. Da es noch immer keine rechtliche Regelung für Hinweisgeberinnen gibt, sind Angestellte auf das offene Ohr ihres Arbeitgebers oder ihrer Arbeitgeberin angewiesen. Andernfalls bleiben nur Plattformen wie WikiLeaks, die Presse – oder vielleicht der politische Gegner, wie im Falle Hildebrand. Ob Hinweisgeberinnen dann Heldinnen oder Kriminelle sind, scheint von vielen Faktoren abzuhängen. Leider weder von rechtlichen noch einheitlichen.

7 Antrag der Linkspartei, in: http://dokumente.linksfraktion.de/drucksachen/22977_1706492.pdf; 3.12.2012.

8 Grundsatzprogramm der Piratenpartei, Whistleblowerschutz, in: https://wiki.piratenpartei.de/Parteiprogramm#Whistleblowerschutz; 3.12.2012.

Kontrolle

Wer kontrolliert das Netz?

Kirsten Fiedler

Als vor Jahrzehnten das Internet entstand, war bereits klar, auf welche unvermeidliche Frage die Welt zusteuerte: Wer kontrolliert das Netz? Dieser Machtkampf findet nicht nur zwischen der westlichen Welt, Demokratien und repressiven Regimes statt, sondern auch Unternehmen, Strafverfolgungsbehörden, Verbraucher und Aktivisten wollen hier mitmischen.

Auf der einen Seite fordern Vertreter der „Internetfreiheit" – vor allem aus den westlichen Großmächten – die Internet-Regulierung so zu lassen, wie sie ist. Dies bedeutet, die Regulierung in den Händen von kleinen gemeinnützigen Gruppen und ehrenamtlichen Organisationen zu lassen, die hauptsächlich in den USA ansässig sind. Die kalifornische Internet Corporation for Assigned Names and Numbers (ICANN) ist für die zentrale Verwaltung des Internets zuständig und regelt die Vergabe von Domainnamen. Durch Verträge mit ICANN kontrolliert das US-Handelsministerium den Betrieb der Root-Zone des Domain-Namen-Systems (DNS) und kann daher entscheiden, ob ein Namensraum und damit eventuell ein ganzes Land im Internet erreichbar ist.

Auf der anderen Seite gibt es Länder wie den Iran, Russland und China, die mehr Kontrolle und Verwaltung auf nationaler Ebene fordern und teilweise bereits ausüben. Dabei ist es verständlich, dass einige Staaten mehr als unzufrieden mit der jetzigen Situation sind und nicht länger dem US-Handelsministerium das letzte Wort in Fragen der Internet-Regulierung überlassen wollen. Manche fordern sogar die Schaffung einer neuen internationalen Institution, die sich ausschließlich mit Netzpolitik befasst. Da dies jedoch eher unrealistisch ist, wurde Ende des Jahres versucht, als Übergangslösung das Mandat der intransparenten und bürokratischen Internationalen Fernmeldeunion (ITU) auf den Bereich der Internet-Regulierung zu erweitern.

Welchen Einfluss Regierungen auf das Internet haben können, sieht man nirgends so deutlich wie in China. Wie auch der Iran baut sich die selbstbewusste Volksrepublik ein eigenes nationales Netz auf. Und dieses Netz entfernt und unterscheidet sich nicht nur sprachlich, sondern auch ideologisch und architektonisch vom westlichen Internet. Wer nun nach dem Arabischen

Frühling denkt, dass das Internet geschlossene Gesellschaften öffnet, geht irrtümlicherweise davon aus, dass das Internet eine exogene und konstant offene Kraft ist. Die Offenheit des Internets ist jedoch von vielen Faktoren abhängig. Staaten haben nicht nur die Macht, die Architektur des Internets zu gestalten, sie beeinflussen und prägen zudem ganz unterschiedliche Visionen dazu, wie das Internet aussehen sollte.

Die Fronten verhärten sich aber nicht nur zwischen autoritären Regierungen und der westlichen Welt, sondern auch zwischen verschiedenen Online-Industriezweigen, Verbrauchern, Bürgern, Hackern und Strafverfolgungsbehörden.

Anfang 2012 fanden in den Vereinigten Staaten Proteste gegen die US-Gesetzentwürfe SOPA und PIPA, die zu einer umfassenden Internetzensur und Einschränkungen der Meinungsfreiheit geführt hätten, statt. Tausende Bürger, Wikipedia, Google und Journalisten wehrten sich erfolgreich gegen die repressiven Vorschläge der mächtigen Film- und Musikindustrie. Einige Monate und Massenproteste später kippten Internetaktivisten dann auch das internationale Urheberrechtsabkommen ACTA in Europa. Währenddessen spielte sich in Neuseeland ein anderer Krimi ab: Als Antwort auf die mediatisierte Megaupload-Razzia schwor das Hacker-Kollektiv Anonymous Rache und legte kurz darauf die Seiten des FBI und des US-Justizministeriums lahm. Im März änderte Google seine Datenschutzerklärung und vereinheitlichte die Nutzungsbedingungen von rund 60 verschiedenen Diensten. Eine Analyse der EU-Datenschutzbehörden ist zu dem Schluss gekommen, dass diese AGBs nicht dem europäischen Datenschutzrecht entsprechen und das Recht auf Privatsphäre verletzen. Im Sommer sperrte Microsoft plötzlich das Cloud-Konto eines Niederländers, der angeblich „unerwünschte" Inhalte hochgeladen hatte. Der US-Konzern behält sich in den Nutzungsbedingungen vor, Konten „jederzeit unangekündigt und ohne Angabe von Gründen zu kündigen oder zu sperren".

Dies verdeutlicht eine weitere politische Herausforderung des Internets: Obwohl es als öffentlicher Raum wahrgenommen und genutzt wird, ist die Infrastruktur des Internets in den Händen von Privatunternehmen. Die meisten von ihnen haben ihren Sitz in Silicon Valley und entscheiden von dort, was der Rest der Welt im Internet sehen und sagen darf. US-Unternehmen drücken uns ihre Moralvorstellungen auf, was dann zum Beispiel dazu führt, dass wir die Autovervollständigung bei Google.de nicht mit den Worten

Arschloch oder Vagina benutzen können oder dass schwule Comics im iTunes Store gelöscht werden. Eine zentrale Frage ist also, ob wir privaten Unternehmen, deren Geschäftsprioritäten sich ständig und auf unvorhersehbare Weise ändern, wirklich die Verantwortung für den Erhalt des Internets überlassen wollen.

Diese vielen kleinen und größeren Spannungen machen deutlich: Wir befinden uns bereits mitten im Kampf um das Internet und die Frage, wer es kontrolliert. Das bisherige System kriselt an allen Ecken und Enden; vor allem an vier Fronten wird gekämpft: Die erste ist das Urheberrecht. Information will frei und ungehindert fließen, so heißt es, und jede Tat im Internet setzt eine Kopie voraus. Künstler jedoch wollen weiterhin an ihren Werken verdienen und Rechteinhaber schärfer gegen Piraterie vorgehen. Die zweite Front ist die der Souveränität. Per Definition ist ein grenzenloses System, das sich wenig um Geographie schert, eine Herausforderung für Nationalstaaten. Die dritte verhärtet sich rund um den Datenschutz. Anonymität im Internet ist wichtig für Kreativität und für politische Dissidenten sogar lebenswichtig – das Recht auf Datenschutz ist ein Grundrecht. Andererseits wollen sich Behörden nicht die Chancen nehmen lassen, die das digitale Zeitalter bietet und auf mehr Daten zugreifen können als jemals zuvor. An der vierten Front rund um Fragen der Sicherheit bekriegen sich Cyber-Sicherheitsexperten, Innenministerien, Hacker und Cypherpunks.

Die Weltkonferenz zur internationalen Telekommunikation (WCIT) der ITU war jedenfalls nur ein Schauplatz unter vielen, auf denen die Frage der Kontrolle über das Netz diskutiert wurde. Weitere Machtkämpfe kommen auf uns zu und lassen Szenarien wie „westliche Welt gegen China“ oder „westliche Welt gegen arabische Staaten“ immer realistischer werden. Aber auch Unternehmen, Bürgerrechtsorganisationen und Hacker-Kollektive haben alle ihre eigenen Vorstellungen, was die Zukunft des Internets betrifft. Eines steht fest: In den kommenden Jahrzehnten werden die Kämpfe zwischen den Staaten und ihren nationalen netzpolitischen Ideologien entscheiden, wie das Leben im Internet aussehen wird.

Die Politik der Internet Governance

Ben Scott und Tim Maurer

Blickt man auf das Jahr 2012 zurück, sieht man einen bemerkenswerten Aufstieg der Internet Governance: von einer diplomatischen Randnotiz zu einem Top-Thema der Außenpolitik. Dafür gibt es eine Reihe an Gründen – die meisten davon mit Geld und Politik zu tun. Mehr als zwei Milliarden Menschen sind heutzutage online, und diese Zahl steigt zusehends, vor allem in Entwicklungsländern. Das führt dazu, dass immer mehr Regierungen erkennen, dass das Internet eine mächtige Kraft in modernen Gesellschaften darstellt. Wie das Internet geregelt wird, bestimmt, wer diese Macht zu welchem Zweck nutzen kann. Die offensichtlichsten Auswirkungen sind finanzieller Natur. Jede Regierung möchte für seine eigene nationale Wirtschaft mehr Wohlstand aus dem Internet generieren und potenzielle Vorteile gegenüber Nachbarn und Konkurrenten gewinnen. Aber eine ebenso starke Motivation ist der katalysierende Einfluss des Internets auf politische Bewegungen – dies wurde vor allem während den Revolutionen im Arabischen Raum deutlich. Die Gegenreaktion auf diese Bewegungen ist nicht nur Gewalt und Krieg, sondern auch das starke Bemühen amtierender Alleinherrscher, Kontrolle über die Informationsnetzwerke zu erlangen, die anscheinend eine Rolle beim Sturz anderer Diktatoren gespielt haben.

Deshalb haben Großunternehmen und mächtige Staaten zunehmend nach Wegen zu gesucht, wie sie Einfluss auf das Internet ausüben können. Was sie entdeckt haben, hat sie jedoch frustriert. Die Regulierungsstruktur des Internets ist ziemlich unkonventionell. Und es ist schwierig, den Prozess für eigene politische Zwecke zu missbrauchen. Jede nationale Regierung hat zwar Kontrolle über den Teil des Netzwerks, der in ihren Grenzen liegt. Aber die grenzüberschreitenden Mechanismen des Internet (beispielsweise wie Daten durch das weltweite Netzwerk hin und hergeleitet werden) werden fast alle von Nichtregierungsorganisationen entschieden, die von Technokraten ohne nationale Agenda oder Loyalität geleitet werden. In diesem sogenannten „Multi-Stakeholder" Modell verwalten nationale Regierungen, international einberufene Institutionen, technische Normierungsgremien und technokratische NGOs jeweils einen oder mehrere wichtige Bestandteile des Internets.

Und jede dieser Organisationen wird informiert durch die komplexe und manchmal chaotische Beteiligung von Experten aus Staat, Unternehmen und Zivilgesellschaft.

Kurz gesagt regelt eine Buchstabensuppe aus Abkürzungen von Organisationen die wichtigste Informations-Infrastruktur der Weltgeschichte. Und als wäre das nicht bemerkenswert genug, ist die größere Überraschung, dass es genau so entworfen wurde – und eigentlich auch ziemlich gut funktioniert. Das dezentrale System der technokratischen Verwaltung entstand in den frühen Tagen des Internets als eine Kompromisslösung, um die Interessen von Regierungen und Unternehmen auszugleichen – die beide das Internet bestimmen wollten. Die Lösung war, beide Seiten mitspielen zu lassen – aber nur in Verbindung mit der Zivilgesellschaft und durch einen auf Konsens basierendem Prozess, der von Dritten geregelt wird. Deshalb haben wir ein „Multi-Stakeholder" Modell der Internet-Governance. Es schleift die Kanten der politischen und wirtschaftlichen Eigeninteressen der beteiligten Akteure, indem ein transparenter und beteiligender Prozess erzwungen wird, der technische Effizienz und häufig Konsensentscheidungen benötigt.

Das dezentrale System der Internet Governance ist konzipiert, Dinge auf technischer Ebene zu verändern und zwar nur nach eingehenden Diskussionen aller Beteiligten. Diese Eigenschaften machen es für Regierungen im Multi-Stakeholder Modell sehr schwierig, ihren Willen einer besseren wirtschaftlichen und politischen Kontrolle über das Netzwerk durchzusetzen. Dazu müssten sie schließlich ein halbes Dutzend oder mehr Institutionen überzeugen, von denen keine besonders gut auf politischen Druck reagiert. Die natürliche Reaktion dieser Nationalstaaten 2012 war der Versuch, internationale Kontrolle über das Internet zu zentralisieren, um die Nutzung dieser Kontrolle leichter zu für eigene Zwecke instrumentalisieren zu können. Also wendeten sie sich an die Internationale Fernmeldeunion ITU – eine UN-Organisation, die seit über einem Jahrhundert die technische Funktionsweise weltweiter Telekommunikations-Netzwerke verwaltet hat. Als zwischenstaatliche Organisation ist sie der einzige Akteur im Multi-Stakeholder Modell, der möglicherweise die verteilte Entscheidungsfindung des derzeitigen Systems aushebeln könnte. Dabei ist es egal, dass die ITU bisher nur eine kleine Rolle in der Internet Governance gespielt hat, denn sie ist die einzige logische Wahl

für Staaten, die das Multi-Stakeholder Modell zugunsten eines zentralen Entscheidungsgremiums abschaffen wollen, das die Verteilung politischer und wirtschaftlicher Macht im Internet schnell verändern kann.

Und so wurde die ITU zu einem Kampfplatz zwischen Nationalstaaten und Interessengruppen, von denen beide die internationale Organisation für ihre eigenen Zwecke nutzen und diese von einer UN-Organisation abgesegnet sehen wollen. Den USA und Europa (und den meisten Industriestaaten) wäre es am liebsten, den Status Quo zu erhalten – also die ITU aus der Internet Governance rauszuhalten. Das pluralistische Modell der Internet Governance hat für diese Staaten gut funktioniert und sie sehen keinen Grund, das zu ändern – und schon gar nicht, die zentrale Autorität an eine einzige politische Bürokratie bei der ITU zu übergeben. Eher autoritäre Staaten (z. B. Russland und China) sehen eine Möglichkeit darin, die ITU dazu zu bringen, Macht von anderen Regierungsinstitutionen zu übernehmen und Internet-Politik weltweit zu regeln. Das würde der ITU die Möglichkeit geben, nationale Regierungen (mit dem expliziten Segen einer UN-Organisation) zur Ausübung größerer wirtschaftlicher und politischer Kontrolle über das Netzwerk zu ermächtigen, indem sie ihnen Macht über technische Aufgaben gibt, die derzeit von multinationalen NGOs verwaltet werden. Diese Umverteilung von Macht würde auf Kosten von freien Märkten und freier Meinungsäußerung im weltweiten Internet geschehen. Schwellen- und Entwicklungsländer streben nach einer besseren Vertretung in Internet Governance Institutionen und Lösungen für ihre Anliegen von bezahlbarem Zugang, Wirtschaftswachstum, Netzwerk-Management und IT-Sicherheit.

Anders ausgedrückt: jeder achtet auf seine eigenen Interessen bei dem Versuch, die Rolle der ITU zu gestalten. Die Belastung, die all das auf das bestehende Multi-Stakeholder-Modell ausübt, ist erheblich. Und abhängig vom Ausgang werden die Debatten von 2012 erhebliche Auswirkungen auf die Zukunft grundlegender Prinzipien des Internets haben, auf Meinungsfreiheit, Datenschutz, Sicherheit und offene Märkte. Natürlich steht auch eine Menge Geld auf dem Spiel für verschiedene Akteure der digitalen Wirtschaft. Aus diesem Grund — der Gefahr/Chance, die Zukunft des Internets zu gestalten —, hat Internet Governance an Bedeutung gewonnen.

Der Höhepunkt 2012 passierte ganz zum Schluss. Während wir diesen Text veröffentlichen, treffen sich Diplomaten aus 193 Staaten in Dubai zur ITU Weltkonferenz zur internationalen Telekommunikation (WCIT), um eine

überarbeitete Version der Internationalen Telekommunikations-Regulierungen (ITR) zu diskutieren. Dieser Vertrag regelt derzeit die Koordination internationaler Telefonnetze. Der große Kampf dreht sich darum, ob der Vertrag in großen oder kleinen Teilen erweitert wird, um auch das Internet zu regulieren. Insbesondere geht es in der Debatte darum, ob die Befugnisse über das Internet von bestehenden dezentralen Institutionen (die einen Multi-Stakeholder-Entscheidungsfindungsprozess haben) weggenommen und bei der ITU geparkt werden (deren Entscheidungen ausschließlich zwischenstaatlich sind). Dies ist die neueste Schlacht innerhalb einer breiteren politischen/philosophischen Debatte zwischen vielen Staaten, ob die Macht über das Internet verteilt oder zentralisiert sein soll.

Darüber hinaus ist die ITU nicht nur *nicht* Multi-Stakeholder, sondern auch *nicht* transparent. Nur Regierungsvertreter dürfen entscheiden. Zivilgesellschaft und Vertreter des Privatsektors haben kein Stimm- und wenig Mitspracherecht. Praktisch nichts über die eingereichten Vorschläge oder das Verfahren der Debatte und Entscheidung wird veröffentlicht (auch wenn die ITU auf heftige Kritik reagierte und Vorhaben bis zu einem gewissen Grad geöffnet hat). In den Monaten vor der WCIT wurden Leaks zum primären Mittel öffentlicher Beurteilung der Vorgänge. Klar ist, dass viele Regierungen versuchen, die Konferenz zu nutzen, um die staatliche Kontrolle über das Internet (und somit ihre eigene Macht über die politische Ökonomie des Netzwerkes) zu erweitern. Die Gründe reichen von Versuchen, politische und wirtschaftliche Vorteile zu erlangen bis zu legitimeren Bedenken wie einem erschwinglichem Zugang zum und Vertretung im Regelungsprozess. Jeder der ITU-Mitgliedstaaten kann einen Vorschlag zur Prüfung bei der WCIT einreichen – wird er in die ITRs aufgenommen, können die Änderungen Teil des verbindlichen internationalen Vertrags werden. Das ist von großer Bedeutung und hat dementsprechend enorme Aufmerksamkeit für und Interesse an einem Feld erzeugt, das bisher in außenpolitischen Kreisen unbekannt oder unterschätzt war.

Eine Vielzahl von aggressiven Vorschlägen wurde im Vorfeld von Regierungen ins Spiel gebracht. Besonders besorgniserregend war beispielsweise ein russischer Antrag. Das Dokument, das nur wenige Wochen vor der WCIT an die Öffentlichkeit gebracht worden war, schlägt eine Überarbeitung des Vertrags vor, um eine Neugestaltung des Internets zu ermöglichen und es nationalen Regierungen zu erleichtern, den Netzwerkdatenaustausch zu überwa-

chen, Menschenrechte zu verletzen und den kommerziellen und politischen Austausch über Grenzen hinweg zu behindern. Alles im Namen der nationalen Sicherheit. Ein anderer Vorschlag lief darauf hinaus, den Telefonunternehmen (die meist auch Internetanbieter sind) durch staatliche Eingriffe und Protektionismus einen größeren Anteil am wirtschaftlichen Potential des Internets zu verschaffen. Diese Idee beinhaltet die Einführung diskriminierender Gebühren für unterschiedliche Arten von Datenverkehr, abhängig von Quelle, Ziel oder Inhalt. Würde das umgesetzt, würde diese Änderung das grundlegende Funktionsprinzip des Internets aushebeln – dass alle Inhalte im Netzwerk (unabhängig von Quelle, Besitz, Ziel oder Inhalt) das gleiche Recht auf Zugang zum Transfer von Sender zu Empfänger haben. Was auch immer bei der WCIT passiert, eins ist klar: diese Debatten werden nicht in nächster Zeit gelöst werden. Das ist eine neue Arena des internationalen Wettbewerbs um politische und wirtschaftliche Bedrohungen und Vorteile. Die WCIT wird die wichtigsten Themen für die kommenden Jahre vorzeichnen. Einige Themen werden verblassen, wenn sie es nicht schaffen, ausreichend Unterstützung in Dubai zu finden. Andere Themen werden im formalen Rahmen des Wettbewerbs noch hitziger. Und neue Themen werden auftauchen, wenn die Diskussionen die Wünsche der Staaten und Regionen und die Möglichkeiten zu Kompromissen und Allianzbildung offenbaren.

Hier ist eine Vorschau der wichtigsten Themen – wonach man Ausschau halten sollte in den Berichten über die WCIT und welche Themen in der Debatte der nächsten Jahre sehr wichtig sein werden, wenn Internet Governance auf der großen Bühne der Außenpolitik bleibt.

Nationale Regierungen vs. Multi-Stakeholder

Jede nationale Regierung hat Kontrolle über das physische Netzwerk innerhalb ihrer Grenzen. Sie kann Inhalte zensieren, überwachen, und die festlegen, welche Arten von kommerziellen und politischen Aktivitäten zulässig sind. Sie können international unter politischen Druck gesetzt werden, wenn sie Menschenrechte und die Prinzipien des freien Marktes verletzen. Das könnte erhebliche Konsequenzen haben, die sich in geringeren Investitionen und einem verminderten moralischen Ansehen in der internationalen Gemeinschaft ausdrücken. Doch jenseits dieser Möglichkeiten gibt es wenig, das die internationale Gemeinschaft tun kann, um nationale Regierungen davon abzuhalten, ihre Netzwerke so zu regulieren, wie sie es für richtig halten. Al-

lerdings kontrollieren Nationalstaaten *nicht* die technischen Kern-Themen, wie zum Beispiel: das effizienteste Routing des Datenverkehrs, die Vergabe von Adressen Namen und Nummern sowie die Entwicklung von technischen Standards für Netzwerke und Geräte, die mit dem Internet verbunden sind. Diese Themen werden alle transnational in einem Multi-Stakeholder Modell entschieden. Nationale Regierungen, die sich gegen diese Entscheidungen wenden, riskieren, sich selbst von den wirtschaftlichen Vorteilen eines weltweiten Handelsplatzes Internet abzuklemmen.

Wenige haben dies bisher getan – was die Bedeutung dieser Interkonnektivität unterstreicht. Würde allerdings die Kontrolle technischer Funktionen des Internets von dem globalen Multi-Stakeholder Prozess auf Nationalstaaten übertragen, würde dies eine fundamentale Änderung in der Internet Governance bedeuten. Dieser Bereich muss genau beobachtet werden. Damit die ITU diese Änderung vornimmt, bräuchte es eine Abstimmung der Mitgliedstaaten, den ITR-Vertrag zu ändern und den Nationalstaaten somit diese Macht zu gewähren. Das ist unwahrscheinlich, aber nicht unmöglich. Trotzdem gibt es eine Vielzahl an Möglichkeiten, wie die derzeitigen Befugnisse des Multi-Stakeholder Modells ausgehöhlt und an Nationalstaaten übertragen werden können. Diese Themen werden in den nächsten Jahren kontrovers bleiben. Die zentrale Frage ist, ob die technischen Institutionen des Multi-Stakeholder-Modells ausreichend repräsentativ für die InternetnutzerInnen dieser Welt werden können, so dass die Kritik des politischen Ungleichgewichts abgestumpft wird und mehr Regierungen das aktuelle Modell begrüßen.

Routing von Datenverkehr im Internet

Das Internet wurde geschaffen, um die technische Effizienz beim Verschieben von Daten zu maximieren und nicht die politische Kontrolle über Inhalte. Daraus resultiert, dass bei der Übertragung von Daten durch das Netz deren Weg nicht etwa nationalen Grenzen oder politischen Allianzen entspricht, sondern dem effizientesten Weg. Jede Mail, jede Webseite, jede Datei die zwischen NutzerInnen versendet wird, wird in kleine Datenpakete zerlegt und auf verschiedenen Wegen durch das Internet geschickt, eh sie an ihrem Zielort wieder zusammengesetzt wird. Manchmal bedeutet das, dass Pakete einer einzigen Mail die halbe Welt durchqueren, um ein Nachbarland oder sogar eine andere Stadt im selben Land zu erreichen. Nationale Grenzen spielen

daher eine untergeordnete Rolle im Routing von Datenverkehr. Einige der wichtigsten Router des globalen Internets befinden sich in westlichen Staaten – ein erheblicher Spannungspunkt für andere Staaten.

Einige Regierungen lehnen diese Art des Routings ab, weil es bedeutet, dass der Internetverkehr aus ihrem Land Router passieren muss, die außerhalb ihrer Kontrolle liegen. Sie möchten gerne nationale Grenzen beim Routen erstellen. Das birgt die Gefahr, das Routen von Traffic ineffizienter zu machen. Wichtiger ist jedoch, dass dadurch ein Tor zu mehr Restriktionen der freien Meinungsäußerung und offenen Märkten geöffnet wird, wenn Staaten mehr Kontrolle über das internationale Telekommunikationssystem erhalten. Zu Ende gedacht, würde eine Kontrolle über das Routing im Internet auf nationalstaatlicher Ebene dazu führen, dass die Nutzbarkeit des Netzwerks nachlässt und eine Zentralisierung politischer Kontrolle über Inhalte stattfindet. Dieses Thema wird in den nächsten Jahren heiß umkämpft sein.

Das wirtschaftliche Modell des Internets

Der überwiegende Datenverkehr wird von privaten Unternehmen transportiert, welche die physischen Netzwerke besitzen. Die größten Internet Service Provider (ISPs) tauschen oft gebührenfrei Traffic untereinander aus, in Zusammenschlüssen die als „Peering" bekannt sind. Die Netzwerkbetreiber generieren ihren Umsatz aus den Gebühren der EndanwenderInnen, die dafür zahlen, Inhalte zu produzieren und ins Netz zu stellen oder sie runterzuladen und zu konsumieren. Seit seiner Gründung beruhte das Internet auf dem „End-to-End" Prinzip. Dieses Prinzip besagt, dass alle Netzwerkbetreiber den Datenverkehr ohne Diskriminierung behandeln. Das wiederum bedeutet schlichtweg, dass keine Online-Inhalte eine besondere Behandlung (zum Beispiel schnellere Überbringung) aufgrund des Senders oder Empfängers erhalten – oder desjenigen, der einen Zuschuss für die besondere Behandlung zahlen kann. Das Ende-zu-Ende Prinzip schaffte einen fruchtbaren Boden für Innovationen, da jeder Content-Entwickler und Dienstleister – von Skype über YouTube bis zu individuellen NutzerInnen – exakt die selben Rechte und Chancen hat, das Netz zu nutzen.

Zu Beginn diesen Jahres legte die European Telecommunication Network Operators Association (ETNO) einen Vorschlag vor, der das Ende-zu-Ende Prinzip gefährdete. Darin wurde vorgeschlagen, Unternehmen das Abschließen von kommerziellen Verträgen zu erlauben, die eine Diskriminierung von

bestimmten Datenpaketen vorsehen. Dies würde das Ende-zu-Ende Prinzip stürzen und durch ein „Pay-to-Play" ersetzen, bei dem InternetnutzerInnen das Recht erwerben müssten, bevorzugt vor anderen Online Inhalten behandelt zu werden. Dies hätte den Effekt, dass die qualitativ hochwertigen Dienstleistungen für große Geschäftskunden reserviert werden würden und nicht-kommerzielle Internet-Inhalte auf diejenige Bandbreite verwiesen werden, die ihnen überlassen werden kann.

Auch wenn es verlockend ist für Unternehmen, diskriminierende Preismodelle zu erschaffen und durch unterschiedliche Preise für verschiedene Produkte die Gewinne zu erhöhen, verringert dies den Nutzen für NutzerInnen und erstickt zukünftige Innovationen. Obwohl dieser Vorschlag ursprünglich von europäischen Telekommunikationsunternehmen gemacht wurde, wird er nun von einigen Entwicklungsländern als ein Weg begrüßt, ausländische Anbieter von Inhalten zu besteuern, um die Entwicklung lokaler Netzwerke zu subventionieren. Auf kurze Sicht könnte dies die Einnahmen erhöhen, auf lange Sicht wäre es jedoch schlecht für das gesamte Internet-Ökosystem, weil jedes Land ein Vergütungs-System von diskriminierenden Netzentgelten einführen würde. Unglücklicherweise wäre dies besonders schädlich für Entwicklungsländer, die Content- und Dienstleistungs-Branchen entwickeln möchten und dringend die Möglichkeiten brauchen, die durch freie Märkte und ein End-to-End Internet geboten wird. Dss zeigt auch die Ablehnung des ETNO-Vorschlags durch die europäischen Regierungen. Es gibt andere, bessere Wege zu Umsatzgenerierung und neuen Geschäftsmodellen für Netzwerkbetreiber, die keine Zerstörung der grundlegenden Prinzipien des Internets vorsehen.

Transparenz

Die Geschichte des Internets zeigt, dass die konkurrierende Suche nach effizienten und einfachen Lösungen ihr volles Potenzial nur in einer transparenten und offenen Umgebung entfalten kann, so dass die TeilnehmerInnen neue Standards und Instrumente hinterfragen und beurteilen können. Traditionelle zwischenstaatliche Prozesse finden üblicherweise unter einem Mantel der Geheimhaltung statt und passieren mit einer Geschwindigkeit, die nicht mit dem dynamischen Tempo des technologischen Fortschritts mithalten kann. Darüber hinaus ist die Vorbereitungsphase der WCIT nicht transparent genug gewesen und wurde der Einbeziehung von wichtigsten Akteu-

ren, trotz einiger Bemühungen den öffentlichen Input zu erhöhen, nicht gerecht. Öffentliche und offene Konsultationen mit Akteuren aus der ganzen Welt fehlten weitgehend.

Da die Anzahl von Internet Governance Entscheidungen steigt, erhöht sich auch die Bedeutung von transparenten und inklusiven Prozessen. Besonderes Augenmerk sollte darauf gelegt werden, ob sich das Internet Governance Forum (ein jährliches Treffen für den Dialog zwischen Stakeholdern) zu einem prominenteren Part der internationalen Internet Governance entwickelt. Das Gebot der Transparenz hat sich zu einem festen Bestandteil der Empfehlungen zur Verbesserung von bestehenden Verfahren durch NGOs entwickelt. Zum Beispiel betonten zivilgesellschaftliche Gruppen, die sich dieses Jahr auf der Best Bits Konferenz in Baku versammelten, einen transparenten Prozess als Schlüssel zum Vertrauensaufbau in Entscheidungsfindungsverfahren von Multi-Stakeholdern. In den kommenden Jahren werden wir sehen, ob diese Aufrufe beachtet werden und Änderungsvorschläge für Governance Entscheidungen öffentlich gemacht werden, mit ausreichend Zeit für zivilgesellschaftliche Gruppen, um kommentieren und Feedback geben zu können. Ein weiterer wichtiger Punkt ist, ob die Sitzungen der WCIT (und andere wichtige Internet Governance Sitzungen) öffentlich sind und als Live-Webcasts mit Video, Audio und Text-Transkripten zur Verfügung gestellt werden, um eine Beteiligung aller zu ermöglichen, einschließlich Menschen mit Behinderungen. Diese Maßnahmen werden dazu beitragen, effektive High-Level Prinzipien zu entwickeln, die dauerhaft halten und Menschenrechte sowie nachhaltiges Wirtschaftswachstum fördern.

Die Rolle der ITU, die Zukunft des Internets zu formen

Der aktuelle politische Wettbewerb, der sich bei der ITU abspielt, bedeutet nicht, dass sich die Institution zwischen zentraler Dominanz der Internet Governance oder dauerhafter Irrelevanz entscheiden muss. Die ITU ist ein Teil des Multi-Stakeholder Prozesses und eine von vielen Quellen, die einen Beitrag zur Verbesserung der Internet Governance leisten. Zum Beispiel hat die ITU ein Standardisierungsgremium, das technische Themen für verschiedene Arten von Protokollen zum Routen des Internet Traffics diskutiert. Diese s Gremium kann ein wichtiger Ort für die Diskussion mit anderen internationalen Institutionen bleiben – getrieben von Technik und Wissenschaft, eher als von Politik. In der ITU gibt es auch eine Gruppe, die sich Entwicklungsfra-

gen widmet und der Lösung von Technologie- und Telekommunikationsproblemen, die für Schwellenländer wichtig sind. Die ITU spielt eine wichtige Rolle beim Schließen der digitalen Spaltung und beim weltweiten Aufbau von Kapazitäten. Sie bietet nützliche Daten durch ihre Forschung und Bemühungen zum Auf- und Ausbau von Breitbandverbindungen. Insbesondere spielt die ITU eine führende Rolle für die Erreichung des Millennium-Entwicklungsziels 8F, das „die Vorteile der neuen Technologien zur Verfügung stellen" will, und auf die Vorteile „insbesondere der Informations- und Kommunikationstechnologie" zielt. Die acht Millennium-Entwicklungsziele sind seit dem Jahr 2000 das Flaggschiff-Programm der internationalen Gemeinschaft, um die Armut weltweit zu reduzieren. Die ITU sollte weiterhin ihre wichtige Entwicklungsarbeit fortführen und ihre Aktivitäten ausweiten, um Menschen weltweit einen erschwinglichen Zugang zu neuen Kommunikationstechnologien ermöglichen und denjenigen mit besonderen Bedürfnissen eine stärkere Stimme zu verleihen. So könnte die ITU einen nachhaltig positiven Einfluss auf die Zukunft des Internets haben und ein wertvolles Erbe hinterlassen.

Von Selbstregulierung zur Zensur durch private Unternehmen

Joe McName

Was macht es bloß mit der Welt, dieses unkontrollierbare Ding namens Internet? Terrorismus, Kinderpornographie und Drogenhandel: Das Netz muss heutzutage für vieles herhalten. Die Frage, wie sich gegen illegale Inhalte im globalen Netz vorgehen lässt, bereitet Regierungen weltweit Kopfzerbrechen. Da der technische Fortschritt meist schneller ist als die Gesetzgebung, sehen viele Politiker die Lösung in der Entwicklung neuer Regulierungsmechanismen, wie der sogenannten „Selbstregulierung".

Selbstregulierung wird seit einiger Zeit im Bereich der Internetwirtschaft eingesetzt, um Unternehmen in der sich schnell entwickelnden Welt der Informationstechnologien mehr Flexibilität zu geben und Verbraucher und Netzwerke effizienter zu schützen – vor Problemen wie Spam zum Beispiel. Mittlerweile werden Provider jedoch mehr und mehr unter dem Motto der „Selbstregulierung" dazu gezwungen oder ermuntert, die eigenen Kunden zu überwachen und sogar zu bestrafen. Dies hat nicht mehr viel mit „Selbst"-Regulierung zu tun – denn anstatt interner Prozesse der Unternehmen werden hier die Nutzer kontrolliert.

Mit diesem Thema beschäftigt sich European Digital Rights (EDRi) nun schon seit mehreren Jahren.[1] Unsere Organisation beobachtet und kritisiert diesen wachsenden Trend, der immer häufiger als „einfache" Lösung gewählt wird, um politischer Ziele zu erreichen und gleichzeitig hierfür weniger Verantwortung übernehmen zu müssen. Daraus resultierte in den letzten Jahren eine Flut von regionalen, nationalen und supranationalen Initiativen, die tiefgreifende Auswirkungen auf den offenen, demokratischen und innovativen Charakter des Internet haben.

Denn die Politik übersieht meist die Tatsache, dass diese entartete Form der Selbstregulierung zu einer regelrechten Privatisierung der Rechtsdurchsetzung führt und die Grundrechte gefährdet. Maßnahmen, die vom privaten

1 EDRi Broschüre: The slide from selfregulation to corporate censorship, in: http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf

Sektor beispielsweise zur Bekämpfung von Urheberrechtsverletzungen durchgeführt werden, haben oft Vorrang vor dem Recht auf Privatsphäre und freie Meinungsäußerung. Ein Beispiel sind Selbstregulierungs-Projekte, wie die CEO Coaltion – das Bündnis für ein kindersicheres Internet, die regelmäßig von der EU-Kommission angestoßen werden. Sie enthalten zumeist nette Ansammlungen von Maßnahmen, die sich zwar ganz gut vermarkten lassen und nicht viel kosten, die der Kommission jedoch auch leider als Ausrede dienen, anstatt ernsthaft und effizient gegen Straftaten vorzugehen. Dies führt dann dazu, dass fast nie versucht wird, vor dem Start der Projekte das Problem genau zu identifizieren oder sich auf Fakten und Folgenabschätzungen zu stützen – denn eigentlich interessiert sich niemand so wirklich für die Effizienz der Maßnahmen oder gar den Kern des Problems.

Wir befinden uns nun an einem Scheidepunkt, an dem der Begriff der Selbstregulierung im herkömmlichen Sinne mehr und mehr als eine Weiterentwicklung der Rechtsdurchsetzung interpretiert und kommuniziert wird und Unternehmen in extremen Fällen zu Polizei, Richter, Geschworenen und Henkern gemacht werden, um gegen mutmaßliche Verstöße vorzugehen und so die Haftung für Taten ihrer Kunden zu vermeiden. Es ist jedoch mehr als fraglich, ob es Providern gestattet sein darf, im eigenen Interesse oder um politische Ziele zu verwirklichen, in den Internetverkehr einzugreifen. Regierungen weltweit sind derzeit dabei, hier irreversible Entscheidungen zu treffen, die sich negativ auf die Offenheit und die Demokratie, Transparenz und die Innovation im Internet auswirken.

Natürlich ist es nicht das erklärte Ziel, einen privatisierten Polizeistaat zu schaffen. Vielmehr werden durch einzelne Projekte und Initiativen das traditionelle Konzept der Rechtsstaatlichkeit und der Rolle der Justiz aufgelöst. Das Resultat ist daher der Tod auf Raten der traditionellen Strafverfolgung und justizielle Transparenz. Ad hoc Überwachungsmaßnahmen, die Unternehmen aufgezwungen werden, haben zudem zur Folge, dass weniger effiziente und weniger abschreckende Maßnahmen vom Staat ergriffen werden.

Im letzten Jahr konnten wir einige Initiativen und Projekten stoppen, die eine Privatisierung der Rechtsdurchsetzung im Sinn hatten. Das prominenteste Beispiel hierfür war das internationale Handelsabkommen ACTA.[2] ACTA sollte die Vertragspartner dazu verpflichten, „Kooperationsbemühungen im

2 Digitale Gesellschaft, ACTA : Häufig gestellte Fragen, in: https://digitalegesellschaft.de/2012/02/acta-haufig-gestellte-fragen/; 5.12.2012.

Wirtschaftsleben“ zu fördern, um im digitalen Raum das Urheberrecht durchzusetzen. Dies heißt konkret, dass die Film- oder Musikindustrie Vereinbarungen mit Providern trifft, um Kunden den Zugang zu Tauschbörsen zu sperren. ACTA wollte gezielt außergerichtliche Überwachung und Sanktionen legitimieren und vorantreiben.

Durch einen Leak brachte EDRi in diesem Jahr ein weiteres Projekt, das eine privatisierte Rechtsdurchsetzung fördern wollte, an die Öffentlichkeit. Boingboing beschrieb das Projekt als das dümmste Paket netzpolitischer Regelungen in der gesamten Menschheitsgeschichte.[3] Das von der EU-Kommission geförderte Clean IT- Projekt sollte Provider zur Selbstzensur ermuntern, „freiwillige Verhaltensregeln“ aufstellen, um die „terroristische Nutzung des Internets einschränken“ und die „illegale Nutzung des Internets bekämpfen“.

Aber auch in unscheinbare Initiativberichte im EU-Parlament schleichen sich ab und zu ähnliche Bestrebungen ein, wie eine kleine Passage im Bericht zum Online-Vertrieb von audiovisuellen Werken[4] in der EU im Sommer 2012 – kurz nach der Ablehnung des ACTA-Abkommens. Der Berichtsentwurf enthielt einige problematische Paragraphen zur Providerhaftung. Er forderte die Kommission unter anderem dazu auf, die „gegenwärtige Tendenz, Betreiber in Bezug auf die Durchsetzung der Rechte des geistigen Eigentums im Internet von ihrer Verantwortung zu entbinden, umzukehren“. Dies ist nicht nur sachlich falsch, es hätte zudem zu einer Privatisierung der Zensur geführt und die Missachtung rechtsstaatlicher Prinzipien bei der Rechtsdurchsetzung gefördert. Durch EDRis Aktivitäten hinter den Kulissen wurde dieser Teil des Berichts dankenswerterweise bei der Endabstimmung im EU-Parlament abgelehnt. Mit dieser Ablehnung unterstrichen die EU-Abgeordneten zudem, dass es Zeit ist, sich von unverhältnismäßigen Maßnahmen zur Durchsetzung eines Urheberrechts zu verabschieden und ein überzeugenderes System zu schaffen.

3 BoingBoing, EU working group produces stupidest set of proposed Internet rules, in: http://boingboing.net/2012/09/25/eu-working-group-produces-the.html; 5.12.2012.

4 Entwurf eines Berichts über den Online-Vertrieb von audiovisuellen Werken in der EU, in: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+COMPARL+PE-480.505+01+NOT+XML+V0//DE

Ein weiterer großer Erfolg war die Absegnung eines Berichts zur digitalen Freiheitsstrategie in der Außenpolitik der EU.[5] Im November forderte das EU-Parlament die Kommission dazu auf, den sicheren Zugang zum offenen und unzensierten Internet als Hauptpriorität in die Strategie für eine EU-Außenpolitik mit einzubeziehen. Der Bericht betont, dass „ein weltweiter Konsens besteht, der sich im internationalen Recht widerspiegelt, dass Beschränkungen der Grundrechte vom Gesetz vorausgesehen werden müssen."

Der Sonderbeauftragte der Vereinten Nationen zum Schutz der Meinungsfreiheit, Frank La Rue, wies nicht umsonst auf die Gefahren der privatisierten Rechtsdurchsetzung hin. In seinem Jahresbericht 2011[6] hinterfragte er bereits, ob Internetprovider, als private Akteure, überhaupt in der Lage seien, zu bestimmen welche Inhalte illegal sind und warnte vor der „besorgniserregenden Tendenz der Staaten, private Akteure zur Herausgabe von Informationen über Nutzer zu verpflichten oder zu drängen".

Das größte Problem ist, dass der Selbstregulierungsansatz weder als politisches Werkzeug diskutiert noch von Kabinetten oder Generaldirektionen der EU-Kommission abgestimmt wurde. Ohne eine klare Stellungnahme und politische Entscheidung der Institutionen ist eine öffentliche Debatte nur schwer möglich. Eine öffentliche Diskussion und Analyse dieses wachsenden Trends der Selbstregulierung im digitalen Raum ist jedoch dringend nötig, um die Kosten für eine derartige Verlagerung der Rechtsdurchsetzung, die Auswirkungen auf die Grundrechte und die Effizienz solcher Maßnahmen einschätzen zu können.

5 Schaake, Marietje 2012: Digital freedom priority in EU foreign policy, in: http://www.marietje-schaake.eu/2012/11/digital-freedom-priority-in-eu-foreign-policy/; 5.12.2012.

6 UN report examines online censorship, in: http://www.edri.org/edrigram/number9.11/un-report-online-censorship

Die neuen Hilfssheriffs des Internets

Constanze Kurz

Die Debatte um die Zukunft der Vergütung von Künstlern und Kreativen im Internet ist in den letzten Wochen dramatisch eskaliert. Aufgeschreckt von radikalen Thesen zur generellen Abschaffung des Urheberrechts, die aus dem Umfeld der Piraten und von den unvermeidlichen Social-Media-Berufsprovokateuren ventiliert wurden, bombardierten Kulturschaffende die deutsche Medienlandschaft mit einer Fülle an Beiträgen, die partiell wie Kriegserklärungen anmuteten. Liest man die Streitschriften am Stück, scheint der Untergang des kulturellen Abendlandes unmittelbar vor der Tür zu stehen, die geistige Leistung des Künstlers nichts mehr wert zu sein. Das Hochkochen der Diskussion wird dabei befeuert von Missverständnissen und Fehleinschätzungen.

Eine dieser Fehleinschätzungen ist die vorgebliche Harmlosigkeit der sogenannten Three- oder Two-Strikes-Modelle. In Frankreich gibt es das sogenannte Three-Strikes-Modell, nach dem zunächst verwarnt, dann der Internet-Anschluss gekappt wird. Dort konnte durch das „Hadopi" genannte drastische Warnmodell mit Internetverbannung tatsächlich ein Rückgang des Filesharens festgestellt werden, allerdings ein ebenso großer Rückgang bei den verkauften Inhalten durch einen schleichenden, aber umfangreichen Boykott kommerziell vertriebener Werke. Der neue Präsident François Hollande versprach im Wahlkampf, das umstrittene Hadopi-Gesetz durch eine Neuregelung zu ersetzen. Er mochte sich nur nicht festlegen, wie diese aussehen würde.

Demokratie wäre Makulatur

In Deutschland wäre „Three Strikes" klar grundgesetzwidrig. Das Recht auf Teilhabe an der digitalen Kommunikation ist so grundlegend, dass seine Verweigerung dem Entzug gleich mehrerer Grundrechte gleichkommt. Daher versucht nun eine heimliche große Koalition, angefeuert von der Inhalteindustrie und neuerdings auch den Kulturschaffenden, ein anderes Warnmodell, auch „Two-Strikes" genannt, durchzusetzen.

Dieses „Warnmodell" setzt bei den Internetanbietern an, die Hilfsdienste leisten sollen. Auf die Idee, den Autobauer für die Fahrgewohnheiten seiner Käufer haftbar zu machen, würde zwar niemand kommen. Im Internet soll das aber nach der Logik der zukünftigen großen Stabilitätskoalition anders sein. Das Warnmodell würde die Provider zwingen, ihre Kunden flächendeckend zu überwachen, Filter einzubauen und diejenigen Kunden mahnend anzuschreiben, die sich anschicken, urheberrechtlich geschützte Dateien zu tauschen.

Die dabei anfallenden Daten ließen sich nur schwerlich vor dem Zugriff der Abmahnanwälte schützen. Denn was nach der zweiten „Warnung" passieren würde, ist absehbar: Abmahnungen, Klagen, Prozesse. Und genau darum geht es beim „Warnmodell": Es sind Pläne zur Privatisierung der Rechtsdurchsetzung. Sind die Internetanbieter erst einmal zum Hilfssheriff degradiert, gibt es keine nennenswerten Hürden mehr, sie auch zur automatischen Datenweiterleitung an die Verwerter-Anwälte zu zwingen. Technisch ist dies durchaus möglich, allerdings nur, wenn man eine Überwachungsinfrastruktur akzeptiert, die unverträglich mit demokratischen Grundwerten ist. Denn fällt diese Technik in die Hände einer Regierung, die Meinungsfreiheit als optional ansieht – angesichts der Erfolge der Nazis in Ungarn oder Griechenland keine unrealistische Annahme –, ist die Demokratie schnell Makulatur.

Scharen krimineller Profiteure

Die Kriminalisierung der Nutzer führt schon jetzt zu einer tiefsitzenden Antipathie gegenüber der Inhalte-Industrie, die sich schnell auf die ökonomischen Grundlagen der Inhalteanbieter auswirken kann. Wer einmal als Jugendlicher tausend Euro Abmahngebühr durch monatelanges Zeitungsaustragen zusammenkratzen musste, wird kaum wieder einen Cent für solche Inhalte ausgeben wollen. Für den sind die Verwerter der Feind, den es auszutrocknen gilt. Diese Auffassung gewinnt immer mehr Anhänger: In fast jeder Schulklasse gibt es einen Betroffenen, unter den Studenten dann schon Hilfeforen.

Die Popularität von kommerziellen Streaming-Seiten wie kino.to und für den Nutzer risikoarmen Verteilungswebseiten wie Megaupload spricht eine deutliche Sprache: Abmahnanwälte und deren Auftraggeber treiben die Kunden in Scharen in die Hände von organisiert kriminellen Profiteuren. Seiten wie Megaupload und kino.to haben jedoch ebenfalls gezeigt: Es gibt nicht nur einen

gigantischen Bedarf nach niedrigschwellig zugänglichen digitalen Inhalten, den die Industrie derzeit nicht deckt, es gibt vor allem eine Explosion des Interesses und damit der Wertschätzung für die dort angebotenen kreativen Werke. Doch diesen Schatz zu heben, dazu fehlt bisher der politische Wille.

Ein fairer Interessenausgleich

Über zweihunderttausend kostenpflichtige Abmahnungen mit einem Durchschnittsbetrag von knapp tausend Euro wurden im Jahr 2011 verschickt. Das ergibt eine Gesamtsumme von mehr als 190 Millionen Euro, die den Besitzer gewechselt haben. Da rollt der Rubel. Doch wohin, wie viel davon ist bei den Künstlern angekommen? Typischerweise nur ein Bruchteil, da die Verwerter das Recht zur Filesharer-Verfolgung oft pauschal an Anwaltskanzleien verkaufen. Die Gerichte werden zeitgleich überschwemmt mit Verfahren, in denen es um ein paar kopierte Songs geht. Die Abmahn-Branche allein hat einen solchen Flurschaden angerichtet, dass ein ausgewogener Dialog zur Findung eines fairen Interessenausgleiches kaum noch möglich scheint.

Doch nur eine Gesetzgebung, die sich auf die Verfolgung von kommerziellen Urheberrechtsverletzungen beschränkt, wird gesellschaftlich akzeptanzfähig. Sobald die Massen der privaten Filesharer kriminalisiert werden, ist eine Eskalation unvermeidlich, die leicht in einem Boykott von kommerziell vertriebenen Werken münden kann.

Ein fairer Interessenausgleich besteht andererseits aber auch nicht in der Abschaffung der Urheberpersönlichkeitsrechte. Allein die Tatsache, dass man dies in der derzeitigen Diskussion hinzufügen muss, offenbart die Gräben in diesem Mehrfrontenkampf. Eine Lösung kann nur in einer Kombination aus dem Zurückdrängen der Abmahnbranche, der Stärkung der Rechte und Verhandlungspositionen der Autoren und Künstler gegenüber den Verwertern und dem Aufbau und der Förderung von innovativen Vergütungs- und Bezahlmodellen liegen. Entgegen der unter Künstlern weitverbreiteten Ansicht ist dies sogar in der Piratenpartei geltende Beschlusslage.

Dieser Text erschien zuerst in der FAZ vom 10. Mai 2012.

Schönes neues Internet-Protokoll: IPv6 & Privacy

Moritz Tremmel

Langsam kommt es, das neue Internet-Protokoll. Im Juni 2012 fand der World IPv6 Launch Day statt – knapp 3.000 Webseiten und Netzbetreiber schalteten IPv6 frei und betreiben es seitdem gemeinsam mit IPv4 im Dual-Stack. Seit September stattet die Telekom neue Privatkunden-DSL-Anschlüsse mit IPv6 aus. Das schon 1998 als Nachfolger für IPv4 standardisierte Protokoll zieht langsam auch in den Internetalltag ein. Ein Grund IPv6 mal etwas genauer unter die Lupe zu nehmen und zu schauen, welche Auswirkungen es eigentlich auf uns hat.

IPv4, NAT, IPv6, Mac-Adresse – wieso, weshalb, warum?

Die 4,3 Milliarden IPv4-Adressen sind schon seit einiger Zeit fast aufgebraucht. Dies konnte noch eine geringe Zeit durch NAT, das Network Address Translation, hinausgezögert werden. Hierzu wurde ein bestimmter IP-Adressraum als privat deklariert, der nicht im Internet verwendet wird. Diese Adressen können in vielen Netzwerken gleichzeitig verwendet werden. Bei der Kommunikation nach draußen ins Internet werden dann die netzwerkinternen, privaten IP-Adressen durch eine öffentliche IP-Adresse ersetzt, die sich alle gemeinsam teilen. Dieser Austausch ist die Aufgabe der NATs.

Bei IPv6 wird ein NAT nicht mehr unbedingt benötigt, da mit den ungefähr 340 Sixtillionen Adressen jedes Gerät mit einer eigenen IP-Adresse ins Internet kann.

Eine IPv4-Adresse: 130.94.122.195

Eine IPv6-Adresse: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344

Die IPv6-Adresse ist dabei in zwei Teile gegliedert: Der erste Teil, der Host-Teil, in der Beispiel-IPv6-Adresse nicht unterstrichen, wird Präfix genannt. Der Präfix wird vom Internet Service Provider (ISP) dem Internetanschluss zugewiesen.

Der zweite Teil, der Client-Teil, in der Beispiel-IPv6-Adresse unterstrichen, „Interface Identifier" genannt, wird von dem jeweiligen Gerät selbst berechnet – meist aus der sogenannten MAC-Adresse. Diese wiederum ist eine jedem Netzwerkadapter fest zugewiesene, eindeutige Adresse und wird deshalb auch Hardware-Adresse genannt. Durch die Berechnung aus dieser eindeutigen Hardware-Adresse entsteht eine eindeutige IP-Adresse. Das Gerät ist auch an anderen Anschlüssen immer wieder erkennbar, da sich von Anschluss zu Anschluss nur das Präfix ändert – der Client-Teil bleibt aber immer gleich und ist weltweit einzigartig.

Die Vorteile von IPv6

Der offensichtlichste Vorteil ist, das es wieder mehr als ausreichend IP-Adressen gibt. Das erleichtert v.a. Das Routing im Internet deutlich.

Außerdem kann jedes Gerät durch eine eigene IP-Adresse vollwertig am Internet teilnehmen. IP basierte Dienste sind einfacher und unterbrechungsfrei nutzbar (z. B. IPTV oder VoIP). Server und Kommunikationsdienste gerade im Hinblick auf die zunehmende Vernetzung von Haushaltsgeräten aber auch sonstigen Alltagsgegenständen werden durch eigene IP-Adressen überhaupt erst in der Masse möglich.

Die Privacy-Probleme von IPv6

Das größte Problem ist die Berechnung des Client-Teils der IP-Adresse (im Beispiel unterstrichen) aus der MAC-Adresse. Dadurch entsteht eine eindeutige Adresse, die auch bei einem Anschlusswechsel erhalten bleibt. Das Gerät und somit der Anwender können durch die immer gleiche Adresse im Internet sofort erkannt werden – damit wäre Usertracking bereits auf IP-Adressebene möglich.

Um diese Problematik zu umgehen wurden die Privacy Extensions entwickelt. Sind diese aktiviert wird ein zufällig berechneter Client-Teil verwendet und in bestimmten (und meist auch bestimmbaren) Intervallen durch neue, zufällige Client-Teile ersetzt.

Bei Microsoft Windows sind die Privacy Extensions ab Windows XP (Service Pack 2) standardmäßig aktiviert. In den meisten Linux-Distributionen sind diese nicht standardmäßig aktiviert. Eine Anleitung wie man diese aktiviert

findet sich auf heise.de.[1] Auch im Apple Betriebssystem Mac OS X sind die Privacy Extensions nicht standardmäßig aktiviert – eine Anleitung zum aktivieren findet sich ebenfalls auf heise.de.[2]

Schlechter sieht es bei den Mobilgeräten aus: Android unterstützt die Privacy Extensions, sie lassen sich aber nicht ohne weiteres freischalten.[3] Mobilsystem iOS (iPad, iPhone) aktiviert die Privacy Extensions erst ab Version 4.3.

Neben dem Client-Teil ist aber auch der Host-Teil (Präfix) datenschutztechnisch problematisch. Die aus der Not der Adressknappheit heraus entstandene dynamische Zuweisung der IPv4 Adressen schaffte im Internet eine gewisse Anonymität, da der immer wieder wechselnden IP-Adresse Nutzer nur bedingt zugeordnet werden konnten.

Wird der Präfix nun statisch zugewiesen, wäre es ähnlich wie bei einer statischen IPv4 Adresse möglich den einzelnen Anschluss immer wieder zu erkennen und zu lokalisieren. Zudem wäre es möglich die verschiedenen Nutzer hinter einem statischen Präfix nach und nach zu identifizieren und die Nutzer und den Ort zu korrelieren. Außerdem wäre es möglich den einzelnen Nutzer über verschiedene statische Präfixe und damit verschiedene Orte hinweg zu verfolgen. Dies ist auch bei eingeschalteten Privacy Extensions, beispielsweise über Cookies oder Anmeldedienste, möglich. Allerdings ist auch bisher schon eine grobe Geolokalisation der dynamischen IPv4/IPv6-Adressen und damit der Geräte möglich. Allerdings sind dies nur grobe Einschätzungen mit statischen IP-Adressen ließe sich die Genauigkeit auf Dauer deutlich steigern.

Weitere Probleme von IPv6

Durch IPv6 ist jedes Gerät ein vollwertiger Teil des Internets mit eigener IP-Adresse. Geräte werden direkt adressierbar und sind nicht mehr vom Internet abgetrennt in einem privaten Netzwerk hinter einem NAT. Dadurch erge-

1 Heise Netze: Linux: Debian/Ubtunu, Fedora, in: http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html?artikelseite=3; 6.12.2012.

2 Heise Netze: Mac OS X, in: http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html?artikelseite=5; 6.12.2012.

3 Heise Netze: Android, in: http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html?artikelseite=4; 6.12.2012.

ben sich neue Möglichkeiten, aber auch neue Gefahren. Jedes Gerät muss nun in der Lage sein sich gegen Angriffe von außen selbst zu schützen, da es direkt ansprech- und dadurch angreifbar ist.

Aktueller Stand und Fazit

Bisher hat IPv6 trotz World IPv6 Launch Day und ersten Telekom Privatkunden-DSL-Anschlüssen noch eine geringe Verbreitung – das kann sich aber recht schnell ändern, wenn große Provider wie die Telekom damit beginnen alle Privatkunden-Anschlüsse freizuschalten. Wann dies geschehen wird und welche Dynamiken es auslöst ist noch nicht absehbar. Genauso unklar ist, ob IPv6 Adressen dynamisch oder statisch zugewiesen werden. Die IPv6-Privatanschlüsse der Telekom erneuern das Präfix bei jeder neuen Einwahl in das Internet.

Für eine datenschutzkonforme Ausgestaltung von IPv6 müssen die Privacy Extensions standardmäßig aktiviert sein. Die Wahlfreiheit der Nutzer schließt ein, dass die Privacy Extensions leicht ein- und ausgeschaltet werden können. Von den Providern müssen die Internetanschlüsse standardmäßig mit dynamischen Präfixen angeboten werden. Den Kunden sollten aber auch Internetanschlüsse mit statischen Präfixen ohne Aufpreis angeboten werden. Bedenkenswert wäre auch die Idee der Zuweisung eines dynamischen und eines statischen Präfixes, welche der Kunde dann für verschiedene Anforderungen nutzen könnte.

Secure-Boot: Wer kontrolliert Ihren nächsten Computer?

Matthias Kirschner

Unsere Gesellschaft hat durch die Entwicklung des Computers über die letzten Jahrzehnte zu einer Universalmaschine ein leistungsfähiges Werkzeug geschaffen, mit dem alle möglichen Aufgaben von einer einzigen Maschine ausgeführt werden können. Unser Mobiltelefon beinhaltet persönliche Daten wie Kontakte, Bilder, Lieblingsmusik, E-Mails, Anruflisten und Kurzmitteilungen. Es ist ein Computer, der dank GPS weiß, wo er ist, mit dem Mikrophon hören und mit der Kamera sehen kann was passiert. Heute sind Computer schon allgegenwärtig, Cory Doctorow drückte es so aus: „Heutige Autos sind Computer in die wir uns setzen, Boing 747 sind fliegende Solaris Computer, wohingegen Hörgeräte und Herzschrittmacher Computer sind, die wir in unseren Körper anbringen."[1]

Doch diese Universalmaschine ist in Gefahr: Mit der Funktion „Secure Boot", die ab diesem Jahr in Computern Einzug hält, streben Hersteller von IT-Hardware und Software danach, sich in eine Position zu bringen in der sie dauerhaft die IT-Geräte kontrollieren, die sie produzieren. Solche Geräte werden aus Sicht der Hersteller „sicher" sein, aber nicht unbedingt aus Sicht des Eigentümers. Durch das Verhindern von Einsatzmöglichkeiten, die der Hersteller nicht vorsieht, kann er beschränken wozu die Universalmaschine Computer (z. B. Ein PC, Laptop, Notebook) genutzt werden kann. Im Falle von IT-Geräten mit Internetzugang kann er diese Benutzungsbeschränkungen zu jeder Zeit verändern, sogar ohne den Geräteeigentümer zu informieren. Infolgedessen können IT-Hersteller nach ihrem Belieben auch nachträglich grundlegende Rechte entziehen, die Eigentümer von Produkten gewöhnlich erhalten.

Die Instanz, die letztendlich kontrolliert welche Software auf einem Gerät ausgeführt werden kann und somit die konkreten Funktionen eines Geräts festlegt, hat schließlich die Kontrolle über alle Daten, die vom Gerät verarbei-

1 *Doctorow, Cory* 2012: The Coming Civil War over General Purpose Computing, in: http://boingboing.net/2012/08/23/civilwar.html; 5.12.2012.

tet und gespeichert werden. Das kann zur Folge haben, dass der Eigentümer des IT-Geräts nicht mehr die alleinige Kontrolle über seine eigenen Daten innehat.

„Secure Boot": Pförtner zum Betriebssystem

Wenn IT-Geräte eingeschaltet werden, führen sie einen Startprozess aus, der Booten genannt wird. Im Falle eines Computers beinhaltet dieser Startprozess das Ausführen von einer sogenannten „Firmware". Diese Firmware wiederum startet ein anderes Programm, genannt „Bootloader", der dann das tatsächliche Betriebssystem lädt, mittels dem dann Anwendungsprogramme ausgeführt werden können. Dieses Jahr wird der industrieweite Übergang bei der Firmware von PCs, Notebooks, Server und anderen Computern vom klassischen BIOS zu UEFI[2] nahezu abgeschlossen sein. Verglichen mit dem klassischen BIOS hat UEFI mehrere Vorteile, wie z. B. Eine kürzere Startdauer, betriebssystemunabhängige Treiber und das Versprechen höherer Sicherheit.

Der Sicherheitsaspekt wird von einer Funktion namens „Secure Boot" abgedeckt. Seit UEFI 2.3.1 (veröffentlicht am 8. April 2011) stellt „Secure Boot" sicher, dass während des Startprozesses ausschließlich Software ausgeführt wird, die mit einer der vorinstallierten kryptographischen Signaturen übereinstimmt. Damit wird verhindert, dass während des Startvorgangs des Computers unerwünschte Software (z. B. Schadsoftware) ausgeführt wird, indem jede Softwarekomponente (verschiedene Teile der UEFI-Firmware, der Bootloader, der Betriebssystemkernel, usw.) kryptographisch verifiziert und erst dann gestartet wird.

Microsoft hat angekündigt[3], dass Computerhersteller UEFI implementieren müssen, um für ihre Geräte eine Windows 8 Zertifizierung zu erhalten, beispielsweise ein „Kompatibel mit Windows 8"-Logo. Deshalb ist ist zu erwarten, dass die große Mehrheit der Computerhersteller „Secure Boot" implementieren wird.

2 Siehe dazu bei der Wikipedia: http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interace.

3 Siehe http://msdn.microsoft.com/en-us/library/windows/hardware/hh748200.asp.

Welche Geräte betrifft das?

Gegenwärtig begründen viele ihre Analyse der Situation in Bezug auf UEFI auf den „Windows 8 Hardware Certification Requirements", die von Microsoft im Dezember 2011 herausgegeben wurden. Es versteht sich von selbst, dass Microsoft keine Versionen dieser Hardware-Zertifizierungsvorgaben öffentlich machen musste bzw. muss, da sie die Grundlage für einen individuellen Vertrag zwischen Microsoft und jedem Hardwarehersteller bilden, der Microsofts Windows 8 Zertifizierung für seine Geräte erhalten will. Daher können sich die „Windows 8 Hardware Certification Requirements" jederzeit ohne öffentliche Bekanntmachung ändern, oder bestimmte Details für die Logo-Zertifizierung können sich zwischen Herstellern unterscheiden: Alles passiert nach Microsofts Willen und größtenteils hinter geschlossenen Türen. Deshalb kann sich niemand auf die veröffentlichten Versionen der „Windows 8 Hardware Certification Requirements" verlassen, sondern soll die Angaben bezüglich „Secure Boot" als ein „bewegliches Ziel" betrachten.

Also ist das Problem von „Secure Boot" nicht beschränkt auf „Connected Standby Systems" (wahrscheinlich ein großer Teil des zukünftigen Markts von Notebooks, Netbooks und PCs) und Computern basierend auf ARM-Mikroprozessoren (hauptsächlich „Tablets" und Mobiltelefone), sondern kann von Microsoft jederzeit auf jede Art von Gerät erweitert werden.[4] Genauso können Hersteller, die keine Geräte für Windows 8 herstellen, UEFI „Secure Boot" oder andere Startprozesse einsetzen, die mit Hilfe der kryptographischen Signaturen beschränkt werden. TiVo tut dies seit einem Jahrzehnt und verschiedene Spielkonsolen, von Sony bis Microsoft, benutzen ebenfalls kryptographisch beschränkte Startprozesse. Andere Gerätehersteller könnten Spezifikationen oder Vorgaben ähnlich den „Windows 8 Hardware Certification Requirements" einsetzen, um die Einsatzmöglichkeiten von IT-Geräten künstlich zu begrenzen.

4 Kaum ein Laptop- und Desktop-Computer wird ohne das „Kompatibel-mit-Windows-8"-Logo vertrieben. Daher hat Microsoft bei x86er-Architekturen mehr Einfluss. Siehe dazu auch JamesnBottomley „The ARM Windows 8 Lockdown", in: http://blog.hansenpartnership.com/the-arm-windows-8-lockdown/.

Beschränkungen für Anwendungsprogramme?

Während die UEFI „Secure Boot"-Spezifikation (sowie die Spezifikationen der Trusted Computing Group, die „Trusted Boot" definieren) den primären Startprozess bis hin zum Betriebssystemkernel abdeckt, ist die Infrastruktur zur Erweiterung der Signaturprüfung aller auf einem Computer ablaufenden Software ausgereift und funktioniere.

Bedrohung für den Universalcomputer

Wenn all diese Maßnahmen unter alleiniger Kontrolle der Geräteeigentümer stünden, könnten sie in ihrem besten Interesse sein, da sie dabei helfen die Sicherheit des Startprozesses zu verbessern, der bis heute weitgehend ungesichert ist. Das wäre der Fall, wenn die vom UEFI-Forum und der Trusted Computer Group (TCG) spezifizierten Sicherheitssubsysteme dem Eigentümer permanente, volle und alleinige Verfügungsgewalt über die Konfiguration und Verwaltung dieser Sicherheitssubsysteme technisch gewährleisteten. Das schließt die Erstellung, Speicherung, Benutzung und Löschung der kryptographischen Schlüssel, Zertifikate und Signaturen mit ein. Aber sobald andere Instanzen neben dem Geräteeigentümer diese Sicherheitssubsysteme kontrollieren können, ermöglicht das ihnen, unbeabsichtigte oder einfach unvorhergesehene Nutzungsformen dieser IT-Geräte zu unterbinden.

Daher kann mit der Implementierung von „Secure Boot" die Verfügbarkeit von echten Universalcomputern unter voller Kontrolle ihrer Eigentümer stark reduziert werden. Von einer Firma, z. B. Durch „Secure-Boot", signifikant beschränkte Geräte, werden gewöhnlicherweise „Appliances" oder „Embedded Systems" genannt (z. B. „Media Centers", Telefone, „E-Book-Reader"). Deshalb werden zumindest einige Geräte mit Windows 8 eher eine „Windows-Appliance" darstellen, als einen gebräuchlichen Computer. Während es für solche Appliances einen Markt geben mag, fordert die Free Software Foundation Europe (FSFE), dass IT-Geräte, die nur auf von einer Firma vorgesehenen Nutzungsmodelle beschränkt sind, eindeutig gekennzeichnet werden müssen, um potentielle Käufer ordentlich zu informieren.

Option: Umgehen dieser Einschränkungen

IT-affine Personen denken womöglich, dass sie solche Maßnahmen bereits gesehen haben, und die meisten davon wurden geknackt. Das war der Fall bei verschiedenen Modellen der PlayStation- und Xbox-Spielkonsolen, sowie bei vielen neueren Mobiltelefonen. Dieses Mal aber ist die Qualität und der Umfang größer:

- UEFI „Secure Boot" zielt hauptsächlich auf herkömmliche PCs ab.
- Es wird von weiten Teilen der IT-Industrie unterstützt, siehe z. B. die Mitglieder des UEFI Forums.[5]
- Das Design und die Spezifikation sind das Ergebnis gemeinsamer Bemühungen von IT-Ingenieuren vieler Firmen. Zudem basiert es auf einem Jahrzehnt Erfahrung mit signaturbasierten Startprozessen und meidet daher viele klassische Fallstricke, z. B. das Fehlen eines ordentlich spezifizierten und kryptographisch gesicherten (UEFI) Firmware-Aktualisierungsprozesses.
- Es verwendet hardwarebasierte Sicherheitssubsysteme, wie z. B. von der TCG spezifiziert (TPM oder MTM und begleitende Spezifikationen): Während die UEFI-Spezifikation keine bestimmte Implementierung eines „geschützten Speichers (protected storage)" für kryptographische Schlüssel, Zertifikate und Signaturen verlangt, passen die aktuellen TCG-Spezifikationen (seit 2011) gut.
- Sicherheitslücken in „Secure Boot"-Implementierungen sind zu erwarten (wie in jeder Software). Da es aber kommerziellen Wettbewerb zwischen UEFI-Anbietern geben wird, liegt es in ihrem besten Interesse diese Sicherheitslücken zu schließen. In der Vergangenheit wurden dagegen kryptographisch beschränkte Startprozesse nur von einzelnen Herstellern für ihre eigenen, speziellen Geräte implementiert: TiVo Inc. für ihre TIVOs, Microsoft für verschiedene Generationen ihrer Xbox sowie Sony für ihre Playstation-Modelle.

Obwohl viele ähnliche Benutzungseinschränkungen in der Vergangenheit geknackt wurden, zeigt dies nur, dass ihre technischen Implementationen mangelhaft und offen für Schadsoftware waren und daher nicht die „Sicherheit"

5 UEFI Overview, in: http://www.uefi.org/about/.

bereitstellten, für die sie ausgelegt wurden. Obgleich dies wahrscheinlich auch für einige „Secure Boot"-Implementierungen gelten wird, kann das Brechen dieser Mechanismen niemals mit der Freiheit und einer vollen Kontrolle durch den Geräteeigentümer gleichgesetzt werden.

Was wird technisch getan?

Microsoft hat die Möglichkeit, alle derzeit entwickelten Umgebungen zu verhindern. Freie-Software-Distributoren versuchen es derzeit zu ermöglichen, dass weiterhin ein freies Betriebssystem einfach installiert werden kann. Die GNU/Linux-Distributoren Redhat und SUSE arbeiten an dem Bootloader „Shim" und die Linux Foundation entwickelt einen eigenen Mini-Bootloader. Allerdings ist es weiterhin so, dass der einzige Schlüssel, der auf jeden Fall vorhanden ist, der von Microsoft ist. Microsoft signiert Programme für Entwickler, die einen Zugang zum „Windows Hardware Dev Center" haben. Um dort Zugriff zu bekommen, muss ein Zertifikat von Verisign gekauft werden um die eigene Identität zu bestätigen und damit einen Entwickler-Account anzulegen. Danach muss noch den rechtlichen Bedingungen zugestimmt werden, erst dann kann man ein Programm an Microsoft schicken, welches dann signiert zurückgeschickt wird. James Bottomley (Linux Foundation) hat beschrieben[6], welche praktischen Probleme in diesem Prozess auftauchen können.

Was wird politisch getan?

Die Bundesregierung hat am 19. November 2012 ein Eckpunktepapier zu „Trusted Computing" und „Secure Boot"[7] veröffentlicht. Dieses greift Forderungen von digitalen Bürgerrechtsorganisationen, wie der Free Software Foundation Europe (FSFE), auf und widerspricht gleichzeitig in mehreren Bereichen den Bedingungen von Microsoft zur Windows 8 Zertifizierung. So fordert die Bundesregierung, dass „ein Geräte-Eigentümer […] über die vollständige Kontrolle (Steuerbarkeit und Beobachtbarkeit) der gesamten „Trus-

6 James Bottomley's random Pages: Adventures in Microsoft UEFI Signing, in: http://blog.hansenpartnership.com/adventures-in-microsoft-uefi-signing/; 6.12.2012.

7 BMI 2012: Eckpunktepapier der Bundesregierung zu „Trusted Computing" und „Secure Boot", in: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/trusted_computing.html; 6.12.2012.

ted Computing"-Sicherheitssysteme seiner Geräte verfügen" muss.[8] Die Bundesregierung stellt klar, dass „eine Delegation dieser Kontrolle an Dritte […] eine bewusste und informierte Einwilligung des Geräteeigentümers" voraussetzt.

Eine andere Forderung der FSFE wird ebenfalls in dem Eckpunktepapier der Bundesregierung aufgegriffen: Käufer müssen vor dem Kauf eines Gerätes über eingebaute technische Maßnahmen und spezifische Nutzungseinschränkungen, sowie deren Folgen für den Eigentümer, informiert werden. „Bei der Auslieferung von Geräten müssen „Trusted Computing"-Sicherheitssysteme deaktiviert sein (‚Opt-in'-Prinzip)" und „Geräte-Eigentümer müssen in der Lage sein, aufgrund der vorausgesetzten technischen und inhaltlichen Transparenz von ‚Trusted Computing'-Lösungen eigenverantwortliche Entscheidungen zur Produktauswahl, Inbetriebnahme, Konfiguration, Anwendung und Stilllegung zu treffen." Außerdem muss „eine spätere Deaktivierung […] ebenfalls möglich sein (‚Opt-out'-Funktionalität) und darf keine negativen Einflüsse auf die Funktionalität der Hard- und Software haben, die nicht die Funktion der ‚Trusted Computing'-Technik nutzen."

Wie können wir Zensur-Boot verhindern?

Diese Forderung ist die erste Stellungnahme einer Regierung zu „Secure Boot". Doch was können wir machen um weiterhin eine breite Verfügbarkeit von Universalcomputern sicherzustellen?

Zunächst ist es wichtig, mehr Menschen über das Thema zu informieren. Verbreitet den Artikel von Cory Doctorov, oder wenn es etwas einfacher sein soll, dann könnt ihr Freunden und Bekannten das TCPA Video[9] mit der kurzen Anmerkung schicken, dass fast das gleiche wieder passiert, jetzt aber unter dem Label „Secure Boot" statt TCPA.

Alle die die Fähigkeit beibehalten wollen in Zukunft beliebige Software zu installieren um letztendlich die exklusive Kontrolle über ihre eigenen Daten sicher zu stellen, sollten in den nächsten Monaten darauf achten, welche Hardware sie kaufen. Nur wenige Menschen beschäftigen sich bisher mit diesem Thema. Aber wir sind Menschen, die von anderen beim Kauf von Hardware

8 Dies war von Anfang an eine Kernforderung meines Arbeitgebers, der Free Software Foundation Europe (FSFE).

9 Video in Englisch http://www.youtube.com/watch?v=VfHEXhYqZ-I und Deutsch http://www.youtube.com/watch?v=-LMYQjzp-B4

um Rat gefragt werden. Daher sollten wir selbst keine Geräte kaufen, die unsere Kontrolle über die Geräte einschränkt und wir sollten unseren Freunden keine solche Geräte empfehlen.[10]

Weiterhin – und für die Netzpolitik etwas unüblich aber erfreulich – sollten wir die Regierung in ihrer Position unterstützen damit sie diese bestärkt umsetzen kann. Bevor Microsoft die eigenen Bedingungen ändert, werden sie zunächst versuchen die Position der Bundesregierung zu ändern. Ihr könnt z. B. Auf Abgeordnetenwatch.de Regierungspolitiker (insbesondere unseren Innenminister) für diese Position loben und sie fragen, wie die nächsten Schritte aussehen um die Position umzusetzen. Wie sie sicherstellen werden, dass wir als Eigentümer der Geräte die Kontrolle haben und wir vor dem Erwerb eines Gerätes klar und deutlich auf die in diesem Gerät implementierten technischen Maßnahmen, sowie über die genauen Nutzungsschranken und die Konsequenzen für den Eigentümer informiert werden.

10 Dies haben bereits 39,976 Einzelpersonen http://www.fsf.org/campaigns/secure-boot-vs-restricted-boot/signers und mehrere Organisationen, wie z. B. Parteien Piratenpartei, Grüne Jugend, Junge Piraten in Deutschland http://www.fsf.org/campaigns/secure-boot-vs-restricted-boot/statement in einer Petition unterschrieben.

Das Meldegesetz: Erst durchgewinkt, dann durchgefallen

Constanze Kurz

Es war bereits der zweite Anlauf im Deutschen Bundestag beim Versuch, eine moderne Gesetzgebung für das Meldewesen zu verabschieden. In der vorangegangenen Legislaturperiode war der erste Entwurf für das neue Bundesmeldegesetz noch vor dem Eingang in die parlamentarischen Mühlen gescheitert. Denn geplant war von der Bundesregierung ursprünglich seit 2007 ein zentrales Register der Bundesdeutschen inklusive Fingerabdruckdatei und Steueridentifikationsnummer.

Doch die Nähe zum „reichseinheitlichen Meldesystem" von 1938 war zu groß. So wurde die Zentralisierungsidee, die wohl ebenfalls das Potential für lautstarke Proteste gehabt hätte, zwar fallengelassen, doch die Blamage der Volksvertreter und die Empörung nach dem Durchwinken waren erheblich. Der Gesetzesbeschluss zum Zeitpunkt des EM-Halbfinalspiels bleibt in der kollektiven Erinnerung durch ein leeres Parlament, dessen Abgeordnete ihre Reden ungesprochen zu Protokoll gaben und im Schnellverfahren über eine weitgehende Informationsfreigabe entschieden, die jeden Bürger betrifft.

SPD-Chef Sigmar Gabriel fand sogleich die Formel „gefährlicher Unsinn". Und Horst Seehofer sagte, was er bei solchen Gelegenheiten immer sagt: „Bayern wird dem nicht zustimmen."

Die Personenerfassungssysteme des Staates haben gegenüber kommerziell betriebenen Datensammlungen über Menschen bei weitem nicht die Detailtiefe, um den Ärger der Betroffenen zu erklären. Diesen Umstand betonten auch umgehend einige der federführenden Ausschussmitglieder mit dem Hinweis auf Facebook und Konsorten. Der Fingerzeig auf die extensive Nutzung der kommerziellen Plattformen, der inzwischen in keiner Datenschutzdiskussion fehlt, sollte wohl das Ausmaß der gesetzlichen Änderung kleinreden.

Die Sperrung der eigenen Daten ist bislang möglich

Doch der Taschenspielertrick verfing beim Wahlvolk nicht, da allzu leicht zu durchschauen ist, dass freiwillig ins Netz gegebene Daten nicht mit den Informationen aus den Melderegistern vergleichbar sind. Denn die staatlich erhobene Sammlung punktet vor allem bei der Glaubwürdigkeit, Verlässlichkeit und Aktualität. Allein in Berlin werden jedes Jahr etwa sechzigtausend Privatauskünfte über Meldedaten erteilt, jeweils mit dem unsichtbaren Siegel der Staatsgarantie versehen.

Der Volkszorn richtete sich vor allem gegen die kurzfristig im Gesetz lancierte Hofierung der Werbewirtschaft, nach der Bürger Auskunftsbegehren ausdrücklich zu widersprechen haben und beim Abgleich oder Aktualisieren bereits vorhandener Adressdateien gar keinen Einspruch mehr geltend machen können.

Dabei hatte das Bundesverwaltungsgericht erst 2006 die Rechtslage für Menschen verbessert, denen an einem werbefreien Briefkasten gelegen ist: Denn Meldebehörden dürfen die sogenannte einfache Melderegisterauskunft nicht erteilen, „wenn diese erkennbar für Zwecke der Direktwerbung begehrt wird und der Betroffene einer Weitergabe seiner Daten für solche Zwecke zuvor ausdrücklich widersprochen hat“. Wer also zuhause nicht belästigt werden möchte, dem steht bislang die Sperrung der eigenen Daten zu Verfügung.

Mit dem Etikett Klientelpolitik

Diese Möglichkeit der Auskunftssperre im Melderegister wurde nun qua Gesetz verwässert. Gleichzeitig wurde das Ansinnen einer modernen Lösung durch eine Vorab-Einwilligung anstelle des Widerspruchs ganz aus dem Gesetzentwurf getilgt. Dass nämlich der Bürger zuvor gefragt werden soll und sich nicht mehr aktiv gegen eine Datenweitergabe wehren muss, war als wesentliche Verbesserung der Rechtslage geplant.

Dieses allzu offensichtliche Entgegenkommen gegenüber Adresshändlern erhielt nicht zu Unrecht das Etikett Klientelpolitik. Die verantwortlichen Politiker dementierten zwar und betonten unisono, von einer Einflussnahme der Werbewirtschaft hin zum ungebremsten staatlich sanktionierten Datenleck

könne keine Rede sein. Dem steht allerdings eine entlarvende Aussage der Staatssekretärin im Bundesministerium des Innern, Cornelia Rogall-Grothe, entgegen.

Die Beauftragte der Bundesregierung für Informationstechnik, gern auch als „Bundes-CIO", Chief Innovation Officer, bezeichnet, gab bei einem Treffen auf Einladung der europäischen Melderegisterauskunft RISER im Mai 2012 zu Protokoll, dass die Verbände der Inkassowirtschaft und der Scoring-Unternehmen wegen der geplanten Neuregelung der einfachen Melderegisterauskunft bereits tätig geworden seien. Zu diesem Zeitpunkt lag der Entwurf des Bundesmeldegesetzes schon vor und galt noch als modern und bürgerfreundlich.

Gestiegene Sensibilität bei Datenfragen

Doch die darin festgehaltenen Einschränkungen für die Werbewirtschaft und den Adresshandel waren den Lobbyisten ein Dorn im Auge. Rogall-Grothe erklärte: „Auch die Widerspruchsmöglichkeit gegen Melderegisterauskünfte per Internet wird aus Sicht dieser Verbände kritisiert. Hier könnte es zu Änderungen kommen, allerdings müssen aus meiner Sicht die Grenzen, die die bereits erwähnte Entscheidung des Bundesverwaltungsgerichtes von 2006 aufzeigt, beachtet werden."

Den Wünschen der Verbände wurde offensichtlich entsprochen, einzig das Urteil des Gerichts fand im neuen Gesetz keinen Widerhall. Doch so einfach ist die werbefreundliche „Fortentwicklung des Meldewesens" diesmal nicht mehr zu haben, denn dass der Bundesrat dem Treiben ein Ende bereitet, gilt schon als ausgemacht. Eigentlich ist keiner mehr dafür. Wohl nur der nimmermüde CSU-Mann Hans-Peter Uhl vom Innenausschuss ist noch immer ein unbeirrter Befürworter des Gesetzes.

Nicht nur eine wachsame Öffentlichkeit hat dazu beigetragen, ein wenig Sand ins gut geölte Getriebe der Lobbyrepublik zu streuen, sondern ebenso sehr eine noch weiter gestiegene Sensibilität der Deutschen bei Datenfragen. Trotz des Vorwurfs, die Diskussion sei geradezu hysterisch, in jedem Falle aber übertrieben, ließen sich die Datengeber nicht beirren: In der Tagesschau-Umfrage zeigten sich 99 Prozent der Bürger mit der Neuregelung im

Melderecht nicht einverstanden. Sie gilt zwar trotz mehr als 75.000 abgegebener Stimmen als nicht repräsentativ, ist aber ein deutlicher Denkzettel für die Parlamentarier.

Dieser Text erschien zuerst in der FAZ vom 19. Juli 2012.

Krieg mit Drohnen: Das Gesicht unserer Gegner von morgen

Frank Rieger

Wir stehen vor einem Wettrüsten für einen Krieg autonomer Roboter. Noch entscheiden Menschen und nicht Drohnen über Leben und Tod. Doch die Debatte darüber, was Maschinen können sollen, muss geführt werden, bevor der Fortschritt den letzten Rest Humanität kassiert.

Schon seit der Frühzeit widmet der Mensch einen beachtlichen Teil seiner Energie, Ressourcen und Intelligenz der kriegerischen Auseinandersetzung. Trotz aller komplexen Waffen, Reittiere, Panzer, Flugzeuge und Interkontinentalraketen ist der bewaffnete Kampf ein Konflikt zwischen Menschen – bisher. Nun rollt auch beim Krieg, wie überall sonst, die Automatisierungswelle. Die militärische Auseinandersetzung und auch ihre kleine Schwester, die flächendeckende Überwachung im Namen der Sicherheit, werden immer stärker von Maschinen und Algorithmen dominiert.

Autonome Systeme, die in ihren Entscheidungen immer weniger auf den Menschen angewiesen sind, werden zum Rückgrat zukünftiger militärischer Auseinandersetzungen. Die Restkriege in Afghanistan und Irak, die neuen Konflikte in Afrika und eine Reihe von wenig bekannten Kampfeinsätzen auf anderen Kontinenten werden zum großen Teil aus der Luft mit ferngesteuerten Drohnen geführt, die nicht nur Kameras, Sensoren und Funküberwachungsinstrumente tragen, sondern auch mit Raketen bewaffnet sind.

In den Planungen der Militärs, auch der Bundeswehr, nehmen Roboter-Kampfmaschinen einen immer größeren Raum ein. Die Produktions- und Betriebskosten sind vergleichsweise niedrig, es muss schließlich keine Rücksicht auf die Bedürfnisse von Piloten oder Fahrern genommen werden. Und die Vorgesetzten müssen sich nicht per Funk mit einem Piloten auseinandersetzen, der eine eigene Wahrnehmung der Gefechtslage hat, der einen Befehl missinterpretiert, ignoriert oder nicht befolgt.

Fatale Irrtümer sind an der Tagesordnung

Der neue Pilot sitzt im Zweifel, nur schräg über den Flur, an der Drohnen-Kontrollkonsole. Die Ausbildung der Drohnen-Fernsteuerer ist wesentlich preiswerter und kürzer als die eines Jetpiloten. Sie können abends nach Hause gehen und den Krieg im ganz normalen Schichtdienst absolvieren. Die Auswirkungen dieser digital vermittelten Distanz zum Krieg auf die Psyche der Soldaten werden erst allmählich sichtbar.

Schon seit einiger Zeit können Computer Flugzeuge fliegen, auch bei hohen Geschwindigkeiten und unter komplizierten Bedingungen. Jedes Passagierflugzeug verfügt über einen Autopiloten, der das Flugzeug von Start bis Landung fliegen könnte. Nur noch die Flugroute wird programmiert. Drohnen werden heute in der Regel genauso gesteuert: Es werden Wegpunkte vorgegeben und angeflogen und Verweilschleifen über Ziele festgelegt, die beobachtet und schließlich beschossen werden sollen. Je nach Situation kann auch noch direkt gesteuert werden, jedoch mit einer durch die Satellitenverbindung bedingten Zeitverzögerung im Sekundenbereich.

Die Frage, gegen welche Ziele die roboterisierten Waffen gerichtet werden und nach welchen Kriterien entschieden wird, ist das Zentrum der derzeitigen Drohnen-Diskussion. Es ist schließlich niemand vor Ort, die Realität wird über Tausende Kilometer hinweg durch Sensoren und Kameras wahrgenommen. Fatale Irrtümer sind an der Tagesordnung, auch die besten Prozeduren und Vorschriften können sie nicht verhindern.

Die Analyse typischer Bewegungsmuster

Die Datenströme aus den Sensoren des massenhaften Drohneneinsatzes überfordern schon jetzt die Kapazitäten der Übertragungssatelliten und entziehen sich der vollständigen Auswertbarkeit durch Menschen schon allein durch ihre schiere Masse. Die logische Konsequenz: Auch hier wird zunehmend mit maschineller Intelligenz gearbeitet, die nach Mustern sucht und daraus Handlungsempfehlungen ableitet. Formal ist der Soldat zwar noch der Raketenschütze, jedoch sind ihm viele wesentliche Entscheidungen, die lange vor dem eigentlichen Schuss liegen, längst aus der Hand genommen worden.

Menschen am Boden werden schon heute aus der Luft mit Raketen angegriffen, nur weil ihre typischen Bewegungsmuster, die ebenfalls von Drohnen erfasst und gegen in Datenbanken gespeicherte Aufzeichnungen abgeglichen werden, den vermuteten Bewegungen von Aufständischen entsprechen. Ob es sich dabei um Ziegenhirten, Schmuggler oder feindliche Soldaten handelt, ist für fliegende Kampfroboter nicht zu erkennen. Heute geschehen solche automatischen Analysen in den Steuerzentralen und Lagezentren, unter der Aufsicht von Menschen. Zukünftig soll dies an Bord der Drohne geschehen, um Zeit, Personal und Übertragungskapazität zu sparen.

Kommandogewalt nur noch auf einer abstrakten Ebene

Die Entwicklungsrichtung ist klar: Nur noch der finale Knopfdruck, das eigentliche Abfeuern der Rakete wird aus rechtlichen und moralischen Gründen dem Menschen überlassen. Er kann sich aufgrund seiner Erfahrung mit den typischen Fehlern der Maschinen derzeit noch entscheiden, nicht zu schießen. Und auch dabei wird er demnächst von Algorithmen beobachtet, die aus seinem Verhalten lernen, um beim nächsten Mal besser zu sein.

Irgendwann, in absehbarer Zeit wird der finale Knopfdruck nur noch ein Ritual, eine Handlung, die eigentlich überflüssig ist, weil sie keine bewusste Entscheidung mehr darstellt, sondern nur noch die althergebrachte Tradition, im Angesicht der technischen Möglichkeiten eine immer ineffizienter und antiquierter erscheinende Moralverpflichtung. Da der Mensch die Kapazität zur Aufnahme, zum Verständnis und zur Einordnung der immensen, von Maschinen für Maschinen generierten Datenströme schlicht nicht hat, bleibt ihm die Kommandogewalt nur noch auf einer abstrakten Ebene erhalten.

Es fällt schwer, greifbare Kategorien für unsere Beziehungen zu algorithmischen „Intelligenzen“ zu finden. Stellen wir uns einen gut trainierten Hund vor. Wir können nicht immer vorhersagen, warum und was er im nächsten Moment tun wird, aber wir können ihm Befehle erteilen, seine Fähigkeiten nutzen und Erfahrungswissen über sein Verhalten und seine Reaktionen sammeln. Unser algorithmisch „intelligenter“ Hund unterscheidet sich jedoch darin, dass er eine nahezu unbeschränkte Aufnahmefähigkeit und ein perfektes Gedächtnis hat.

„Search and Destroy“

Das tatsächliche Verständnis der Drohnen-Piloten für die Konstruktion, die Fehler und Probleme der Maschinen, die sie bedienen, bewegt sich ungefähr auf dem Niveau eines Hundeführers, der seine Tiere einigermaßen gut kennt. Er weiß nichts über die Neuronenverknüpfung im Hirn des Hundes, , aber viel über das typische Verhalten. Genauso wenig kennt der Drohnen-Pilot die Steuer-Software im Detail, er ist nur an das typische Output-Muster gewöhnt. Der gravierende Unterschied ist, dass die Menschheit schon ein paar tausend Jahre Erfahrung mit den Eigenarten und Eigenschaften von Haustieren hat, die sich nur relativ langsam verändern.

Wir stehen am Beginn eines Wettrüstens im Bereich der Algorithmen für letale Autonomie. Wer schneller ist und weniger Hemmungen hat, solche Systeme trotz aller Mängel auch einzusetzen, kann, so die Logik des neuen Wettrüstens, erhebliche strategische und finanzielle Vorteile haben und möglicherweise etwas Abschreckung verbreiten.Das neue Wettrüsten markiert einen Wendepunkt auch für Forscher, die sich im akademischen Bereich mit Robotern und künstlicher Intelligenz beschäftigen. Nun ist fast jedes Forschungsthema in diesem Feld relevant für den Bau neuer, intelligenterer Waffen.

Die beliebten Wettbewerbe für universitäre Roboterforscher haben neben dem Fußballspiel oft als Szenario das „Search and Rescue“, das Auffinden von Personen in unübersichtlichen Situationen und Geländen zum Zwecke ihrer Rettung aus Notlagen. Beim Militär gibt es eine von den Anforderungen her ausgesprochen ähnliche Mission: „Search and Destroy“. Dabei geht es ebenfalls um das Auffinden von Personen in unübersichtlichem Gelände. Nur das diese dann nicht gerettet, sondern getötet werden. Aus technischer Sicht ist der Unterschied nur, dass der Drohnenschwarm dann der gefundenen Person keine Markierungs-Bake mit Verbandspäckchen vor die Füße wirft, sondern eine Granate.

Mit hundertprozentiger Tödlichkeit

Das Ziel der aktuellen Entwicklungen sind noch nicht die aus Science-Fiction-Werken bekannten vollautonomen Roboter à la Terminator. Die Realität tödlicher Maschinen wird viel banaler, aber nicht weniger furchterregend. Auf den Schlachtfeldern der nächsten Jahre werden sogenannte intelligente „Area

denial"-Waffen auftauchen. Aus Computerspielen als „Sentinel" (Wächter) bekannt, handelt es sich um Roboterwaffen mit der überschaubaren Intelligenz einer modernen Alarmanlage. Ihre Aufgabe: auf alles, was sich in dem ihnen zugeteilten Geländeabschnitt, der sogenannten „kill box", bewegt, zu feuern, bis sich nichts mehr bewegt.

An die Sensor- und Reaktionssysteme lassen sich je nach Bedarf und Produktkonzept von „weniger tödlichen" Optionen wie Gummigeschossen über Maschinengewehre bis zu kleinen Granatwerfern die verschiedensten Schießgeräte adaptieren. Der Effekt ist der eines Minenfeldes mit hundertprozentiger Tödlichkeit.

Entwickelt wurden solche Systeme schon in Israel und Südkorea, um Grenzverletzer automatisch zu erschießen. Das gleiche Prinzip gibt es auch in Form fliegender Einweg-Drohnen, die über einem Schlachtfeld kreisen und auf das Auftauchen eines Ziels warten, um sich dann autonom auf dieses zu stürzen und zu explodieren, die „loitering ammunition".

Eine allesvernichtende Killermaschine

Über die Prioritäten und Maßgaben für zukünftige Entwicklungen wird derzeit in Militärkreisen heftig diskutiert. Dabei orientiert sich die militärakademische Diskussion nicht etwa an einer utilitaristischen Ethik, bei der abgewogen wird, welche Handlungen den größten Nutzen für die meisten Menschen ergeben. Diese Art der Abwägung wäre schlicht inkompatibel mit dem Ziel, eine größtmögliche Flexibilität bei der Definition von Missionszielen für die tödlichen Maschinen zu erhalten.

Die Militärforscher setzen vielmehr auf eine spezielle Ethik, bei der formal spezifizierte Verbote und Genehmigungen für einzelne Handlungen logisch kombiniert werden. Die Kriegsroboter sollen sich analog zu den heutigen „Rules of Engagement" verhalten, wie sie in Kriegen an westliche Soldaten ausgegeben werden, um zu regeln, wann und unter welchen Umständen Waffengewalt eingesetzt werden darf. Zwangsläufig werden dabei, wie schon heute in Afghanistan und im Irak, die Abgrenzungsprobleme, wer ein feindlicher Kämpfer und wer ein Zivilist ist, zu tödlichen Fehlentscheidungen führen. Bei entsprechend aggressiver Konfiguration von Erlaubnissen und Verboten lässt sich ein derart gesteuerter Roboter auch als allesvernichtende Killermaschine benutzen.

Die Debatte muss geführt werden

Hinzu kommt, dass die derzeit eher theoretischen Überlegungen zur Implementierung einer Kriegsroboter-Ethik von fehlerfreier Funktionsweise der Systeme ausgehen. Die notwendige Software für autonome Systeme ist jedoch derart umfangreich und komplex, dass diese Annahme realitätsfern bleibt. Das hält die Militärstrategen jedoch nicht davon ab, für eine schnelle Entwicklung immer autonomerer Systeme zu werben. Dabei wächst insbesondere im Westen die Furcht davor, dass ein Gegner – implizit ist meistens China gemeint – schneller und mit weniger Rücksicht auf etabliertes Kriegsrecht voranpreschen könnte. In einer aktuellen Studie des amerikanischen Militärs wird etwa argumentiert: „Autonome Bodensysteme müssen gegen die größte Bedrohung auf dem Schlachtfeld konzipiert werden: ein hochmobiles, extrem letales feindliches autonomes System, das nicht über die höheren kognitiven Funktionen verfügt, die notwendig wären, um Kampfhandlungen auf den Rahmen der internationalen Verträge und des Landkriegsrechts einzugrenzen".

Die Diskussion um die aktuelle Forderung der Bundeswehr nach bewaffneten Drohnen muss mit klarem Blick auf die Tendenz zukünftiger Autonomie-Entwicklungen geführt werden. Sind die Drohnen einmal bewaffnet, greift die Wettrüsten-Logik der Militärs, die wohlklingende Gründe für immer mehr Autonomie anführen werden. Heute sind es Funkverbindungen, die störanfällig und schmalbandig sind. Bald wird es die Reaktionsgeschwindigkeit des Menschen sein, die nicht mehr gegen einen mit Computergeschwindigkeit agierenden autonomen Kampfroboterschwarm ausreicht. Die Debatte um die Bewaffnung von Robotern, um Nutzen und Grenzen von maschineller Autonomie und ihre ethischen Implikationen muss geführt werden, bevor diese vermeintlichen Sachzwänge mit absehbarem Ausgang die Grundfesten moralischen und humanistischen Handelns erodieren. Sonst ist der Weg zu einer Welt, wie sie Daniel Suarez in „Kill Decision" beschreibt, nicht mehr weit.

Dieser Text erschien zuerst in der FAZ vom 20. September 2012.

Überwachung

Funkzellenabfrage: Die millionenfache Handyüberwachung Unschuldiger

Andre Meister

In diesem Jahr setzte netzpolitik.org das Thema Funkzellenanfrage auf die Agenda der Politik in Berlin. Nach zwei Wochen Recherche veröffentlichten wir am 19. Januar eine Ermittlungsakte, in der die Durchführung dieser Maßnahme angeordnet wurde.[1] Damit konnten wir das eher abstrakte Thema an einem konkreten Beispiel illustrieren.

Zum Fall: Im Oktober 2009 findet die Berliner Polizei in Friedrichshain „angebrannte Gegenstände" unter einem Auto, dadurch „entstand ein geringer Sachschaden am Pkw". In Berlin brennen hunderte Autos pro Jahr. Im Jahr 2007 hatte die Polizei 14 Verdächtige gefasst, von denen neun ein Handy dabei hatten. Deswegen gehen die Ermittler davon aus, dass auch diesmal der Täter oder die Täterin ein Handy einstecken hatte. Also fordert die Polizei „sämtliche Verkehrsdaten" der 13 am Tatort zu empfangenden Funkzellen über einen bestimmten Zeitraum vor und nach der Tat an. Ein Gericht bewilligt den Antrag und die vier Betreiber der deutschen Mobilfunknetze geben die Daten heraus. Die Kommunikationsdaten aller Handys und Mobilgeräte aus einem ganzen Stadtviertel landen damit in Datenbanken der Polizei.[2]

Diese Information haben wir als interaktive Karte aufbereitet und damit sichtbar gemacht, welches Stadtgebiet von dieser Maßnahme betroffen war. Dazu haben wir die juristischen Hintergründe, eine politische Einordnung sowie offene Fragen geliefert.[3] Bis zu diesem Zeitpunkt konnte oder wollte uns keine der angefragten verantwortlichen Stellen Antworten auf unsere Fragen liefern: Wie viele Verkehrs- und Verbindungsdaten wurden in diesem

1 Massenhafte Funkzellenabfrage jetzt auch in Berlin: Was Vorratsdatenspeicherung wirklich bedeutet, in: http://netzpolitik.org/2012/massenhafte-funkzellenabfrage-jetzt-auch-in-berlin-was-vorratsdatenspeicherung-wirklich-bedeutet/; 5.12.2012.

2 *Kopietz, Andreas* 2012: Millionen Handys überwacht, in: http://www.berliner-zeitung.de/berlin/auto-brandstiftungen-millionen-handys-ueberwacht,10809148,11485872.html; 5.12.2012.

3 Nachlese zur Funkzellenabfrage: Noch viele Fragen offen, in: https://netzpolitik.org/2012/nachlese-zur-funkzellenabfrage-noch-viele-fragen-offen/; 5.12.2012.

einen Fall übermittelt? Wie viele Mobilfunkanschlüsse bzw. Rufnummern sind davon betroffen? Von wie vielen Mobilfunkanschlüssen wurden die Stammdaten eingeholt? Wie viele solcher Funkzellenanfragen gibt es?

Nach unserer Veröffentlichung erfolgte ein breites Medien-Echo, mit dem wir nicht ganz gerechnet hatten. Jede Berliner Tageszeitung und viele überregionale Medien griffen unseren Fall auf und berichteten darüber. Der Tenor der Berichterstattung bezeichnete diese Art der Funkzellenabfragen als einen Skandal. Wie schon bei der massenhaften Auswertung von Mobilfunk-Daten bei Anti-Nazi-Protesten in Dresden 2011, wurde auch hier die Verhältnismäßigkeit bezweifelt, da die Kommunikationsdaten und Aufenthaltsorte tausender Unschuldiger gespeichert und gerastert wurden. Politiker und Datenschützer zeigten sich überrascht von dem Fall und dem Ausmaß dieser Maßnahme.

Dass der geschilderte Fall nicht einzigartig ist sondern Methode hat, konnten wir drei Tage später nachweisen. Am 22. Januar veröffentlichten wir auf netzpolitik.org erneut Akten, in denen eine weitere Funkzellenabfrage angefordert wurde.[4] Wieder ging es um eine Brandstiftung, diesmal mit 4.000 Euro Schaden. Dafür sollten die liebevoll „Turmdaten" genannten Datenberge sogar einen Zeitraum von acht Stunden umfassen. Erneut visualisierten wir das Stadtgebiet und, da sich dieser Fall in unmittelbarer Nähe des ersten Falls abspielte, legten die beiden Gebiete der abgefragten Funkzellen übereinander. Dadurch wurde sichtbar, dass tausende Anwohner potentiell in den Datenbergen beider Abfragen auftauchten. Zu dieser Zeit wurde auch langsam öffentlich, dass diese Maßnahme „absolut üblich" ist und innerhalb von zwei Jahren mehrere Millionen Handys von nur einem einzigen Mobilfunkanbieter an die Behörden übermittelt wurden.

Dieses Ausmaß wurde am 23. Januar ganz offiziell bestätigt.[5] An diesem Tag thematisierten gleich mehrere Ausschüsse im Berliner Abgeordnetenhaus diese fragwürdige Ermittlungsmethode. Widerwillig musste Polizeivizepräsidentin Koppers dort zugeben, dass in den vier Jahren seit dem Gesetz zur Vorratsdatenspeicherung fast 1.000 Funkzellenabfragen vorgenommen wurden – nur in Berlin und nur wegen Autobrandstiftungen. Dabei sammelte der

4 Funkzellenabfrage in Berlin: Und noch ein Fall, in: https://netzpolitik.org/2012/funkzellenabfrage-in-berlin-und-noch-ein-fall/; 5.12.2012.

5 Funkzellenabfrage im Berliner Innenausschuss: Vier Millionen abgefragte Daten, kein Ermittlungserfolg, in: https://netzpolitik.org/2012/funkzellenabfrage-im-berliner-innenausschuss-vier-millionen-abgefragte-daten-kein-ermittlungserfolg/; 5.12.2012.

polizeiliche Staatsschutz mehr als vier Millionen Verkehrsdaten, also Daten über einzelne Telefonanrufe und SMS. Pro Funkzelle sind zwischen 5.000 und 15.000 Verkehrsdatensätze zusammen gekommen. Von fast 1.000 Handys wurden Namen und Adressen der Anschlussinhaber gesammelt. Millionen Datensätze waren noch immer nicht gelöscht. Gebracht hat die Sammelwut gar nichts: obwohl bei einem Viertel aller Auto-Brände Funkzellenauswertungen durchgeführt wurden, konnte kein einziger Tatverdächtiger ermittelt werden.

Im Verlauf des Jahres stiegen die Zahlen, die an die Öffentlichkeit gelangten, weiter.[6] Kurz nach der ersten Ausschusssitzung gab Berlins Innenstaatssekretär Krömer bekannt, dass die massenhafte Handyüberwachung auch in anderen Fällen eingesetzt wird. In den drei Jahren 2009 bis 2011 wurden in 800 weiteren Fällen Funkzellenabfragen durchgeführt und bis zu acht Millionen Verbindungen in der Hauptstadt ausgewertet. Die Zahl der Funkzellenabfragen nahm jedes Jahr zu, obwohl gleichzeitig die Kriminalitätsrate abnahm. Im August wurden noch höhere Werte im Berliner Innenausschuss genannt. Zwar informierte der Senat weiterhin nur über ein Fünftel der 1.400 Funkzellenabfragen, jedoch konnte daraus hochgerechnet werden, dass in vier Jahren mehr als 30 Millionen Datensätze allein in der Hauptstadt gesammelt wurden. Statistisch gesehen ist damit jeder Berliner pro Jahr zwei Mal verdächtig.

Alle bisher genannten Fälle spielten sich in Berlin ab. Doch auch in anderen Bundesländern werden Funkzellenanfragen durchgeführt. Leider war es uns im Laufe des Jahres nicht möglich, Details und Zahlen zu erhalten, genau wie uns vor der öffentlichen Berichterstattung auch in Berlin die Auskunft verweigert wurde. Offizielle Statistiken sind laut Gesetz nicht vorgeschrieben, aber laut Hochrechnungen könnte es über 1.500 Funkzellenabfragen pro Jahr in Deutschland geben. Im Oktober wurde bekannt, dass auch bei den Ermittlungen zum Nationalsozialistischen Untergrund mehr als 20 Millionen Funkzellendatensätze und fast 14.000 Datensätze über Anschlussinhaber erhoben, gespeichert und zusammengeführt wurden. Die Aufklärungsquote dieser Datenberge wurde weiter oben bereits genannt.

6 Funkzellenabfrage geht weiter: Jeder Berliner ist jedes Jahr zwei Mal verdächtig in: https://netzpolitik.org/2012/funkzellenabfrage-geht-weiter-jeder-berliner-ist-jedes-jahr-zwei-mal-verdachtig/; 5.12.2012.

Dem Berliner Landesbeauftragten für Datenschutz, Dr. Alexander Dix, war bis zu unserer Veröffentlichung kein einziger solcher Fall der Datenauswertung in der Hauptstadt bekannt. Er zeigte sich immer wieder erstaunt und schockiert von der Masse an Daten und der weiten Verbreitung dieser Ermittlungsmaßnahme. Vor allem erzürnte ihn, das keine einzige betroffene Person je darüber informiert worden ist, weil der Polizei laut Eigenaussage ein „Interesse an einer Benachrichtigung nicht ersichtlich" war. Die Gesetze sagten ausdrücklich, dass eine Benachrichtigung erfolgen muss und die Regel zu sein hat, so Dix. Jede Nicht-Benachrichtigung müsse einzeln begründet werden. Zudem teilt er unsere Einschätzung, dass nicht nur die mehr als 5.000 Menschen, deren Namen und Adressen vorhanden sind, benachrichtigen werden können. Von den übrigen Hunderttausenden wurden schließlich die Telefonnummern gesammelt – und im Gesetz wird nicht festgesetzt, dass die Benachrichtigung per Brief erfolgen muss. Wieso also nicht einfach mal anrufen? Vielleicht fürchten die Polizeibehörden ja, dass sich die Mehrheit der Bevölkerung dann gegen eine Vorratsdatenspeicherung aussprechen würde, weil dann deutlich wäre, dass vor allem Unschuldige betroffen sind.

Dr. Dix kündigte noch im Januar eine gründliche Überprüfung der allgemeinen Praxis und stichprobenartiger Fälle bei der Berliner Polizei an. Am 4. September stellte er diesen Prüfbericht vor und kam darin zu dem Schluss, dass die Funkzellenabfrage „offensichtlich zum alltäglichen Ermittlungsinstrument geworden ist, das routinemäßig und ohne hinreichende Beachtung der gesetzlichen Vorgaben eingesetzt wird."[7] Nach der Auswertung von über einhundert Ermittlungsakten, Kontrollen bei der Zentralstelle Telekommunikationsüberwachung im Landeskriminalamt und Gesprächen mit Staatsanwaltschaft und Polizeipräsident kam der Datenschützer zu einem vernichtenden Urteil: Die Behörden machten so ziemlich jeden Fehler, der möglich ist und missachteten regelmäßig gesetzliche Vorgaben.

Immer wieder wurden Funkzellenabfragen angeordnet, obwohl sie nicht erforderlich waren. Das Gesetz sieht dieses Mittel eigentlich nur als „Ultima Ratio" vor, also erst wenn andere Ermittlungswege nicht zum Erfolg führten. Stattdessen wurden Funkzellenabfragen durchgeführt, ohne vorher Gutachten abzuwarten oder Zeugen zu befragen. In manchen Fällen lag nicht mal eine Straftat vor (technischer Defekt statt Autobrandstiftung), in anderen war

7 Berliner Datenschutzbeauftragter: Funkzellenabfrage ist Routinemaßnahme, die regelmäßig Gesetze verletzt, in: https://netzpolitik.org/2012/berliner-datenschutzbeauftragter-funkzellenabfrage-ist-routinemasnahme-die-regelmasig-gesetze-verletzt/; 5.12.2012.

die Straftat nicht „von auch im Einzelfall erheblicher Bedeutung", wie es das Gesetz vorschreibt (100 Euro Schaden). Eine Prüfung der Verhältnismäßigkeit „erfolgte in der Regel unzureichend und zum Teil überhaupt nicht". Laut Gesetz muss es Hinweise dafür geben, dass eine Funkzellenabfragen zum Erfolg führen kann, trotzdem wurde sie oft angewendet, einfach weil heute jeder ein Handy hat. Klar rechtswidrig, wie der Datenschutzbeauftragte feststellte.

Die Löschbestimmungen, die für solche Daten gelten, wurden laut Dix „regelmäßig nicht beachtet". Auch bei abgeschlossenen Verfahren konnte der Datenschützer in 90 % der Fälle keine Löschung der Daten nachvollziehen. In einem Fall wurden die erhobenen Daten nicht mal ausgewertet, sollten aber für geschlagene 30 Jahre gespeichert werden. „Aufgrund dieser Prüfungsergebnisse ist daher davon auszugehen, dass die Staatsanwaltschaft überwiegend die Erforderlichkeit der weiteren Speicherung der Daten aus Funkzellenabfragen nicht fortlaufend kontrolliert und daher die gesetzlichen Vorgaben zur Löschung dieser Daten größtenteils nicht umsetzt", so Dix.

Besonders stört ihn, dass die Betroffenen „im Allgemeinen nicht von der Maßnahme benachrichtigt" werden. Dabei ist die Benachrichtigung von Betroffenen eindeutig gesetzlich vorgeschrieben. Die Nicht-Informierung stellt daher einen weiteren klaren Gesetzesbruch dar. Die von ihm geforderte Benachrichtigung der Betroffenen von 1400 Funkzellenabfragen in Berlin ist unseren Wissens nach bis heute nicht passiert. Weiterhin forderte Dix, dass alle Daten, die nicht „nachweislich weiterhin zur Strafverfolgung erforderlich" sind, unverzüglich gelöscht werden. Das können wir nicht nachprüfen.

Bei all dieser Kritik ist darüber hinaus die Wirksamkeit der Funkzellenabfrage generell sehr begrenzt. Fast alle Verfahren wurden trotz massenhafter Handydaten ohne Tatverdacht eingestellt. Kein einziger Auto-Brandstifter konnte damit gefasst werden. Nur zwei Betrüger wurden erwischt. Vor diesem Hintergrund fordert der oberste Berliner Datenschützer eine „gesetzliche Einschränkung" und „klare Grenzen" der Funkzellenabfrage. Die bestehenden Gesetze sind zu ungenau und werden zudem teilweise ignoriert.

Auch die Grünen fordern sowohl auf Landes- als auch auf Bundesebene eine Einschränkung der Funkzellenabfrage, die Linkspartei hat sogar einen Gesetzesvorschlag zur Abschaffung der Maßnahme eingebracht. Doch die Regierungskoalitionen im Deutschen Bundestag und im Berliner Abgeordneten-

haus halten trotz aller Kritik an der Funkzellenabfrage als Ermittlungsinstrument fest. Vor allem CDU und SPD können an der massenhaften Handyüberwachung überwiegend Unschuldiger nichts problematisches erkennen.

Konsequenterweise korreliert diese Haltung mit der Einstellung der Parteien zur Vorratsdatenspeicherung. Dabei verdeutlichen gerade diese millionenfach von Unschuldigen erhobenen Datensätze bei der Funkzellenabfrage, was die manchmal abstrakte Vorratsdatenspeicherung wirklich bedeutet. Die rechtliche Grundlage der Funkzellenabfrage wurde bereits 2001 kurz nach dem 11. September von der rot-grünen Bundesregierung geschaffen und war ursprünglich befristet, wurde aber immer wieder verlängert. Erst mit dem Gesetz zur Vorratsdatenspeicherung wurde die Befristung im Jahr 2007 komplett abgeschafft.

Auch das Urteil des Bundesverfassungsgerichts im März 2010 änderte daran nichts. Das Gericht untersagte darin nur die Verpflichtung zur Speicherung, die Anbieter speichern aber auch ohne Verpflichtung freiwillig weiter. Und die Behörden nutzen diese Daten fleißig.

De facto gibt es also auch im Bereich Mobilfunk immer noch eine Speicherung von Daten auf Vorrat, auf deutsch: Vorratsdatenspeicherung. Und diese Daten werden viel umfassender genutzt als uns in der Diskussion um die Vorratsdatenspeicherung immer verkauft werden soll. Jeder kann betroffen sein.

Interview mit Ulf Buermeyer: „Auf Vorratsdatenspeicherung verzichten“

netzpolitik.org: Warum bist du gegen die Vorratsdatenspeicherung, hast Du was zu verbergen?

Ulf Buermeyer: Ja, natürlich – meine Privatsphäre, so wie jeder Mensch, der nicht zum Exhibitionismus neigt. Aber mal ernsthaft: Die massenweise Speicherung sensibler Daten lässt sich mit meinem Verständnis eines freiheitlichen Rechtsstaats nicht vereinbaren. Wenn es überhaupt Vorteile für die polizeilichen Ermittlungen geben sollte – alle Kriminalstatistiken sprechen eher dafür, dass die Vorratsdatenspeicherung wirkungslos ist – dann stehen die minimalen Erfolge in keinem Verhältnis zu den gravierenden Einbußen, was die Privatsphäre aller Bürgerinnen und Bürger angeht. Deswegen bin ich gegen die Vorratsdatenspeicherung, obwohl ich selbst jeden Tag Strafverfolgung betreibe.

netzpolitik.org: Deutschland hat zwar im Moment keine Vorratsdatenspeicherung, aber viele Provider speichern trotzdem viele dieser Daten. Wo ist das Problem?

Ulf Buermeyer: Das Problem liegt darin, dass es keine hinreichend präzisen gesetzlichen Vorgaben gibt, welche Daten Provider wie lange speichern dürfen – und diesen Graubereich nutzen manche Provider aus, um möglichst viel zu speichern. Mit den Daten lässt sich schließlich Geld verdienen, da jede Auskunft an die Polizei vergütet wird. So rächt sich übrigens auch, dass der Bund die Provider nicht für ihre erheblichen Investitionen entschädigt, zu denen er sie mit der Vorratsdatenspeicherung gezwungen hat.

netzpolitik.org: Was ist denn die Alternative zur Vorratsdatenspeicherung? *Ulf Buermeyer:* Keine: Man kann ersatzlos auf sie verzichten, weil ohnehin bereits genug Daten für polizeiliche Ermittlungen zur Verfügung stehen, die man allerdings „auf Zuruf“ einfrieren können sollte – insoweit teile ich die Auffassung des Bundesdatenschutzbeauftragten und der Bundesministerin der Justiz.

netzpolitik.org: Funkzellenabfragen sind doch praktisch, warum hast Du was dagegen?

Ulf Buermeyer: Ich habe nichts gegen das Instrument der Funkzellenabfrage. Mir geht es allerdings darum, dass es mit Bedacht eingesetzt wird: Die nicht personalisierte Funkzellenabfrage (also die Abfrage der sog. „Turmdaten") greift massiv in die Telekommunikationsfreiheit von tausenden Bürgerinnen und Bürgern ein, die praktisch alle vollkommen unverdächtig sind. Eine Maßnahme mit einer solchen Breitenwirkung ist nur verhältnismäßig, wenn es tatsächlich um schwerste Straftaten geht, also etwa um Tötungsdelikte oder andere Schwerverbrechen, bei denen langjährige Freiheitsstrafen drohen.

Außerdem darf die Maßnahme nicht dazu missbraucht werden, jedenfalls faktisch davon abzuschrecken, an Demonstrationen teilzunehmen: Demonstrationen sind nach den Maßstäben des Grundgesetzes „gut" (Art. 8 Grundgesetz), auch wenn sie der Polizei mitunter viel Arbeit machen. Ich würde mir wünschen, dass die Sicherheitsbehörden konsequenter dem Eindruck entgegenwirken, es sollte per se davon abgeschreckt werden, dieses Grundrecht auch wahrzunehmen: Ich will nicht unterstellen, dass diese Überlegung zum Beispiel in Dresden eine Rolle gespielt hat. Aber es entsteht ein fataler Eindruck, wenn systematisch die Teilnehmer von Demonstrationen überwacht werden, nur weil einige wenige unter ihnen sich möglicherweise strafbar gemacht haben. Polizei und Justiz leben von dem Vertrauen der Bürgerinnen und Bürger, dass sie jederzeit unsere Verfassung schützen. Vorgehensweisen, wie sie der Sächsische Datenschutzbeauftragte kritisiert hat, sind nicht geeignet, dieses Vertrauen zu stärken.

netzpolitik.org: Viele der vorgesehenen Kontrollmöglichkeiten funktionieren nicht. Was schlägst du stattdessen vor?

Ulf Buermeyer: Es gibt keine Alternative zum Richtervorbehalt, aber man muss sich darüber im klaren sein, dass er derzeit längst nicht immer die Gewähr dafür bietet, dass eine beantragte Maßnahme tatsächlich rechtmäßig ist, auch wenn die Anordnung des Ermittlungsrichters sie natürlich formell zunächst legitimiert. Um den Richtervorbehalt zu stärken, kommt eine Vielzahl von Maßnahmen in Betracht. Sinnvoll wäre etwa eine deutlich geringere Arbeitsbelastung der Kolleginnen und Kollegen, so dass sie alle Akten auch

wirklich lesen können, sowie der Einsatz von besonders erfahrenen Richterinnen und Richtern, die bereits einmal befördert wurden (Besoldungsgruppe R2).

Bezogen auf Funkzellenabfragen und Telekommunikationsüberwachung müsste aber auch die Strafprozessordnung reformiert werden: Bislang sind die Voraussetzungen für beide Maßnahmen mit sehr weiten Begriffen formuliert. Nötig wäre es, stattdessen konkrete Maßstäbe für die Verhältnismäßigkeit vorzusehen. Ich würde vorschlagen, dass eine bestimmte Strafe – z. B. Ein Jahr Freiheitsstrafe – im konkreten Fall mindestens zu erwarten sein muss, damit eine Funkzellenabfrage durchgeführt oder ein Telefonanschluss abgehört werden kann. Bisher geht es danach, ob das verletzte Strafgesetz abstrakt einen entsprechenden Strafrahmen enthält. Die Strafrahmen des Strafgesetzbuchs sind aber so weit gefasst, dass diese Voraussetzung in der Praxis fast immer erfüllt ist, z. B. Ist ein einfacher Ladendiebstahl theoretisch mit bis zu fünf Jahren Freiheitsstrafe bedroht. Der Ermittlungsrichter hat also nach geltenden Recht viel zu wenig konkrete Maßstäbe an der Hand, nach denen er wirklich kritisch prüfen könnte.

netzpolitik.org: Eine Funkzellenabfrage betrifft tausende Menschen. Müssen die Betroffenen darüber informiert werden?

Ulf Buermeyer: Das sollte selbstverständlich sein, denn wo kein Kläger, da kein Richter: Wenn die Polizei nicht über eine Funkzellenabfrage informiert, entsteht der fatale Eindruck, die Behörden hätten etwas zu verbergen. Das haben Polizei und Justiz aber nicht nötig – wir sollten mit offenen Karten spielen und jeden informieren, der von einer Funkzellenabfrage erfasst worden ist. Nur so kann übrigens auch der Eingriff in das Fernmeldegeheimnis im Nachhinein abgemildert werden.

netzpolitik.org: Der Digitale Gesellschaft e. V., dessen Mitglied zu bist, hat dieses Jahr einen Gesetzentwurf zur Lösung der Störerhaftung vorgestellt. Welches Ziel verfolgt dieser?

Ulf Buermeyer: Es geht darum, dass kleine private und gewerbliche Anbieter lokaler Funknetze (WLANs) – ebenso wie bisher schon große Provider – nicht mehr für mögliche Rechtsverletzungen haften sollen, die unbekannte Nutzer ihrer Netze begehen.

netzpolitik.org: Welche Alternativen zu Eurem Vorschlag sind momentan in der Diskussion?

Ulf Buermeyer: Echte Alternativen sind bisher nicht diskutiert worden – die SPD hat unseren Vorschlag zwar aufgegriffen, aber bisher leider nicht in Form eines konkreten Gesetzentwurfs, sondern nur mit einem Prüfauftrag an die Bundesregierung. Die Fraktion der Linken hat den Entwurf des Vereins Digitale Gesellschaft hingegen in den Bundestag eingebracht. Ich würde mich freuen, wenn auch andere Fraktionen den Schutz der Bürgerinnen und Bürger ernst nehmen und sich dem anschließen würden.

netzpolitik.org: Bedeutet ein Ausschluss der Haftung für offene WLANs nicht das Ende der Verfolgung aller Urheberrechtsverletzungen, da ein Verletzer nur angeben muss, sein WLAN sei offen gewesen?

Ulf Buermeyer: Ein Missbrauch ist nicht zu befürchten, da er das im Zweifel beweisen muss. Außerdem gibt es bereits heute zahllose Möglichkeiten, anonym das Netz zu nutzen. Unsere Initiative wird kaum Auswirkungen auf die Rechteinhaber haben, aber sie würde die notwendige Rechtssicherheit für die Betreiberinnen und Betreiber von WLANs schaffen. Hier hat unser Parlament die Chance, unser Land nahezu ohne Aufwand und Kosten ein Stück fairer und menschlicher zu gestalten – ich hoffe sehr, dass der Bundestag diese Chance auch wahrnimmt.

netzpolitik.org: Was hat Euer Vorschlag mit Freifunk zu tun? *Ulf Buermeyer:* Auch die Freifunker würden von der Haftungsfreistellung profitieren, soweit sie Internet-Zugang für die Öffentlichkeit anbieten.

Passenger Name Records: Absturz der Privatsphäre

Alexander Sander

Die Terroristen, die am 11. September 2001 die Anschläge auf die USA verübten, benutzten bekanntermaßen Flugzeuge, um ihre Tat durchzuführen. Das veranlasste die westliche Welt, die Sicherheitsstandards im Luftverkehr zu überdenken und zu überarbeiten. Das Fliegen soll sicherer werden, derartige Anschläge müssen bereits im Vorfeld verhindert werden – so der Tenor nicht nur der Sicherheitsbehörden. Dies führte zu teilweise völlig irrwitzigen und willkürlichen Regelungen, wie jener, dass Passagiere nur noch mit 150ml Flüssigkeiten reisen dürfen.

Auch eine intensive Debatte über Nacktscanner wurde und wird geführt. Die teuren Geräte sollen für mehr Sicherheit sorgen. Den berühmt gewordenen Unterhosenbomber hätte man mit Hilfe der Geräte aber auch nicht aufspüren können.

In den USA ist man sogar soweit gegangen, sogenannte Sky-Marshals einzusetzen. Dabei handelt es sich um bewaffnete Flugsicherheitsbegleiter, die im Ernstfall den Terroristen mit Waffengewalt niederstrecken sollen. Dass diese Marshals jedoch ebenso von Terroristen überwältigt werden können, hat man wohl nicht bedacht.

In Deutschland wurde sogar der Vorschlag in die Debatte eingebracht, von Terroristen gekaperte Passagiermaschinen abschießen zu dürfen, sollten diese sich in besiedelte Gebiete bewegen. Dieses gegeneinander Abwägen von Menschenleben ist sicher einer der perversesten Auswüchse der Anti-Terror-Debatte.

Weniger offensichtlich sind die Bemühungen der Ermittlungsbehörden, die persönlichsten Informationen von den Bürgerinnen und Bürgern zu erhalten. Bis tief in die Privatsphäre eines jeden Einzelnen hinein – verdächtig oder nicht – wird ermittelt. Die Kompetenzen und Zugriffsrechte sollen immer weiter ausgeweitet werden. Angefangen von der Vorratsdatenspeicherung von Telekommunikationsdaten über die Übermittlung von Bankdaten zu Analysezwecken an die USA bis hin zur Auswertung des Reiseverhaltens der Bürgerinnen und Bürger.

Die abwegige Logik der Ermittlungsbehörden besteht seit 2001 grob zusammengefasst daraus, dass „mehr Daten“ auch zu „mehr Sicherheit“ führen. Genauer gesagt, wollen Ermittlungsbehörden immer weiter reichende Zugriffsrechte auf personenbezogene Daten der Bürgerinnen und Bürger. Dabei beschränkt sich der Datenzugriff keineswegs nur auf den Moment, wo eine Person verdächtig ist und ein Richter den Verdacht bestätigt. Die Behörden wollen auf die Daten zugreifen, um vermeintliche Verdächtige überhaupt erst zu finden – Voraussetzung dafür ist natürlich, dass es keinen Richtervorbehalt gibt, sondern auf die Daten zu jederzeit einfach zugegriffen werden kann. Durch Profiling und Datamining werden Menschen kategorisiert und es wird versucht, mit Hilfe der Analyse der Datensätze vermeintliche Verdächtige zu finden.

Doch über was für Daten reden wir eigentlich genau? Nun, personenbezogene Daten gibt es viele. Angefangen vom Namen, über das Alter bis hin zu Kreditkarten- und Kontoinformationen reicht das Spektrum der Informationen über eine Person. Auch sogenannte „sensible“ Daten gehören dazu, zum Beispiel die Religionszugehörigkeit.

Genau jene Daten werden zum Beispiel von Airlines gesammelt, um einen perfekten Reiseablauf für die Passagiere zu garantieren. Bis zu 60 Einzelinformationen werden von den Airlines für einen einzigen Flug eines einzigen Passagiers gesammelt, wie Menüwünsche (über die sich Rückschlüsse auf die Religionszugehörigkeit ziehen lassen), Informationen über den gesundheitlichen Zustand eines Reisenden oder mögliche Anschlussflüge.

Die Airlines benötigen all diese Informationen, um auf die speziellen Wünsche der Passagiere eingehen zu können. Reisende wollen vegetarisches Essen während ihres Flugs bestellen, den Anschlussflug erreichen, neben der Person sitzen, mit der man gemeinsam reist und das Gepäck wieder bekommen, wenn man endlich am Ziel angekommen ist. Für alle diese Momente braucht man die sogenannten PNR-Daten – Passenger Name Records.

Genau diese PNR-Daten wurden mit den Anschlägen 2001 für Ermittlungsbehörden auf einmal interessant. Mit Hilfe der Daten will man Reisebewegungen, mögliche Netzwerke und kommende terroristische Attentate sowie kriminelle Handlungen aufdecken. Die Amerikaner begannen die Daten sämtlicher Flüge auszuwerten, auch von europäischen Flügen. Dies fand jedoch im Geheimen und ohne Zustimmung der Europäer statt. Schnell wurde, nach-

dem diese Praxis bekannt wurde, ein Abkommen zwischen der Europäischen Union und den USA geschlossen, welches die Datenübermittlung und Auswertung auf eine rechtliche Grundlage stellen sollte. Jedoch stellte sich heraus, dass jenes Abkommen nicht den rechtlichen Standards entsprochen hat. Ein neues Interimsabkommen wurde geschlossen, welches dann 2011 durch erneute Verhandlungen zwischen der EU-Kommission und dem DHS, dem Amerikanischen Heimatschutzministerium, ersetzt werden sollte. Das Abkommen zur Übermittlung von Fluggastdaten wurde dann mit breiter Mehrheit im EU-Parlament angenommen und durch den EU-Rat bestätigt. Seit Ende 2011 dürfen nun die Amerikaner sämtliche PNR-Daten von Flügen von Europa in die USA und zurück bekommen und auswerten. Die Daten werden für 15 Jahre gespeichert und auch von Geheimdiensten genutzt. Eine gigantische Datenbank steht seitdem, mit europäischem Segen, den USA zur Verfügung, um Daten europäischer Bürger jederzeit auswerten zu können und für Profiling und Datamining zu nutzen.

Noch während der Verhandlungen mit den USA stellte die EU-Kommission einen eigenen Vorschlag vor, wie innerhalb Europas die PNR Daten ausgewertet werden sollen. In ihrem Vorschlag vom Februar 2011 stellt die Kommission verschiedene Möglichkeiten vor, wie PNR-Daten genutzt werden sollen. So sollen die Daten in Echtzeit analysiert werden, „damit bisher „unbekannte" Verdächtige identifiziert und ein Datenabgleich mit verschiedenen Datenbanken für gesuchte Personen und Gegenstände durchgeführt werden können." Die Daten sollen darüber hinaus auch proaktiv „zur Analyse und Bestimmung von Prüfkriterien, die für eine Überprüfung der Fluggäste vor ihrer Ankunft oder Abreise herangezogen werden können." genutzt werden. Dadurch kommt es natürlich unweigerlich zu der Überprüfung unverdächtiger Personen. Damit geraten unbescholtene Bürger in das Visier von Ermittlungsbehörden – und dies ohne jede richterliche Genehmigung. Rechtsstaatliche Prinzipien werden völlig auf den Kopf gestellt.

Problematisch ist jedoch nicht nur, dass unbescholtene Bürgerinnen und Bürger überwacht werden und in das Visier von Ermittlungsbehörden geraten, vielleicht sogar unter Terrorverdacht stehen, sondern auch, dass die Datenanalyse kein Allheilmittel ist. Wie der Sicherheitsexperte Bruce Schneider bereits 2006 darlegte, hat die Auswertung derartiger Daten massive Mängel. Um Terroristen fassen zu können, muss es zuvor bestimmte Kriterien geben, die einen Terroristen auszeichnen, die dann dazu führen, dass andere Perso-

nen in dem Datensatz ebenfalls als Terroristen identifiziert werden können. Nur gibt es derartig wenige Terroristen, als dass man verlässliche Kriterien für die Datenanalyse finden könnte. Damit entstehen zwei Probleme: Erstens führt dies zu sogenannten positive false alerts – das bedeutet, dass Personen als Terroristen identifiziert werden, die gar keine sind und zweitens zu negative false alerts – das betrifft tatsächliche Terroristen, die jedoch durch das Raster fallen und dadurch nicht überwacht werden. Das bedeutet, dass zum einen Kräfte gebunden werden, um unbescholtene Bürger zu überwachen und zum anderen genau jene Kräfte fehlen, um die tatsächlichen Terroristen überführen zu können.

Damit zeigt sich, dass die Auswertung von Fluggastdaten nicht nur rechtsstaatliche Probleme mit sich bringt sondern auch aus ermittlungstechnischer Sicht nicht erfolgreich sein kann. Die Debatte um die Auswertung der PNR Daten machte deutlich, was künftig droht: Die Total-Überwachung aller Reisebewegungen. Einige Vertreter der Mitgliedstaaten, beispielsweise die Briten und auch einige Abgeordnete im EU-Parlament haben bereits jetzt für eine Ausweitung der PNR-Analyse plädiert. So sollen etwa auch innereuropäische Flüge überwacht werden, sowie auch der Zug- und Schiffsverkehr. Bei der Autovermietung werden ebenfalls PNR-Daten gesammelt, sodass auch dies künftig überwacht werden könnte.

Mit der Einführung derartiger Maßnahmen wie der Vorratsdatenspeicherung von Reisedaten wird der Rechtsstaat immer weiter ausgehöhlt und bis zur Unkenntlichkeit deformiert. Ein fürsorglicher Präventionsstaat wird stattdessen aufgebaut, der alle Bürgerinnen und Bürger zu jeder Zeit wie Verdächtige behandelt. Dass mit derartigen Maßnahmen Terroristen und schwere Kriminelle gefasst werden können, wurde bisher nicht belegt – im Gegenteil, die Maßnahmen stellen sich als unwirksam heraus. Es wird also eine völlig unverhältnismäßige und in die Grundrechte eingreifende Maßnahme eingeführt, die keine Wirksamkeit entfalten kann.

Wir brauchen daher dringend eine ernsthafte Evaluation sämtlicher Sicherheitsgesetze. Da selbst die EU-Kommission die Richtlinie für gescheitert erklärte, ist darüber hinaus die Abschaffung der Vorratsdatenspeicherung von Telekommunikationsdaten längst überfällig. Die Vorratsdatenspeicherung von Reisedaten darf nicht eingeführt werden, die Abkommen mit Drittstaaten zur Übermittlung von PNR-Daten sind unverzüglich abzuschaffen.

Regierungen sind noch immer die größte Gefahr für ein freies Netz

Jillian C. York

Manche Dinge ändern sich, andere bleiben gleich. Während sich die Arten von Gefahren, denen Internetnutzer/innen auf der ganzen Welt ausgesetzt sind, in den letzten Jahren verändert haben – von gezielt eingesetzter Schadsoftware bis zu DDoS-Angriffen – ist eines gleich geblieben: Regierungen, die Kontrolle über ihre Bevölkerung ausüben wollen, sind noch immer die größte Gefahr für ein offenes Internet.

Nachgiebige Unternehmen

Das wird nirgends deutlicher als im letzten Transparenzbericht[1] von Google. Wie Dorothy Chou auf dem öffentlichen Policy Blog[2] von Google erklärt, steigt die Zahl der Anfragen von Regierungen sowohl nach Nutzerdaten als auch nach der Entfernung von Inhalten weiter an. Die Anträge auf Löschung von Inhalten blieben eine Zeit lang gleich, so Chou, erreichten aber in der ersten Jahreshälfte 2012 einen neuen Höchststand, als weltweit 1.791 Anfragen von Regierungsbeamten auf Löschung von 17.746 Suchergebnissen verzeichnet wurden.

Es gibt unzählige Begründungen für diese Anfragen, für Regierungen ist allerdings „Verleumdung" die Hauptursache und macht fast 40 % aller Anfragen aus, gefolgt von Datenschutz/Sicherheit, die sich laut Chou auf „Anfragen der Regierung nach Entfernung von Inhalten unter bestimmten Datenschutzgesetzen" beziehen, die „sich auf eine Einzelperson oder PolitikerIn/Polizei beziehen". Solche Anfragen können entweder von Gerichten oder anderen staatlichen Behörden kommen. Nicht jedem dieser Anträge kommt Google nach, der Transparenzbericht zeigt die Erfüllungsrate pro Land.

1 Google Transparenzbericht, in: http://www.google.com/transparencyreport/; 3.12.2012.

2 Google Public Policy Blog, in: http://googlepublicpolicy.blogspot.com/; 4.12.2012.

Zensur in Demokratien

Also, welche Länder sind die schlimmsten Missetäter? Wenig überraschend führen die USA die Liste mal wieder an, gefolgt von Deutschland und Brasilien. Diese drei Staaten dominieren seit Beginn der Transparenzberichte 2010 fast durchgehend die Spitze. Andere Übeltäter sind 2012 Argentinien, die Türkei und Indien.

Es ist bemerkenswert, dass alle Länder an der Spitze der Liste Demokratien sind. Noch bemerkenswerter ist, dass einige dieser Länder Anfragen stellten, die Google als unseriös empfand. Sie erhielten beispielsweise fünf Anfragen und eine gerichtliche Anordnung aus den USA auf Löschung von sieben YouTube-Videos wegen ihrer Kritik an lokalen und staatlichen Behörden, Strafverfolgung oder Beamten – politische Aussagen, die klar vom Ersten. Zusatzartikel zur US-Verfassung geschützt sind. Während YouTube rechtlich nicht verpflichtet ist, diese Inhalte weiterhin der Öffentlichkeit anzubieten (und es lobenswerterweise trotzdem tut), sollten sich die Beamt/innen schämen, die diese Anfragen gestellt haben. Ebenso erhielt Google eine Anfrage einer britischen Strafverfolgungsbehörde auf Löschung eines YouTube-Videos, in dem die Behörde als rassistisch kritisiert wurde – sie kamen dieser Anfrage ebenfalls nicht nach.

Diese unverantwortlichen Anfragen sind leider als Anzeichen für ein Zensurverhalten zu sehen, das sich in mutmaßlich demokratischen Staaten entwickelt. Das Vereinigte Königreich hat in diesem Jahr Provider und Computerhersteller dazu gezwungen, Kindersicherungen einzurichten,[3] während Russland – bislang meist als Demokratie bezeichnet – im Herbst diesen Jahres begann, erstmals Webseiten zu sperren.[4]

Der lange Arm des indischen Gesetzes

Unternehmen zur Zensur von Online-Inhalten zu zwingen, ist ein recht neues Phänomen; manche Länder bevorzugen eher traditionelle Mittel, andere nutzen eine Kombination aus verschiedenen Taktiken. Indien, über das die

3 *Shipman, Tim* 2012: PM steps in to curb menace of online porn: Cameron to ensure parents are led through a filter process on all new computers, in: http://www.dailymail.co.uk/news/article-2234264/David-Cameron-ensure-parents-led-filter-process-new-computers.html; 4.12.2012.

4 *Elder, Miriam* 2012: Censorship row over Russian internet blacklist, in: http://www.guardian.co.uk/world/2012/nov/12/censorship-row-russian-internet-blacklist; 4.12.2012.

EFF schon in der Vergangenheit Bedenken geäußert hat,[5] machte im November wieder einmal Schlagzeilen: Zwei junge Frauen wurden verhaftet, nachdem sie die Lahmlegung Mumbais aufgrund der Beerdigung eines rechtsextremistischen Hinduführers auf Facebook kritisiert hatten. Eine der Frauen hatte einen Artikel dazu verfasst, die andere lediglich auf „Gefällt mir" geklickt.

Obwohl Pranesh Prakash vom Zentrum für Internet und Gesellschaft in Bangalore diesen Vorfall eine „falsche Anwendung" des Gesetztes nannte[6] (§ 295A des indischen Strafgesetzbuches, der das „Empören religiöser Gefühle einer Klasse" verbietet), bemerkte er auch, dass das Gesetzt schon einmal leichtsinnig in Maharashtra angewendet worden war. Prakash wirft ebenso die Frage auf, wie die Polizei es geschafft hat, den Kommentar der jungen Frau herauszugreifen.

Gegen Kaution wurden die beiden Frauen Ende November wieder freigelassen.

Kein Frühling für die Vereinigten Arabischen Emirate

Knapp zwei Jahre nach Beginn der tunesischen Revolution verbreiten ihre Schockwellen im Nahen Osten und Nordafrika weiter Unruhe. Obwohl die Vereinigten Arabischen Emirate (VAE) den Protesten weitestgehend ausweichen konnten, erließ der Präsident am 12. November eine Verordnung, welche die Veröffentlichung von Material verbietet, das „die Sicherheit des Staates gefährdet". Darüber hinaus werden Haftstrafen für diejenigen erlassen, die einen Regimewechsel fordern, Demonstrationen organisieren oder anderweitig die „Justiz bedrohen".

Die VAE gerieten unter Beschuss von Menschenrechtler/innen, weil sie sechs Aktivisten, die das regierende Regime kritisiert hatten, die Staatsangehörigkeit aberkannten und 60 Menschen, die aufgrund einer Verbindung zur inländischen islamistischen Gruppe Islah verhaftet wurden, den Rechtsbei-

5 *York, Jilian* 2012: India's Downward Spiral, in: https://www.eff.org/deeplinks/2012/02/india%E2%80%99s-downward-spiral; 4.12.2012.

6 P*rakash, Pranesh* 2012: Arbitrary Arrests for Comment on Bal Thackeray's Death, in: http://cis-india.org/internet-governance/blog/bal-thackeray-comment-arbitrary-arrest-295A-66A; 4.12.2012.

stand verweigerten und möglicherweise sogar folterten. Im Oktober rief das Europäische Parlament die VAE dazu auf, die Menschenrechte zu respektieren und politische Gefangene sofort aus den Gefängnissen zu entlassen.

Anstieg der Zensur weltweit

Im Rest der Welt sieht es auch nicht viel besser aus. China hat während des Parteitages der Kommunistischen Partei die Kontrollen im Internet ausgeweitet. Syrien manipuliert und überwacht weiterhin das Netz, Ende November wurde es sogar ganz abgeschaltet. Und es wimmelt weiterhin von Gerüchten, dass Israel Gaza vom Internet abklemmen könnte.

Auf der globalen Ebene bestehen Bedenken, dass die Weltkonferenz zur internationalen Telekommunikation (WCIT) in Dubai den Regierungen – vor allem den repressiven wie China und Russland – zu viel Kontrolle über das Internet zugesteht. Die WCIT könnte beschließen, dass die Kontrolle über das Internet an die Internationale Fernmeldeunion (ITU), eine von Regierungen kontrollierte Sonderorganisation der Vereinten Nationen, übergeben wird. Ein erschreckender Gedanke, wenn man bedenkt, dass einige der Vorschläge, die dort auf den Tisch gebracht wurden, die Privatsphäre bedrohen und Zensur und Überwachung legitimieren. Unter denjenigen, die diesen Kontrollausbau der ITU verhindern wollen, ist auch ein breites Bündnis von globalen Organisationen, einschließlich der Electronic Frontier Foundation (EFF) und Google.

Die Menschen kontrollieren die Regierungsmacht

Wer stellt sich gegen die Macht von Regierungen, wenn das freie Internet in Gefahr ist? Die Menschen tun es. Während Regierungen auf der ganzen Welt vorschlagen, das Internet zu filtern, zu zensieren und abzuklemmen, sei es durch Erlasse oder Gesetzgebung, konnten koordinierte Aktionen und Proteste diese Gefahren wiederholt zurückdrängen. Letztes Jahr haben sich italienische Wikipedianer/innen entschlossen, die italienische Seite der Wikipedia für einen Tag offline zu nehmen um gegen ein vom Parlament behandeltes Abhör-Gesetz zu protestieren, dass massiv die Pressefreiheit bedroht hätte – sie schafften es, das Gesetz zu kippen. Wenige Monate später inspirierte diese Aktion den Widerstand gegen SOPA/PIPA in den USA – die überwältigenden Proteste halfen dabei, die gefährliche Gesetzgebung zu Netz-Sperren in Repräsentantenhaus und Senat zu stoppen. Diese Taktiken inspirierten

wiederum AktivistInnen in Jordanien und auf den Philippinen, wo nach der Verabschiedung eines Cybercrime-Gesetzes Anfang Oktober 2012 starke Zweifel der Zivilbevölkerung (inklusive der EFF) den Höchsten Gerichtshof der Philippinen dazu bewegen konnten, das Gesetz für 120 Tage auszusetzen.

Zivilgesellschaft und Nichtregierungs-Organisationen wie die EFF schlagen Alarm, wenn Regierungen das offene Internet gefährden. Wir kämpfen mit juristischen Analysen und Klagen, aber auch mit Werkzeugen, die den Regierungen das Filtern und Blockieren von Informationszugängen erschweren. Freie Meinungsäußerung ist ein fundamentales Menschenrecht, das nicht verschwindet, wenn man online geht. Und wenn Regierungen die größte Gefahr für ein offenes Internet sind, dann sind Bürger/innen die größte Hoffnung, um es zu schützen.

Clean IT: Der geheime Plan der EU, der keiner war

Ben Hayes

Seit dem Leak des „vertraulichen" Entwurfs von Empfehlungen des Clean IT Projekts gab es ein großes Interesse an dem Projekt bei EU-Politik-Interessierten und Netz-Aktivisten. „Die EU plant Polizei-Patrouillen auf Facebook und Twitter gegen Terroristen" titelte der britische Daily Telegraph. Cory Doctorow bloggte, dass eine „EU-Arbeitsgruppe" die „dümmste Sammlung an Vorschlägen für Internet-Regeln in der gesamten Geschichte der Menschheit" produziert hat. Die Blogosphäre füllte sich bald mit Berichten über ein neues ACTA. Es gab nur ein Problem: Clean IT ist keine Arbeitsgruppe der EU und dessen Vorschläge sind kein Plan der EU.

Also, worüber war die ganze Aufregung? Clean IT ist ein transnationales Projekt, das vom 2007 eingerichteten, 600 Millionen Euro schweren Programm „Kriminalprävention und Kriminalitätsbekämpfung" (ISEC) finanziert wird. Während das ISEC-Programm verwendet werden kann, um „von der Kommission initiierte und verwaltete Projekte europäischer Dimension" zu unterstützen, ist Clean IT ein nationalstaatliches Projekt, das vom Büro des niederländischen Koordinators für Terrorismusbekämpfung geleitet und seinen Amtskollegen aus Belgien, Deutschland, Großbritannien und Spanien als Partnern unterstützt wird. Das Projekt erhielt 325.000 Euro, um vier Workshops, zwei Konferenzen und das jetzt glücklos aussehende Projektteam in Den Haag zu finanzieren. Das erklärte Ziel des Projektes ist es, einen „nichtlegislativen ‚Rahmen'" zu entwickeln, der „aus allgemeinen Grundsätzen und Best Practices" besteht.

Die Rolle der EU bei Clean IT

Worüber wir also wirklich sprechen, sind ein paar Treffen in Europa, auf denen Vertreter von Strafverfolgungsbehörden, Industrie und Regierung zusammen kommen, um die „terroristische Nutzung des Internets" zu diskutieren. Für die meisten der Teilnehmer war es wohl einfach „jolly" (ein freier Tag, der als Arbeit zählt – Anm. d. Ü.), für die Projektleitung war es wahrscheinlich die Speerspitze der Cyber-Terrorismus-Bekämpfung. Wie auch immer, die „terroristische Nutzung des Internets" wird derzeit an vielen Orten

diskutiert, unter anderem bei den Vereinten Nationen und im Europarat, wobei diese Initiativen anscheinend sehr viel weniger kritische Aufmerksamkeit auf sich gezogen haben.

Hätten sie nicht eine so unglaublich dumme Sammlung an Vorschlägen produziert, würden nur wenige Menschen Clean IT so viel Aufmerksamkeit schenken, wenn überhaupt jemand. Es ist eine traurige Wahrheit, dass die Europäische Kommission derzeit so viel von unserem Geld auf „Sicherheits"-Projekte wirft, die, würde man all ihre „Empfehlungen", „Grundsätze" und „best practices" in Biokraftstoff umwandeln, Brüssel wahrscheinlich klimaneutral machen könnten. Aber heiße Luft zu produzieren ist nicht das selbe wie die Entwicklung konkreter EU-Politik oder sogar nationaler Politik – weit entfernt.

Es ist leicht zu erkennen, wo die Verwirrung herkommt: Die riesige EU-Flagge auf der Webseite von Clean IT und die Tatsache, dass in der Tat ein Großteil der EU-Politik auf solchen „Jollies" internationaler Strafverfolgungsbehörden geschliffen wird. Darüber hinaus hat EDRi Recht, dass die Kommission im Bereich „Cyberkriminalität" nur zu gerne undurchsichtige Beratungen dieser Art sponsert und „freiwillige" Maßnahmen zur Privatisierung der Rechtsdurchsetzung fördert.

Aber wen interessiert es, dass es nicht wirklich ein Plan der EU war? Durch das rücksichtslose Naming-und-Shaming sah sich die EU-Kommissarin für Inneres gezwungen, Clean IT mit einem Tweet öffentlich zu verstoßen. Hat also das bisschen Übertreibung nicht der Welt einen Gefallen getan und die Initiative getötet? Die kurze Antwort ist: „Ja, auf Nimmerwiedersehen" Die längere Antwort ist: „Ja, aber …", und hierbei handelt es sich um ein wirklich wichtiges „aber".

Nicht die Fehler von INDECT wiederholen

Ein Beispiel spricht Bände. Vor ein paar Jahren kamen Berichte über eine EU-finanzierte Initiative namens INDECT auf. Die Berichterstattung darüber ähnelte der über Clean IT sehr. INDECT hatte zwölf Millionen Euro aus dem 1,4 Milliarden Euro schweren Sicherheitsforschungsprogramm erhalten und behauptet, es würde die Überwachungs-Äquivalente von Genfood, Stammzellenforschung und „Fracking" entwickeln.

INDECT versprach, Gesichtserkennung, Internet-Überwachung, intelligente Videoüberwachung und Drohnen als Teil einer Sammlung an „Werkzeugen zur Erkennung von Bedrohungen" zu entwickeln. Als INDECT dieses schreckliche PR-Video produzierte, begannen einige, die Glaubwürdigkeit des Projekts in Frage zu stellen. Aber da war die Katze schon aus dem Sack und Aktivisten erzählten der Welt, dass INDECT Drohnen für FRONTEX (EU-Grenzpolizei) und Datenbanken für EUROPOL (Europäisches Polizeiamt) baut und auf Demonstrationen ausgerichtet ist – während nichts davon stimmte. (Ironischerweise hat eine ganze Reihe anderer, wenig beachteter EU-finanzierter Projekte im Grunde genau das getan.) Die weit verbreiteten Übertreibungen und Falschdarstellungen gipfelte in diesem hoffnungslos falschen Video von Anonymous, das behauptet, dass INDECT zu den Olympischen Spielen 2012 in London das erste Mal eingesetzt werden sollte.

Das ist nicht gut. Wie brauchen Aktivisten, die mit Fakten bewaffnet sind, um die wahren Bösewichte ins Ziel zu nehmen, denn die sind Legion (viele, Anm. d. Ü.). Und wir brauchen NGOs und Journalisten, die sich darauf konzentrieren, konkretere Bedrohungen für die Freiheit des Internets zu skandalisieren. Es besteht die Gefahr, genau wie es bei INDECT passiert ist, dass Clean IT der Fokus von fehlgeleitetem Aktivismus wird, während viel anspruchsvollere und letztlich viel gefährlichere Initiativen unter dem Radar segeln, komfortabel und wohl wissend, dass währenddessen die Amateure bei Clean IT viele ihrer Kritiker beschäftigt haben.

Wir können natürlich sicher sein, dass es Elemente in Europa gibt, die sehr gerne die Wunschliste von Clean IT in die Praxis umgesetzt sehen würden (darunter viele aus den Strafverfolgungsbehörden und der sie unterstützenden Industrie sowie auch einige aus der Europäischen Kommission selbst), aber wir sollten genau zwischen transnationalen Schwatzbuden, EU-Arbeitsgruppen und Entwürfen für EU-Politik unterscheiden. Wir sollten auch verstehen, dass es viele Clean ITs braucht, um uns in diesen Weg zur Tyrannei zu führen.

Die Ursachen der Probleme in den Fokus rücken

In diesem Sinne können wir mehr erzielen, wenn wir zumindest einen Teil unserer Aufmerksamkeit darauf richten, wie diese schrecklichen Initiativen überhaupt finanziert werden, nicht zuletzt weil die EU derzeit dabei ist, sich auf seinen mehrjährigen Finanzrahmen (MFR) für den Zeitraum von 2014 bis

2020 zu einigen. Was den Bereich „Sicherheit" betrifft, gibt es überhaupt keine Anzeichen für eine Sparsamkeit, mit der Wohlfahrtsprogramme und andere Bereiche der öffentlichen Politik verwüstet werden. Der vorgeschlagene Finanzrahmen umfasst einen 11 Milliarden Euro Fonds für innere Sicherheit (eine 40-prozentige Steigerung gegenüber dem vorherigen Finanzrahmen), aus dem viele Maßnahmen zum „besseren Schutz der Bürger und Unternehmen im Cyberspace" sowie „Maßnahmen gegen Terrorismus, Radikalisierung und die Rekrutierung von Terroristen" finanziert werden.

Weitere 3,8 Milliarden Euro sind für das neue Sicherheitsforschungsprogramm im Rahmen von „Horizon 2020" vorgesehen. Dennoch kritisiert fast niemand aus der europäischen Community für Menschen- und Grundrechte diese konkreten „Goldesel", fast niemand stellt sie in Frage. Das ist nicht gut, denn die antidemokratische Kultur, die der Vielzahl von Clean ITs dieser Welt zugrunde liegt, erwächst genau aus der Art und Weise, wie „Sicherheit" heutzutage definiert und finanziert wird.

Ben Hayes ist Projektmanager bei Statewatch und Fellow beim Transnational Institute.

Nach INDECT: Ein Plädoyer für eine fundiertere Überwachungskritik

Matthias Monroy

Auf netzpolitik.org veröffentlichte Beiträge von Ben Hayes und Alexander Sander diskutieren, wie dem von der Europäischen Union angeheizten Überwachungswahn Einhalt geboten werden kann. Alexander Sander kritisiert, dass Kampagnen gegen das EU-Sicherheitsforschungsprojekt INDECT andere Vorhaben ungeschoren davonkommen lassen: Für durchaus problematischere Projekte stünden sogar weit mehr Gelder zur Verfügung. Er schlägt vor, statt der reflexhaften Kritik an einzelnen Programmen lieber das neue Sicherheitsforschungsprogramm der EU aufs Korn zu nehmen, das derzeit unter dem Namen „Horizon 2020" rund 3,8 Milliarden Euro für neue Forschungen locker machen soll.

Ben Hayes unterstreicht den Fokus auf „Horizon 2020" und bittet um mehr Genauigkeit in der Kritik von Projekten wie „Clean IT". Eine dortige Beschäftigung mit dem Einsatz von Filtertechnologien im Internet wird zwar von der EU finanziert. Die mediale Aufmerksamkeit wird laut Ben Hayes aber der Bedeutungslosigkeit von „Clean IT" kaum gerecht. Er weist auch darauf hin, wie die Berichterstattung über das Freihandelsabkommen ACTA oder INDECT von Übertreibungen oder Falschinformationen geprägt ist: So wurde ventiliert, die automatisierte Auswertung von Bildern aus Überwachungskameras von INDECT würde bei der EURO 2012 getestet – obschon die EU-Kommission dies längst dementiert hatte.

Eine linke Kritik an der EU-Sicherheitsforschung?

Beide Kritiker lassen offen, auf welche Weise gegen „Horizon 2020" protestiert werden soll. Wie üblich werden die dort eingetüteten einzelnen Forschungsvorhaben zu zwei Dritteln aus EU-Mitteln finanziert. Dafür aber nur die EU-Kommission zu kritisieren, vernebelt die wahren Akteure der gegenwärtig 188 zweifelhaften Programme: An allen Projekten sind neben WissenschaftlerInnen auch private Firmen und Polizeien gleichermaßen beteiligt.

Oft wird nicht deutlich, wieso vielen AktivistInnen vor allem die EU-Kommission als Symbol der Umsetzung von Orwells „1984" gilt – obwohl die EU im ironischerweise im gleichen Jahr ihr erstes Forschungsrahmenprogramm auflegte.

Statt sich weiter an INDECT abzuarbeiten, könnten Kampagnen auch die nationalen Sicherheitsforschungsprogramme adressieren, die im Falle von Polen oder Deutschland den EU-Vorhaben um nichts nachstehen. In Polen kämpft die nationalkonservative Abgeordnete Barbara Bubula zwar gegen INDECT, nicht aber die viel umfangreicheren Forschungen der „Polnischen Plattform für Heimatschutz". INDECT muss wohl als Container für eine nationalistische Kritik an der Europäischen Union herhalten. Nicht verwunderlich, dass zum letzten internationalen Aktionstag gegen INDECT im Sommer auch rechte Gruppen mobilisierten. Mit welcher Haltung also – und vor allem mit wem – am 20. Oktober wieder gegen weltweite Überwachungssysteme demonstrieren?

Diskutiert werden muss, wie eine dezidiert linke Kritik an der gegenwärtigen Sicherheitsforschung aussehen kann. Thilo Weichert, der Leiter des Unabhängigen Datenschutzzentrums in Schleswig-Holstein, kritisiert INDECT, weil es „konzeptionell mit europäischem und deutschem Datenschutz- und Verfassungsrecht im Widerspruch" steht. Er befürwortet den Einsatz technischer Mittel aber grundsätzlich: Diese könnten zu einer „Effektivierung" der Arbeit von Sicherheitsbehörden beitragen, müssten aber auf die Einhaltung von Grundrechten kontrolliert werden. Wie wenig sich auch deutsche Polizeien darum scheren, hat jedoch die Nutzung von Mobilfunkdaten bei antifaschistischen Protesten in Dresden gezeigt. Die groß angelegte Funkzellenauswertung wurde erst öffentlich, als deren Erkenntnisse auch in den Akten zu Ermittlungen wegen geringfügiger Verstöße gegen das Versammlungsrecht auftauchten.

Gern wird gegen INDECT & Co. vorgetragen, dass zu viele Unbeteiligte ins Visier der Behörden geraten. Weil die Ausforschung und Verhaltenserkennung unbemerkt vonstatten geht, würden sich Menschen womöglich nicht mehr frei im öffentlichen Raum bewegen. Das ist richtig, und wird im Falle Deutschlands sogar vom Bundesverfassungsgericht bestätigt: Richter erklärten im Urteil zur Vorratsdatenspeicherung vom 2. März 2010 die „anlasslose

Speicherung" für grundgesetzwidrig, da diese ein „diffus bedrohliches Gefühl des Beobachtetseins" hervorrufe. Die „unbefangene Wahrnehmung der Grundrechte" sei dadurch beeinträchtigt.

Die Macher von Überwachungsplattformen wollen diese Kritik an der Aushöhlung der Unschuldsvermutung jetzt ins Leere laufen lassen. Der INDECT-Mitarbeiter Jan Derkacz dichtet dem Projekt beispielsweise einen Datenschutzanspruch an, wenn er auf die dort beforschte Unkenntlichmachung von Gesichtern oder Nummernschildern verweist. Tatsächlich wird in INDECT eine Anwendung entwickelt, die Bilder aus Überwachungskameras teilweise anonymisiert. Derkacz zeigt aber ein durchaus fragwürdiges Verständnis von Datenschutz. Denn die Entscheidung, welche Bilder für die Polizei von Interesse sind, trifft eine Software. Die Anonymisierung entpuppt sich als eine „Maskierung", die jederzeit wieder rückgängig gemacht werden kann.

Privatsphäre vs. polizeilich-industrielle Verwertungsinteressen

Eine grundsätzliche Problematik digitaler Überwachungsplattformen wird wenig thematisiert: Maschinen versuchen, das Risiko von Personen zu errechnen. Projekte wie INDECT wollen hierfür eine größtmögliche Anzahl weiterer „Sensoren" einbinden, etwa Mikrofone, Infrarotkameras, RFID-Lesegeräte oder auch lokalisierte Telefone. Eine deutsche Firma wirbt mit Detektoren zum Aufspüren von Alkohol in der Atemluft im Fußballstadion.

Wenn die Gefährlichkeit von AkteurInnen im öffentlichen Raum mathematisch bestimmt wird, müsste aus datenschutzrechtlicher Perspektive die Funktionsweise der eingesetzten Software bekannt sein. Eine Offenlegung des Quellcodes von Software zu „Data Mining" oder „vorhersagender Analyse" werden die Hersteller wie beim Staatstrojaner empört zurückweisen. Und doch würde mit dieser diskursiven Forderung deutlich, dass die Privatsphäre den polizeilich-industriellen Verwertungsinteressen unversöhnlich gegenübersteht.

Von PolitikerInnen und Bürgerrechtsgruppen wird hin und wieder eine Exportkontrolle von Überwachungstechnologie an autoritäre Regimes gefordert. Eine derartige Grundrechts-Firewall greift aber zu kurz: Weil es sich nicht um militärische Technologie handelt, wird der Verkauf der digitalen Werkzeuge normalerweise nicht sanktioniert. Reporter ohne Grenzen

forderte deshalb gestern, die Spionagewerkzeuge mit Kriegsgerät auf eine Stufe zu stellen. Doch wer soll über die Definition eines autoritären Regimes bestimmen?

Auch das deutsche Außenministerium hatte sich erfolgreich für die Aufnahme von Abhörschnittstellen in die EU-Sanktionsliste für Syrien und den Iran eingesetzt. Schon letztes Jahr erklärte Außenminister Guido Westerwelle, Sanktionen müssten „neue Formen der Repression wie der Kontrolle des Internets berücksichtigen". Dass eine staatliche Exportkontrolle aber von politischem Gutdünken abhängt, illustriert das Bundeswirtschaftsministerium. Die Behörde von Philipp Rösler umwarb im September Industrievertreter aus Bahrain, Katar, Kuwait, Oman, Saudi-Arabien und den Vereinigten Arabischen Emiraten. Erklärtes Ziel einer Veranstaltung in Düsseldorf war das Ankurbeln von Exporten zur technikgestützten Migrationsabwehr, Sicherung von Handelswegen, Kraftwerken und Kommunikationsinfrastruktur.

Die Bereitstellung von Abhörschnittstellen gilt in Deutschland genauso wie in Bahrain als unabdingbar, um überhaupt Aufträge zur Errichtung von Telekommunikationsanlagen zu erhalten. Diese Grundausstattung des polizeilichen Zugriffs auf digitale Kommunikation hatten US-Behörden kürzlich in einer Ausschreibung für den Irak beschrieben. Noch deutlicher hatte sich ein Sprecher von Nokia-Siemens anlässlich der Niederschlagung der Revolte im Iran vor drei Jahren ausgedrückt: Demnach hatte das deutsch-finnische Joint-Venture nur eine „Standardarchitektur" zur Überwachung geliefert.

Zur Angleichung dieser Standards treffen sich die Sicherheitsbehörden mit Herstellern und Anbietern von Telekommunikationsdiensten in informellen Arbeitsgruppen und Netzwerken. Dazu zählt beispielsweise die „Europäische öffentlich-private Partnerschaft für Robustheit" (EP3R), aber auch das bekanntere „European Telecoms Standards Institute" (ETSI). Seit über zehn Jahren macht der österreichische Internetreporter Erich Möchel gegen das Institut mobil. Im Sommer wies er darauf hin, dass die im ETSI vertretenen Behörden zunehmend in der „Cloud" ausgelagerte Daten ausforschen wollen.

„Endnutzer“ und Hersteller aufs Korn nehmen!

Das ETSI unterhält ein „Technisches Komittee TC LI“ („Lawful Interception“), in dem Geheimdienste den Bedarf skizzieren und rechtliche Rahmenbedingungen erörtern. Eine weitere Arbeitsgruppe „SA3 LI“ setzt diese Vorgaben der Behörden in weltweite Überwachungsstandards um. Stets mit an Bord: Das Bundesamt für Verfassungsschutz und die Bundesnetzagentur unter der Verantwortung des Wirtschaftsministeriums.

In Deutschland organisieren sich die überwachenden Behörden in der „Kommission Grundlagen der Überwachungstechnik“ (KomGÜT). Auf Ebene der Landesinnenministerien betreiben die Länderpolizeien einen „Unterausschuss Information und Kommunikation“ (UA IuK), der beim „Arbeitskreis II – Innere Sicherheit“ der Arbeitsgemeinschaft der Innenministerien der Länder angesiedelt ist. Zu den international aktiven Akteuren gehören neben dem Bundeskriminalamt und dem Bundesamt für die Sicherheit in der Informationstechnik auch das Landesamt für Zentrale Polizeiliche Dienste (LZPD) der Landespolizei Nordrhein-Westfalens. Das LZPD übernimmt für andere Bundesländer den Versand von „Stillen SMS“ und wertet Daten aus Funkzellenabfragen aus.

Warum richtet sich eine radikale Überwachungskritik also nicht gegen die Polizeien und Geheimdienste, die in internationalen Gremien die Standardisierung der weltweiten Überwachung vorantreiben? Auch in der EU-Sicherheitsforschung spielen sie eine entscheidende Rolle: Als teilnehmende Partner gelten sie als „Endnutzer“, die zu Beginn von Projekten wie INDECT den Zuschnitt der zu entwickelnden Lösung definieren dürfen. Im Verlauf der Vorhaben testen sie Prototypen und konkretisieren den Bedarf. Nach Leistungsschauen beim „Europäischen Polizeikongress“ in Berlin oder der „Milipol“ in Paris beschaffen sie später die serienreifen Produkte.

Wie zielsicher Proteste und Kampagnen aber die privaten Firmen treffen, hat die Skandalisierung von Trojaner-Software durch den Chaos Computer Club vor einem Jahr gezeigt. Die Öffentlichkeit begann sich dafür zu interessieren, dass die britische Gamma International an einschlägigen Verkaufsmessen für den arabischen Raum teilnimmt. Nach Medienberichten wurden Angebotsunterlagen der Firma auch nach der Stürmung eines Büros der Staatssicher-

heit in Kairo gefunden. Über einen Anwalt versuchte Gamma International unter Strafandrohung, die kritische Berichterstattung über Geschäftsbeziehungen mit Ägypten zu behindern.

Auch die Firma DigiTask, der damalige Hoflieferant des Bundeskriminalamts, geriet unter Druck: Ein Anwalt teilte Journalisten mit, sie sollten zukünftig verschweigen dass der Geschäftsführer vor zehn Jahren wegen Korruption zu einer mehrjährigen Haftstrafe verurteilt wurde. Es ging dabei um Bestechung in Millionenhöhe. Als Gegenleistung wollte der DigiTask-Chef bei Aufträgen des Zollkriminalamts bevorzugt werden.

Vermutlich hat die internationale Berichterstattung auch dafür gesorgt, dass sich die Aachener Überwachungssparte von Utimaco und die italienische Area Spa – jedenfalls offiziell – aus dem Geschäft mit Überwachungstechnik in Syrien zurückgezogen haben. Ähnlich ließe sich die oben bereits erwähnte Stellungnahme von Nokia-Siemens interpretieren: Viele Hersteller fürchten angesichts kritischer Presseberichte um Marktanteile. Schließlich bestellt auch die Bundesregierung ihre Trojaner nicht mehr bei DigiTask.

Aktivismus

ACTA und die Folgen

Markus Beckedahl

Das Thema ACTA verfolgt netzpolitik.org bereits seit den ersten Leaks 2008. Seitdem kamen ganze 386 Artikel zusammen. Dieser Rückblick wird nicht die gesamte Geschichte erzählen, sondern lediglich einen groben subjektiven Rückblick auf die Ereignisse in 2012 werfen.

Auf dem 28. Chaos Communication Congress Ende 2011 saßen die üblichen Verdächtigen unter den europäischen Aktivisten zu Mitternacht in einem Kellerraum und berieten, wie man denn bloß das Anti-Produktpiraterie-Handelsabkommen (ACTA) verhindern könnte. Die Diskussion um ACTA lief seit 2008, aber abgesehen von sehr kurzen medialen Feuern rund um einzelne Leaks mit skurrilen Forderungen war das internationale Handelsabkommen kein Thema der Öffentlichkeit. Weder die Politik, noch die Medien und am wenigsten die Bürgerinnen und Bürger interessierten die möglichen Auswirkungen auf Grundrechte und Innovation. Leicht demotiviert, aber mit dem Willen trotzdem bis zum Ende zu kämpfen, ging die Runde in dieser Nacht auseinander.

Anfang 2012 eskalierte dann die US-Debatte rund um die beiden Gesetzesvorhaben SOPA (Stop Online Piracy ACT) und PIPA (Protect IP ACT), die beide Lobbyforderungen der Unterhaltungsindustrie zur stärkeren Durchsetzung von Urheberrechten beinhalteten. Eine breite Koalition aus zivilgesellschaftlichen Gruppen wie der Electronic Frontier Foundation oder Wikimedia aber auch Communities wie Reddit oder Wordpress und Unternehmen wie Google organisierten daraufhin am 18. Januar einen Black-Out-Day. Das Ziel war, möglichst viele Webseiten zu verdunkeln, um auf die Auswirkungen von SOPA und PIPA hinzuweisen und mediale Aufmerksamkeit und damit eine politische Debatte zu schaffen. Der Aktionstag wurde ein voller Erfolg. Vor allem die (in den USA) geschwärzte Wikipedia trug zu einer globalen Medienberichterstattung bei, die auch Einschränkungen der Meinungsfreiheit durch eine eskalierende Urheberrechtsdurchsetzung zum Thema hatte.

Wir wiesen in Deutschland darauf hin, dass unser SOPA/PIPA ACTA heiße und in den nächsten Monaten im EU-Parlament zur Debatte stehe. Vereinzelt wurde auch dies in der Berichterstattung aufgenommen.

Von SOPA zu ACTA

Und dann fingen plötzlich Demonstrierende in Polen an, bei Minustemperaturen auf der Straße gegen ACTA zu hüpfen. Die Motivationen dahinter waren vielfältig, was es anfänglich etwas schwer machte, das Phänomen genau zu verstehen. Ausgelöst von der SOPA/PIPA-Debatte sahen viele durch ACTA ihre digitale Lebenswelt bedroht. Was wir seit Jahren unermüdlich erklärten, wurde in Polen auf einmal Thema für Straßendemonstrationen. Anonymous-Masken wurden dabei ein popkulturelles Element und Erkennungszeichen für den Protest. Auch einige DDoS-Attacken auf polnische Regierungswebseiten führten dort zu einer Debatte über ACTA und seine Auswirkungen. Das ging so weit, dass die Opposition ihre Chance nutzte, um sich auf die Seite der Protestierenden zu schlagen und die linksliberale Fraktion Ruch Palikota im Parlament einen Auftritt mit Anonymous-Masken inszenierte, dessen Bilder um die Welt gingen.

Damit wurden die polnischen ACTA-Proteste auch zu einem Thema in deutschen Medien. Irgendwas mit Internet, Anonymous-Masken und hüpfenden Polen sorgte für wachsendes Interesse unter Journalisten. Dass die Demonstranten hüpften, lag vor allem an den Temperaturen. Bei Minus 20 Grad steht man ungern herum. Aber es sorgte für ein weiteres Wiedererkennungsmerkmal, das später auch von anderen Demonstrierenden europaweit übernommen wurde.

Durch die Berichterstattung in Deutschland über die Proteste in Polen und den Wikipedia-Blackout wurden auch hier die Rufe nach Demonstrationen laut. Wir waren zuerst skeptisch, ob es gelingen würde ausreichend Menschen zu einem Thema wie ACTA bei Minustemperaturen im Februar auf die Straße zu bringen. Glücklicherweise funktioniert das Netz dezentral und es fanden sich Motivierte, die unter wiki.stoppacta-protest.info ein Wiki aufsetzten und Informationen rund um die geplanten Demonstrationen in mehr als 200 europäischen Städten zusammentrugen. Der 11. Februar wurde als Stichtag gesetzt und dank internationaler Koordination wurde daraus schnell ein europäischer Aktionstag. Als die Piratenpartei zunehmend auf ACTA aufmerksam wurde, entdeckte sie ein altes Aufklärungsvideo einer Anonymous-Gruppe aus Hamburg. Die hatte vor Jahren auf Grund der Berichterstattung über geleakte Zwischenstände der ACTA-Verhandlungspapiere ein rund sieben Minuten langes Animationsvideo erstellt, das aber wieder in der Versen-

kung verschwunden war. Bruno Kramm, ein Piraten-Aktivist mit eigenem Tonstudio, übersetzte das englische Video ins Deutsche. Es verbreitete sich rasant im Netz und durch das neue Einstellungsdatum gingen viele davon aus, dass es sich um aktuelle Informationen handeln würde, die die Endfassung des verhandelten Abkommens beschrieben.

In der Schlussphase der internationalen Verhandlungen hin hatte sich jedoch noch einiges geändert. Manche Forderungen waren rausgeflogen, andere wurden unschärfer verpackt, so dass nur noch zwischen den Zeilen der Geist und die Leitlinie einer Privatisierung der Rechtsdurchsetzung zu finden waren. Das Video wurde viral, auch weil viele aufgrund der zahlreichen überzogenen Forderungen und Versuche der Unterhaltungsindustrie-Lobby in den Jahren zuvor daran glaubten, dass die Ideen Gesetz werden könnten, z. B. Dass das Tauschen von Kochrezepten durch ACTA illegal wird. In Zeiten, wo windige Anwälte teure Massenabmahnungen wegen dem nicht-kommerziellen Bloggen von Brötchen-Fotos verschicken, klingt dieser Gedanke immerhin nicht ganz abwegig.

Das Video, aber auch die steigende mediale Berichterstattung, führte dazu, dass eine Gruppe auf das Thema aufmerksam wurde die bisher eher nicht durch politisches Engagement aufgefallen waren: „Youtube-Stars". Auf Youtube finden sich zahlreiche Kanäle, auf denen auf unterschiedlichste Art und Weise vor allem junge Menschen ihr eigenes Fernsehprogramm machen und damit ein Massenpublikum anziehen. Kanäle wie der von „Die Außenseiter" hatten im Februar über 700.000 Abonnenten, mehr als manche Sendung im herkömmlichen Fernsehen an Zuschauern hat. Durch ACTA kamen die unterschiedlichsten Gruppen, darunter etablierte Bürgerrechtsorganisationen, aber auch Anonymous-Mitglieder und „Youtube-Stars", in Kontakt. Viele Youtube-Protagonisten trafen sich am Mittwoch vor dem europäischen Aktionstag, um mögliche Auswirkungen von ACTA zu thematisieren. In unterschiedlichen Ansprachen, immer im eigenen individuellen Stil, appellierten sie gemeinsam an ihre Zuschauer, gegen ACTA aktiv zu werden, eine Petition zu unterzeichnen und am kommenden Samstag auf die Straße zu gehen.

Parallel lief auf der amerikanischen Kampagnen-Plattform Avaaz.org eine Petition gegen ACTA, die (wie häufig bei Avaaz) sehr emotional verpackt ACTA als Untergangsszenario thematisierte und zur Unterschrift aufforderte. Die Petition sollte zum Ende hin über 2,8 Millionen Mitzeichner erhalten, davon alleine rund eine Million aus Deutschland. Gleichzeitig wurde durch Spen-

denaufrufe allein aus Deutschland ein sechsstelliger Betrag an Avaaz gespendet. Leider kam davon nichts bei den europäischen Anti-ACTA-Aktivisten an, die mit viel Aufwand und Mühe und ohne große finanzielle Ressourcen jahrelang den Widerstand organisiert und letztendlich auch vor Ort in Brüssel, Straßburg und den einzelnen EU-Staaten durchgeführt haben.

Dann überstürzten sich die Ereignisse. Überraschenderweise meldete sich zwei Tage vor dem 11. Februar unsere Bundesjustizministerin Sabine Leutheusser-Schnarrenberger mit der Aussage, dass Deutschland ACTA erst mal nicht unterzeichnen und eine Entscheidung des EU-Parlaments abwarten werde. Das überraschte insofern, als dass das Bundeskabinett unter Federführung des Bundesjustizministeriums Ende 2011 ACTA bereits durchgewinkt hatte. Deutschland hatte das Abkommen lediglich noch nicht unterzeichnet, weil der passende Botschafter zur feierlichen Unterzeichnungszeremonie nicht in Japan war.

Die Stellungnahme der Bundesjustizministerin brachte ACTA das erste Mal in die Abendnachrichten und damit drehte sich die mediale Aufmerksamkeitsspirale weiter.

Die EU-Kommission war „not amused" und verwies darauf, dass Deutschland seit Beginn der Verhandlungen immer mit am Tisch saß und alles mitgetragen habe. Das führte dazu, dass unser Co-Blogger Mathias Schindler eine Anfrage nach dem Informationsfreiheitsgesetz stellte, wer denn von deutscher Seite an den Verhandlungen teilgenommen hatte und später vom Bundesjustizministerium die Antwort erhielt, dass dies im Interesse der Öffentlichen Sicherheit nicht mitgeteilt werden könne.[1]

Der 11. Februar 2012 sollte alles verändern. Bei Minus 10 Grad standen wir mit unserem kleinen LKW in Berlin am Neptunbrunnen nahe Alexanderplatz in Berlin und warteten auf die Demonstrierenden. Es war vollkommen ungewiss, wie viele tatsächlich kommen würden, dazu war in den Tagen zuvor einfach zu viel passiert. Der Polizei hatten wir 600 Teilnehmer angemeldet. Es kamen dann rund 10.000, was uns erfreute, die Polizei aber erst mal logistisch überforderte, trotz eines vollkommen friedlichen Protestes. Das Medieninteresse war groß und als Zahlen aus anderen Städten kamen, z. B. Dass in München bis zu 16.000 Demonstranten auf der Straße waren, war klar,

1 S. dazu auch den Beitrag in diesem Buch: „Informationsfreiheitsgesetz - Das Jahr, in dem wir Kontakt aufnahmen."

dass abends die Tagesschau mit ACTA eröffnen würde. Selbst in den RTL2-Nachrichten, sonst kein Ort netzpolitischer Debatten, gab es einen Bericht. Bis zu 100.000 Menschen in über 60 Städten waren alleine in Deutschland auf die Straße gegangen. Insgesamt gab es in über 200 europäischen Städten Demonstrationen und Aktionen gegen ACTA, alles dezentral organisiert. Was klar war: So viele Menschen waren noch nie weltweit auf die Straße gegangen, um für ein offenes Internet und gegen eine eskalierende Urheberrechtsdurchsetzung auf die Straße zu gehen.

Es verbreitete sich so etwas wie Revolutionsstimmung. Tagelang berichteten Medien wohlwollend über die Proteste und ihr Anliegen, und versuchten zu verstehen, was da gerade passierte. Es war lange her, dass so viele junge Menschen gemeinsam auf die Straße gegangen waren, um gegen etwas zu protestieren. Und hier hatten wir es mit einem neuen Phänomen zu tun: Die Demonstranten gingen auf die Straße, um ihre digitale Umwelt zu schützen. Die Kritikpunkte an ACTA kamen in die öffentliche Debatte, der Protest bekam Gesichter.

Die großen Proteste blieben leider ein kurzes Strohfeuer. Zwei Wochen später kamen nur noch rund 1000 Personen in Berlin und insgesamt 20.000 zu Demonstrationen in ganz Deutschland. Aber das Thema war auf der politischen Tagesordnung. Auf EU-Ebene waren viele aufgeschreckt, die ACTA bisher noch nicht auf dem Schirm oder dem Abkommen bisher nicht genug Aufmerksamkeit geschenkt hatten. So viele Menschen auf der Straße, so viele Unterstützer einer Online-Petition und die damit verbundene mediale Aufmerksamkeit führten dazu, dass ACTA auch in Brüssel Thema wurde. In Deutschland startete währenddessen eine Konterrevolution: Die Zeit der offenen Briefe begann, die sehr emotional geführte Urheberrechtsdebatte war da.

Die EU-Kommission wurde von den Protesten und der gewachsenen Aufmerksamkeit aufgeschreckt. Auf einmal griffen die EU-Beamten auf eine Idee zurück, deren Umsetzung in den vergangenen Jahren von ACTA-Kritikern gefordert wurde: Dass vor dem Europäischen Gerichtshof (EuGH) geprüft werden solle, inwiefern der ACTA-Text mit den europäischen Grundrechte vereinbar ist. Die Intention dahinter war offensichtlich. Eine Prüfung durch den EuGH würde rund zwei Jahren benötigen, eine drohende Abstimmungsniederlage könnte damit besser verhindert und die Proteste einfach ausgesessen werden. Auch war dies längst nicht mehr die Forderung von ACTA-Kritikern, gab es doch mittlerweile eine Reihe von Gutachten, die alle Fragen längst ge-

klärt hatten. Vielen EU-Abgeordneten wurde bewusst, was eine Verschiebung bedeuten würde: Dass ACTA möglicherweise kurz nach den nächsten EU-Wahlen zur Abstimmung kommen würde.

Von der Straße ins EU-Parlament

Die harte Arbeit würde uns jedoch noch bevorstehen. Die große Herausforderung zu diesem Zeitpunkt war das Wissen aller Beteiligten , dass eine Abstimmung noch Monate vor uns lag und das mediale sowie das Protestinteresse schnell versanden würden. So kam es dann auch.

Der Kampf auf dem parlamentarischen Parkett in Brüssel begann. Dabei wurde auf Erfahrungen aus früheren Protesten gegen die Softwarepatente-Richtlinie und rund um das Telekom-Paket zurückgegriffen. Das lag auch daran, dass zum inneren Kreis der europäischen Aktivisten rund um European Digital Rights (EDRi) viele Erfahrene aus den früheren Debatten waren, die mittlerweile das Europaparlament und seine Prozesse gut kannten. Außerdem hatte sich die Stimmung gegenüber dem 28c3 Mitternachtstreffen radikal geändert: Das Spiel war zu gewinnen, da waren wir uns sicher. Wir mussten nur dranbleiben und hartnäckig sein. Also wurden in Brüssel Appartements angemietet, um Aktivisten unterzubringen, die dann die Abgeordneten ihres jeweiligen Landes mit Informationen in ihrer Sprache versorgen konnten. Gleichzeitig arbeiteten zivilgesellschaftliche Organisationen in verschiedenen Ländern daran, Bürger zu motivieren sich konstant an ihre Abgeordneten zu wenden, damit das Interesse an ACTA nicht unterging. In Deutschland baute der Digitale Gesellschaft e. V. Auf einer Idee aus Dänemark auf, mit einem Tool eine Brücke nach Brüssel zu bauen. Unter acta.digitalegesellschaft.de waren alle 99 deutschen EU-Abgeordneten mit ihren Kontaktdaten und ihrem zu erwartenden Abstimmungsverhalten aufgelistet. Diejenigen, die bereits öffentlich gesagt hätten, dass sie gegen ACTA stimmen würden, wurden farblich markiert, so dass sich interessierte Bürger auf die anderen konzentrieren konnten. Wenn ein Bürger eine positive Antwort erhalten hatte, wurde das vermerkt. Allmählich wurden es immer weniger Befürworter aus Deutschland.

In fünf Ausschüssen im Europaparlament standen Abstimmungen mit einer Wahlempfehlung für das Plenum an. Pessimistisch gingen wir von einem knappen Abstimmungsverhalten aus, was zwei oder drei Ausschüsse gegen ACTA und die anderen für ACTA ergeben würde. Umso überraschter waren

wir, als es am Ende 5:0 stand. Selbst der Rechtsausschuss, der sich im Jahrzehnt zuvor immer mehrheitlich pro Ausweitung von Urheberrechten und ihre stärkere Durchsetzung gestimmt hatte, empfahl knapp eine Ablehnung.

Trotzdem fieberten wir der Abstimmung entgegen. Nach vielen Niederlagen auf EU-Ebene waren wir daran gewöhnt, am Schluss zu verlieren. Zuviele taktische Manöver waren von ACTA-Befürwortern probiert worden, so dass immer noch die Chance bestand, dass es eine Mehrheit für eine Verschiebung und für ein Abwarten einer EuGH-Entscheidung geben könnte.

Am 4. Juli war es soweit. Kurz vor der Sommerpause kam es im Europaparlament in Straßburg zur Abstimmung über ACTA. Überwältigende 478 Stimmen waren dagegen, bei 165 Enthaltungen und 39 Befürwortern. Aus Deutschland stimmten acht Konservative für ACTA und 33 Abgeordnete von FDP und Union enthielten sich. Zum ersten Mal hatte es eine mehrheitliche Ablehnung eines Vorschlages der EU-Kommission gegeben, mehr noch als 2005 bei der Abstimmung über die EU-Softwarepatente-Richtlinie.

Was folgt daraus?

ACTA ist Geschichte, aber die Bedrohung noch lange nicht vorbei. Die Industrie-Lobbys hinter ACTA werden weiterhin jede Chance nutzen, die Ideen der schärferen Durchsetzung eines dringend reformbedürftigen Urheberrechts auf allen Wegen in Gesetze zu gießen. Im Sommer und Herbst alarmierten die Verhandlungen um das Kanadisch-Europäische Handelsabkommen CETA die interessierte Teilöffentlichkeit. Die „Koalition der Willigen“ unter Federführung der USA steht vor dem Abschluss des Trans-Pacific-Partnership-Agreement (TPP), das viele Forderungen enthält, die in den ACTA-Verhandlungen durch die EU gestrichen wurden. Und in Deutschland sind die Forderungen nach der Einführung eines Warnmodell-Systems immer noch in der politischen Debatte.

Die Entscheidung in Straßburg hat viele Folgen. Es brachte der EU ihr Zensursula-Erlebnis. Auf einmal steht Netzpolitik auf der politischen Tagesordnung, weil falsche Entscheidungen viele junge Menschen über die EU verteilt auf die Straße bringen können. Gegen das Netz Gesetze zu machen, wird immer schwieriger. Über alle Parteien hinweg werden die Rufe nach einer zeitgemäßen Netzpolitik und die damit verbundenen Schritte durch offene und partizipative Prozesse lauter.

Die Erfahrung zeigt auch, dass ein politisches Momentum zufällig entsteht und transnationale Öffentlichkeiten möglich sind. In diesem Fall war es eine Verkettung glücklicher Umstände. ACTA hätte auch leicht unter dem Radar der Öffentlichkeit bis zur Abstimmung bleiben können, wie das so oft bei EU-Themen der Fall ist. Die Schwärzung der US-Wikipedia im Protest gegen SOPA/PIPA, hüpfende Polen, ein missverstandenes Video und hartnäckige Aktivisten bildeten Bausteine zum Erfolg. Vor allem sollte man berücksichtigen, dass ACTA nicht nur eine inhaltliche Entscheidung war. Es war vor allem ein für das EU-Parlament erfolgreicher Machtkampf um Rechte und ein gesteigertes Selbstbewusstsein gegenüber der EU-Kommission.

Was ACTA ebenfalls zeigte: Die Ablehnung hätte auch scheitern können, wenn der Protest nicht ins EU-Parlament getragen worden wäre. Die Unterhaltungslobby hätte es vielleicht geschafft den ganzen Protest zu diskreditieren, wenn nicht zugleich mit guten Argumenten und in vielen Einzeltreffen mit den Abgeordneten weiter vorgegangen wäre. In der deutschen Debatte wurde immer wieder von Seiten der Unterhaltungsindustrie-Lobbys auf den manipulativen Charakter des Anonymous-Videos hingewiesen, durch das sich die Protestidee erst richtig entfaltete. Über den Effekt des Videos und darüber, ob eine solche Überspitzung in der politischen Debatte in Ordnung ist, kann man durchaus diskutieren. Man sollte aber auch berücksichtigen, dass die Macher des Videos nichts dafür konnten, dass es zwei Jahre später übersetzt und neu verbreitet wurde – während sich der Verhandlungsstand signifikant geändert hatte. Und wenn man selbst mit Kampagnen wie „Hart aber gerecht“ / „Raubkopierer sind Verbrecher“ jedem Kinobesucher suggeriert, dass man für das Kopieren von CDs und Filmen bis zu fünf Jahre in den Knast kommt, sollte man sich auch eher zurückhalten. Was auch bedacht werden solle: Die Inhalte des Videos fanden in der Begründung ihrer Ablehnung durch EU-Abgeordneten keine Berücksichtigung. Wohl aber die Argumente der zivilgesellschaftlichen Organisationen, die transnational vernetzt seit Jahren den Widerstand organisiert hatten.

Was bleibt

Die kontinuierliche Arbeit vieler Aktivisten und ihre über die letzten Jahre gewachsenen und zunehmend professionalisierten Infrastrukturen und Netzwerke rund um European Digital Rights und seine Mitgliedsorganisationen haben sich ausgezahlt. Im richtigen Moment gab es die passenden Argumente, schlagkräftige Netzwerke und die notwendige Fachexpertise um den öffentlichen Diskurs zu gewinnen.

ACTA ist Geschichte. Wer hätte das vor einem Jahr geglaubt?

25.000-Euro-Kampagne: Der Waffenindustrie das Fürchten gelehrt

John F. Nebel

Es war wohl eine der schönsten, aggressivsten und erfolgreichsten Kampagnen gegen die deutsche Waffenindustrie seit langem: im Mai 2012 lobte die Aktionskünstlergruppe „Zentrum für politische Schönheit" (ZPS) 25.000 Euro für Hinweise aus, die zu einer Verurteilung der Haupteigner des Panzerkonzerns Krauss-Maffei Wegmann führen würden.

Doch es ging dabei nicht um eine Verurteilung wegen illegalen Waffenexports oder Verstöße gegen Waffenkontrollgesetze. Weil diese Gesetze nicht greifen und die Bundesregierung den Panzerdeal mit Saudi-Arabien unterstützt, sollten die Eigentümer wegen Steuerhinterziehung, Korruption, illegaler Beschäftigung von Haushaltshilfen oder ähnlicher Vergehen hinter Gitter.

Kern der Kampagne war die Webseite 25000-euro.de, auf der mit Steckbriefen und Fahndungsfotos die Haupteigner des Familienkonzerns aufgelistet wurden. Aus offen zugänglichen Quellen wie dem Handelsregister hatten die Aktionskünstler erst die Eigner und dann die Lebensläufe der Mitglieder der Panzerfamilien recherchiert und diese dann mit dem Kampagnenstart der Öffentlichkeit zugänglich gemacht.

Hinter der bürgerlichen Fassade

Diese Methode brach die bürgerliche Fassade der Waffenproduzenten auf: Wer hätte vermutet, dass sich die Eigentümer einer Panzerfirma in der Humanistischen Union engagieren, Kunstausstellungen machen oder als Psychotherapeutinnen arbeiten? Ihre Kinder auf Waldorfschulen schicken, als 68er aktiv waren, grünen Stiftungen Häuser vermieten und als Lehrerinnen an Berufsschulen arbeiten?

Alte Freunde der Eigner waren vor den Kopf gestoßen. Auf einmal wussten sie, mit wem sie es zu tun hatten. Gerade noch ein Freund, jetzt Panzerhersteller für das Regime in Saudi-Arabien. Die politische Debatte um Krieg, Menschenrechte und Panzer wurde direkt vor die Haustüren der Firmenbesitzer – und somit auf eine vollkommen persönliche Ebene getragen.

Die Waffenfirma stand ratlos da. Der Angriffsvektor der Kampagne hatte den wunden Punkt getroffen. Mit Kampagnen gegen das Unternehmen selbst kennen sich Rüstungskonzerne aus. Sie stehen seit Jahren im Fokus der Friedensbewegung und machen bei deren Aktionen das, was sie immer tun, wenn irgendetwas passiert: beobachten, totschweigen, aussitzen.

Doch dieses Mal war die Überraschung zu groß, die Kampagne zu radikal, der Ansatz zu neu.

Maskottchen der Rüstungsindustrie

Anfangs zeigte sich Kurt Braatz, der Sprecher von Krauss-Maffei Wegmann, entsetzt über die Kampagne, „vor allem aus moralischen Gründen." Doch Waffenfirmen haben naturgemäß keine Glaubwürdigkeit in Sachen Moral, weswegen diese Strategie nicht fruchtete und dann schnell aufgegeben wurde. Zumal das ZPS jetzt auch den Pressesprecher persönlich attackierte und ihn auf der Webseite als Maskottchen der deutschen Rüstungsindustrie präsentierte.

Der Kampagne gelang es wegen der Schärfe der Aktion und der umstrittenen Methode mit den Steckbriefen schnell, das Thema Panzer für Saudi-Arabien auf die Agenda zu setzen. Die kritischen Fragen wie „Darf man das?" oder „Geht das nicht zu weit, wenn man Privatpersonen an den Pranger stellt?" wurden geschickt als Hebel benutzt, um die politische Kampagne bundesweit bekannt zu machen. Und das in einer Situation, in der es praktisch keine Berichterstattung zum Panzerdeal mehr gab.

Hilflose Reaktionen

Krauss-Maffei Wegmann selbst und auch die Eigner wollten immer wieder die Verantwortung der Bundesregierung zuschieben, um selbst aus dem Fokus zu geraten. Der Pressesprecher erdreistete sich gar dem Bayrischen Rundfunk zu sagen: „Wir haben doch gar keine andere Wahl„[1] – man müsse die Bundesregierung fragen, die ja das Geschäft politisch verantworte.

Ein durchschaubarer Versuch, auf den sich die Aktivisten nicht einließen.

1 MP3: http://cdn-storage.br.de/on3/words/56/5efcf3da14f3ca87199d33bbe2fa45724c748db1.mp3

Immer mehr Medien berichteten nun über die Kampagne und begannen auch über Krauss-Maffei Wegmann zu recherchieren. Den Aktivisten selbst wurden weitere Details über die Eigner aus deren Umfeld zugespielt. Sie reichten diese umgehend an Journalisten weiter oder schlachteten sie direkt auf der Webseite aus.

Im Verlauf führte die Kampagne sogar dazu, dass sich mit Burkhart von Braunbehrens einer der Eigner öffentlich gegen den Deal stellte und in der Folge seinen Posten im Aufsichtsrat des Konzerns verlor. Heute lässt der 70-jährige kaum eine Gelegenheit aus, seine Version der Geschichte zu erzählen.[2] Er kämpft um seine Ehre in den Medien – und ist damit ein PR-Super-Gau für den verschwiegenen Waffenkonzern. Angeblich prüft Krauss-Maffei Wegmann mittlerweile, wie der „Nestbeschmutzer" komplett ausgeschlossen werden kann.

Sowohl der Konzern wie auch die Anteilseigner trauten sich lange Zeit nicht, mit rechtlichen Mitteln gegen die Kampagne vorzugehen, wohl wissend, dass dies noch mehr Öffentlichkeit bedeutet hätte. Sie spekulierten auf das Versanden, denn viele Kampagnen verhungern nach ein paar Tagen, weil die Aktivisten kein neues Futter nachlegen können. Eine Stärke der Kampagne war jedoch der von Anfang an voll gepackte Rucksack an Tools, um immer wieder etwas neues in den Ring werfen zu können.

Voll gepacktes Kommunikationsarsenal

Die Kampagne startete mit Großflächenplakaten und der Webseite. Ein an ein Crowdfunding-Spendenmeter erinnernder Balken zeigte auf der Seite den Prozentwert der eingegangenen Hinweise an: „Schon 30 % Hinweise, noch 70 % bis es zur Anzeige reicht". Kurz darauf folgte ein animiertes Video von Alexander Lehmann[3], das den Leopard-Panzer im Einsatz gegen Demonstranten zeigte. Dann wurden Steckbriefe zum Ausdrucken bereit gestellt, die an den Wohnorten der Eigner aufgehängt wurden. Ein paar Tage später wurden die Waffenproduzenten in künstlerischen Videos porträtiert, während auf der Webseite Mitarbeiter des Konzerns zum Leaken von Informationen

2 *Mayer, Verena* 2012: Die Panzerfamilie, in: http://www.tagesspiegel.de/politik/waffenhandel-mit-70-will-burkhart-braunbehrens-es-nochmal-wissen/7121806-3.html %29; 6.12.2012.

3 YouTube: https://www.youtube.com/watch?v=DlXF-hURVyU

aufgerufen wurden. Gefakte Blogs[4] wurden zur Verstärkung eingesetzt, ein Bundeskanzler aus der Zukunft[5] sprach eine Videomessage. Unterstützer wurden zum Herstellen von User Generated Content animiert – und begannen tatsächlich Videos, Briefe und Blogs zu erstellen. Es wurden Petitionen gestartet und sogar Werke der Panzerfirmeneigner verlost. Menschenrechtler aus Bahrain sagten per Videobotschaft, warum der Panzerdeal ein Problem sei. Bürger erklärten den Panzerherstellern den Krieg und schickten ihnen einen Brief mit Patronen.[6] Es gab sogar einem T-Shirt-Shop mit den Konterfeis der Panzerfamilie. Und der Sprecher der Bundesregierung wurde derart auf Twitter mit Fragen bombardiert, dass er reagieren musste. In der Anfangsphase war die Kampagne von einem veritablen Shitstorm begleitet. Mit immer neuen Tools und Einfällen konnten die Aktivisten mehr als vier Wochen lang das Thema aufrecht erhalten.

Zwar verlagerte sich die Berichterstattung schon recht bald weg von der Kampagne hin zu Details über den Rüstungskonzern, der Eigentumsverhältnisse des Familienunternehmens[7] und zur Haltung der Bundesregierung zum Panzerdeal mit den Saudis. Die Presse stellte nun Transparenz[8] im wenig beleuchteten Feld eines familiengeführten Rüstungskonzerns her. Medien aus Frankreich, Dänemark, Russland und vielen anderen Ländern berichteten.

Das Zentrum für politische Schönheit hatte an diesem Punkt schon das eigentliche Kampagnenziel mehr als erreicht: eine Debatte anfachen und den politischen Preis für den Panzerexport nach oben treiben. Dass irgendjemand in den Knast gehen würde, hatten die Aktivisten nie geglaubt. Das war immer nur der Aufhänger für die Kampagne gewesen.

4 Vgl.: http://petergegenkraussmaffei.wordpress.com/

5 YouTube: http://youtu.be/_SAc-9Xzgsk

6 Vimeo: http://vimeo.com/43501013

7 *Treser, Tanja* 2012: Die verschwiegenen Macher der Leopard-2-Panzers, in: http://www.focus.de/finanzen/news/unternehmen/tid-26350/wirtschaft-die-macher-des-leopard-2_aid_768153.html; 6.12.2012.

8 *Weber, Stefan* 2012: Stur wie ein Panzer, in: http://www.sueddeutsche.de/wirtschaft/ruestungsfirma-kraus-maffei-wegmann-stur-wie-ein-panzer-1.1388959; 6.12.2012.

Abmahnungen und Streisand

Erst nachdem sich die große mediale Welle gelegt hatte, musste das ZPS Anfang Juli eine Unterlassungserklärung unterschreiben, die nicht mehr abgewendet werden konnte. Fortan durfte kein „Kopfgeld" mehr ausgesetzt und keine „Fahndung" mehr betrieben werden. Bestimmte Formulierungen, Sätze und Bilder mussten von der Kampagnenseite entfernt werden.

Von diesem juristischen Erfolg bestätigt, versuchten die Anwälte der Eigner nun weitere Inhalte der Kampagne aus dem Netz zu klagen. Sie drohten der Verfasserin des trashigen Videos „Schnuppivera"[9], das die Eignerin und Psychotherapeutin Vera von Braunbehrens auf die Schippe nimmt, mit einer Klage, wenn sie das Video nicht entfernen würde. Das ZPS veröffentlichte das Anwaltsschreiben – und löste damit den Streisand-Effekt aus. Das Video, das bis dahin nur ein paar hundert Klicks hatte, wurde schlagartig auf zahlreiche Plattformen kopiert – und hat heute alleine auf Youtube mehr als 42.000 Abrufe. Nach diesem Schuss vor den Bug stellten die Anwälte ihre Aktivitäten gegen die Kampagne und ihre Unterstützer ein.

Gleich mehrere Ziele erreicht

Auch wenn die Kampagne danach erwartungsgemäß abflaute, erreichte sie gleich mehrere Ziele: Das Google-Karma des Konzerns Krauss-Maffei Wegmann und seiner Anteilseigner ist nachhaltig und langfristig beschädigt. Wer heute nach dem Konzern sucht, kommt an der Kampagne nicht vorbei. Die Besitzer des Familienkonzerns sind heute weithin im Netz sichtbar. Außerdem wurde die Struktur des Konzerns von Medien intensiv dargestellt und ist heute präsenter denn je.

Die Kampagne hat ein Grundrauschen verursacht, das die Berichterstattung zum Panzerdeal und Waffenexporten auch heute noch verstärkt. Gleichzeitig haben einzelne Mitglieder der Panzerfamilie mediale Aktivitäten entwickelt, die der Hinterzimmerlogik und lautlosen Vorgehensweise von Rüstungskonzernen diametral entgegenstehen.

9 YouTube: https://www.youtube.com/watch?v=Qn5KE_h3-tM

Gleichzeitig wurde der politische Preis für den Rüstungsexport so hoch getrieben, dass Stimmen aus der Bundesregierung unter vorgehaltener Hand sagen, dass der Panzerdeal mit den Saudis nicht mehr vor der Bundestagswahl 2013 zustande kommen wird.

Lernen für andere politische Kampagnen

Aktivisten können von der Panzerkampagne lernen, dass mit wenig Ressourcen, klugen Angriffsvektoren und einem bunten Strauß von Kampagnentools manchmal mehr möglich ist als mit einem breiten zivilgesellschaftlichen Bündnis, das klassisch aufgestellt ist. Eine Vorgehensweise, die auch Methoden der Kommunikationsguerilla einstreut, ist dabei vielversprechend und unterstützt die Überraschungseffekte.

Kampagnen brauchen dabei viel Munition um langfristig den Druck aufrecht zu erhalten: sie müssen sowohl den Unterstützern wie auch der Presse immer wieder Neues bieten. Dabei sollten sowohl das ganze Arsenal der Onlinekommunikation wie auch einige Offline-Mittel genutzt werden, weil so eine Verstärkung der Kampagne stattfindet und das Anliegen für den Gegner sichtbar auf die Straße getragen wird.

Ist der Gegner wie die Rüstungsindustrie in einer moralisch schwachen Position, lassen sich auch aggressive Kampagnen gegen ihn fahren, die trotz ihrer Radikalität eine breite Unterstützung der Öffentlichkeit genießen.

Vermutlich hat die Aktion des Zentrums für politische Schönheit nur ein paar tausend Euro und viele hundert Arbeitsstunden gekostet: der Effekt ist der einer Millionenkampagne. Chapeau!

Grundlage dieses Artikels ist ein Hintergrundgespräch mit zwei Aktivisten des Zentrums für politische Schönheit.

Anonymous: Leuchtfeuer der digitalen Freiheit

Gabriella Colemann

Es ist der späte Januar 2012. Regierungen auf der ganzen Welt bereiten sich darauf vor, ein neues, US-geführtes Handelsabkommen zu unterzeichnen, das Urheberrechtsverletzungen eindämmen soll: das Anti-Produktpiraterie-Handelsabkommen ACTA. Dann hatte es umfassende Proteste gegeben, on- und offline: Für das als „Anonymous" bekannt gewordene lose Kollektiv von Aktivisten, Hackern und Internet-Bewohnern aller Art stellt ACTA der Versuch dar, die grundsätzlichen Freiheiten des Internets zu beschränken und zu kontrollieren, insbesondere den enormen kulturellen Austausch von Ideen und Informationen, der durch Filesharing ermöglicht wird.

In Polen war das Abkommen bereits unterzeichnet worden; einzig eine Mehrheit im Parlament war noch nötig, um es in nationales Recht umzusetzen. Dann war die Webseite der Regierung offline, vom Netz genommen durch eine Distributed Denial of Service (DDoS) Attacke von Anonymous. Dies war eine klare Botschaft an die PolitikerInnen, die überlegten, für das Abkommen zu stimmen. In der letzten Januarwoche versammelten sich mehr als 10.000 Menschen in Krakau zu einem allerletzten Protest, um die Abstimmung zu beeinflussen. Und dann geschah etwas Unerwartetes: Am 26. Januar 2012 setzen sich einige Mitglieder der polnischen Regierung während der Stimmabgabe im Parlament Guy Fawkes Masken aus Papier auf. Diese Maske, mittlerweile das Symbol von Anonymous, ist für Demonstranten auf der ganzen Welt zum verbreiteten Zeichen des Protests geworden, vom Tahrir-Platz in Ägypten bis zu den Occupy-Protesten in London. Aber jetzt übernahmen öffentlich Bedienstete das Symbol zum ersten Mal. Das Bild verbreitete sich wie ein Lauffeuer in den sozialen Medien.

Obwohl polnische PolitikerInnen das Symbol verwendeten, um einen spezifischen Protest gegen ACTA zu starten, trug die Geste und ihre fotografische Erinnerungsfunktion stark zur Legitimierung von Anonymous bei. „Diese Abgeordneten hatten Anonymous Guy Fawkes Masken auf", bloggte ein Aktivist von Anonymous, „während die Website des Parlaments wegen einem DDoS von Anonymous offline war. Wir können diesen Fakt nicht genug betonen – das ist ein Wendepunkt."

Nicht einmal einen Monat später ging ein ganz anderes Bild von Anonymous um. Am 21. Februar 2012 berichtete das Wall Street Journal, dass General Keith Alexander, der Direktor der amerikanischen Nationalen Sicherheitsbehörde (NSA), in einem geheimen Meeting im Weißen Haus Beamte darüber informiert hatte, dass Anonymous „dazu fähig ist, innerhalb der nächsten ein, zwei Jahre durch einen Cyberangriff einen begrenzten Stromausfall zu erzeugen". Damit wurde die Gruppe nur wenige Wochen nach dem „Wendepunkt" als bevorstehende und glaubwürdige Bedrohung beschrieben.

Was es bedeutetet zur Erzeugung eines Stromausfalls „fähig" zu sein, blieb undefiniert. Könnte das heißen, dass Hacker bereits Passwörter erlangt haben, die ihnen Zugang zu Stromanlagen ermöglichen? Oder beruhte diese Warnung auf dem Hinweis eines Informanten, der mit Anonymous gearbeitet hatte? Jedenfalls waren die Behauptungen von General Alexander beängstigend und gewagt, aber auch ungenau. Ein Angriff auf Stromnetze würde Chaos verursachen und könnte möglicherweise sogar Leben gefährden. Es ist unwahrscheinlich, dass wir jemals herausfinden, ob die Einschätzung der NSA auf glaubwürdigen Informationen beruhte oder ob damit Anonymous einfach verunglimpft und diskreditiert werden sollte. Weitere Nachrichtenberichte zitierten AktivistInnen und SicherheitsexpertInnen und wiesen die Behauptungen der NSA als „Panikmache" zurück. Es ist bis heute nicht bekannt, dass die Gruppe mit all ihren verschiedenen, legalen und illegalen Taktiken, jemals öffentlich zu einem solchen Angriff aufgerufen hätte – und es gibt keine Anzeichen dafür, dass sie es auch nur in Erwägung zieht. Eine solche Taktik wäre sehr untypisch für das Kollektiv, das, wenn häufig auch subversiv, in der Regel ethischen Normen entspricht und zivile Freiheiten verteidigt.

Obwohl Anonymous nie unkontrovers war, wurden sie ab Februar 2012 als eine Open-Source-Marke radikaler Protest-Politik dargestellt und nicht unbedingt als Hooligans, die darauf versessen sind, extremistische und chaotische Taten wie das Abschalten von Stromnetzen auszulösen. Noch wichtiger: Während der Name verwendet wurde, um ein Spektrum unabhängiger Anliegen von Umweltrechten bis zum Aufdecken von Pädophilen-Ringen zusammenzubringen, sind Anonymous Aktivisten am wirksamsten und energischsten im Kampf gegen Zensur. Mit Kampagnen wie Operation Payback, die auf Konzerne wie MasterCard zielte als diese ihre Dienste für WikiLeaks einstellten, oder OpTunisia als Antwort auf das Vorgehen der tunesischen Regierung

gegen Demonstranten und Journalisten, oder OpJapan und OpMegaupload, die als Antwort auf vorgeschlagene Gesetze zum Urheberrecht gestartet wurden: Anonymous-Aktivisten sind am wirksamsten, wenn sie die grundlegenden Freiheiten des Internets verteidigen und die Überwachung von Staaten und Unternehmen aufdecken.

Die Nachricht der NSA über die ernste Bedrohung von Anonymous schaffte es nicht, im öffentlichen Bewusstsein Fuß zu fassen. Vielleicht hätte sie es geschafft, wenn sie früher gekommen wäre, zum Beispiel zwischen Mai und Juli 2011 auf dem Höhepunkt der von LulzSec angeführten Angriffe. Im Gegensatz zu den meisten anderen Aktionen von Anonymous handelte LulzSec, eine abgespaltene Hacker-Gruppe, launenhaft und die Hacks waren auch nicht immer mit einem politischen Anliegen verbunden. Manchmal hackte LulzSec, um ein politisches Statement abzugeben, in anderen Fällen „for the Lulz", umgangssprachlich im Internet für Lachen. In dieser Zeit richtete sich die Medienaufmerksamkeit, die riesig war, am meisten auf Anonymous als Hacker und nicht als allgemeine Protest-Gruppe.

Aktivitäten unter dem Label Anonymous, wie die von LulzSec, zeigen, dass obwohl Anonymous durch seinen Einsatz für freie Meinungsäußerung und Privatsphäre ein gewisses Maß an Respekt erhalten hat, es trotzdem berüchtigt ist für seinen respektlosen und umstrittenen Ansatz des Dissens. Um es klar zu stellen: die meisten der Aktivitäten sind legal, aber ein kleiner Teil – wie DDoS Attacken und Hacks – sind illegal und eindeutig Straftaten. Diese Taktiken erzielen auch die meisten Schlagzeilen. Einige Maßnahmen, wie zum Beispiel „doxing" (das Veröffentlichen von persönlichen, vertraulichen Informationen wie Sozialversicherungsnummern oder Anschriften) befinden sich in einer rechtlichen Grauzone, weil sich die gewonnen Informationen auf öffentlich zugänglichen Webseiten finden lassen.

Im Laufe einer einzigen Operation können verschiedene TeilnehmerInnen auch alle drei Modelle anwenden: legale, illegale und rechtlich uneindeutige Taktiken. Nehmen wir Operation Bart im August 2011. Anonymous konzentrierte sich darauf, bekannt zu machen, dass Beamte des öffentlichen Nahverkehrs in San Francisco (BART) den Handyempfang auf Bahnsteigen abgeschaltet haben, um geplante Proteste gegen Polizeigewalt zu vereiteln. Wenig später half Anonymous dabei, Demonstrationen auf der Straße zu organisieren. Einige wenige hackten sich jedoch in das BART-Netzwerk und veröffentlichten Kundendaten, um die Aufmerksamkeit der Medien zu wecken – so er-

klärte es zumindest einer der TeilnehmerInnen im Fernseh- und Radioprogramm Democracy Now gegenüber Amy Goodman. Jemand fand außerdem ein gewagtes, halb-nacktes Bild des offiziellen Sprechers von BART, Linton Johnson, auf dessen persönlicher Webseite. Das wurde dann auf der Webseite „bartlulz" mit einigem Wirbel veröffentlicht, zusammen mit der schamlosen Begründung: „Wenn du dich gegenüber der Öffentlichkeit wie ein Arsch verhältst, dann hast du sicherlich auch kein Problem damit, deinen Arsch der Öffentlichkeit zu zeigen". Im Laufe einer Operation werden Verletzlichkeit und Schwäche häufig erkannt und ausgenutzt. Diese Art von Aktionen provoziert Kontroversen (auch innerhalb Anonymous) und findet ihren Weg in Schlagzeilen, die das öffentliche Profil der Gruppe stärken.

Manchmal sind die Mitglieder des losen Kollektivs absichtlich hinterlistig und verbreiten Falschinformationen über ihre Aktivitäten. Das kann in einigen Fällen eine Taktik zum Selbstschutz sein, oder auch um die Medien dazu zu bringen, falsche Schlagzeilen zu produzieren, was auch als eine Art von Hacking gesehen werden kann. AntiSec, eine der bekannteren an Anonymous angeschlossenen Hacker-Gruppen, könnte beispielsweise einen Hack für sich beanspruchen, ohne überhaupt an der Aktion beteiligt gewesen zu sein. Hacker sind häufig auf Botnetze (Netzwerke infizierter Computer) angewiesen, um eine Webseite kurzzeitig vom Netz zu nehmen, bewerben das aber nicht in Pressemitteilungen. Am 10. und 11. September 2012 behauptete AntiSec beispielsweise, sich 12 Millionen eindeutige Indentifikationsnummern von Apple iOS Geräten beschafft zu haben, indem sie sich in den Laptop eines FBI-Agenten gehackt hätten. Wie sich herausstellte, waren die Identifikationsnummern zwar echt, jedoch war die Quelle dafür eine Entwickler-Firma für iPhone und iPad, Blue Toad. Weil die Taktiken von oberflächlich über kontrovers bis zu illegal reichen und weil das Kollektiv dafür bekannt ist, einen Hype über die eigenen Aktivitäten zu generieren, kann es leicht selbst zur Zielscheibe werden. Verschleierung und Täuschung tragen zur Mystik und Macht von Anonymous bei, machen es aber auch anfällig für Desinformationskampagnen von Anderen.

Die größte Lehre, die aus Anonymous gezogen werden kann, ist, dass das Internet die Aktionen von Einzelpersonen, Unternehmen und Regierungen bewerten wird – und das häufig sehr schnell. Und mit Internet meine ich die unzähligen Hacker und Geeks von São Paulo bis Sydney, die verstehen, wie das

Internet funktioniert, einen kleineren Teil der weiß, wie man Router und Protokolle austrickst und ein größere Masse, die sich versammelt, wenn das Internet und seine Werte in Gefahr sind.

Das heißt nicht, dass jeder Geek und Hacker Anonymous unterstützt. Tatsächlich mögen viele davon Anonymous oder ihre umstrittenen Taktiken wie DDoS eher nicht; manche Hacker vertreten entschlossen und unnachgiebig die Position, dass ein DDoS selbst eine Art von Zensur ist. Darüber hinaus gibt es viele verschiedene Arten, das Internet zu verteidigen, zum Beispiel das Programmieren freier Software oder der Eintritt in die Piratenpartei. Anonymous ist ein eigener, aufstrebender Teil dieser vielfältigen und aufkeimenden politischen Landschaft.

Die wahre Drohung von Anonymous liegt nicht so sehr in der Fähigkeit, digitale Angriffe zu organisieren, sondern in der Art wie es sich zu einem Leuchtfeuer entwickelt hat, einer vereinten Front gegen Zensur und Überwachung. Es könnte am Besten verstanden werden als jähzorniger und provokativer Protestflügel der entstehenden Bewegung für freie Meinungsäußerung und Datenschutz im Internet. Obwohl es bestimmte Themen zur ungünstigsten Zeit für die betroffenen Einzelpersonen, Gruppen oder Unternehmen in den Fokus der Öffentlichkeit rückt, verdeutlicht es damit auch einen wichtigen Trend: In einer Zeit, in der der Wert von Datenschutz und Anonymität immer schneller ausgehöhlt wird, dramatisiert Anonymous den Wert von beiden. Anonymous setzt sich natürlich für Anonymität ein, das spiegelt sich sowohl in der mit ihm verbundenen Ikonografie als auch seinem Verhaltenskodex wider. Es ist beispielsweise tabu, individuelle Anerkennung oder Ruhm erlangen zu wollen; es wird erwartet, dass für das Team gearbeitet wird und nicht zum eigenen Vorteil oder Status. Die Bewegung bildet daher in Taten, Worten und Symbolen eine seltene Gegenmaßnahme zu einer Welt, die Menschen dazu ermutigt, ihr Leben zu offenbaren, wo das Internet sich an alles über uns erinnert, wo unsere Geschichte permanent in Suchmaschinen und Regierungsdatenbanken gespeichert wird – und zu einer Zeit, in der die Fähigkeit der Regierungen, ihre BürgerInnen zu überwachen exponentiell steigt, dank günstiger allgegenwärtiger digitaler Technologien und neuer, öffentlich-privater Partnerschaften.

Wie brisant Anonymous heute auch ist, die anhaltende Anwesenheit auf der Weltbühne wird sicherlich nicht immer andauern. Das Kollektiv ist geplagt von internen Machtkämpfe, Zersplitterung und einer Überanstrengung der

Marke. Die Paranoia erreichte ihren Höhepunkt im Frühling 2012, als herauskam, dass Hector Xavier Monsegur, besser bekannt unter seinem Hacker-Nick „Sabu", als FBI-Informant enttarnt worden war.

Am gefährlichsten für das langfristige Überleben von Anonymous ist das Durchgreifen von Regierungen: seit dem Sommer 2011 wurden über 100 mutmaßliche Teilnehmer weltweit verhaftet, aus Rumänien, der Türkei, Italien, Großbritannien, den USA, Chile und Deutschland.

Doch selbst wenn das lose Kollektiv langsam verblasst, ist es unwahrscheinlich, dass der respektlose Protest im Internet aufhören wird. Seit 2008, als Einzelpersonen begannen, diverse kollektive Aktionen unter dem Banner von Anonymous zu organisieren, wurde ein lebendiges Vorbild geschaffen, das der Welt zeigt, wie eine radikale Politik des Widerspruchs im Internet aussieht. Selbst wenn Anonymous verschwindet, seine Geschichte, die Hacks und das Propagandamaterial werden bleiben; es wird wahrscheinlich andere geben — in anderen Formen und unterschiedlichen Gestalten — die dessen Platz einnehmen werden.

Weniger klar ist, was schließlich aus der Meinungsfreiheit im Internet werden wird, angesichts zunehmender Fähigkeiten zur Überwachung, Zensur und Kontrolle weltweit. Ist Anonymous lediglich die Feier auf der Beerdigung der Online-Freiheit? Oder vertritt es die respektlosen Clowns, die AufrüherInnen und Trickser, die den Sensenmann in Schach halten und es anderen ermöglichen, von den Demonstrierenden auf den Straßen bis zu den Abgeordneten in Parlamenten, am rauen politischen Karneval teilzunehmen und die Bedrohungen für persönlichen Datenschutz und Freiheit zu bekämpfen?

Zeitleiste

Dezember 2010

Operation Payback zielt auf Unternehmen und startet DDoS Attacken gegen Mastercard und andere Firmen, die Spendenmöglichkeiten für WikiLeaks eingestellt hatten. WikiLeaks hatte auf ihrer Webseite tausende diplomatischer Depeschen veröffentlicht.

Januar 2011

OpTunesia beginnt als Reaktion auf die Sperrung von WikiLeaks durch die tunesische Regierung. Anonymous Aktivisten nehmen Webseiten der Regierung vom Netz, als Vergeltung für Unterdrückung von Protest und Repression von JournalistInnen. Sie helfen dabei, „Care-Pakate" an Demonstrierende zu verteilen, die Informationen und Werkzeuge enthalten, wie sie sich anonym im Netz bewegen und Videos über staatliche Gewalt an Protestierenden schleusen können.

Februar 2011

Als Antwort auf die Unterdrückung von Online-AktivistInnen durch die ägyptische Regierung startet Anonymous die OpEgypt und beginnt mit DDoS Attacken auf die Webseiten des Informationsministeriums und der Nationaldemokratischen Partei.

Als der Geschäftsführer der Sicherheitsfirma HBGary Federal behauptet, Anonymous infiltriert zu haben, rächen sich die Hacker mit OpHBGary und demütigen Barr durch das Eindringen in HBGary-Server, das Leaken von 68.000 Firmen-Mails und das Löschen von Backups. In den Daten der Firma stoßen sie zufällig auf eine detaillierte PowerPoint-Präsentation mit dem Namen „Die Wikileaks Gefahr" und einen Vorschlag, WikiLeaks und sympathisierende JournalistInnen im Namen der Bank of America zu diskreditieren.

August 2011

OpBART wird als Antwort auf die Entscheidung des öffentlichen Nahverkehrs in San Francisco (BART) gestartet, den Handyempfang auf Bahnsteigen zu blockieren, um Proteste gegen Polizeigewalt zu verhindern. Anonymous sendet Massen an E-Mails und Faxe an Angestellte von BART, veranstaltet örtlichen Protest mit lokalen Aktivisten, hackt die BART Webseite und veröffentlicht private Kundendaten.

Dezember 2011

AntiSec, eine Splittergruppe von Anonymous, behauptet, die Sicherheits- und Nachrichten-Firma Stratfor gehackt und tausende von E-Mails sowie Informationen über Kunden-Kreditkarten gestohlen zu haben. Ein E-Mail-Gespräch, das Monate später im August 2012 veröffentlicht wird, weist darauf hin, dass der Stratfor-Hack zu Enthüllungen über die Existenz von TrapWire führte, ein globales Überwachungssystem der US-Regierung.

Januar 2012

Die OpMegaupload folgt auf den Stop Online Piracy Act (SOPA) Blackout am 17. Januar, den auch Anonymous AktivistInnen sehr unterstützt haben. Mit dieser Op startet die bisher größte DDoS Attacke, durch die Nutzung von Botnetzen (Netzwerke infizierter Computer) wurde der Zugang zu folgenden Webseiten blockiert: Justizministerium der USA, Universal Music Group, FBI, Motion Picture Association of America, Universal Music, der Beglische Anti-Piraterie-Verband, Verband der Musikindustrie in den USA, die französische Urheberrechtsbehörde HADOPI, US Copyright Office, Universal Music France, die Seite des Senators Christopher Dodd, Vivendi Frankreich, das Weiße Haus und die Warner Music Group. Das ist eine direkte Antwort auf die Beschlagnahme und Abschaltung der Webseite megaupload.com und die Verhaftung des Inhabers Kim Dotcom durch das FBI und das Justizministerium.

Mai 2012

Operation Quebec, eine Studentenbewegung gegen Studiengebühren, erhält nach der Annahme des der Bill 78 durch die Nationalversammlung Unterstützung von Anonymous. Das Gesetzt führt neue Regelungen für Versammlungen und Protestaktivitäten ein und untersagt u. a. Das Tragen von Masken auf Demonstrationen. Am 20. Mai ruft Anonymous die sozialliberale Partei von Quebec dazu auf, das Protest-Recht der BürgerInnen zu respektieren. Am 21. Mai startet Anonymous dann DDoS Attacken auf die Webseite der Partei sowie auf einige Seiten der Regierung und der Polizei.

Juni 2012

OpJapan, eine Reihe von DDoS Attacken gegen den Verband der japanischen Wirtschaftsorganisationen, kommt in Gang. Diese Operation ist eine koordinierte Antwort auf die drakonische neue Urheberrechtsgesetzgebung in Japan, die als Strafen für das Besitzen von urheberrechtlich geschützten Werken Geldstrafen von 25.000 Dollar oder Haftstrafen von zwei Jahren vorsieht.

Dieser Beitrag erschien zuerst in der Ausgabe „Digital Frontiers" des Magazins von Index on Censorship.

Big Picture

Digitale Solidarität. Perspektiven der Netzpolitik

Felix Stalder

Wir stehen vor einer historischen Chance, neue Formen solidarischen Handelns zu erfinden. Das politisch-ökonomische System in Europa, aber auch darüber hinaus, steckt in einer tiefen Krise. Diese hat viele Gründe. Einer davon ist, dass sich im Kern der avanciertesten Bereiche der Ökonomie ein Widerspruch verschärft. Auf der einen Seite haben wir die zunehmende Bedeutung der Momente der sozialen Interaktion, des Austauschs, des vernetzen Wissens- und Handelns, auf der anderen Seite haben wir eine sich verschärfende Logik der privaten Aneignung dieser gemeinsam hervorgebrachten Werte. Während die eine Seite sich immer wieder der Aneignung zu entziehen versucht, und mit freien Lizenzen auch teilweise Mittel gefunden hat, das zu tun, sucht die andere nach immer neuen Wegen, um Wissen und Kultur zu privatisieren und läuft Gefahr, damit die Voraussetzungen für die Entstehung neuen Wissens und neuer Kultur zu zerstören. Es wird sich noch herausstellen, ob wir es hier mit einem Widerspruch zwischen Produktions- und Eigentumsformen zu tun haben, den Karl Marx als Voraussetzung für einen Wechsel in der Produktionsweise diagnostizierte. Es ist denkbar, aber sicher ist das nicht.

Labor der sozialen Innovation

Wie dem auch sei, in den letzten zwei Jahrzehnten war das Internet ein Labor der sozialen Innovation. Eine der erstaunlichsten Entdeckungen, die wir in diesem Labor machen konnten, war, dass es neben Markt und Staat weitere institutionelle Formen gibt, um Produktion und soziale Koordination in großem Umfang zu organisieren: Die Commons. Ob diese nun eine neue Erfindung oder eine Wiederentdeckung sehr alter, nicht-kapitalistischer Institutionen sind, ist eine offene Frage. Wichtig ist, dass sich diese neuen institutionellen Formen in gewissen Bereichen bereits als produktiv, nachhaltig und skalierbar erwiesen haben, obwohl sie lange Zeit auch von den Akteuren selbst kaum verstanden wurden, dem herrschenden Zeitgeist zutiefst widersprachen und sich in einem politischen Umfeld entwickeln mussten, das in keiner Weise auf diese institutionellen Formen angepasst war.

Aufgabe der Netzpolitik muss es sein, dieses Labor offen zu halten, und die Voraussetzungen des Wachstums dieser neuen Formen solidarischen Handelns zu verbessern. Aufgabe eine progressiven Politik ganz allgemein sollte es sein, diese Erfahrungen ernst zu nehmen und Bestrebungen zu fördern, sie auch auf andere Felder zu adaptieren.

Solidarität als Erfahrung

Eine progressive Politik ohne das Motiv der Solidarität kann nicht gelingen. Solidarität in diesem Sinne, als Grundlage einer konkreten Politik, ist keine Abstraktion. Sie ist keine menschliche Konstante, nur weil der Mensch ein soziales Wesen ist. Solidarität lässt sich auch nicht verordnen, sonst wird sie rasch zum Vorwand für zynische Bevormundung. Nein, Solidarität als Grundlage einer emanzipatorischen Politik ist Solidarität, die sich aus der täglichen Erfahrung speist, sich in den gemeinsamen Handlungen erneuert, und sich in der praktischen Einsicht ausdrückt, dass sich die eigenen Wünsche und Ziele nur im Verbund mit anderen, und nicht ohne sie und nicht gegen sie, erreichen lassen. Solidarität wächst horizontal, sie ist nie einfach vorhanden, sondern muss erneuert werden und widerstrebenden Dynamiken widerstehen können.

Eines dieser Felder, in denen Erfahrungen der Solidarität erneuert werden können, ist die Kultur und eines der Instrumente ist die Netzpolitik, die politische Instrumente suchen muss, um solche Prozesse zu verstärken. Die digitale Kultur stellt eine konkrete, gelebte Realität dar, die vielfach als positiv und ermächtigend erlebt wird. Die ACTA-Proteste haben gezeigt, dass sie mittlerweile auch ein hohes politisches Mobilisierungspotential gewonnen hat. Die digitale Kultur ist ein günstiges Feld für progressive Politik, weil man hier meint, den Wind der Geschichte im Rücken zu spüren, während einem der Wind bei anderen Themen all zu oft ins Gesicht bläst.

Arbeiter wird sozialer, kommunikativer, komplexer und vernetzter

Die Arbeitswelt und ihre Anforderungen haben sich extrem verändert. Das ist besonders deutlich im Bereich der sogenannten „Wissensarbeit“, aber nicht nur darauf beschränkt. Die Arbeit ist sozialer, sie ist kommunikativer, sie ist komplexer und sie ist vernetzter geworden. Mit „sozial“ meine ich, dass soziale Fähigkeiten wie Teamarbeit und emotionale Identifikation wichtiger geworden sind. „Kommunikativ“ in diesem Zusammenhang bedeutet, dass ein

wesentlicher Teil der Arbeit aus Koordination mit anderen besteht, deren Zustände und Befindlichkeiten kontinuierlich abgefragt und in die eigene Planung einbezogen werden müssen. Die Komplexität, die jedem einzelnen im Alltag dabei begegnet, ist so groß, dass niemand mehr von sich selbst behaupten kann, seinen Bereich, und sei der auch noch so klein und spezialisiert, selbst überschauen zu können. Die Realität Wissensgesellschaft drückt sich auch ganz stark in der Erfahrung des eigenen Nicht-Wissens aus. Dies um so mehr, weil Wissen ganz allgemein immer an Wert und Nützlichkeit verliert. Anwendbarkeit und damit Gültigkeitsdauer von Wissen schrumpft in einer sich flexibilisierenden Gesellschaft. Aber die Arbeitswelt wird auch immer vernetzter und damit steigen die Möglichkeiten, das eigene Nicht-Wissen und Nicht-Können durch Kooperation produktiv zu machen. Auch wenn man etwas nicht weiß, etwas nicht kann, so besteht doch immer die Erwartung, dass es irgendwo jemanden gibt, der gerade dies weiß, der gerade jenes Problem lösen kann. Im Bezug auf die Entwicklung von Freier- und Open Source Software gibt es diesen berühmten Satz „Given enough eyeballs, all bugs are shallow", was bedeutet, dass es für jedes Problem, das man selbst nicht lösen kann, jemanden gibt, der genau dieses Problem lösen kann, wenn nur der Pool der Personen, die zu Rate gezogen werden können, groß genug ist. Das wird oft als Credo für die Schwarmintelligenz gehandelt. Davon halte ich wenig. Es geht nicht darum, viele zu finden, sondern aus einer großen Menge die eine Person, zu der produktive Unterschiede bestehen. Mit Suchmaschinen, sozialen Netzwerken, und anderen Plattformen haben wir heute erste Infrastrukturen, die uns erlauben, genau solche Differenzen aufzuspüren. Diese Differenzen dürfen nicht zu klein sein, sonst entsteht nichts neues in ihrer Vernetzung. Die Differenzen dürfen aber auch nicht zu groß sein, sonst lassen sich keine Protokolle der Vernetzung etablieren. Nur das richtige Maß an Differenz erzeugt jene Spannung, die neue Netze hervorbringen kann.

Dies führt zu jener merkwürdigen Vermischung von Kooperation und Konkurrenz, die die heutige Arbeitswelt prägt. Die wirtschaftliche Konkurrenz wird durch den Markt vorangetrieben, die Kooperation durch die veränderten Herausforderungen des vernetzten Arbeitens und Lebens. Im Moment radikalisieren sich beide Dynamiken. Es entsteht so etwas wie ein systemischer Widerspruch. Inwiefern sich dieser Widerspruch politisch nutzen lässt, oder ob er wieder eingefangen und entschärft werden kann, wird sich zeigen. Das ist eine der Herausforderungen der Netzpolitik.

Individualisierung

Die zweite Quelle, die den Wind der Geschichte blasen lässt, ist die bereits angesprochene gesellschaftliche Individualisierung. Sie ist das große, positive Vermächtnis der neuen sozialen Bewegungen der letzten 40 Jahre. Individualisierung bedeutet zunächst nur, dass die Spannbreite wächst, innerhalb derer Menschen ihre Identität und ihr Lebensweisen artikulieren können, ohne in einen tiefen Konflikt mit der Gesellschaft zu geraten. Dahinter kann und soll es kein Zurück geben. Das ist nicht gleich zu setzen mit gesellschaftlicher Atomisierung und Entsolidarisierung, auch wenn das die neoliberale Ideologie sehr erfolgreich getan hat. Dass man sich von anderen unterscheidet, und diese Unterschiede betont, muss noch nicht heißen, dass man mit ihnen keine Erfahrungen teilen kann. Das ist der große Unterschied zwischen progressiven Ideen der Gemeinschaft, die nach vorne als Vielfalt gedacht werden, und konservativen Ideen von Gemeinschaft, die rückwärts als Einheit entworfen werden.

Diese Form der positiven Differenzen zeichnet die kooperativen Dimensionen der digitalen Kultur aus. Sie ermöglichen es, ein anderes Verhältnis zwischen Individuum und Gemeinschaft erfahrbar zu machen, eines, das das Verhältnis der beiden nicht als Widerspruch artikuliert. Die Vernetzung ist eben kein Kollektivierungsprozess im traditionellen Sinne, bei dem die internen Differenzen minimiert werden. Im Gegenteil, das Gemeinsame wird als Voraussetzung der Individualisierung erfahrbar. Bei aller Konkurrenz, die innerhalb freiwilliger Projekte herrscht, sei es bei freier Software oder in der Wikipedia-Community, so ist doch immer klar, dass der eigene Status nur durch die Gemeinschaft überhaupt erworben werden kann. Und somit der eigene Status über eine Stärkung des Gemeinsamen vergrößert wird. Das bedeutet noch keineswegs, dass die internen Prozesse konfliktfrei ablaufen, aber es gibt ihnen eine andere Dynamik.

Infrastrukturen der Horizontalität

Der dritte Punkt betrifft die Technologie selbst. Es stehen heute Infrastrukturen zu Verfügung, die es erlauben, große Projekte anders, das heißt, offener und kooperativer, zu organisieren. Der Druck zur Hierarchisierung und Bürokratisierung, der noch vor einer Generation innerhalb jeder Organisation parallel mit ihrem Wachstum zunahm, ist heute deutlich schwächer. Die erhöhten Kommunikationsanforderungen, die horizontale Koordination ver-

langen, lassen sich heute effizient und kostengünstig bewältigen. In einigen Fällen klappt das schon sehr gut – Freie und Open Source Software ließen sich auch hier als Paradebeispiel anführen. In anderen Fällen sind wir noch sehr am Anfang der Lernkurve. Erstaunlicherweise wird das bei der Piratenpartei, und deren Nutzung von Twitter, gerade besonders deutlich. Aber, ganz generell, war es früher ein Privileg der Eliten mit ihren Privatsekretariaten, große soziale Netzwerke zu unterhalten, so kann das heute jeder. Aber wir sind noch erst am Anfang. Hier ist noch viel soziale und technische Innovation notwendig, um die Potentiale zu realisieren.

Wenn wir also davon ausgehen, dass die digitale Kultur neue Felder gelebter Solidarität eröffnet, kann und sollte Netzpolitik darauf ausgerichtet sein, genau diese Momente zu stärken.

Was bedeutet das konkret?

Einschränkungen der freien Kommunikation müssen abgebaut werden.

Freie Kommunikation ist die Voraussetzung für horizontale Kooperation und der Entstehung von Solidarität. Dass sie online mehr eingeschränkt wird als offline, das muss unbedingt verhindert werden.

1. *Urheberrecht*, die Hauptprobleme hier sind die obsolete Unterscheidung zwischen privater und öffentlicher Nutzung. Im Zeitalter sozialer Medien ist diese Unterscheidung nicht mehr anwendbar. Sie muss gestrichen werden, und mit einer Unterscheidung von kommerzieller und nicht-kommerzieller Nutzung ersetzt werden, sei das durch eine neue Schranke, eine Bagatellklausel oder ähnliches. Das zweite Hauptproblem ist, dass jede Veränderung eines Werkes vom Rechteinhaber verhindert werden kann. Das verunmöglicht die freie Kommunikation in einer Welt, die fast nur aus kulturellen Werken besteht. Hier brauchen wir eine starke, umfassende Regelung zur freien transformativen Werknutzung. Im wesentlichen muss es darum gehen, dass die soziale Kommunikation und Alltagskreativität vom Urheberrecht nicht mehr erfasst wird.
2. der zweite wesentliche Punkt ist der *Kampf gegen Netzsperren* aller Art.

3. Der dritte Wesentliche Punkt um die freie Kommunikation zu stärken ist der freie Zugang zu Information. *Open Data / Open Access*. Informationsmonopole und Wissensdifferentiale verhindern horizontale Kooperation.

Mechanismen des Vertrauens müssen gestärkt werden.

1. *Schutz der Privatsphäre* ist und bleibt wichtig. Die ganze „Post-Privacy" Ideologie wird von Menschen betrieben, die selbst dermaßen privilegiert im gesellschaftlichen Mainstream leben, dass sie den Schutz, den die Privatsphäre bietet, nie in Anspruch nehmen müssen.

2. *Schutz vor Überwachung*. Das betrifft natürlich den ganzen Bereich von Vorratsdatenspeicherung, geht aber auch darüber hinaus. Wir müssen verhindern, dass die zunehmende Semi-Öffentlichkeit des Alltags dazu benutzt wird, dass bestehende Informationen systematisch gesammelt und für Sicherheitsinteressen ausgewertet werden. Wir müssen neue Schutzmechanismen für diese semi-öffentlichen sozialen Formen finden.

3. Eine Möglichkeit sind *intelligente Authentifizierungsformen*, die es durch Pseudonyme erlauben, Daten getrennt voneinander zu halten.

Drittens, und das ist jetzt der schwierigste Punkt, wir müssen

neue Formen der Einhegung

bekämpften. Damit meine ich, die Nutzbarmachung und Optimierung der Kommunikationsflüsse für kommerzielle Interesse. Dies wird ermöglicht durch die zunehmende Zentralisierung und Privatisierung der Kommunikationsmittel. Ich möchte dafür 3 Beispiele geben:

1. *Zensur:*

   Josh Begley, ein Student aus New York, entwickelte eine App, die auf Basis von Informationen des Londoner Bureau Of Investigative Journalism rudimentäre Information zu den Opfern US-Amerikanischer Drohnenangriffe darstellt. Apple hat es bisher drei Mal abgelehnt, diese App in den App Store aufzunehmen. Jedes mal mit einer anderen Begründung, zuletzt damit dass es sich hier um „Inhalte

handle, an denen viele Anstoß nehmen könnten." Die Begründung ist gar nicht so wichtig, wichtig ist vielmehr, dass hier eine Instanz entstanden ist, die nach eigenem Gutdünken entscheiden kann, was veröffentlicht wird.

2. Schwieriger zu bekämpfen sind die Einhegungen, die dadurch geschehen, dass die Formen und Mittel, mit denen wir kommunizieren, bereits so angelegt sind, dass sie die Kommunikation in bestimmte, für den Besitzer der Kommunikationsmittel nützliche Bahnen lenkt. Hier geht es also nicht mehr um Zensur, sondern um die Formatierung unserer Ausdrucksformen durch kommerzielle Interessen. Das klassische Beispiel ist der fehlende Dislike-Button. Facebook erlaubt nur positive Gefühle und vermeidet soziale Konflikte. Wir können mit der Antifa sympathisieren, aber wir können nicht die Nazis ablehnen.

3. Am schwierigsten zu bekämpfen sind Formen der Einhegung, die im Hintergrund passieren. Ein Beispiel von vielen hier etwa ist Googles neue Politik des sogenannten Downrankings. Seiten, die mit vielen Urheberrechtsbeschwerden belegt werden, werden im Ranking zurückgestuft und erscheinen dann nicht mehr auf Seite 1, sondern vielleicht auf Seite 15 der Suchergebnisse. So verändert sich das Bild der Welt, das uns diese Medien vermitteln, von dem, was ist, zu dem, wie es mächtige Interessen gerne hätten.

Dies sind einige der klassischen Themen der Netzpolitik. Wenn wir Netzpolitik aber nicht nur als reine Themenpolitik sehen, sondern als Schaffung der kommunikativen Grundlagen, um neue Formen gesellschaftlicher Solidarität zu ermöglichen, dann dürfen wir uns sich nicht darauf beschränken. Sondern wir müssen uns überlegen, wie wir die neuen Potentiale, welche die digitale Kultur als praktische Utopie bereits in Ansätzen realisiert hat, auch in anderen Felder fruchtbar machen können. Und wir müssen uns überlegen, welche Anpassungen in anderen Politikbereichen notwendig sind, um solche Prozesse auch in anderen Bereichen zu fördern.

Über den Bildschirmrand der Netzpolitik hinaus

Hier nun einige Beispiele, wie die Netzpolitik über sich selbst hinaus weisen kann. Warum etwa ist es sinnvoll, die Nutzung freier Software voran zu treiben? Nebst den bekannten Gründen wie Sicherheit, Transparenz, Kostenersparnis und größerer Autonomie gegenüber Software- und Dienstleistungsanbietern ist auch ein wesentlicher Grund, dass dadurch ökonomische Akteure gestärkt werden, die ein vitales, positives Interesse an gemeinschaftlichen Ressourcen – in diesem Fall freiem Software Code – haben. In diesem Sinne, kann das als ein mögliches Steuerungselement gesehen werden, um einen wirtschaftlichen Umbau zu fördern, der weg von Wissensmonopolen und hin zu offenen Wissensressourcen führt. Als ein Weg, der dezentrale, lokale Lösungen fördert, und nicht auf zentralisierte, globale Lösungen angewiesen ist, ohne deshalb vom Strom globaler Innovation abgekoppelt zu sein.

Damit stärkt man langfristig die politische Basis gegen neue Privatisierungsversuche und für Regulierungen, die die Commons unterstützen. Dass in Europa die Softwarepatente nicht durchgesetzt werden konnten, liegt wesentlich an der Klein- und mittelständisches Struktur der Europäischen Softwarebranche. Der Einsatz freier Software fördert genau diese Strukturen, diese wiederum können Teil einer politischen Basis werden, die vorhanden sein muss, will man wirklich das geistige Eigentum reformieren.

Oder die Kulturpolitik. Sie folgt nach wie vor einem klassischen bürgerlichen Kulturverständnis. Da werden kulturelle Werke gefördert, die dann über den Markt oder öffentlich finanzierte Kanäle vertrieben und irgendwann mal als Erbe konserviert werden. Die Rolle der Mehrheit ist die des Publikums, das mehr oder weniger stumm Kultur rezipieren darf. Was würde es hier bedeuten, das Publikum als Teil einer vernetzten Gemeinschaft zu aktivieren? Welche Bedingungen müssten da geschaffen werden, dass Menschen sich kulturelle Werke nicht nicht anschauen, sondern aneignen können, um dadurch selbst Teil einer kulturell aktiven Öffentlichkeit zu werden? Was müsste sich ändern, damit Archive und Museen nicht mehr Aufbewahrungsorte, sondern Produktionsmittel für alle werden? Das ist nicht nur eine Frage des geistigen Eigentums. Es ließe sich, zumindest für zukünftige Werke, auch über die Veränderung der öffentlichen Förderung und ihrer Lenkungsfunktion angehen. Was hindert uns daran, die Zusage öffentlicher Mittel an die Verpflichtung zu

verknüpfen, dass Werke nach der meist sehr kurzen Zeit der kommerziellen Auswertung wieder als Ressource Anderen zu Verfügung gestellt werden müssen? Nicht das Urheberrecht.

Oder was würde das bedeuten, Wirtschaftsförderung – nicht Sozialförderung, Wirtschaftsförderung – verstärkt auch non-profits, wenn sie sich um gemeinschaftliche produktive Ressourcen kümmern, zugänglich zu machen? Oder wie müsste Landwirtschaftspolitik aussehen, wenn eines ihrer Ziele wäre, die Almenden im ganz traditionellen Sinne wieder zum Blühen zu bringen? Das führt natürlich weg von der Netzpolitik. Aber auch vielleicht gar nicht so weit, denn alle diese noch zu erschaffenden Commons werden zu einem wesentlichen Teil auf Basis digitaler Kommunikationsflüsse organisiert werden.

Das Internet ist ein wichtiges Labor gesellschaftlicher Innovation, und einer der erstaunlichsten Entdeckungen, die in diesem Labor gemacht wurden, ist die gesellschaftliche Bedeutung des Teilens. Teilen als Modus des Austausches hat sich gegen alle Erwartungen, bereits in vielen Bereichen als äußerst produktiv und stabil erwiesen: Gegen alle Widerstände und gegen einen ungeheuer mächtigen Zeitgeist, der so etwas gar nicht mehr denken kann.

Und Teilen beschreibt nichts anderes als eine gelebte Praxis der Solidarität.

Natürlich wirft diese Praxis, die Institution der Commons, auch neue Probleme auf. Nicht alle Gemeinschaften sind progressiv und auch in Gemeinschaften, denen man mit großer Sympathie begegnet, lassen sich ohne weiteres deutliche Schattenseiten ausmachen. Die Wikipedia liefert hier ein reiches Anschauungsmaterial.

Und: nicht alle Bereiche des Lebens können oder sollen als Commons organisiert werden. Öffentliche Infrastrukturen und öffentliche Einrichtungen bleiben wichtig. Wenn man die neuen Commons und die öffentliche Hand als Gegensatz zueinander positioniert, ist man schnell bei neoliberaler Politik im zeitgeistigen Mäntelchen. Wir erleben das aktuell in Großbritannien, wo der Slogan der „Big Society" als Euphemismus für Sozialabbau und den Rückzug des Staates dient.

Es ist eine große politische Aufgabe, zu bestimmen, auf welchen Feldern neue Formen des Gemeinschaftlichen institutionalisiert werden können. Eins scheint aber sicher: der Bereich jenseits von Markt und Staat wird wachsen.

Es ist also die große Aufgabe der Netzpolitik dafür zu sorgen, dass das Internet als Labor der sozialen Innovation offen bleibt und die Potentiale des Netzes zu fördern, solidarisches Handeln hervorzubringen. Es ist Aufgabe einer progressiven Politik, diese Erfahrung ernst zu nehmen, und Wege zu finden, sie auf anderen Feldern des Lebens fruchtbar zu machen.

Dieser Beitrag ist die verschriftlichte Form der Keynote-Rede auf der netzpolitischen Konferenz der Fraktion DIE LINKE im Bundestag und der Rosa-Luxemburg-Stiftung am 15. September 2012 in Berlin.

Netzpolitik in Österreich

Thomas Lohninger

2012 war ein sehr bewegtes Jahr für die österreichische Netzpolitik. Eine vormals recht geschlossene und oft auch nach innen gerichtete Szene hat es geschafft an vielen Stellen in den Mainstream überzuschwappen und mit ihren Themen in Politik, Medien und am wichtigsten: der Zivilgesellschaft anzukommen. Dieser Jahresrückblick versucht einen kurzen Abriss in einigermaßen chronologischer Reihenfolge zu liefern. So wie alle Jahresrückblicke ist auch dieser subjektiv und selektiv.

Um einen Jahresrückblick über die Netzpolitik in Österreich für 2012 zu erzählen muss man im September 2011 beginnen, als vier Aktivisten des österreichischen Arbeitskreis Vorratsdatenspeicherung im Büro von Sender.fm in der Neubaugasse die *Bürgerinitiative gegen die Vorratsdatenspeicherung* und für eine Evaluation sämtlicher Terrorgesetze in Österreich online geschaltet haben. Damals war die Vorratsdatenspeicherung schon seit April 2011 beschlossene Sache und lange kein Thema mehr in den Medien oder der öffentlichen Wahrnehmung. Die vier Aktivisten hatten keinen einzigen Cent Werbebudget, gerade einmal einen Verteiler von wenigen hundert Interessierten und ein paar Pressekontakte. Nach einer Woche hatten sie 500 Unterschriften gesammelt, nach drei Monaten 3.000 und in den ersten 24h, als die Bürgerinitiative am 21. Dezember auf der Parlamentshomepage online unterschrieben werden konnte, schon weit über 10.000. So startete die kleine österreichische Netzpolitikszene ins Jahr 2012.

Als erstes großes Ereignis dieses Jahres gilt wohl die *Hausdurchsuchung* bei dem IT-Experten Michael R., der für den „Chef" von Anonymous Österreich (auch bekannt als „the_Dude") gehalten wurde. Im Jahr davor hat der österreichische Ableger von Anonymous mit einem Leak persönlicher Datensätze von Polizisten, GIS Zahlern und Krankenversicherten von sich hören gemacht. Michael R. wurde inzwischen vom österreichischen Staat bestätigt , dass er nicht der Chef von Anonymous Österreich ist und versucht nun aufzuklären mit welchen hahnebüchenen Ermittlungs- und Überwachungsmethoden er ins Fadenkreuz der Ermittler gekommen ist.

Ein weiteres nennenswertes Ereignis im Januar war die Gründung der Lobby-Plattform *„Kunst hat Recht"*. Unter dem Dach der Verwertungsgesellschaften und mit dem professionellen Auftritt einer PR-Firma „spezialisiert auf sensible und erklärungsbedürftige Themen" wird seitdem versucht, mit dem Mandat der Künstler im Urheberrechtsdiskurs mitzumischen. Positiv zu bemerken ist, dass es seitdem überhaupt einen Urheberrechtsdiskurs über der Wahrnehmungsschwelle von Liebhabern in Österreich gibt. Negativ ist die starke Frontenbildung, welche Kunst hat Recht durch die Abgrenzung von „den Künstlern" und der „Gratiskultur" im Internet zieht.

Der einzig wirklich kalte Monat in Österreich war der Februar 2012. Genau zu dieser Zeit schwappte die *ACTA-Protestwelle* nach Österreich und es kam zu insgesamt drei Demonstrationen ungeahnter Größe und Kreativität. So wie in fast allen europäischen Hauptstädten sah man sehr junge, alte, maskierte, kreative, lustige und wütende Menschen auf der Straße. Auch Österreichs Politik musste ihre Position von einer anfänglichen Pro-ACTA Haltung revidieren und entschloss sich am Ende dazu, das Abkommen abzulehnen. Zum ersten Mal gab es in Österreich bei einem netzpolitischen Thema ein Umschwenken der Politik aufgrund von Protesten aus der Zivilgesellschaft. Die Selbstverteidigungskräfte des Internets haben funktioniert!

Mit dieser positiven Grundstimmung im Rücken startete der AK Vorrat sein zweites großes Projekt. Die Bürgerinitiative gegen die Vorratsdatenspeicherung lief noch und hatte damals gerade die 80.000 Unterschriften-Marke überschritten. Trotzdem drohte die Einführung der vor einem Jahr beschlossenen Vorratsdatenspeicherung am 1. April (nein, das ist kein Scherz). Mit dem Inkrafttreten des Gesetzes eröffnete sich auch der Gang vor den *Verfassungsgerichtshof*. Ähnlich wie bei der Bürgerinitiative wollte der AK Vorrat sich aber nicht alleine hinstellen und kritisieren, sondern auch den Menschen eine Möglichkeit geben, selbst etwas gegen die Vorratsdatenspeicherung zu tun. Deshalb konnte man auf verfassungsklage.at eine Vollmacht ausfüllen, dann ausdrucken, unterschreiben, per Post an den AK Vorrat schicken und damit selbst Mitkläger vorm Verfassungsgerichtshof werden. So kamen insgesamt 11.139 Klägerinnen und Kläger zusammen, die die Vorratsdatenspeicherung für verfassungswidrig halten. Das Verfahren läuft bis heute, eine Entscheidung darüber ob der Verfassungsgerichtshof sich mit der Klage befassen wird erwartet der AK-Vorrat noch 2012.

Anlässlich der Einführung der Vorratsdatenspeicherung wurde jedoch nicht nur die Klage vorgestellt, es kam auch wieder zu Protesten. 1.000 Aktivisten zogen auf der größten Einkaufsstraße Wiens in einem *Trauermarsch* zwei lebensechte Särgen hinterher um die Privatsphäre in Österreich zu Grabe zu tragen.

Vor der Sommerpause gab es im Juni noch die letzte ACTA Demonstration, welche jedoch schon unter dem Vorzeichen des Scheitern des Handelsabkommens stand. Innerhalb der Sommerpause aber starteten die Aktivisten der Initiative für Netzfreiheit gemeinsam mit dem Verein für Internet Benutzer Österreich eine *Kampagne zur Netzneutralität* in Österreich auf unsernetz.at. Das Ziel war klar: Bewusstsein für das Thema Netzneutralität schaffen und für eine gesetzliche Verankerung eintreten. Damit veränderte sich in der österreichischen Netzpolitikszene auch etwas: anstatt wie bisher immer nur gegen ein Anliegen zu sein, das andere auf die Agenda gehoben hatten, wird hier zum ersten Mal ein Thema selbst gewählt, bei dem noch dazu die Netzpolitik Szene mit einem eigenen Gestaltungsanspruch herangeht.

Der Herbst begann mit der ersten *Netzpolitik Konferenz* in Österreich, der „Daten, Netz und Politik". Dort wurde zwei Tage lang über Themen wie Urheberrecht, Smart-Meter, EU-Datenschutzreform, Vorratsdatenspeicherung oder Netzneutralität gesprochen. Die Konferenz war der Versuch die verstreute Szene aus ganz Österreich unter dem passenden Motto *„das Jahr des Aufbruchs"* an einen Ort zu bringen. Durch das erste physische Treffen der österreichweiten Szene wurde ein Anfang gemacht und Veranstalter unwatched.org hat auch schon angekündigt die Konferenz 2013 wieder auszurichten.

Im Herbst erwachten auch die österreichischen *Piraten* aus ihrem jahrelangen Fiebertraum und wählten einen neuen Vorstand. Abstimmungen mittels Liquid Feedback können nun direkt in das Parteiprogramm, die Statuten und die Geschäftsordnung einfließen. Im November wurde der erste (nicht später aus der Partei ausgeschlossene) Mandatar der Piraten gewählt, nämlich Philip Pacanda in Graz.

Am 8. Oktober wurde die *Elektronische Gesundheitsakte* (kurz: ELGA) im Parlament beschlossen. Die Umstellung war lange diskutiert worden und ist bei weitem nicht unumstritten. Die heftigsten Kritiker kamen zuletzt aus der Ärztekammer, da keine der österreichischen Datenschutz- oder Netzpoliti-

korganisationen dieses Thema gebührend behandelte. In der Abstimmung im Plenum des Nationalrats weigerten sich immerhin zwei Abgeordnete gegen den sonst vorherrschenden Klubzwang und stimmten entgegen ihren Fraktionen jeweils gegen (Karin Hackl, ÖVP) oder für (Kurt Grünewald, Grüne) die Einführung von ELGA.

Nach diesem Debakel für den Datenschutz kamen die *Big Brother Awards* wie gerufen. Am 14. Oktober rief die alt-ehrwürdige quintessenz zur jährlichen Gala in den Rabenhof um die größten Datenschutzsünder öffentlich an den Pranger zu stellen. Die Choreographie der Veranstaltung versuchte wie schon in den letzten Jahren einen Spagat zwischen moralisch entrüstet, bemüht komisch und selbstironisch zu schaffen. Stargast des Abends war der US-amerikanische Netzaktivist Jacob Appelbaum, der für seine Leistungen für das TOR Projekt mit dem Preis „Defensor Libertatis" ausgezeichnet wurde.

In den darauf folgenden Monaten zeichnete sich immer mehr das aktuell bestimmende Thema der österreichischen Netzpolitik ab: die für das Frühjahr 2013 bevorstehende *Urheberrechtsnovelle* und was sie mit sich bringt. Die größten Neuerungen sind nach derzeitigem Wissensstand eine Ausweitung der Festplattenabgabe, also einer Leermedienvergütung auf alle Arten von Speichermedien, jedoch ohne damit einhergehende Stärkung der privaten Nutzung urheberrechtlich geschützter Werke, und ein neuer Auskunftsanspruch bei angeblichen Urheberrechtsdelikten. Die gute Situation aktuelle in Österreich ist ja, dass Abmahnanwälte keine reguläre Möglichkeit besitzen, auf die Person hinter einer IP-Adresse zu kommen – genau das soll sich aber ändern. Es wird sogar diskutiert, der Abmahnindustrie Zugriff auf Vorratsdaten zu geben, eine alte Forderung des ÖVP-dominierten Justizministeriums. Am 17. Oktober wurde deshalb wieder demonstriert, nämlich von Kunst hat Recht und Konsorten *für* die Einführung einer Festplattenabgabe, und am selben Tag von der Initiative für Netzfreiheit *gegen* die Festplattenabgabe und für eine Reform des Urheberrechts. Um dem Diskurs etwas mehr Struktur zu geben, veranstaltet der Verein für Internet Benutzer Österreich (Vibe!AT) seit November eine Reihe von Diskussionsveranstaltungen zum Urheberrecht im 21. Jahrhundert, kurz Ur21.

Am 23. November veröffentlichte die Initiative für Netzfreiheit einen *Bericht zur tatsächlichen Sicherheit der Vorratsdaten* in Österreich. In dem Bericht wird aufgezeigt, dass es nicht nur fast keine Vorgaben zur Speicherung der Vorratsdaten bei den Providern gibt, sondern auch, dass die Organisation, die ei-

gentlich die Sicherheit überprüfen sollte – die Datenschutzkommission – auch sieben Monate nach der Einführung der Vorratsdatenspeicherung noch nicht einen einzigen Provider kontrolliert hat. Des Weiteren kritisiert die Initiative für Netzfreiheit die mangelnden Kompetenzen und Ressourcen der Datenschutzkommission, die sie neben den fehlenden Strafen bei Verstößen bei der Datensicherheit komplett ungeeignet für die Aufgabe macht, die Sicherheit der Vorratsdaten zu kontrollieren. Der Bericht schlug medial große Wellen und wurde im Vorfeld des *Hearings im Justizausschuss* veröffentlicht, in dem die Bürgerinitiative des AK Vorrat behandelt wurde. Die Aktivisten des AK Vorrat sammelten insgesamt 106.067 Unterschriften, bis sie zum ersten Mal im Petitionsausschuss behandelt wurden. Behandelt bedeutet hier, dass in den ersten zwei Sitzungen keine fünf Minuten über das Anliegen der Bürgerinitiative diskutiert wurde, man dem Anliegen dann aber endgültig am 28. November in Form eines großen Experten-Hearings Beachtung schenken wollte.

Im Vorfeld haben die Aktivisten dazu aufgerufen, die Abgeordneten im Ausschuss anzuschreiben und auf eine Behandlung des Anliegens der Bürgerinitiative zu drängen. Als das Hearing dann am 28. November abgehalten wurde, war die Hoffnung groß, aber leider vergebens. Die Politiker im Justizausschuss haben sich zwar von zwölf Experten genau erklären lassen, was alles falsch und verfassungswidrig an der Vorratsdatenspeicherung ist, am Ende wurde die größte Bürgerinitiative der jüngeren Geschichte der zweiten Republik aber einfach nur zur Kenntnis genommen und damit schubladisiert. Die Enttäuschung und Wut im Lager des AK Vorrat war groß.

Das Scheitern der Bürgerinitiative in ihrem Anliegen ändert aber nichts am neu gewonnenen Mut und Selbstverständnis der österreichischen Netzpolitik. Auch wenn die Politik noch nicht soweit ist diese Themen ernst zu nehmen, die Bevölkerung hat ihr Interesse bewiesen!

EU-Strategie zur Cybersicherheitspolitik im internationalen Umfeld

Annegret Bendiek und Ben Wagner

Im Dezember 2012 wollen Vertreter aus 193 Ländern die 1988 unterzeichneten International Telecommunications Regulations (ITR) neu verhandeln und über die Zukunft des Internets entscheiden. Die sich derzeit in Ausarbeitung befindende EU- Strategie zur Cybersicherheitspolitik wird für die Positionierung der EU als größter Binnenmarkt in der globalen Cybersicherheitspolitik elementar sein. Das Ziel der EU-Strategie sollte die Demokratisierung des Internets EU-intern sowie in der internationalen Ordnungspolitik sein. In enger transatlantischer Absprache wäre eine Verrechtlichung von Netzsicherheit anzustreben, die die Wirtschaft und Parlamente stärker in die Pflicht nehmen sollte.

Die globale Cyberpolitik befindet sich in einer entscheidenden Phase. Im Dezember 2012 werden in Dubai Vertreter von über 190 Staaten über die normativen Grundlagen des zukünftigen Internet beraten. Wie viel Freiheit soll das Internet gewährleisten, welche Sicherheitsvorkehrungen muss es gegen Kriminalität und Terrorismus geben und wo sollen die Grenzen zwischen nationaler Selbstbestimmung und globalem Raum verlaufen? Wird es zukünftig überhaupt noch ein globales Internet geben oder verstärkt sich der bereits zu beobachtende Trend einer Fragmentierung des Netzes und zunehmender nationaler Kontrolle über Zugang und Inhalte?

Die EU ist für diesen Diskurs von nicht zu unterschätzender Bedeutung. Sie koordiniert die nationalen Politiken ihrer 27 Mitgliedstaaten und verwaltet den größten Binnenmarkt der Welt. Entscheidungen, die hier getroffen werden, haben automatisch eine hohe Relevanz für den Rest der Welt. Sowohl Brüssel als auch die Mitgliedstaaten sind sich dieser Bedeutung durchaus bewusst. Aktuell gibt es in der EU eine Vielzahl von Abstimmungsprozessen, in denen die zukünftige Politik Europas und seine Positionierung im globalen Diskurs festgelegt werden.

In dieser Debatte stoßen grundlegend unterschiedliche Verständnisse des angemessenen Verhältnisses von Staat und Gesellschaft, von Sicherheit und Freiheit und von intergouvernemental versus parlamentarisch geprägter Politik aufeinander. Wie sie miteinander in Beziehungen gesetzt werden und welche langfristigen Entscheidungen hier getroffen werden, wird die neue öffentliche Ordnung des Cyberspace in den nächsten Jahren entscheidend prägen.

Freiheitsrechte und Sicherheit

In der europäischen Debatte zur Zukunft des Internet lassen sich zwei grundsätzlich konkurrierende Vorstellungen über die Rolle der EU und die anzuwendenden Instrumente zur Regulierung des Internet unterscheiden.

Die vorherrschende Sichtweise der Politik auf das Internet ist die eines umfassenden Sicherheitsproblems. Den Verteidigungspolitischen Leitlinien der Bundesregierung vom Mai 2011 zufolge steht die Cybersicherheit bereits an zweiter Stelle von Bedrohungen der Sicherheit. Bis Juni 2012 haben 10 EU-Staaten nationale Cybersicherheitsstrategien verabschiedet. In mehr als 30 Ländern weltweit bestehen heute Cybereinheiten im Rahmen der Streitkräfte. Cyberangriffe sind faktisch zum strategischen Kalkül einer neuen computergestützten Auseinandersetzung sowohl zwischen nichtstaatlichen und staatlichen Akteuren sowie zwischen Staaten geworden.

Eindrückliche Beispiele für dieses Verständnis sind die seit 2010 zwischen den EU-Staaten und den USA regelmäßig stattfindenden Übungen zur Abwehr von Cyberangriffen. Dieser Trend setzt sich auch in der im November 2010 gegründeten EU-USA-Arbeitsgruppe zur Cybersicherheit fort.

Auch der befürchtete Schaden für die Wirtschaft ist nicht minder gering. Der Schutz vor Wirtschaftsspionage ist ein wichtiger Standortfaktor. Der elektronische Handel macht EU-weit vier Prozent des Gesamthandels aus, mit stark steigender Tendenz. Eine Untersuchung von 13 hochentwickelten Staaten schätzt, dass das Internet zwischen 2004 und 2009 zu 11 Prozent des GDP-Wachstums beigetragen hat. Schätzungen zufolge könnten die Verbraucher insgesamt über 200 Milliarden Euro sparen, würde der elektronische Handel stärker genutzt. Dies setzt aber hohes Vertrauen in die Netzsicherheit voraus.

Laut der aktuellen Eurobarometer-Umfrage vom Juli 2012 sind Internetbenutzer sehr besorgt über die Cyber-Sicherheit und Datenschutz. Das Grundproblem jeder Regulierung ist, dass die Geschwindigkeit und Nichtvorhersehbarkeit von Angriffen, die Herkunft des Gegners und dessen Motive kaum zu bestimmen sind (Attribution-Problematik). Eine eindeutige Identifizierungsmöglichkeit für Nutzer ist deswegen eine zentrale Forderung. In diesem Sinne drängen Exekutiven mit Verweis auf Geheimhaltung und Sensibilität auf einen möglichst großen Handlungs- und Verhandlungsspielraum. Forderungen nach parlamentarischer Kontrolle und rechtlich verbindlichen Regulierungen spiegeln sich derzeit weder auf der internationalen, europäischen noch auf der nationalen Ebene wider.

Sicherheitsprobleme stellen zweifellos eine wichtige Herausforderung für die Regulierung des Internet dar. Eine übermäßige Betonung des Sicherheitsaspektes und eine Vernachlässigung der Idee des Cyberspace als eines globalen öffentlichen Gutes drohen allerdings leicht selbst zu einer Gefahr für die Grundrechte und damit die Demokratie zu werden. Sicherheit sollte nicht als ein Gegenstand der Politik verstanden werden, der oberhalb der Demokratie steht.

Wie und im Rahmen welcher Maßnahmen so genannte „kritische Infrastrukturen" (Energie, Verkehr, Gesundheit) geschützt werden und wie bei diesem Schutz mit den privaten Informationen umgegangen wird (Stichwort: Datenvorratsspeicherung) darf nicht nur in abgeschotteten Expertengremien beraten und entschieden werden, sondern gehört letztlich ins Parlament. Private Selbstregulierung ist gut und wichtig. Wenn allerdings Fragen der informationellen Selbstbestimmung, der Freiheit und der demokratischen Grundrechte tangiert werden, dann kann eine demokratieverträgliche Lösung nur eine demokratisch rechtsstaatliche und damit parlamentarisch geprägte Lösung sein.

Neuere EU-Initiativen

Das Thema der Sicherheit und Freiheit im Internet ist erst seit dem Arabischen Frühling in der breiteren außenpolitischen Debatte der EU angelangt. Die Rolle von Facebook hat den Blick dafür geschärft, dass es bei der Debatte um die zukünftige Verfassung des Internet auch um die Förderung von Demokratie und die Überwindung autoritärer Strukturen geht. Im November 2011 organisierte die britische Regierung eine erste größere Konferenz zur

Normenentwicklung im Cyberraum. In Vorbereitung auf die Konferenz haben die drei Kommissarinnen Nele Kroes (DG CNECT), Cecilia Malmström (DG HOME) und Catherine Ashton (HR/VP EAD) im Oktober 2011 ein „Food-for-Thought Paper" zu Verhaltensnormen im Cyberraum entwickelt. Die hier noch recht stark betonte Rolle von demokratischen Werten hat inzwischen in dem neuen Kommunikationsvorschlag der Kommission vom Mai 2012 einem pragmatischeren Ansatz Platz gemacht. In der Kommunikation werden die Schaffung eines sicheren digitalen Umfelds für Bürger, Unternehmen und Verwaltungen sowie die Verhinderung von Cyberkriminalität zum Ziel erklärt.

Der Vorschlag fügt sich nahtlos ein in die von Kommissarin Kroes betriebene „Digitale Agenda für Europa" von Mai 2010. Hiermit will die EU einen digitalen Binnenmarkt schaffen, der auf einem schnellen Internet und interoperablen Anwendungen und selbstregulierenden privaten Konzernen beruht. Es ist bezeichnend, dass die EU-Justizkommissarin Viviane Reding, deren zentrales Anliegen aktuell die Schaffung eines übergreifenden Datenschutzrechtes ist, nicht in diese Initiative eingebunden ist. Strengere Datenschutzvorgaben für soziale Netze und Institutionen soll es nach Reding künftig in ganz Europa geben. Zu den geplanten Neuerungen gehört das Recht auf Vergessen. Soziale Netzwerke müssten Daten in Zukunft auf Wunsch ihrer Nutzer wieder löschen. Verstoßen Unternehmen gegen die Datenschutzregeln, so würden ihnen nach den neuen Datenschutzregeln hohe Strafen drohen. Frankreich, Irland, Luxemburg und Litauen sind dafür, dass der Staat nach den gleichen Datenschutzregeln arbeiten muss wie die Privatwirtschaft.

Das von Ashton angekündigte Mainstreaming von Menschenrechten in der Europäischen Außenpolitik, das in EAD-Dokumenten an prominenter Stelle steht, findet in dem Kommunikationsvorschlag nur noch nachgelagerte Bedeutung. Einwände der in der Cyberpolitik führenden fünf Mitgliedstaaten (G5, Deutschland, Frankreich, Großbritannien, Niederlande und Schweden) blieben ebenfalls bisher unberücksichtigt. Die G5 haben sich auf Druck von Schweden und Niederlande auf eine über den Bereich der Sicherheit hinaus angelegte Cyberstrategie geeinigt. Erklärtes Ziel ist es, eine ganzheitliche Strategie zu formulieren, die ökonomische und soziale Aspekte, Aspekte der Infrastruktur und e-commerce sowie die Entwicklungszusammenarbeit integriert. Richtungsweisend sind hier e-diplomacy Initiativen, die ihren Ursprung in den Vereinigten Staaten haben und bestrebt sind, „Cyber"-Themen

außenpolitisch zu besetzen, die eine breitere Betrachtung des Themenfelds zulässt. Mit dem Implementierungsbericht zur Europäischen Sicherheitsstrategie hatte auch der Europäische Rat die EU schon im Dezember 2008 ausdrücklich dazu aufgefordert, die Möglichkeiten für ein umfassendes Konzept der EU zu erarbeiten.

Die EU auf dem Pfad der Sicherheit

Auf den ersten Blick erscheint es als selbstverständlich, dass die Gefahrenabwehr und der Schutz staatlicher und wirtschaftlicher Interessen sowie der Infrastruktur und des Bürgers im Vordergrund der geplanten EU-Strategie stehen sollten. Und hierbei wären die Aspekte der Sicherheit gegen die Rechte des Einzelnen auf Freiheit und Selbstbestimmung abzuwiegen. Eine überzeugende Antwort auf diese Herausforderung bleiben die bisher vorgelegten Vorschläge allerdings schuldig. Der eingeschlagene EU-Pfad ist inhaltlich eindeutig zugunsten der Sicherheitsagenda wie institutionell zugunsten einer Stärkung der für Sicherheit relevanten EU-Institutionen ausgerichtet.

Das Anfang Dezember 2009 erklärte Ziel, das „Mehrjahresprogramm für einen Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger" umzusetzen, wird zunehmend zugunsten sicherheitspolitischer Maßnahmen interpretiert. Das sogenannte Stockholmer Programm des Europäischen Rates zielt auf „eine umfassende Unionsstrategie der inneren Sicherheit" ab, bei der datenschutzrechtliche Fragen nur noch untergeordnete Bedeutung haben. Die Kommission reagierte auf das Stockholmer Programm nicht mit einem umfassenden Aktionsplan zur Ausdehnung von Bürgerfreiheiten und -rechten, sondern mit einer Mitteilung, in der sie schwere und organisierte Kriminalität, Cyberkriminalität, Terrorismus, Grenzsicherung und Katastrophenabwehr als akuteste gemeinsame Probleme benannte.

Die Cybersicherheitspolitik müsse zwar ebenfalls „auf gemeinsamen Werten aufbauen (…), u. a. auf dem Grundsatz der Rechtsstaatlichkeit und der Achtung der Grundrechte", doch wird diesem Punkt inhaltlich kaum Rechnung getragen. Das Unionskonzept geht ausführlich auf die sicherheitspolitischen Herausforderungen, Zielsetzungen und auf notwendige Maßnahmen ein, vernachlässigt aber die parallele Entwicklung eines umfassenden Rahmens für den Schutz der informationellen Grundrechte von Bürgern gegenüber expansiven staatlichen Maßnahmen. Auch im angehängten Katalog der vorgesehenen Maßnahmen findet sich nichts zu diesem Thema.

Im September 2010 legte die EU-Kommission einen Vorschlag für eine Richtlinie zur Bekämpfung neuer Formen von Cyberkriminalität wie Cyber-Großangriffen vor. Konkret wird vorgeschlagen, die Herstellung und den Verkauf von Schadprogrammen unter Strafe zu stellen und die polizeiliche Zusammenarbeit in Europa zu verbessern. Einige EU-Länder sind, was die Strafverfolgung und die Prävention derartiger Delikte anbelangt, fortgeschrittener als andere, ein ausgewogenes Schutzniveau auf europäischer Ebene ist aber erst im Begriff zu entstehen. Darüber hinaus wollen sich EU-Regierungen und -Regionen in einem Computer Emergency Response Team (CERT) über sicherheitsrelevante Vorfälle austauschen und Bedrohungen diskutieren können. Neue CERTs sollen die Informationslücken zwischen dem privaten und öffentlichen Sektor schließen und den eigenen EU-CERT, als auf die EU-Ebene spezialisierte Gruppe von IT-Sicherheitsfachleuten, ergänzen.

Ab 2013 soll das „EU-Zentrum zur Bekämpfung der Cyberkriminalität" seine Arbeit aufnehmen und gegen Online-Betrügereien krimineller Vereinigungen sowie den Diebstahl von Kreditkarteninformationen durch Mafia-Gruppen vorzugehen. Groß angelegte Cyberangriffe gegen zentrale Infrastrukturen in EU-Ländern sollen zukünftig untersucht und kriminelle Netze ausgeschaltet werden. Auch die institutionelle Dynamik der EU ist einseitig auf die Sicherheitsagenda ausgerichtet. In der EU befassen sich ENISA, Europol, das European Police College (CEPOL), die European Maritime Safety Agency (EMSA) und der Europäische Auswärtige Dienst (EAD) mit Fragen der Cybersicherheit und -kriminalität. Die bereits 2007 gegründete europäische Grundrechteagentur, der europäische Datenschutzbeauftragte sowie der Sonderbeauftragte für Menschenrechte der EU sind hingegen an keiner Stelle in die Cybersicherheitspolitik der EU eingebunden.

Die EU-Strategie zur Cybersicherheitspolitik

Strategie wird im allgemeinen Sprachgebrauch als planvolles Streben nach einem bestimmten längerfristigen Ziel oder als planvolle Verwirklichung eines bestimmten längerfristigen Interesses verstanden. Mit jeder Zielsetzung ist auch ein Interesse verbunden, dem durch die Verwirklichung der strategischen Politik gedient werden soll. Das selbstgesteckte Ziel der EU, eine demokratische Rechtsgemeinschaft zu schaffen, hätte damit bei der Entwicklung einer europäischen Cybersicherheitspolitik oberste Priorität. Eine zukünftige

EU-Strategie sollte zudem nicht nur nach Innen wirken, sondern ebenfalls als Scharnier zwischen den Mitgliedstaaten und der internationalen Ebene fungieren.

Das Internet demokratisieren: EU-interne Reformen

Die EU plant im Rahmen ihrer neuen Cybersicherheitsstrategie eine ganze Reihe von nach Innen wirkenden Maßnahmen. Hierzu gehören die Verbesserung ihrer Verteidigungsfähigkeit, die Schaffung eines gemeinsamen Marktes für Sicherheitstechnologien, die Bekämpfung von Cyberkriminalität, die Förderung zwischenstaatlicher Kooperation zwischen Staaten sowie weitere Maßnahmen zur Aufklärung und Forschung. In allen diesen Bereichen sind demokratiepraktische Defizite zu beobachten.

Grenzen der Selbstregulierung

Die Digitale Agenda zielt auf eine Ordnungsstruktur ab, die von einem Zusammenspiel zwischen staatlichen und nicht-staatlichen Akteuren (Unternehmen, Zivilgesellschaft, Wissenschaft und technische Community) gekennzeichnet ist. Dieses Zusammenspiel stellt einen auf den ersten Blick auch durchaus unstrittigen Ansatzpunkt dar. Ein Informationsaustausch zwischen Sicherheitsbehörden, staatlichen Institutionen und Unternehmen ist beispielsweise schon deswegen unerlässlich, weil wesentliche Expertise ausschließlich in privater Hand liegt.

Hinzu kommt, dass ein Großteil dessen, was allgemein unter dem Begriff „kritische Infrastrukturen“ (Energie, Sicherheit, Verkehr) verstanden wird, sich im Besitz privater Anbieter befindet. Gleichzeitig allerdings sind auch die zum Teil recht gegensätzlichen Interessenlagen nicht zu übersehen. Viele Unternehmen stehen beispielsweise einer umfassenden Meldepflicht für Angriffe, der aus Gründen des Schutzes von kritischen Infrastrukturen nötigen Offenlegung von Sicherheitsstandards und verbindlichen staatlichen Regelungen mit großer Skepsis gegenüber. Wenn der Einfluss Privater auf den Regelsetzungsprozess zu groß wird, dann steht zu befürchten, dass legitime öffentliche Anliegen nur ungenügend berücksichtigt werden. Freiwillige Verhaltenskodizes stellen keine Garantie dar, dass das öffentliche Interesse ausreichend gewahrt wird.

Bessere Standards für Sicherheitstechnologien

Die EU zielt darauf ab, in den nächsten Jahren die Kooperation zwischen den Mitgliedstaaten im Bereich der Sicherheitstechnologien zu intensivieren. Hierzu soll unter anderem eine von der Wirtschaft getragene Institution, die Hardware-Hersteller zertifiziert, gegründet werden. Eine Zertifizierung von Sicherheitstechnologie soll helfen zu vermeiden, dass beispielsweise einzelne Unternehmen ihre Marktposition dazu ausnutzen, illegal Daten zu sammeln. Der chinesische Anbieter für Breitbandtechnologie „Huawei Technologies" wurde beispielsweise von allen Bundesausschreibungen ausgeschlossen, weil er seine Produkte mit einer Technologie ausgestattet hatte, die genau dieses erlaubt hätte. Auch die Exporteure von Informations- und Kommunikationstechnologie müssen stärker politisch und juristisch in die Pflicht genommen werden. Autoritäre Staaten setzen zunehmend auf die technischen Restriktionen des Internets, die von europäischen und nordamerikanischen Unternehmen wie Area in Italien, Ultimaco in Deutschland oder Blue Coat Systems in den USA hergestellt werden.

Der Einsatz von solchen Technologien wurde in autoritären Staaten wie Syrien, Libyen, Bahrain, Tunesien, Iran oder Weißrussland dokumentiert, wobei davon auszugehen ist, dass solche Technologien in vielen weiteren autoritären Staaten eingesetzt werden. Diese Entwicklung ist weder im strategischen Interesse Europas, noch steht sie im Einklang mit den Zielen einer GASP, Gefahren für die internationale Sicherheit und die Nichtverbreitung zu verhindern. Eine europäische Harmonisierung der nationalen Rüstungsexportpolitiken und ihre Ausdehnung auf technische Systeme wären notwendig, die besonders geeignet sind, den Zugang zum Internet zu beschränken oder die massenhafte Überwachung von Internet-Nutzern zu ermöglichen. Daher wären das Europäische Parlament und die nationalen Parlamente künftig stärker in die Rüstungsexportentscheidungen einzubeziehen. In verschiedenen Ausschüssen des EPs, aber auch des Bundestages werden andere Sachverhalte auch unter Geheimhaltung behandelt. Die bisherige Kontrollpraxis des EU code of conduct und der Dual-use-Verfahren sind jedenfalls unzureichend.

Kriminalitätsbekämpfung und Individualrechtsschutz

Die Kommission verabschiedete im September 2010 einen Vorschlag für eine Richtlinie über Angriffe auf Informationssysteme. Mit dieser soll die Bekämpfung der Cyber-Kriminalität durch die Angleichung der einzelstaatlichen Strafvorschriften und die Verbesserung der Zusammenarbeit zwischen den Justizbehörden und sonstigen zuständigen Behörden verstärkt werden. Im Internet und bei den verfügbaren Daten stößt die Polizei an ihre Grenzen. Das Internet hat keine lokale Begrenzung auf einen kriminalgeografischen Raum. Noch werden IP-Adressen nicht wie Autokennzeichen gespeichert. Vorstöße wie die geplante Richtlinie – Attacken auf Informationssysteme, European Cybercrime Centre, EU Initiative gegen Botnetze etc. – zielen auf eine Vorratsdatenspeicherung ab. Die Versuche der EU, eine allgemeine Richtlinie zur Datenvorratsspeicherung durchzusetzen stoßen in Deutschland allerdings auf heftigen Widerstand. Die vom Bundestag vorgesehenen Umsetzungsmaßnahmen wurden vom Bundesverfassungsgericht mit dem Argument zurück gewiesen, dass es sich hier um einen übermäßigen Eingriff in das Post- und Fernmeldegeheimnis handele. Um derartige Konflikte in Zukunft zu vermeiden, müssen sowohl europäische Rechtsakte als auch ihre innerstaatlichen Umsetzungsmaßnahmen – mehr als bisher – vor dem Hintergrund eines Bewusstseins über die Grenzen legitimer europäischer Interventionen und zu respektierender individueller Freiheitsrechte formuliert werden.

Parlamentarisierung und Transparenz in der Cyberpolitik

Die Cyberpolitik in der EU ist noch fest in der Hand der für die Innere Sicherheit zuständigen Institutionen. Mit der von der dänischen Ratspräsidentschaft vorgeschlagenen Einführung des EU-Verfahrens „Gruppe der Freunde der Präsidentschaft zu Cyber" wird das Forum der mit diesem Thema befassten Institutionen nur unwesentlich erweitert. Der Kommissionsentwurf zur EU-Strategie zielt auf eine Stärkung der offenen Methode der Koordinierung ab. Vorgesehen sind rechtlich unverbindliche intergouvernementale Verfahren, die auf Benchmarking, best-practices und freiwilliges Lernen setzen. Rechtlich verbindliche und an der Charta der Grundrechte orientierte Verfahren sind hingegen nicht vorgesehen. Notwendig ist hingegen eine Öffnung der europäischen Cybersicherheitspolitik für die Parlamente und die breitere interessierte Öffentlichkeit.

Angemessen wäre eine europaweite Debatte über das angemessene Verhältnis von Freiheit und Sicherheit. Ebenfalls sollten die EU und ihre Mitgliedstaaten der Open Government Partnership (OGP)-Initiative beitreten und damit für mehr Transparenz sorgen. Für die Initiative hatten sich im September 2011 auf Anregung der USA und Brasiliens 50 Staaten zusammengeschlossen. Sie wollen politische Offenheit, Transparenz und die Zusammenarbeit staatlicher Stellen mit der Zivilgesellschaft fördern. Konkret soll hiermit der Zugang zu amtlichen Dokumenten erleichtert werden. Eine generelle Veröffentlichungspflicht würde die demokratische Meinungs- und Willensbildung fördern, eine bessere Kontrolle staatlichen Handelns ermöglichen und damit einen Beitrag zur Korruptionsprävention leisten.

Außenwirkung der EU-Strategie

Maßnahmen der EU haben alleine schon wegen der Größe des europäischen Marktes einen hohen Einfluss auf die globale Regulierung des Internet. Die EU sollte sich daher auch im Hinblick auf die Frage nach den angemessenen globalen Regelungsinstrumenten frühzeitig positionieren. In der aktuellen Debatte stehen sich zwei grundlegende und gleichermaßen unbefriedigende Positionen gegenüber. Auf der einen Seite wurde von den Mitgliedern der Shanghai-Gruppe (China, Russland, Usbekistan und Tadschikistan) 2011 die Verabschiedung eines zwischenstaatlichen „Internationalen Verhaltenskodex für Informationssicherheit" vorgeschlagen. Dieser sollte globale Standards für „unannehmbares staatliches Verhalten" formulieren. Die von Aktivitäten im Internet bedrohte Souveränität von Staaten solle gestärkt und jede Einmischung in die inneren Angelegenheiten eines Staates verboten werden. Institutionell sollte zudem die International Telecommunication Union (ITU) gestärkt werden, die ITR überarbeitet und die derzeit bei dem US-Unternehmen Internet Corporation for Assigend Names und Numbers (ICANN) angesiedelte Vergabe von Internetdomains auf die ITU übertragen werden.

Den chinesisch-russischen Vorschlägen steht das von den USA und der EU präferierte sogenannte Multistakeholder-Modell gegenüber. Es läuft im Wesentlichen darauf hinaus, all jenen die Teilhabe an der Regulierung des Internet zu ermöglichen, die entweder über relevantes Expertenwissen (Unternehmen), politische Autorität (Staaten) oder über gesellschaftliche Legitimation (Zivilgesellschaft) verfügen. Es ist eine sehr viel pluralistischere Form der Regulierung, die sowohl einer starken Rolle der VN als auch verbindlichen zwi-

schenstaatlichen Verträge mit großer Skepsis gegenübersteht. Die im Mai 2011 von US-Präsident Obama verkündete International Strategy for Cyberspace setzt auf intensivierte transnationale Dialoge über Verhaltensnormen, vertrauensbildende Maßnahmen sowie die Einbindung nichtstaatlicher Akteure. Einen internationalen Vertrag hingegen lehnen die USA mit dem Argument ab, dass dieser zu starr, zu wenig verifizierbar und zu sehr auf staatliches Handeln ausgerichtet sei.

Aus einer demokratiepraktisch sensibilisierten Sicht kann keine der beiden Positionen überzeugen. Während der russisch-chinesische Vorschlag zu einseitig auf die Ausdehnung staatlicher Kontrollmacht abzielt, bringt das Multistakeholder-Modell fast ausschließlich die Interessen der technologisch überlegenen USA und finanzstarker Unternehmen zum Ausdruck. Keine der beiden Positionen sieht letztlich eine mehr als marginale Rolle für nationale Parlamente vor. Ein Kernelement der geplanten EU-Strategie sollte im Gegensatz zu den beiden Vorschlägen auf die vollständige Implementierung des Europarats-Übereinkommen und die Übertragung dieses Modells auf die internationale Ebene gerichtet sein.

Dieses sogenannte Budapest-Übereinkommen aus dem Jahr 2001 (seit 2004 in Kraft) enthält bereits gemeinsame Definitionen der verschiedenen Arten von Internetkriminalität und bildet eine konstruktive Grundlage für eine engere Zusammenarbeit zwischen den Mitgliedstaaten des Europarates sowie einigen außereuropäischen Staaten wie den USA, Japan und Kanada. Auch private Akteure sollen in die Formulierung neuer Regeln eingebunden werden. Die bestehende Architektur des Internets mit seinen offenen Standards und der dezentralen Verwaltung sollte beibehalten werden. Hinzu sollte hier noch ein Instrument zur Beförderung rechtlicher Verbindlichkeit treten. Werden Verstöße bekannt, könnten Sanktionen durch den VN-SR verhängt werden.

Zudem wäre das bestehende Multistakeholder-Modell so weiter zu entwickeln, dass die Expertise privater Unternehmen konstruktiv eingebunden werden und dass diese gleichzeitig auf eine Einhaltung globaler Standards in den Bereichen Sicherheit, informationelle Selbstbestimmung und Datenschutz festgelegt werden können. Es ginge somit darum, eine transnationale Sicherheits- und Rechtspartnerschaft zu etablieren, die sowohl Staaten als auch Unternehmen umfasst und die neben der Sicherheit den Werten der Demokratie und der Rechtsstaatlichkeit verpflichtet ist. Es wäre damit eine Stra-

tegie, die nicht Sicherheit gegen Freiheit oder Staat gegen Private auszuspielen sucht. Es wäre vielmehr eine Strategie der Vermeidung falscher Gegenüberstellungen und der Ausdehnung von Demokratie auf die neuen Realitäten des 21. Jahrhunderts. Um das Internet zu demokratisieren, wäre eine enge transatlantische Abstimmung im Vorfeld eine wesentliche Erfolgsbedingung für europäisches Handeln.

Enge transatlantische Abstimmung

Die EU-Strategie zur Cybersicherheitspolitik kann nur international Wirkung entfalten, wenn sie mit den USA abgestimmt ist. Die Nato hat in den letzten Jahren institutionelle Neuerungen im Bereich der Cybersicherheit geschaffen. Nach den Cyber-Angriffen auf Estland 2007 hat die Nato 2008 in Tallin ein Exzellenzzentrum zur Cyberverteidigung geschaffen (CCDCOE), dass seit 2009 eines der wichtigsten Konferenzen zu Konflikten und kriegerischen Auseinandersetzungen im Cyberraum veranstaltet, die sogenannte CyCon. Als Verteidigungsbündnis bleibt ihr Auftrag auf die militärischen Aspekte von Cybersicherheit begrenzt. Auch wurden in der OSZE, in der auch Russland als Mitglied mitwirkt, auf informeller Ebene unter amerikanischer Führung Arbeiten aufgenommen, um vertrauensbildende Maßnahmen zu befördern. Hier stellt sich allerdings die Frage, ob Parameter der Rüstungskontrolle auf die Kontrolle des Cyberspace übertragbar sind.

Vielversprechender ist es, an die EU-USA-Arbeitsgruppe anzuknüpfen, die seit November 2010 über Fragen der Cybersicherheit berät. Wesentliche Impulse für nationale Cybersicherheitsstrategien in Europa sind aus den USA gekommen, aus dem Land, das sich gerade sehr energisch für die Kriegsführung mit den Mitteln des Internets rüstet. Die EU wird diesen technologischen Vorsprung im militärischen Bereich absehbar nicht einholen (können/wollen). Gleichzeitig sind die USA wie die EU die größten Verfechter des Mulitstakeholder-Ansatzes. Die Stakeholder, die sich um Funktionen, Stabilität und Sicherheit des Internets kümmern, organisieren das Internet pragmatisch und gehören keiner Regierung an. Keine Regierung verfügt über die Expertise und das Tempo, mit den Entwicklungen im Internet Schritt zu halten. Finanzknappheit und Entscheidungsblockaden behindern gleichzeitig die Arbeit der ITU.

Im amerikanischen Kongress machen sich Republikaner und Demokraten gemeinsam stark gegen die Verlagerung und Ausweitung der Kontrolle des Internets. Sie fürchten den Einflussverlust, wenn zentrale Instanzen der Internetverwaltung an die ITU übergeben würden. China und Russland wollen, dass die Aufgabe der Adressenverteilung, die bislang von ICANN übernommen wird, zumindest teilweise in die Verantwortung der ITU gegeben wird. Im Zuge der Neuverhandlungen der ITR von 1988 spricht vieles dafür, dass sich die Mitgliedstaaten auf eine Strategie zur Cybersicherheitspolitik einigen und dabei die oben ausgeführten Defizite der Selbstregulierung, Standards für Sicherheitstechnologien, des Individualschutzes bei der Kriminalitätsbekämpfung sowie der Parlamentarisierung und Transparenz in der Cybersicherheitspolitik international und in enger transatlantischer Absprache beheben.

Dieser Beitrag erschien zuerst in IP – Internationale Politik, Ausgabe November/Dezember 2012.

Das Jahr, in dem die Netzpolitik Emotionsbingo spielte

Falk Lüke

Was wäre ein netzpolitischer Jahresrückblick ohne die Niederungen der Metaebene? Wo steht die Netzpolitik am Ende des Jahres 2012?

Es war eine kleine Runde: Vor mehr als einem Jahr im Sommer 2011 saßen mehrere netzpolitisch Interessierte zu einem Roundtable in der Berliner US-Botschaft zu einem Meinungsaustausch zusammen. Neben WikiLeaks und dem Schicksal Bradley Mannings, Google, den Datenschutz und das Internet Freedom-Programm des State Departments warfen die deutschen Netzmenschen auch ein Thema auf, von dem die Botschaftsmitarbeiter zu diesem Zeitpunkt offensichtlich noch nicht viel gehört hatten: ACTA. Das sollte sich 2012 deutlich ändern. Denn die erste Hälfte des Jahres war netzpolitisch von eben jenem internationalen Abkommen zur Durchsetzung von Urheberrecht und Markenschutz dominiert, dem Abkommen, das ein halbes Jahrzehnt vorverhandelt wurde und dann im Sommer 2012 endgültig von den Europaparlamentariern in den Mülleimer befördert wurde. ACTA war ein Symbol für die netzpolitischen Akteure in Europa: erstmals wurde ein unglaublich komplexes Thema soweit heruntergebrochen, dass ein wirklicher politischer Massenprotest entstand.

Die ACTA-Proteste zogen sich von Polen ausgehend quer durch Europa, vorwiegend durch die mittel- und osteuropäischen EU-Mitgliedstaaten. Um die 100.000, vorwiegend junge, Menschen zog es im Februar 2012 allein in Deutschlands Städten auf die Straße. War es im kalten Winter noch ein wärmendes „Wer nicht hüpft der ist für ACTA!“ – durchaus eindrucksvoll, wenn mehrere Tausend Menschen vor dem Bundesjustizministerium vorbeihüpfen – waren es später vor allem die direkten Ansprachen der Europaparlamentarier.

Mit ACTA hat die digitale Zivilgesellschaft einen Vorzeigeerfolg hinbekommen, der aber nun die Messlatte darstellt. Aber auch an anderer Stelle hat ACTA etwas bewirkt: für viele der Netzmenschen ist „Brüssel“, also die EU, keineswegs mehr solch ein abstraktes und weit weg befindliches Gebilde. Ihnen ist klar geworden, dass ihre Zukunft zwar auch in Berlin entschieden

wird, aber keineswegs exklusiv. Brüssel hatte plötzlich Namen: Karel de Gucht, Viviane Reding, Neelie Kroes – nie war die Brüsseler Kommissarsriege so präsent in den deutschen Netzdebatten wie in jenen Monaten.

Die Diskussion um ACTA hat zugleich aber auch etwas anderes befördert: die Diskussion um die Grundlagen des Urheberrechts und seine konkrete Ausgestaltung. Während die einen – die Künstler – um ihre Lebensgrundlage fürchten, fürchten die anderen sich vor einem Überwachungsstaat, einer Gängelung durch den Gesetzgeber – Eingriffen in ihre Lebensrealität, die sie für unverhältnismäßig zum Schutzzweck „Geistiges Eigentum" empfinden. Die Unversöhnlichkeit der Positionen zeigte sich in teils absurden, öffentlichkeitswirksamen Teufel-an-die-Wand-Malwettbewerben vor allem der Seite, die ihre Rechte für unzureichend geschützt hält und der potenziell jedes Mittel zur Durchsetzung ihrer Position recht zu sein scheint. Ob Websperren, Filtertechnikeinsatz oder der Entzug des Internetzugangs: all diese Punkte werden nach wie vor von Lobbyisten, aber auch von Künstlern, deren Nachdenken über die Auswirkungen ihrer Forderungen oft überschaubar weit scheint, in schöner Regelmäßigkeit vorgetragen.

Sie fühlen sich nicht respektiert in ihrem Wirken. Ungeachtet dessen, dass ein nennenswerter Teil der „Kreativwirtschaft", aus der man, um ihre tatsächliche Größe zu ermitteln, erst einmal den Internetkreativwirtschaftsbereich abziehen muss, ungeachtet der Tatsache, dass diese Bereiche zu nennenswerten Teilen am Tropf von Subvention und Gebührenzahlern hängen, ist das problematisch. Denn ist der Internetgeneration tatsächlich das in die Welt gesetzte Werk – finanziell, denn darum geht es im Kern dieser sich mit der Medienwirtschaftskrise vermischenden Debatte – nichts wert? Als teilnehmender Debattenbeobachter bekam man ein teils flaues Gefühl im Jahre 2012: die Debatte um die Zukunftsfähigkeit des Urheberrechts als Broterwerbsbeihilfeinstrument fand jahrelang statt, ohne dass die „Kulturschaffenden" diese ernsthaft führten. Für sie war alles schön, wie es war, wenn auch nicht unbedingt optimal. Doch nun standen sie plötzlich unter Zugzwang – während die netzpolitischen Akteure sich zu fragen schienen: „Huch, wo kommt Ihr denn her? Was wollt Ihr denn noch? Wir haben doch alles bereits x-fach rauf und runter diskutiert?" Auch das ist natürlich eine Fehlannahme. Denn wirkliche Lösungswege aus dem Dilemma der großflächigen Nichtdurchsetzbarkeit von Urheberrechten gibt es kaum, sondern nur einzelne Elemente, die Auswege aufzeigen. Dass dieser Streit mit voller künstlerischer Verve auf der

einen und einem vielleicht zutreffenden, aber wenig hilfreichem netzpolitischen „Ihr habt gar keine Ahnung, was ihr da fordert" auf der anderen Seite ausgetragen wird, führt zu einem Emo-Patt – überbordende Emotionen haben einen gordischen Knoten herbeigezaubert, dessen Durchschlagen nun im Ring der Politik liegt. Sie wird es nicht allen Beteiligten Recht machen, allerdings auf absehbare Zeit auch nur wenig tun können.

Eine Großreform des Urheberrechts ist frühestens in drei Jahren überhaupt einmal zu überlegen, wenn eine neugewählte EU-Kommission installiert und die Europa- (2013) und Bundestagswahlen (2012) lange durch sind. Zeit, in der alle Seiten ihre Argumente wägen und formulieren sollten, Klarheit schaffen und das ein oder andere Argument der Gegenseite vielleicht nicht ganz so pauschal zu verwerfen, sondern emotionsarm zu prüfen, ob nicht doch ein Fünkchen Wahrheit daran sein könnte.

Überhaupt, Empfindungen haben, neben rationalen Argumenten, einen Großteil der netzpolitischen Debatten 2012 beeinflusst. Nicht nur in der Diskussion um Urheberrecht, auch bei der Dauergroßbaustelle Datenschutz prallen Emotionen aufeinander – wenn auch aus vollkommen anderen Gründen. Die einen glauben, dass die Vereinheitlichung des Datenschutzniveaus auf europäischer Ebene den deutschen Grundrechtsschutz zu unterlaufen drohe. Andere glauben, dass das Datenschutzrecht per se innovationsfeindlich sei und eigentlich ein ganz neuer Ansatz notwendig sei, allerdings ohne dass sie auch nur annähernd konkrete und als Alternative ernstzunehmende eigene Vorschläge präsentierten. Dritte wiederum halten das alles für Augenwischerei, vielen Kritikern des aktuellen Datenschutzkonzepts ginge es primär darum, die Interessen von Wirtschaftsakteuren zu schützen. Und einige sehen die Reform als Chance, dem Datenschutz nach vielen Jahren weitgehend papierner Existenz tatsächlich Zähne zu verleihen und streiten über den richtigen Weg.

Auch andere überaus trockene Themen wurden 2012 hochgradig emotionalisiert. Ob die Debatte um das von der schwarz-gelben Bundesregierung vorgeschlagenen Leistungsschutzrecht für Presseverleger oder die Frage, wer eigentlich die institutionell-faktische Herrschaft über das Netz und seine Infrastrukturen ausübt, und damit der Streit um die Zusammenschaltungs- und Interoperabilitätsregularien der vor fast 150 Jahren gegründeten Internationalen Fernmeldeunion ITU. Und fast immer mit am Tisch in diesen emotio-

nalen Debatten: die Wirtschaftsunternehmen der Nachfolger oder Überlebenden der New Economy mit ihren spezifischen Interessen auf einer Seite und die Telekommunikationsriesen auf einer anderen.

Nun gibt es aber einen Teil der Politik, der ist eher weniger emotional aufgeladen. Irgendwo in Berlin, unweit der Spree, hat man vor drei Jahren 17 Parlamentarier und ihre etwa 30 Mitarbeiter, dazu 17 sogenannte Sachverständige, von denen etwa ein Drittel auf eigene Mitarbeiter für diese Arbeit zurückgreifen kann, sowie einige Sekretariatsmitarbeiter, die inzwischen sogar fast verstehen, worüber dort den ganzen Tag gesprochen wird, im Paul-Löbe-Haus eingekerkert und lässt sie nur noch selten ans Tageslicht. Manchmal macht jemand die Tür auf und schwupps, laufen zwei bis vier, an spektakulären Debattentagen auch einmal neun oder zehn Menschen auf die Besuchertribüne. Heimliches Ziel dieser parlamentarischen Übung ist das endgültige Abholzen der Wälder. So zumindest der Eindruck bei allen, die sich mit der „Enquete-Kommission Internet und Digitale Gesellschaft des Deutschen Bundestag" (kurz: EIDG, ein Kürzel, von dem nur Spötter sagen, dass es für „Es ist das Grauen" stehen würde) seit ihrem Start beschäftigen. Koalitionsbank, von den Koalitionsparteien benannte Sachverständige und Oppositionsbank und von den Oppositionsparteien benannte Sachverständige sitzen einander unversöhnlich gegenüber oder nebeneinander. Das Spiel lautet: Du bist doof und ich bin klug, und weil ich so klug bin, versteck ich Dir was in einem Textwust und hoffe, dass eure Fach- oder Fraktionsreferenten schlafen.

Die EIDG beschäftigt sich zwar auch mit dem Internet und der digitalen Gesellschaft, produziert aus Versehen immer wieder erstaunlich lesenswerte (leider wird sie niemals jemand lesen) Texte. Aber immer, wenn es um die Wurst geht, heißt diese padeluun: der von der FDP benannte Sachverständige aus Bielefeld ist meist der pivotale, der entscheidende Spieler, der entweder einen Einlauf von den Regierungsfraktionen und Mitsachverständigen ebendieser bekommt, weil er mit der Opposition stimmt. Oder aber er ist im Kreuzfeuer der Kritik der Opposition, wenn er für die Textzeilen der Koalitionsfraktionsbank stimmt – denn padeluun gehört eigentlich zur digitalen Bürgerbewegung, und immer, wenn er mit dem BITKOM-Geschäftsführer und dem Musiklobbyisten Dieter Gorny stimmt, hebt Blogger Fefe irgendwo schon den Zeigefinger um damit umgehend auf padeluun zu schießen. Mit ihm tauschen würde wohl niemand gerne.

Nun soll aus dieser etwas unglücklich und in der Tagespolitik gefangenen Enquete-Kommission ein ständiger netzpolitischer Ausschuss hervorgehen, der auch den derzeit existierenden Unterausschuss Neue Medien des Kulturausschusses ablösen dürfte. Vor der Bundestagswahl 2013 wird hier zwar sicherlich nichts mehr passieren, doch die spannende Frage ist: was passiert nach dieser? Wird es einen eigenen Internetminister geben? Das scheint unwahrscheinlich. Werden netzpolitische Fragestellungen einem bereits bestehenden Ressort zugeordnet, beispielsweise dem Innen-, Verbraucher- oder dem Wirtschaftsressort? Und: wäre das sinnvoll? Oder wird es eine dem Bundesbeauftragten für Kultur und Medien vergleichbare Stelle eines Internetstaatsministers im Kanzleramt geben? Auf jeden Fall würde ein solcher Themenquerschnittsausschuss ein entsprechendes Pendant auf Seiten der Regierung benötigen.

Ist die Netzpolitik im Jahr 2012 also ein Stück vorangekommen? Auf jeden Fall hat sie es geschafft – sicher auch unter dem Eindruck des Einzugs der Piratenpartei in vier Landesparlamente zwischen September 2011 und Mai 2012 – dass sie zu einem „normalen" Medienöffentlichkeitsthema geworden ist. Sie ist auch auf der politischen Agenda nicht mehr ein absolutes Exotenthema, sondern einigermaßen ernstzunehmender Aspekt des politischen Betriebs. Nur eben: auch nicht mehr. Wenn im September 2013 der nächste Bundestag gewählt wird und die nächste Bundesregierung gebildet, dann werden sich einige Dinge ändern. Zum einen wird es für die drei Netzpolitiker der FDP im Bundestag noch mehr als für die Gesamtpartei knapp, wieder einzuziehen. Und zugleich ist klar, dass mit jeder Wahl jüngere und internetaffinere – dadurch aber keineswegs automatisch netzpolitisch interessierte, aber die Themen als weniger exotisch wahrnehmende – Bundestagsabgeordnete nachrücken. Und einige der Urgesteine der Bundestagsdebatten werden einfach ausscheiden. Das könnte die Debatten nachhaltiger verändern als die Streitpunkte, die 2012 die Agenda bestimmte.

Spannend dürfte auf jeden Fall werden, wie die verschiedenen mit der Digitalisierung in Berührung stehenden Ministerien damit umgehen. Sowohl das Innen- als auch das Außenministerium haben die Themen in dieser Legislatur für sich erkannt, das Wirtschaftsministerium ist offenbar auf der Suche nach Leitlinien einer modernen Netzpolitik, das Verbraucherministerium versucht zu tun, was es mit minimalem Personaleinsatz kann und das Justizministerium hat sich als Freiheitsverteidiger darstellen können. Doch von ei-

ner koordinierten und aktiven Netzpolitik einer Regierung kann bislang kaum die Rede sein – das könnte sich nach der nächsten Wahl dann ändern, je nach Perspektive zum Guten wie zum Schlechten.

AutorInnenverzeichnis

Jan-Phillip Albrecht ist Abgeordneter des Europäischen Parlaments für die Grünen und vertritt die Bürgerinnen und Bürger aus Niedersachsen, Hamburg und Schleswig-Holstein. Jans Themen sind Innen- und Justizpolitik, dabei geht es um die Reform des Europäischen Datenschutzrechts, das Recht auf anwaltlichen Beistand, die Europäische Ermittlungsanordnung, Polizeipolitik und Rechtsextremismus. Besonders am Herzen liegen ihm „Bürgerrechte im digitalen Zeitalter".

Markus Beckedahl ist Gründer und Chefredakteur von netzpolitik.org. Er ist Vorsitzender des Digitale Gesellschaft e. V., Veranstalter der re:publica-Konferenzen und Partner bei der newthinking GmbH.

Annegret Bendiek ist wissenschaftliche Mitarbeiterin der SWP und stellvertretende Forschungsgruppenleiterin der FG „EU-Außenbeziehungen".

Mirko Boehm ist Open-Source-Hacktivist, Softwareentwickler und Ökonom. Er ist seit 1997 Contributor am KDE-Projekt, einer der weltweit größten Open-Source-Communities. Von 1999 bis 2006 war er Mitglied des Vorstands des KDE e. V., und trägt heute zur Weiterentwicklung von KDE und zur Arbeit der Free Software Foundation Europe insbesondere in Fragen der Governance und zum Urheberrecht bei. Mirko lehrt zu Open Source in der digitalen Gesellschaft am Fachgebiet Innovationsökonomie der Technischen Universität Berlin. Er ist verheiratet und lebt mit seiner Frau und zwei Kindern in Berlin.

Jörg Braun ist seit Sommer 2010 Mitarbeiter von MdB Petra Sitte und da insbesondere aktiv im Rahmen ihrer Tätigkeit für die Internetenquete des Bundestages. Das war bisher vor allem Urheberrecht, Medienbildung und Digitalisierung in Bildung und Forschung. Über die Enquete hinaus hat Jörg in den vergangenen zwei Jahren vor allem an den Vorschlägen der LINKEN Bundestagsfraktion zur Urheberrechtsreform mitgeschrieben.

Ulf Buermeyer ist Richter am Landgericht Berlin und dort derzeit Beisitzer der Großen Strafkammer 22 (Schwurgericht); daneben ist er verantwortlicher Redakteur der Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht (HRRS). Die Schwerpunkte seiner wissenschaftlichen Arbeit liegen im Verfassungsrecht (insbesondere Telekommunikationsfreiheiten & informationelle Selbstbestimmung) sowie im Strafrecht (inkl. Strafprozess & Strafvollzug).

Gabriella Coleman ist Inhaberin des Lehrstuhls für Scientific and Technological Literacy am Institut für Kunstgeschichte und Kommunikationswissenschaften der McGill University in Montreal, Kanada.

Leonhard Dobusch, Jurist und Betriebswirt, forscht als Juniorprofessor für Organisationstheorie am Management-Department der Freien Universität Berlin zu transnationaler Urheberrechtsregulierung sowie zum Management digitaler Gemeinschaften.

Kirsten Fiedler arbeitet bei European Digital Rights als Advocacy Manager. Ein Europastudiengang führte sie nach Liverpool, Aix-en-Provence und Köln, jetzt bloggt sie auf vasistas-blog.net und netzpolitik.org und ist aktiv bei der NURPA (Net Users' Rights Protection Association) in Belgien. Kirsten ist Schatzmeisterin des Digitale Gesellschaft e. V.

Karina Fissguss ist Online Journalistin und Mutter zweier Söhne. Sie arbeitet nach ihrer Elternzeit wieder für die newthinking Communications und promoviert zum Thema Online Angebote des öffentlich-rechtlichen Rundfunks. Wenn dann noch Zeit bleibt, bloggt sie unter generationnetz.blogspot.de und hält Vorträge an Elternabenden zum Thema Kinder und Computer.

Kilian Froitzhuber ist Politologe und Mitarbeiter eines Europaabgeordneten.

Volker Grassmuck ist Mediensoziologe, freier Autor und Aktivist. Er arbeitet am Zentrum für Digitale Kulturen der Leuphana Universität Lüneburg über die Zukunft der öffentlich-rechtlicher Grundversorgung. Er hat die Konferenzserie Wizards-of-OS.org und das Informationsportal zum Urheberrecht iRights.info geleitet, die Initiativen mikro-berlin.org, privatkopie.net und CompartilhamentoLegal.org mit gegründet und bloggt unter vgrass.de.

Johnny Haeusler ist Autor, Blogger, Musiker, Radiomensch und re:publica-Mitgründer. In seiner Freizeit denkt er sich neue Sachen aus, die man so machen kann.

Christian Heise ist wissenschaftlicher Mitarbeiter an der Leuphana Universität Lüneburg, wo er zum Thema Open Science promoviert. Zuvor war er als Manager bei der Deutschen Presse Agentur und bei ZEIT ONLINE tätig. Er ist Vorstandsmitglied bei der Open Knowledge Foundation Deutschland sowie im Förderverein für freie Netzwerke.

Jeanette Hofmann ist eine von vier Direktoren des Institut für Internet und Gesellschaft und zuständig für den Bereich Internet Policy & Governance. Die Politikwissenschaftlerin forscht am Wissenschaftszentrum Berlin zu den Themen Global Governance, Regulierung des Internet, Informationsgesellschaft und Wandel des Urheberrechts. Sie ist zugleich research associate am Centre for Analysis of Risk and Regulation (CARR) der London School of Economics and Political Science (LSE).

Jōichi „Joi" Itō ist ein japanischer Aktivist, Unternehmer und Investor für Risikokapital. Er ist Mitglied im Vorstand von Creative Commons und Vorstandsmitglied der Mozilla Foundation. Seit 2011 leitet er das MIT Media Lab in Cambridge.

Andrea Jonjic schließt gerade ihr Studium der Politikwissenschaft in Frankfurt am Main ab und ist Redakteurin des Sicherheitspolitik-Blog.de.

Matthias Kirschner ist Fellowship Coordinator und German Coordinator bei der Free Software Foundation Europe.

Julia Kloiber arbeite als Project Coordinator für die Open Knowledge Foundation Deutschland und ist in der Digitalen Gesellschaft aktiv. Sie hat in den letzten Monaten mehrere Projekte im Bereich Open Data umgesetzt, darunter Open Data in Kommunen, Stadt Land <Code> und Apps and the City. Ihr Ziel für 2013: das Thema Open Data so aufzubereiten, dass eine breitere Masse an Menschen versteht, wie wichtig und wertvoll offene Daten für Demokratie und Gesellschaft sind und Open Data so stärker auf die politische Agenda rückt.

Constanze Kurz ist Informatikerin und Hackerin, arbeitet als wissenschaftliche Projektleiterin am Forschungs- und Weiterbildungszentrum „Kultur und Informatik" an der Hochschule für Technik und Wirtschaft in Berlin. Ihre Forschungsschwerpunkte sind Ethik in der Informatik, informationelle Selbstbestimmung, Biometrie und Überwachungstechnologien. Sie berät als technische Sachverständige die Enquête-Kommission „Internet und digitale Gesellschaft" des Deutschen Bundestags. Sie ist ehrenamtlich Sprecherin des Chaos Computer Clubs sowie Autorin und Publizistin.

Lawrence Lessig ist Professor für Rechtswissenschaften an der Harvard Law School. Er gründete das Center for Internet and Society und die Creative-Commons-Initiative. Lessig wurde 2002 mit dem Free Software Foundation Award ausgezeichnet und ist Vorstandsmitglied des im Februar 2005 gegründeten Software Freedom Law Center.

Falk Lüke, 31, verdient sein Geld hauptsächlich mit Journalismus. Er ist gelernter Politikwissenschaftler und beschäftigt sich vor allem mit Politik- und Technologiethemen. Hat im Jahr 2010 den Verein Digitale Gesellschaft e. V. mitgegründet, ist derzeit Mitglied in insgesamt fünf Vereinen (Berufsvereinen, Interessenvereinen).

Lorenz Matzat ist Journalist und Unternehmer in Berlin. Er ist Mitglied des Digitale Gesellschaft e. V., schreibt das Blog datenjournalist.de, ist Mitbegründer der Datenjournalismusagentur OpenDataCity und leitet die Kartensoftwarefirma Lokaler.

Tim Maurer ist Program Associate des Open Technology Institute der New America Foundation in Washington DC und Non-resident Fellow beim Global Public Policy Institute in Berlin. Er forscht und schreibt zu außenpolitischen Themen und Netzpolitik.

Joe McNamee ist Geschäftsführer bei European Digital Rights (EDRi), einer Dachorganisation von 32 Bürgerrechts- und Datenschutzorganisationen in Brüssel. Er studierte in Brüssel, Swansea und Bristol, arbeitet bereits seit 1995 im Bereich der neuen Technologien und ist nebenbei im Beirat der EFF und im Beratungsgremium eines Datenschutzprojekts der UNESCO.

Andre Meister ist Sozialwissenschaftler und Systemadministrator. Er begleitet diverse netzpolitische Zusammenhänge wie AK Vorrat, AK Zensur oder CCC und ist Mitgründer des Digitale Gesellschaft e. V. Anfang 2012 konnte Andre das Bloggen auf netzpolitik.org zu seinem Beruf machen.

Matthias Monroy ist Journalist, Aktivist und Wissenschaftlicher Mitarbeiter des Mitglieds des Bundestages Andrej Hunko der Fraktion DIE LINKE.

John F. Nebel begann seine journalistische Tätigkeit bei einem mittlerweile eingestellten Stadtmagazin als Nachtlebenkolumnist. Bei Metronaut.de schreibt er über Grundrechte, Freiheit, Überwachung, Netzpolitik und Public Relations.

Frank Rieger, Jahrgang 1971, ist technischer Geschäftsführer eines Unternehmens für Kommunikationssicherheit. Er ist Mitgründer erfolgreicher deutscher Startup-Unternehmen in den Bereichen Datensicherheit, Navigationsdienste und E-Reading. Seit 1990 ist er einer der Sprecher des Chaos Computer Clubs, der immer wieder eindrucksvoll auf Datenmissbrauch aufmerksam macht.

Alexander Sander arbeitet für den Europaabgeordneten Martin Ehrenhauser und hat die Kampagne NoPNR gegründet. Ist hier und da Mitglied. Beschäftigt sich mit den Themen Innere Sicherheit, Datenschutz und Netzpolitik.

Ben Scott ist Senior Advisor des Open Technology Institute der New America Foundation in Washington DC und Visiting Fellow bei der Stiftung Neue Verantwortung in Berlin. Zuvor war er Berater für Innovation beim Außenministerium der Vereinigten Staaten, wo er an der Kreuzung von Technologie- und Außenpolitik tätig war.

Felix Stalder ist Professor für Digitale Kultur und Theorien der Vernetzung an der Zürcher Hochschule der Künste sowie unabhängiger Forscher und Organisator unter anderem beim Institut für Neue Kulturtechnologien in Wien.

Moritz Tremmel studiert Politikwissenschaft, Soziologie und Rechtswissenschaft an der Universität Tübingen. Er schreibt zum Themenkomplex Datenschutz, Überwachung und Kontrolle wissenschaftliche Arbeiten und Artikel. Außerdem hält er Workshops und Vorträge zum Thema. Moritz Tremmel ist Teil des Forschernetzwerks surveillance-studies.org, bloggt bei netzpolitik.org und ist Mitglied des Vereins Digitale Gesellschaft.

Ben Wagner ist Doktorand am Europäischen Hochschulinstitut in Florenz und Visiting Fellow beim European Council on Foreign Relations in Berlin.

Stefan Wehrmeyer ist bei der Open Knowledge Foundation Deutschland und Projektleiter von FragDenStaat.de. Er lebt als Softwareentwickler und Open-Data-Aktivist in Berlin.

Jillian C. York ist Direktorin für internationale Meinungsfreiheit bei der Electronic Frontier Foundation. Sie schreibt regelmäßig Kolumnen für Global Voices Online und Al-Dschasira.