Internet & Gesellschaft

<Co:llaboratory.at>

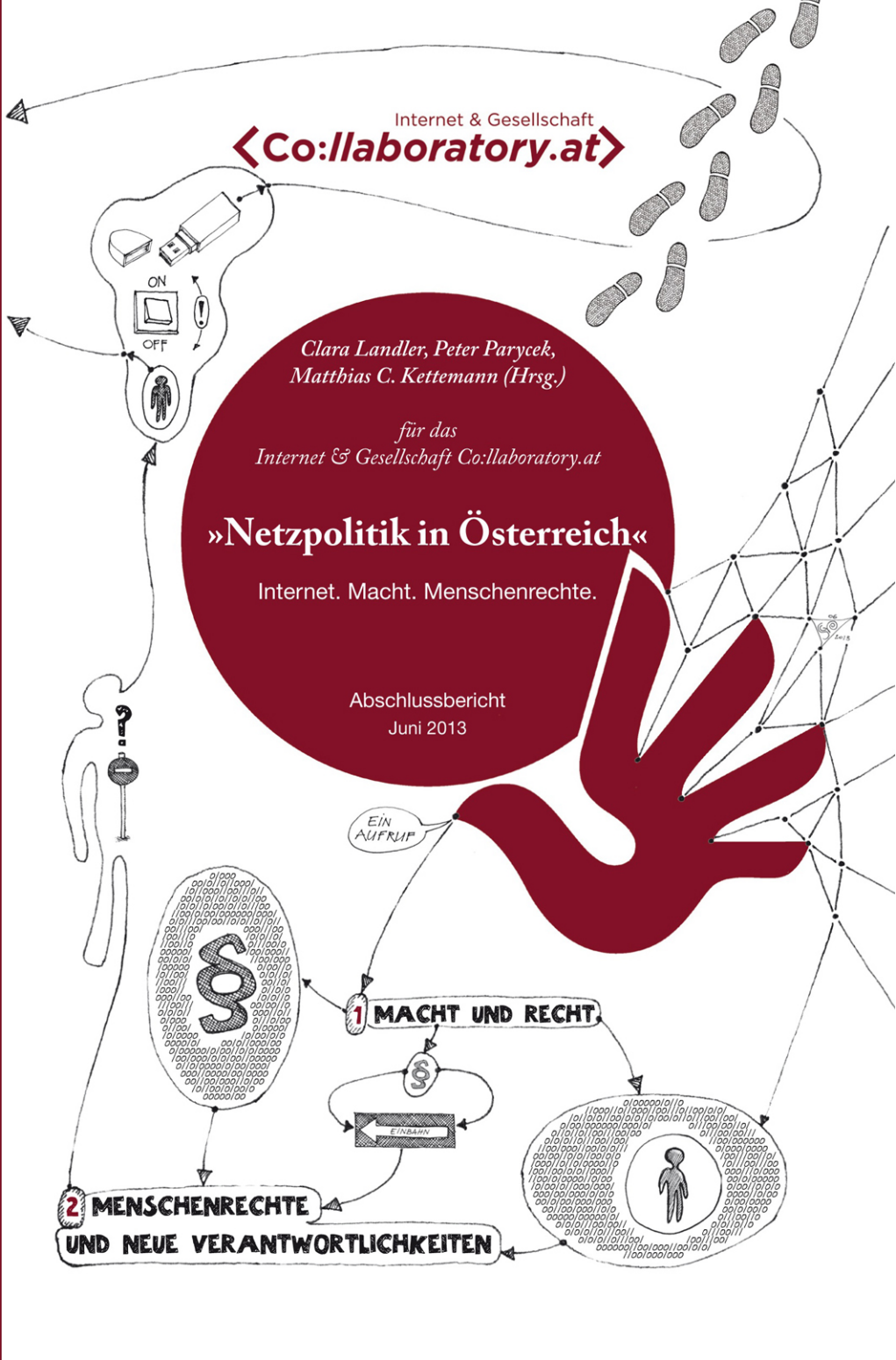
Clara Landler, Peter Parycek,
Matthias C. Kettemann (Hrsg.)

für das
Internet & Gesellschaft Co:llaboratory.at

»Netzpolitik in Österreich«

Internet. Macht. Menschenrechte.

Abschlussbericht
Juni 2013



Netzpolitik in Österreich.

Internet. Macht. Menschenrechte

Eine Publikation des
Internet & Gesellschaft
Co:llaboratory AT

Abschlussbericht
Juni 2013

1. Auflage
ISBN 978–3–902505–33–0

Impressum

http://www.collaboratory.at
E-Mail: kontakt@collaboratory.at
Online Publikation:
http://publikationen.collaboratory.at/mri

Konzept & Erstellung
Peter Parycek, Clara Landler, Judith Schoßböck
HerausgeberInnen
Clara Landler, Peter Parycek, Matthias C. Kettemann
VerfasserInnen
Julian Ausserhofer ° Michael Bauer ° Sylvia Johnigk ° Wolfgang Gumpelmaier ° Matthias C. Kettemann ° Thomas Kreiml ° Andreas Krisch ° Clara Landler ° Joachim Losehand ° Eva Jana Messerschmidt ° Christian Möhlen ° Tassilo Pellegrini ° David Röthler ° Markus Sabadello ° Stephan Schlögl ° Judith Schoßböck ° Viktor Szabados ° Leonie Maria Tanczer ° Christof Tschohl ° Hans Christian Voigt ° Heinz Wittenbrink

Projekt- & Inhaltliche Koordination, Lektorat, Gestaltung, Layout, Produktion
Clara Landler
Korrektorat/Lektorat
Eva Schörkhuber
Covergestaltung
Philipp Markus Schörkhuber
Designkonzept der Co:llaboratory Gesamtreihe
Louis Grosser, www.louisgrosser.com

Ansprechpartner des Co:llaboratory AT Lenkungskreises
Peter Parycek (Donau-Universität Krems) ° Thorsten Koch (Google.at) ° Philipp Müller (SMBS, CSC) ° Thomas Obernosterer (Landtagsdirektion NÖ)

Die Anschubfinanzierung des Co:llaboratory AT erfolgte über das Internet & Gesellschaft Co:llaboratory e.V. Berlin, besonderer Dank gilt Sebastian Haselbeck.

Internet & Gesellschaft Co:llaboratory AT, www.collaboratory.at
Abschlussbericht, Zweite Initiative (2012–2013):
Netzpolitik in Österreich.
Internet. Macht. Menschenrechte.
Publisher: Edition Donau-Universität Krems, Juni 2013
Druckerei und Auslieferung: Verlagshaus Monsenstein und Vannerdat OHG
www.mv-verlag.de
Dieser Band steht unter einer Creative Commons Namensnennung 3.0
Unported Lizenz.: https://creativecommons.org/licenses/by-nc/3.0/deed.de

ISBN: 978–3–902505–33–0

Inhaltsverzeichnis

VORWORT 3

NETZPOLITIK IN ÖSTERREICH – EIN AUFRUF. 7

DIE FÜNF ZENTRALEN THESEN DER INITIATIVE 8

DIE THESEN IM DETAIL 9

TEIL 1: MACHT UND RECHT 15

1.1. ETHIK, RECHT UND MENSCHENRECHTE (CHRISTOF TSCHOHL) 17

1.2. RECHTE EINES JEDEN MENSCHEN _AM_ INTERNET (HANS CHRISTIAN VOIGT) 27

1.3. MACHT SPRACHE INTERNET? (CLARA LANDLER) 43

1.4. POST, GENDER, INTERNET? (LEONIE MARIA TANCZER) 53

1.5. DAS INTERNET IN DER ARBEITSRECHTLICHEN KAMPFZONE (THOMAS KREIML) 71

1.6. GUTE FILTER, BÖSE FILTER? (JULIAN AUSSERHOFER) 83

TEIL 2: MENSCHENRECHTE UND NEUE VERANTWORTLICHKEITEN 91

2.1. NEUE MENSCHENRECHTE FÜR DAS INTERNET? (MATTHIAS C. KETTEMANN) 93

2.2. GIBT ES EIN RECHT AUF POLITISCHEN ONLINE-PROTEST? (CHRISTIAN MÖHLEN) 97

2.3. INTERNETSPERREN UND MENSCHENRECHTE (EVA JANA MESSERSCHMIDT) 111

2.4. PARADIGMENWECHSEL VORRATSDATENSPEICHERUNG IM EU-DATENSCHUTZRECHT (CHRISTOF TSCHOHL) 123

2.5 DIE REFORM DES EU-DATENSCHUTZRECHTS (ANDREAS KRISCH) 139

TEIL 3: GOVERNANCE UND NETZPOLITIK 153

3.1. GRENZEN STAATLICHER INTERNETPOLITIK (MATTHIAS C. KETTEMANN) 155
3.2. NETZNEUTRALITÄT (TASSILO PELLEGRINI) 161
3.3. MENSCHENRECHTE UND OGD (CHRISTOF TSCHOHL) 171
3.4. IST FACEBOOK EIN NEUER ÖFFENTLICHER RAUM? (M. C. KETTEMANN) 183
3.5. WELTÖFFENTLICHKEIT (STEPHAN SCHLÖGL) 189
3.6. HASSREDEN IM INTERNET (VIKTOR SZABADOS) 207

TEIL 4: BILDUNG UND EMANZIPATION 217

4.1. DIGITALE TECHNOLOGIEN UND PARTIZIPATION (MIHI BAUER) 219
4.2. WEB LITERACIES UND OFFENE BILDUNG (HEINZ WITTENBRINK, JULIAN AUSSERHOFER) 225
4.3. ZU VIEL IM NETZ? (JUDITH SCHOßBÖCK) 237
4.4. „SUBSCRIBE NOW!“ (JOACHIM LOSEHAND) 249

TEIL 5: AKTIVITÄT UND ENGAGEMENT 255

5.1. SCHUTZ AUS STRAßBURG (MATTHIAS C. KETTEMANN) 257
5.2. WIE KÖNNEN WIR DIE PRIVATSPHÄRE SCHÜTZEN? (MARKUS SABADELLO) 263
5.3. DEMOCRACY LIVE? (DAVID RÖTHLER) 271
5.4. DAS AKTIVISTISCHE POTENZIAL VON CROWDFUNDING (WOLFGANG GUMPELMAIER) 279
5.5. CYBERPEACE STATT CYBERWAR (SYLVIA JOHNIGK) 287

DIE AUTORINNEN 299

Vorwort

Das Internet ist zu einem zentralen Resonanzraum verschiedenster Ideen, Vorstellungen und Wünsche geworden. Es können Heimgärtnervereine ebenso wie Revolutionen gestartet, Musikvideos betrachtet, aber auch Filme über Menschenrechtsverletzungen angesehen werden. Menschen können sich im Internet austauschen, Informationen oder Unterhaltung suchen und konsumieren, politisch aktiv werden und sich organisieren. Den Möglichkeiten des Internets scheinen kaum Grenzen gesetzt.

Das Internet verstärkt aber auch Ungleichheiten. Wer beispielsweise in Österreich keinen Zugang zum Internet hat, ist benachteiligt. So können sich Studierende an manchen Universitäten nur noch online zu Lehrveranstaltungen anmelden, Behörden setzten zunehmend auf Online-Angebote für BürgerInnen, aber auch reine Vereinfachungen eines Lebensalltags wie die Möglichkeit, online einzukaufen, gewinnen an Bedeutung. Damit reicht das Internet mit seinen vielseitigen Potentialen zunehmend weit in die Lebensrealität jedes einzelnen Individuums hinein, was unter anderem die Frage verschärft, wer in welcher Form Zugang haben kann (und haben muss) – und wer von den Möglichkeiten des Internets ausgeschlossen bleibt.

Hier sind netzpolitische Ideen und Lösungen gefragt, zumal in diesem Sinne kaum noch zwischen physischer und virtueller Realität unterschieden werden kann. Noch stärker als bisher betrifft im Informationszeitalter das Ringen seitens Wirtschaft, Politik und Zivilgesellschaft um Macht und Einfluss im, auf und über das Internet jeden einzelnen Menschen. Auch 20 Jahre nach Beginn der Kommerzialisierung des Internets muss daher betont werden, dass das Internet *kein rechtsfreier Raum* ist. Recht gilt offline wie online. Und vor allem: *Menschenrechte* gelten offline wie online. Verstöße werden offline wie

online verfolgt, wenngleich sich dies in virtuellen Sphären häufig schwieriger gestaltet.

Jedwede Möglichkeit einer Verfolgung ist aber zumeist auch eine Frage des Vermögens – und das Recht somit häufig auf Seiten jener, die es sich (in jeglicher Hinsicht) leisten können. Im Sinne einer Gerechtigkeit bedürfen wir also einer menschenrechtssensiblen Netzpolitik, die angesichts der Bedeutung des Internets gleichermaßen Rechts- wie Infrastruktur-, Wirtschafts- wie Bildungs- und Sozialpolitik zu sein hat.

Der vorliegende Band ist das Ergebnis der 2. Initiative des *Co:llaboratory Österreich* (Co:Lab AT, *Internet und Gesellschaft*) zum Thema *Netzpolitik in Österreich – Internet. Macht. Menschenrechte.* Die rund 30 teilnehmenden Netz-ExpertInnen aus Wissenschaft und Praxis (von denen 21 TeilnehmerInnen jeweils einen bis mehrere Beiträge zum vorliegenden Band verfasst haben) untersuchten im Rahmen dieser Initiative die Rolle der Menschenrechte im Internet und die sich daraus ergebenden Notwendigkeiten für eine österreichische Netzpolitik. Die thematische Zuordnung wurde 2012 größtenteils im Rahmen der drei ganztägigen Arbeitstreffen in Graz (Juni), Salzburg (September) und Wien (November) vorgenommen:

Die Beiträge in **Teil 1** widmen sich dem Zusammenhang von Macht und Recht im Internet und den Folgen von dessen Vermachtung und Verrechtlichung (auch in ökonomischer Hinsicht). In **Teil 2** werden neue menschenrechtliche Herausforderungen im Internet im Detail diskutiert. **Teil 3** greift zentrale Fragen der Internet Governance und des internationalen Rahmens für nationale Netzpolitik auf. Dem emanzipatorischen Potenzial des Internets widmet sich **Teil 4**, das Bildung und *web literacies* als zentrale Faktoren für eine Gesellschaft identifiziert, in der das Internet als Rahmen eines sozialen Wandels begriffen wird und seinerseits sozialen Wandel fördern kann. Das abschließende **Teil 5** stellt den ersten vier Kapiteln, die neben praktischen Überlegungen stets auch theoretische Aspekte mitbehandeln,

Seiten des Engagements gegenüber, indem es verschiedene Spielarten eines Internet-Aktivismus und dessen Ziele beleuchtet.

Als offene Kollaborationsplattform konzipiert, entwickelt sich das Co:llaboratory Österreich laufend weiter und soll für Einflüsse aus verschiedensten Richtungen offen sein. Ziel ist die Vernetzung von Internet-Expertinnen und -Experten aus allen gesellschaftlichen Bereichen sowie eine Sensibilisierung der Öffentlichkeit für die stetig wachsende Relevanz von Netzpolitik. Dieses Buch ist als Beitrag dazu gedacht. Es sucht bestehende Diskursfäden über Netzpolitik in Österreich zu bündeln und neue Ideen einzubringen.

Als „living instrument", das dem Charakter des Themas entsprechend weiterlebt, wird der vorliegende Band online weiterbearbeitet – auf zusätzliche Inputs seiner LeserInnen und deren Kollaboration hoffend. Parallel und ergänzend finden sich daher alle Inhalte und damit die aktuellste Version dieser und zusätzlicher Beiträge dieser Initiative auf http://publikationen.collaboratory.at/mri.

Dank gilt der Unterstützung des *Co:llaboratory.de* – im Besonderen Sebastian Haselböck. Darüber hinaus danken die HerausgeberInnen allen UnterstützerInnen der Arbeitstreffen, die zu diesen Gelegenheiten Räumlichkeiten und Infrastruktur zur Verfügung stellten: die Karl-Franzens-Universität Graz, das ICT&S Center der Universität Salzburg und das quartier21/QDK. Darüberhinaus sei allen TeilnehmerInnen und AutorInnen für ihre aktive, kreative und ideenreiche Mitwirkung gedankt.

Graz/Wien/Krems, Juni 2013

Matthias C. Kettemann und Clara Landler

Netzpolitik in Österreich – ein Aufruf.

Im Internet muss das Recht nicht neu erfunden werden. Im Internet müssen die Menschenrechte nicht neu konzipiert werden. Und im Internet muss Politik nicht gänzlich neu gedacht werden. Dennoch stellt die Netzpolitik formative soziale Kräfte vor neue Herausforderungen. Um das politische Emanzipationspotenzial des Internets nutzen zu können, bedarf es einer menschenrechtlich sensiblen, entwicklungsorientierten und technisch informierten Netzpolitik. Die Autorinnen und Autoren dieses Bandes haben in einer halbjährigen Arbeit zentrale Thesen aufgestellt, die als Leitlinien für die Netzpolitik Österreichs dienen können. Sie zeigen auf, wie diese zwischen Macht und Recht navigieren und zentrale gesellschaftliche Werte im und durch das Internet schützen kann. Dieser Band möchte zeigen, was Netzpolitik leisten muss, leisten kann und leisten soll.

Matthias C. Kettemann und Clara Landler

Die fünf zentralen Thesen der Initiative

1. Recht begrenzt die Macht im Internet, doch über „Hintertüren“ wie Interessenspolitik, Sprache, Sozialstruktur und Code hält die Vermachtung wieder Einzug.
2. Alle Menschenrechte, die offline gelten, gelten auch online. Im Internet stehen sie allerdings neuen Herausforderungen gegenüber, denen mit einer klaren Rückbesinnung auf ihre Kerngehalte und einer entsprechenden Inpflichtnahme aller AkteurInnen zu begegnen ist.
3. Um das Demokratisierungs- und Emanzipationsversprechen des Internets einzulösen, bedarf es einer menschenrechtlich sensiblen, entwicklungsorientierten und alle Menschen einschließenden Netzpolitik.
4. Umfassende und gleichberechtigte Beteiligung an der Informationsgesellschaft verlangt Internet-Bildung, eine Öffnung exklusiver Wissenslandschaften, eine sozial informierte Bewirtschaftung der Internet-Allmende und proaktive Maßnahmen zur Überwindung bestehender und sich vertiefender sozialer digitaler Gräben, gerade auch innerhalb eher homogener Gesellschaften.
5. Das Internet befördert sozialen Aktivismus und politisches Engagement durch Transparenz, die Nivellierung von Partizipationshindernissen und Informationsfreiheit. Dabei kann Online-Aktivismus zivilgesellschaftliches Engagement auch in Offline-Kontexten unterstützen, aber nicht ersetzen.

Die Thesen im Detail

1. Recht begrenzt die Macht im Internet, doch über „Hintertüren“ wie Interessenspolitik, Sprache, Sozialstruktur und Code hält die Vermachtung wieder Einzug.

- Netzpolitik auf nationaler und internationaler Ebene ist an den Menschenrechten zu messen. Partikuläre wirtschaftliche und nationale Interessen müssen zurücktreten. Dies begründet das Primat der Netzneutralität. *(Kapitel 1.1., Christof Tschohl)*
- „Das Internet“ ist eine komplexe, sich stets neu erfindende Ressource. Es verändert gesellschaftliche Prozesse und transformiert umgekehrt unsere Gesellschaften. Deshalb greift ein Recht auf „Zugang“ zum Internet zu kurz, vielmehr benötigen wir ein Recht auf umfassende Teilhabe am Internet – vor allem an Prozessen der Weiterentwicklung, Verwaltung und Regulierung. *(Kapitel 1.2., Hans Christian Voigt)*
- Sprache begrenzt das Denken: Das Internet ist mit dem Entstehen sozialer Medien zunehmend gesellschaftlicher wie individueller „Handlungsraum“ geworden, die etablierten Begriffe für darin agierende Menschen haben diesen Wandel aber nicht mitvollzogen. *(Kapitel 1.3., Clara Landler)*
- Das geschlechtsneutrale Ideal einer Post-Gender-Gesellschaft ist eine bislang unerreichte Utopie und das Internet ein Spiegel der Gesellschaft mit denselben Sexismen, Hierarchien und Ausschlussmechanismen wie in der „Offlinewelt“. *(Kapitel 1.4., Leonie Maria Tanczer)*
- Weitgehende Interessenkonflikte in Arbeitsverhältnissen, beispielsweise das Eingrenzen bestimmter Freiheitsansprüche von ArbeitnehmerInnen durch Macht- und Kontrollinteressen der ArbeitgeberInnenseite, führen das Internet betreffend zu neuen rechtlichen Herausforderungen. *(Kapitel 1.5., Thomas Kreiml)*

- Algorithmen und das personalisierte Internet manipulieren unsere Wahrnehmung. Wollen wir im Web Öffentlichkeit und Kreativität bewahren, dann braucht es einen Ein-/Aus-Schalter für solche Personalisierungen. *(Kapitel 1.6., Julian Ausserhofer)*

2. Alle Menschenrechte, die offline gelten, gelten auch online. Im Internet stehen sie allerdings neuen Herausforderungen gegenüber, denen mit einer klaren Rückbesinnung auf ihre Kerngehalte und einer entsprechenden Inpflichtnahme aller AkteurInnen zu begegnen ist.

- Wir brauchen keine neuen Menschenrechte für das Internet, sondern müssen die geltenden mit Augenmaß anwenden. *(Kapitel 2.1., Matthias C. Kettemann)*
- So wie es nicht nur *eine* Form von Online-Protest gibt, gibt es auch nicht *das* eine Recht auf Online-Protest. AktivistInnen können sich auf die Anwendbarkeit der Menschenrechte im Internet berufen, ob eine Aktion die Grenzen des Erlaubten überschreitet, ist allerdings eine Frage des Einzelfalles. *(Kapitel 2.2., Christian Möhlen)*
- Der Einsatz von Internetsperren nimmt weltweit zu. Infolge solcher Maßnahmen kann es neben der Beeinträchtigung der Meinungsfreiheit auch zur Verletzung anderer Menschenrechte kommen. Netzsperren müssen daher stets *ultima ratio* bleiben und entsprechende gesetzliche Vorgaben entwickelt, angewandt sowie transparent umgesetzt werden. *(Kapitel 2.3., Eva Jana Messerschmidt)*
- Die durch die Vorratsdatenspeicherung legalisierte präventive Überwachung des Kommunikationsverhaltens aller in Europa lebenden und elektronisch kommunizierenden Menschen stellt einen unumkehrbaren Paradigmenwechsel dar, der mit dem Konzept eines von Grund- und Freiheitsrechten geprägten Rechtsstaates unvereinbar ist. *(Kapitel 2.4., Christof Tschohl)*

- Auf EU-Ebene wird aktuell an einer Reform und weiteren Vereinheitlichung des europäischen Datenschutzrechts gearbeitet. Nicht zuletzt aufgrund des massiven Drucks von Wirtschaftsvertretern für eine Aufweichung des Datenschutzes ist es wichtig, dass die Zivilgesellschaft für einen starken und tatsächlich durchsetzbaren Schutz personenbezogener Daten eintritt. *(Kapitel 2.5., Andreas Krisch)*

3. Um das Demokratisierungs- und Emanzipationsversprechen des Internets einzulösen, bedarf es einer menschenrechtlich sensiblen, entwicklungsorientierten und alle Menschen einschließenden Netzpolitik.

- Staatliche Internetpolitik kennt mit den Menschenrechten und dem Völkerrecht klare Grenzen. Schon anlässlich der Weltgipfel zur Informationsgesellschaft 2003 und 2005 haben sich die Staaten der Welt zu einer völkerrechtlichen Ordnung des Internets bekannt. Dieses Bekenntnis zu UN-Charta und Allgemeiner Erklärung der Menschenrechte gilt es zu respektieren und zu operationalisieren. *(Kapitel 3.1., Matthias C. Kettemann)*
- Die zunehmende Unternehmenskonzentration im Internet kaschiert einen Trend der wachsenden kulturellen Homogenisierung und Einschränkung der Menschenrechte. Die Debatte um Netzneutralität ist hierbei eine Blaupause für Verteilungskonflikte, die aufgrund ungleicher Machtverhältnisse zulasten der Öffentlichkeit – und zugunsten des Kapitals auszugehen drohen. *(Kapitel 3.2., Tassilo Pellegrini)*
- Als lebendiges Instrument am Puls der Zeit verstanden, gebieten Grund- und Menschenrechtsgarantien, den Grundgedanken von Open Government Data in einem modernen demokratischen Staat als grundsätzliche rechtliche Verantwortung anstelle einer freiwilligen Serviceleistung aufzufassen. *(Kapitel 3.3., Christof Tschohl)*

- Soziale Netzwerke entwickeln sich vermehrt zu öffentlichen und quasi-öffentlichen Räumen; dort gelten dann nicht mehr (nur) die Allgemeinen Geschäftsbedingungen, sondern verstärkt auch öffentliches Recht und Menschenrechte. *(Kapitel 3.4., Matthias C. Kettemann)*
- Neue Kommunikationstechnologien haben das vermeintliche Potenzial, Menschen in einer computervermittelten Weltöffentlichkeit zusammenzubringen. Diese Entwicklungen machen es nötig, den Blick verstärkt auf die neuen Typen struktureller Ungleichheit zu lenken, die diese Technologien mit sich bringen. *(Kapitel 3.5., Stephan Schlögl)*
- Die Komplexität des Internets, die grundsätzlich keine geographischen Grenzen kennt, macht in Fällen wie der juristischen Verfolgung von Hassreden, den Schutz von Menschenrechten besonders herausfordernd. *(Kapitel 3.6., Viktor Szabados)*

4. Umfassende und gleichberechtigte Beteiligung an der Informationsgesellschaft verlangt Internet-Bildung, eine Öffnung exklusiver Wissenslandschaften, eine sozial informierte Bewirtschaftung der Internet-Allmende und proaktive Maßnahmen zur Überwindung bestehender und sich vertiefender sozialer digitaler Gräben, gerade auch innerhalb eher homogener Gesellschaften.

- Digitalisierung erleichtert die politische Partizipation. Allerdings nicht für alle: Menschen, die wenig technisches Grundwissen besitzen, werden weiterhin wenig wahrgenommen. Technologie hilft der Öffnung der Gesellschaft nur, wenn sie von allen genutzt und verstanden wird. *(Kapitel 4.1., Michael Bauer)*
- Wer aktiv an den Möglichkeiten des Internets teilnehmen möchte, braucht Fähigkeiten auf den Gebieten des Informationsmanagements, der Medienproduktion sowie des

Identitäts- und Netzwerkmanagements. Diese Kompetenzen zu vermitteln, ist daher auch eine der wichtigsten Aufgaben eines Bildungssystems. *(Kapitel 4.2., Julian Ausserhofer und Heinz Wittenbrink)*

- Kinder nutzen das Internet zunehmend häufig und unabhängig von der Aufsicht Erwachsener – unter anderem aufgrund mobiler Zugänge. Die bislang konzentrierte Anwendung von Kriterien wie Nutzungsdauer und -häufigkeit zur Beurteilung, was als problematischer Internetkonsum gewertet wird, greift daher zu kurz und gehört neu überdacht. *(Kapitel 4.3., Judith Schossböck)*
- Durch Abonnement-Modelle und technische Schutzmaßnahmen lassen sich die Zugänge zu digitalen Medien jederzeit, überall und völlig legal steuern, einschränken oder verhindern. Der öffentlich-gesellschaftliche Auftrag von Wissenseinrichtungen ist damit durch privat-kommerzielle Interessen gefährdet. *(Kapitel 4.4., Joachim Losehand)*

5. Das Internet befördert sozialen Aktivismus und politisches Engagement durch Transparenz, die Nivellierung von Partizipationshindernissen und Informationsfreiheit. Dabei kann Online-Aktivismus zivilgesellschaftliches Engagement auch in Offline-Kontexten unterstützen, aber nicht ersetzen.

- Internationale Menschenrechtsgerichte schützen vermehrt die Aktivitätenvielfalt im Internet; nationale Behörden müssen diese Leitlinien beachten und Internetnutzerinnen und -nutzer können in vielen Bereichen auf richterlichen Schutz zählen – auch wenn noch viel Sensibilisierung nötig ist. *(Kapitel 5.1., Matthias C. Kettemann)*
- Technologie alleine ist keine Lösung, spielt aber eine wichtige Rolle zur Beurteilung und zum Schutz von Privatsphäre und Menschenrechten im Internet. Technologische Gegenmodelle im

Sinne von „Privacy-By-Design“-Lösungen können Abhilfe schaffen. *(Kapitel 5.2., Markus Sabadello)*

- Online-Videoübertragungen erhöhen für viele Menschen die Zugänglichkeit von Parlamenten. Sie sind ein Schritt hin zu mehr Transparenz in der Politik und damit Vorraussetzung für politische Partizipation. *(Kapitel 5.3., David Röthler)*
- Crowdfunding ist der Zwischenschritt vom Clicktivism zu aktiver Beteiligung, weil durch die finanzielle Unterstützung Projekte konkret umgesetzt werden können. *(Kapitel 5.4., Wolfgang Gumpelmaier)*
- Die nationale Aufrüstung erhöht das Risiko für die Zivilgesellschaft. Im Zuge der Vernetzung und Digitalisierung der Welt steigt die Verletzlichkeit und Abhängigkeit von IT-Systemen. Vergessen wird, dass sich im digitalen Raum nationale Grenzen, Verantwortlichkeiten und Zuständigkeiten auflösen. Zu fordern ist ein umfassender Cyberpeace-Ansatz, um Konflikten vorzubeugen. *(Kapitel 5.5., Sylvia Johnigk)*

Teil 1:
Macht und Recht

1.1. Ethik, Recht und Menschenrechte (Christof Tschohl)

Der Zusammenhang von Ethik und Recht und die Rolle der Menschenrechte

Keywords: Menschenrechte, Ethik, Recht, Philosophie, Gesellschaftsvertrag

1. Die Ideengeschichte der Menschenrechte 17
2. Von der Legitimation staatlicher Gewalt 21
3. Vom Abwehrrecht zum Gewährleistungsanspruch 23
4. Der Gesellschaftsvertrag in der Netzpolitik 24

1. Die Ideengeschichte der Menschenrechte

„Alle Menschen sind frei und gleich an Würde und Rechten geboren", lautet Artikel 1 der *Allgemeinen Erklärung der Menschenrechte* vom 10. Dezember 1948 der Vereinten Nationen. Diesen Grundsatz erkannte die Philosophie der Aufklärung bereits im 18. Jahrhundert, dennoch sollte es beinahe 200 Jahre dauern, bis sich die Menschheit über die Organisation der Vereinten Nationen darauf einigen konnte, ihn auch als obersten Rechtssatz zu formulieren. Die Maxime der unantastbaren Menschenwürde beansprucht universelle Geltung, und zwar nach Artikel 2 der *Allgemeinen Erklärung der Menschenrechte* „ohne irgendeinen Unterschied, etwa nach Rasse, Hautfarbe, Geschlecht, Sprache, Religion, politischer oder sonstiger Überzeugung, nationaler oder sozialer Herkunft, Vermögen, Geburt oder sonstigem Stand." Die Achtung der Menschenwürde ist Wurzel und Leitlinie für alle in der Folge formulierten Menschenrechte. Freilich ist damit noch keine Aussage darüber getroffen, in welchem Maß die Nationen der Erde diese Verpflichtung des Völkerrechts auch in die Realität umge-

setzt haben, doch allein die normative Einigung ist schon ein Meilenstein der geistigen Evolution. Damit ist jedenfalls das oberste Prinzip der Moral formuliert und dieses mit universellem Geltungsanspruch zugleich im Recht verankert. Doch welche Rolle spielt es, dass Recht und Moral im Einklang stehen?

Um dieser Frage nachzuspüren, erscheint es nützlich, das philosophische Gedankenexperiment des „Gesellschaftsvertrages" etwas näher zu betrachten. Die Theorien zum Gesellschaftsvertrag sind von der Motivation getragen, die Legitimation des Systems von Autorität und Recht innerhalb einer Gesellschaft auf moralischer Ebene zu begründen. Diese Überlegungen standen somit im Gegensatz zum schlichten Glauben an die Autorität, der in der Neuzeit lange vom göttlichen Herrschaftsanspruch feudaler Herrscher geprägt war und im Zweifel mit physischer Gewalt durchgesetzt wurde. Die Überlegungen zum Gesellschaftsvertrag versuchen demgegenüber, die Legitimation auf die von Vernunft getragene Zustimmung aller Individuen zu stützen. Ausgangspunkt ist dabei ein hypothetisch gedachter „Naturzustand" des Menschen, der allerdings bei den verschiedenen Philosophen auch völlig unterschiedlich aussieht.

Thomas Hobbes (1588–1679) etwa ging davon aus, dass in einem hypothetischen Naturzustand völlige Anarchie herrsche, die in einen „Krieg aller gegen alle" münde. Der Bürgerkrieg zwischen Anhängern des Königs einerseits und des Parlaments andererseits im England des 17. Jahrhunderts prägte das Menschenbild des Gelehrten Hobbes dabei wohl nachhaltig. In seinem berühmten Werk „Leviathan" formuliert Hobbes 1651 entsprechend seine Variante des Gesellschaftsvertrages, durch den sich die Menschen aus dem unerträglichen Naturzustand freiwillig in einen geordneten Gesellschaftszustand begeben. Hobbes spricht den Menschen dabei eine allumfassende gleichverteilte Freiheit zu, die den Individuen jedoch nur garantiert werden kann, indem das Gewaltmonopol an einen allmächtigen Herrscher delegiert wird, der die Einhaltung der Gesetze durchzusetzen

vermag. Damit begründete Hobbes eine Theorie des aufgeklärten Absolutismus. Revolutionär war dabei der Gedanke, dass der Herrschaftsanspruch nicht durch Gottes Gnaden via Erbfolge, sondern durch die unbeschränkte Autonomie der Individuen legitimiert ist, welche allerdings bewusst und zum Wohle aller an eine übergeordnete allmächtige Instanz – bildlich eben den Leviathan – übertragen wird.

Vor demselben historischen Hintergrund verfasste auch *John Locke* (1632–1704) seine Theorien zum Gesellschaftsvertrag, denen zufolge die Staatsgewalt ebenfalls aus der freien gegenseitigen Übereinkunft entspringt. Freiheit, Gleichheit und Unverletzlichkeit von Person und Eigentum entspringen nach Locke dem Naturrecht und werden im Gegensatz zur Theorie von Hobbes auch durch den „Eintritt" in den Staat nicht aufgehoben. Dieser hat vielmehr die Aufgabe, diese Rechte zu sichern und zu schützen. In seinem politischen Hauptwerk „Two Treatises of Government", erschienen im Jahr 1690, begründet Locke, dass die Regierung den Menschen zu dienen habe und die Macht des Herrschenden daher eingeschränkt sein soll.

Bemerkenswert ist, dass er zur Sicherung dieser Freiheiten die Trennung der gesetzgebenden und der ausübenden Gewalt fordert. Auch der Herrscher steht bei Locke nicht über dem Gesetz und verliert durch Missbrauch seiner Gewalt den Legitimitätsanspruch. Insofern werden in den Schriften Lockes erstmals die Ansätze des modernen Konstitutionalismus, also der durch eine Verfassung gleichsam legitimierten wie eingeschränkten Staatsgewalt, ausführlich begründet.

Diese Idee wurde 1748, also knapp 60 Jahre später, von *Montesquieu* (1689–1755) in seinem zentralen Werk „Vom Geist der Gesetze" aufgegriffen. Dieser pflegte bei seinen Reisen stets eine große Truhe mitzuführen, in der er die Schätze geistiger Erkenntnisse sammelte, auf die er bei seinen Studienreisen gestoßen war. Unter ihnen befanden sich auch die Schriften Lockes, dessen Ansätze zur Gewaltenteilung er noch erweiterte, indem er nicht nur die Trennung von Legislative und Exekutive postulierte, sondern zusätzlich auch die Unabhängigkeit der

Judikative von den anderen Gewalten als wesentliche Bedingung der Freiheit formulierte. In dieser Form ist noch heute die Lehre von der Gewaltenteilung bekannt, die zumeist ausschließlich Montesquieu zugeschrieben wird, aber schon bei Locke ihre Wurzeln hat.

Jean-Jacques Rousseau (1712–1778), einer der geistigen Väter der Französischen Revolution, ging in seiner Gesellschaftsvertragstheorie von einem weitaus positiveren Menschenbild aus. Aus einem an sich friedlichen, geradezu tierähnlichen Naturzustand wird der Mensch nach Rousseaus Ansicht gleichsam herausgerissen, nachdem sich das Konzept des Privateigentums durchsetzt, das die Menschen in Klassen spaltet. Um zur Freiheit zurückzukehren, die dem Menschen im Naturzustand eigen ist, ordnet sich jeder Bürger freiwillig einem rechtmäßig geordneten gesellschaftlichen Zusammenleben unter. Die Grundlage des Gesellschaftsvertrags ist der Gemeinwille, der auf das Wohl des ganzen Volkes gerichtet ist. Im Gegensatz zu Montesquieu will Rousseau das Volk dabei in allen Bereichen miteinbeziehen und nicht nur auf die Mitwirkung in der gesetzgebenden Gewalt (Legislative) beschränken.

Nach *Immanuel Kant* (1724–1804), einem der bedeutendsten Philosophen der Aufklärung, entwickelt sich die Vernunft im Zusammenleben der Menschen, aus der weiter das Recht entsteht, welches die Gesellschaftsordnung schrittweise zunehmend bestimmt. Dies führt schließlich zu einer vollkommenen bürgerlichen Verfassung. Dabei formuliert Kant mit dem „Kategorischen Imperativ“ die entscheidende Prämisse für die weitere Entwicklung der Grund- und Menschenrechte: Die angeborene, unabhängig vom positiven Recht existierende Würde des Menschen. Unter den verschiedenen Formulierungen des Kategorischen Imperativs erscheint die „Menschheitszweckformel“ am anschaulichsten: *„Handle so, dass du die Menschheit sowohl in deiner Person, als in der Person eines jeden andern jederzeit zugleich als Zweck, niemals bloß als Mittel brauchst.“*

2. Von der Legitimation staatlicher Gewalt

Die eben dargestellten Theorien zum Gesellschaftsvertrag haben gemeinsam, dass sie den Legitimationsanspruch staatlicher Gewalt nicht allein durch den Rückgriff auf rein religiöse Glaubensdogmen, sondern vielmehr durch Vernunft und Ethik zu begründen versuchen. Viele der solcherart im Zeitalter der Aufklärung entwickelten Ideen fanden schließlich Eingang in die ersten systematischen Zusammenfassungen in ein Gesetzeswerk (Kodifikationen) der Menschenrechte, allen voran die *französische Erklärung der Menschen- und Bürgerrechte 1789* am Höhepunkt der Französischen Revolution. Im Zentrum stand dort die angeborene gleichverteilte Freiheit aller Individuen, die sich in einem demokratischen Staat zusammenschließen, wobei die Kodifikation der Menschenrechte als Verfassung im Rechtsstaat zugleich Legitimation und Schranken der – auf verschiedene Institutionen aufgeteilten – staatlichen Gewalt bildet.

Es sollte noch ein weiteres Jahrhundert dauern, bis sich die Idee des Konstitutionalismus auch auf die größten Teile des restlichen Europas ausbreitete. Im Vordergrund der Entwicklung des 19. Jahrhunderts stand dabei der Kampf des aufkommenden Bürgertums gegen einen übermächtigen, reaktionären, monarchischen und absolutistischen Staat. Zwar fanden einige Ideen der Aufklärung schon Eingang in die ersten umfassenden Kodifikationen des Zivilrechts[1], allerdings regelten diese Normen die Rechtsbeziehungen der BürgerInnen untereinander, während der monarchische Herrscher noch außerhalb stand und seinen Anspruch auf absolute und letztlich willkürliche Herrschaft von Gottes Gnaden ableitete. Die revolutionäre Forderung nach kodifizierten Grundrechten stellte diesen Anspruch in Frage.

---

[1] So fand sich beispielsweise innerhalb der K. und K. Monarchie im Allgemeinen Bürgerlichen Gesetzbuch (ABGB) von 1811 die Norm in § 16: „*Jeder Mensch hat angeborne, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten. Sclaverey oder Leibeigenschaft, und die Ausübung einer darauf sich beziehenden Macht, wird in diesen Ländern nicht gestattet.*“

Als sich die revolutionären Kräfte in der zweiten Hälfte des 19. Jahrhunderts schließlich auch in der Donaumonarchie durchsetzten, resultierte dies in der Dezemberverfassung von 1867, mit der unter anderem die demokratische Mitbestimmung durch die Mitwirkung des Reichsrathes bei der Gesetzgebung sowie ein Grundrechte-Katalog konstituiert wurden. Das „Staatsgrundgesetz vom 21. Dezember 1867 über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder" (StGG) – welches in Österreich noch heute in Kraft ist – war vor allem darauf ausgelegt, einen *Abwehranspruch gegen willkürliche Akte der Vollziehenden Gewalt* zu begründen, die nach wie vor ein Vorrecht des Kaisers war. Nicht verwirklicht war im StGG allerdings die Idee, dass auch dem (demokratisch legitimierten) Gesetzgeber durch Grundrechte materielle Schranken auferlegt werden sollten. Vielmehr wurde die Zulässigkeit eines Eingriffs in die dort formulierten Grundrechtspositionen grundsätzlich daran gebunden, dass dieser auf einem formellen Gesetz zu beruhen hat. Weitere inhaltliche Grenzen wurden zu diesem Zeitpunkt nicht geschaffen, das Vertrauen in die Gerechtigkeit der unter demokratischer Beteiligung entstehenden Gesetze bei gleichzeitiger Bindung der Vollziehung an diese Gesetze schien sehr hoch.

Die Unrechtserfahrungen des 20. Jahrhunderts, vor allem des verbrecherischen Regimes des Nationalsozialismus, zeigten jedoch, dass der *Rechtsstaat alleine* bei weitem *keine hinreichende Garantie* dafür ist, dass formelles positives Recht automatisch zu Gerechtigkeit führt. Gerade die Nationalsozialisten legten großen Wert darauf, ihren Machenschaften durch entsprechende formelle Rechtsnormen den Anschein der Legitimation zu verleihen. Insofern war selbst Hitlers Deutsches Reich ein Rechtsstaat, allerdings weder ein demokratischer noch ein gerechter.

Dies führte beim Wiederaufbau nach 1945 zur Einsicht, dass Menschenrechtskataloge nicht nur den jeweiligen Schutzbereich formulieren sollten, sondern darüber hinaus durch eindeutige materielle

Schranken auch den Gesetzgeber binden sollten. Dementsprechend enthält beispielsweise die *Europäische Menschenrechtskonvention (EMRK) von 1950* zu jeder Bestimmung eine – wenngleich auch sehr abstrakt formulierte – Aufzählung von Zielen, die in einer demokratischen Gesellschaft als legitim gelten. Auf diese Weise lässt sich zumindest auf der normativen Ebene absichern, dass die Kernidee der Legitimation durch Menschenrechte als oberste Prinzipien aufrecht bleibt und schutzwürdige Interessen einer Minderheit nicht einfach durch (demokratische) Entscheidungen der Mehrheit verletzt werden.

3. Vom Abwehrrecht zum Gewährleistungsanspruch

Die weitere Entwicklung der Menschenrechte hat sich seitdem vor allem durch die Rechtsprechung unabhängiger Höchstgerichte gewissermaßen von den rein politischen Prozessen erfolgreich emanzipiert. So wurde etwa die EMRK durch den Europäischen Gerichtshof für Menschenrechte (EGMR) so ausgelegt, dass diese nicht nur ungerechtfertigte Eingriffe verbietet, *sondern den Staat unter Umständen auch zum positiven Handeln zwingt*. Auf diese Weise wurde die Idee entwickelt, dass aus den Menschenrechten umfassende *Gewährleistungsansprüche* erwachsen, die auf eine effektive Durchsetzung der Garantien abzielen. Dabei hat der Staat durch entsprechende Gesetze und Institutionen auch dafür zu sorgen, dass die Menschenrechte auf der horizontalen Ebene – also die Beziehungen der Menschen untereinander betreffend – ebenfalls ihre Wirksamkeit entfalten können.

Modernere Entwicklungen gehen noch einen Schritt weiter und formulieren *wirtschaftliche, soziale und kulturelle Rechte als Leistungs- und Teilhabeansprüche*. In diesem Zusammenhang ist auch die Rede von „Menschenrechten der zweiten Generation". Darunter fallen beispielsweise das Recht auf Bildung, das Recht auf bezahlte Arbeit, gleicher Lohn für gleichwertige Arbeit oder auch das Recht auf soziale Sicherheit. Die EU-Grundrechte-Charta, die seit Dezember 2010

rechtsverbindlich ist, enthält hier gegenüber der EMRK schon deutliche Erweiterungen.

Wenig ruhmreich ist die Geschichte der Menschheit bislang hinsichtlich der Forderung der Länder des globalen Südens nach *kollektiven sozialen Rechten der Völker*, die in Artikel 28 der Allgemeinen Erklärung der Menschenrechte eine Stütze findet. Die kollektiven sozialen Rechte, sogenannte „Menschenrechte der dritten Generation", hätten das Potential, den Gedanken der Legitimation und Friedenssicherung durch Menschenrechte auch auf globaler Ebene nachhaltig zu implementieren. Zunächst besteht kein unmittelbarer Zusammenhang zwischen diesen Rechten und dem Einsatz von Informationstechnologie (IT). Die globale internationale Vernetzung durch das Internet kann aber wesentlich dazu beitragen, die Maxime der *gleichen Freiheit und Würde aller Menschen* für mehr als nur einen kleinen wohlhabenden Teil der Weltbevölkerung zu realisieren. Insbesondere der erleichterte Zugang zu Informationen aller Art und damit in Zusammenhang stehend bessere Bildungschancen, aber auch mehr Transparenz für faire Handelsbeziehungen haben unmittelbare Auswirkungen auf das soziale Niveau und die Entwicklungschancen von Gesellschaften, die aufgrund historischer wie gegenwärtiger Umstände nicht angemessen am – prinzipiell bestehenden – globalen Wohlstand partizipieren. Die technischen Voraussetzungen, die Möglichkeiten der Informationstechnologie in diesem Sinne zu nutzen, stehen eigentlich schon zur Verfügung, die Globalisierung der Idee des Gesellschaftsvertrags kommt bislang allerdings noch nicht richtig vom Fleck.

4. Der Gesellschaftsvertrag in der Netzpolitik

Das Modell des US-amerikanischen Philosophen *John Rawls* (1921–2002), dem bekanntesten zeitgenössischen Denker der Gesellschaftsvertragstheorien, lässt die Menschen hinter einem Schleier des Nichtwissens darüber nachdenken, welche Gesellschaftsordnung aus ihrer Sicht die gerechteste ist, wobei keine/r der Teilnehmenden weiß, wie

und wo er/sie in der Gesellschaft später verortet sein wird. Dieses Gedankenexperiment erscheint sehr passend zur Natur des Internets und ist es schon deshalb jedenfalls Wert, weiter gedacht zu werden. In sozialen Netzwerken im Internet, dem sogenannten Web 2.0, stehen sich NutzerInnen regelmäßig unabhängig von ihrer Herkunft und ihren wirtschaftlichen Möglichkeiten als freie und gleiche Individuen gegenüber. Diese Grundhaltung sollte sich durch jeden Ansatz staatlicher oder internationaler Regulierung des Internets ziehen, um jeder Art von regulierenden Eingriffen in das – grundsätzlich nicht hierarchische – System des globalen Informationsnetzwerks jene Legitimation zu verleihen, die der Idee des Gesellschaftsvertrags immanent ist. Aus diesem Ansatz ergeben sich konkrete Konsequenzen, beispielsweise im Sinne eines klaren Bekenntnisses zur Netzneutralität (vgl. Tassilo Pellegrini, Kapitel 3.2. *Netzneutralität*). Die Grund- und Menschenrechte in ihrer Eigenschaft als Wertvorstellungen und Orientierungsnormen sind jener Raster, auf den sich die globale Gemeinschaft in Form der Vereinten Nationen im Rahmen der Allgemeinen Erklärung der Menschenrechte im Jahr 1948 in einem bislang historisch geradezu einzigartigen Akt einigen konnten. Alle aktuell und künftig anstehenden Maßnahmen der Netzpolitik auf nationaler und internationaler Ebene müssen sich daher an diesem Raster messen lassen, um grundsätzlich als legitim in einer modernen Informationsgesellschaft zu gelten. Die Praxis zeigt in dieser Hinsicht jedenfalls noch großen Aufholbedarf.

1.2. Rechte eines jeden Menschen _am_ Internet (Hans Christian Voigt)

Ein Plädoyer für die generelle Forderung nach gleichberechtigter Mitbestimmung bei der Regelung und Verwaltung des Internets

Keywords: Menschenrechte, Zugang, Infrastruktur, Mitbestimmung, Regulierung, Macht, Teilhabe

1. Recht oder Privileg? 27
2. Begründungen des Rechtsanspruchs 28
3. Des Internets Metamorphosen 30
4. Asymmetrien verstärkend oder entschärfend? 32
5. Abwehr- und Teilhaberechte 34
6. Das für jeden Menschen Wesentliche am Internet 37
7. Conclusio 41

1. Recht oder Privileg?

Debatten zu Internet und zu Menschenrechten gibt es seit geraumer Zeit. Die Formulierung der gesellschaftlichen Forderung eines allgemeinen Rechts auf Zugang zum Internet ist beinahe so alt wie das Internet selbst. Wirft mensch die Suchmaschinen an und beginnt „*internet*“, „*access*“ und „*right*“ einzugeben, so werden Auto-Ausfüllfunktionen vielleicht zusätzlich „*human right*“ oder „*or privilege*“ vorschlagen. Die Suchtreffer verweisen jedenfalls darauf, dass diese Diskussion auf vielen Ebenen geführt wird, dass die Vereinten Nationen offensichtlich der Ansicht sind, der Zugang zum Internet sei ein fundamentales Recht, und dass einzelne Staaten ein entsprechendes Recht bereits kodifiziert haben. Die Frage, ob es angesichts des Inter-

nets neuer Menschenrechte bedarf, ist also in der einen und anderen Form schon ein paar Mal beantwortet worden. Sie wurde 2003 am ersten *World Summit on the Information Society*[1] diskutiert und ist auch auf der Ebene der Vereinten Nationen bis heute Thema. Sie wird weiter gestellt werden. Sie wird noch des Öfteren in die eine oder andere Richtung beantwortet werden.

Matthias C. Kettemann legte in *Neue Menschenrechte für das Internet? (*Kapitel 2.1.) dar, dass er aus juristischer Perspektive die Notwendigkeit neuer Menschenrechte für das Internet nicht sieht. Vielmehr müsse um- und durchgesetzt werden, dass *was offline gilt, auch online gelten muss*. Es gilt den errungenen Menschenrechten erster, zweiter und dritter Generation zur Durchsetzung zu verhelfen (siehe Christof Tschohl, Kapitel 1.1. *Ethik, Recht und Menschenrechte*).

So stimmig diese Sicht und so wichtig dieser Zugang ist, so komme ich angesichts der grundlegenden Fragestellung doch zu einem anderen Schluss: Die Formulierung und Etablierung von universalen Rechten eines jeden Menschen in Bezug auf das Internet wären ein immenser gesellschaftlicher Fortschritt. Es wäre zu hoffen, und das durchaus im Sinne der Parolen der Französischen Revolution und aus der Perspektive der Menschenrechte, dass die politischen, ökonomischen, kulturellen und also gesamtgesellschaftlichen Kämpfe zur Durchsetzung dieser Rechte irgendwann erfolgreich sind.

Welche Rechte jeder und jedes Einzelnen am Internet alleine vor dem Hintergrund der Menschenwürde abgesichert sein sollten und warum es sich lohnen würde, für die Rechte aller am Internet zu kämpfen, soll im Folgenden entwickelt werden.

2. Begründungen des Rechtsanspruchs

Das Recht auf Zugang soll absichern helfen, dass niemand gegen den eigenen Willen vom Internet ausgeschlossen werden kann. Dass ein

[1] vgl. http://www.itu.int/wsis/index.html (Letzter Aufruf: 15.4.2013)

erzwungener Ausschluss vom Internet eine eminente Benachteiligung darstellt, ist im zweiten Jahrzehnt des einundzwanzigsten Jahrhunderts nicht mehr bestreitbar. Frühe Forderungen aus den 1990er Jahren zeigen, dass diese Entwicklung lange absehbar war und früh gesehen wurde. Die dominante Argumentationslinie für das Recht auf Internetzugang stellt, damals wie heute, den ungehinderten Zugang zu Information (Informationsfreiheit) und das Recht auf freie Meinungsäußerung sowie deren Bedeutung für liberale demokratische Gesellschaften in den Vordergrund: Das Internet als Informations- und Publikationsraum, der für die Teilhabe an gesellschaftlichen Debatten und an politischen Meinungsbildungsprozessen grundlegend geworden ist. Folgen wir der Argumentation von Matthias C. Kettemanns Beitrag (Kapitel 2.1. *Neue Menschenrechte für das Internet?*) in diesem Band, müsste tatsächlich von den bestehenden Menschenrechten der Informationsfreiheit und dem Recht auf freie Meinungsäußerung ableitbar sein, dass niemandem der Zugang zum Internet prinzipiell verwehrt werden darf, weil das diese universalen Rechte verletzen würde. Internetsperren widersprechen demnach eigentlich fundamentalen Menschenrechten (siehe Jana Messerschmidt, Kapitel 2.3. *Internetsperren und Menschenrechte*).

Der Fokus auf Informations- und Meinungsfreiheit lässt in den Hintergrund treten, dass es „das Internet" auch für eine Reihe anderer Menschenrechte braucht. Es steht heute im Rang grundlegender Infrastruktur, ähnlich dem Post- und Verkehrswesen oder der Strom- und Gasversorgung. Wer keinen Zugang hat und wer keine E-Mail-Adresse nutzen kann, ist in unserer Gesellschaft schlechter gestellt als andere und diese Benachteiligung geht soweit, dass unfreiwillige Internetferne als ein Indikator für Segregation gelten kann. Über keine E-Mail-Adresse verfügen zu können steht in einer Reihe mit *kein Bankkonto haben* und *keine Telefonnummer angeben können* für gesellschaftlichen Ausschluss.

„Das Internet“ in seiner gegenwärtigen Form ist essentiell für das Recht auf Bildung, das Recht auf Arbeit, das Recht auf Teilhabe am kulturellen Leben, das Recht auf Selbstbestimmung der Völker, das Recht auf Entwicklung, um nur die offensichtlichen Menschenrechte zu nennen, die ohne Zugang zum Internet für viele nicht (mehr) sicher gestellt sind. Freilich stellt das Internet in seiner gegenwärtigen Form auch eine Bedrohung grundlegender Rechte dar, vorrangig der Persönlichkeitsrechte und des Rechts auf Freiheit vor willkürlichen Eingriffen in die Privatsphäre (vgl. Thomas Kreiml, Kapitel 1.5. *Das Internet in der arbeitsrechtlichen Kampfzone*; Christof Tschohl, Kapitel 2.4. *Paradigmenwechsel Vorratsdatenspeicherung*; Andreas Krisch, Kapitel 2.5. *Die Reform des EU Datenschutzrechts*).

3. Des Internets Metamorphosen

„Das Internet“ ändert sich. Es ist schwierig zu sagen, was das Internet auch nur gegenwärtig ist, geschweige denn, wie es in drei, in fünf oder erst recht in zwanzig Jahren aussehen und in seiner ganzen Komplexität funktionieren wird. Zur Zeit der frühen Forderungen nach einem Menschenrecht auf Internetzugang konnte möglicherweise etwas wie ein Breitbandanschluss oder ein Internet of Things (IoT)[2] antizipiert werden, aber unmöglich die gesellschaftliche Bedeutung von Google oder Facebook (s. dazu auch Matthias C. Kettemann, Kapitel 3.4. *Ist Facebook ein neuer öffentlicher Raum?*), die Entwicklungen eines SEO-Gewerbes[3], der Branchen der Social Media Manager[4] oder der „Data Dealer“[5], die Emergenz neuer gesellschaftlicher Modi der Selbstorga-

[2] vgl. http://de.wikipedia.org/wiki/Internet_der_Dinge (Letzter Aufruf: 15.4.2013)
[3] vgl. http://de.wikipedia.org/wiki/Suchmaschinenoptimierung (Letzter Aufruf: 15.4.2013)
[4] vgl. http://de.wikipedia.org/wiki/Social_Media_Manager (Letzter Aufruf: 15.4.2013)
[5] vgl. http://www.zeit.de/digital/games/2012-03/spiel-data-dealer/komplettansicht (Letzter Aufruf: 15.4.2013)

nisation wie im Fall von *Anonymous*[6], beim *GuttenPlag*[7] oder – früher – einer *Wikipedia*.

Das, wozu wir Zugang haben und wofür wir für alle Menschen gleichermaßen ein allgemeines Zugangsrecht sichern wollen, weil es für die Freiheiten der Einzelnen und für die demokratische Verfassung aller so elementar ist, das bleibt über die Zeit hinweg nicht stetig identisch. Mit diesem Gedanken schiebt sich ein unangenehmer Verdacht ins Blickfeld. Was, wenn „das Internet" irgendwann nicht mehr dieses „das Internet" ist, dem wir diese Bedeutung zumessen. In den letzten Jahren häufen sich die Warnungen vor einem drohenden „Ende des freien Internets" (zur Verifizierung einfach die Phrase in eine Suchmaschine eingeben).

Heute fällt es uns gerade noch schwer, uns einen personenspezifischen vollkommenen Ausschluss vom Internet vorzustellen, ob durch staatliche Gewalt oder die Willkür eines Unternehmens durchgesetzt („*Ich kann immer noch bei jemanden anderen und mit anderen Geräten surfen*"). Dabei könnte das immer konzentriertere Vorgehen gegen Anonymität irgendwann darin enden, dass der Internetzugang ohne biometrische Identifizierung nicht mehr möglich oder erlaubt ist. Dieses eine Beispiel soll lediglich zeigen, dass „das Internet" unsere Vorstellung überfordert, nicht zuletzt weil es in der Menschheitsgeschichte immer noch relativ neu ist. Das, was es ist, entwickelt sich laufend weiter, ebenso das, was es alles bedeutet, was es alles evoziert und so weiter. Wir wissen nicht, was „das Internet" in einiger Zeit sein wird.

Es wäre töricht, für die angesprochenen laufenden Veränderungen dessen, was das Internet ist, automatisch einen Fortschritt im Sinne positiver Weiterentwicklung anzunehmen. „Das Internet" ist im Großen und Ganzen ebenso wie in vielen Teilbereichen Objekt komplexer

---

[6] vgl. http://de.wikipedia.org/wiki/Anonymous_(Kollektiv) (Letzter Aufruf: 15.4.2013)

[7] vgl. http://de.wikipedia.org/wiki/Guttenplag (Letzter Aufruf: 15.4.2013)

gesellschaftlicher Kämpfe und das gleichzeitig auf globaler Ebene ebenso, wie auf transnationalen, auf regionalen und nationalen Ebenen. Wenn „das Internet" sich aber laufend ändert, stellt sich die Frage nach der Tragweite einer Forderung, die sich auf den Aspekt des Zugangs beschränkt. Mitte der 1990er hatte mensch mit einem Internetzugang zu einem anderen Internet Zugang als 2005. Der Begriff „*Web 2.0*" benennt genau diesen Punkt, die Emergenz von etwas Neuem mit neuen Systemlogiken, wodurch etwas entsteht, das nicht mehr so funktioniert und zu verstehen ist wie „vorher". Bald ein Jahrzehnt später unterliegt das Internet weiterhin rasanten Entwicklungen. Und es hat rasante Entwicklungen wie den so genannten „arabischen Frühling" und den tiefgreifenden Strukturwandel des massenmedialen Systems befördert.

Simpel zusammengefasst: Gesellschaft ändert Internet, Internet ändert Gesellschaft. (Wie wäre der Turbofinanzkapitalismus ohne Internet und Glasfaserkabel[8] oder auch: Wie wäre das Internet in seiner gegenwärtigen Form ohne die erste Generation der Freie-Software-Bewegung denkbar?[9])

4. Asymmetrien verstärkend oder entschärfend?

Heute wird allenthalben vom Recht auf Zugang zu Facebook, Twitter oder Youtube gesprochen. Der Ausschluss von einer dieser Plattformen entspricht mittlerweile in einigen Fällen dem, was das Recht auf Internetzugang grundsätzlich verhindern sollte: Den Ausschluss von Informations- und Meinungsfreiheit. In diesen Fällen genügte es nicht, den allgemeinen Zugang zum Internet als Menschenrecht abzusichern. Umgekehrt bliebe auch nicht viel von der Intention über, wenn der allgemeine Zugang irgendwann zu etwas führt, was jede und jeden

---

[8] vgl. http://www.telegraph.co.uk/technology/news/8753784/The-300m-cable-that-will-save-traders-milliseconds.html (Letzter Aufruf: 15.4.2013)

[9] vgl. http://glossar.sozialebewegungen.org/freie-software (Letzter Aufruf: 15.4.2013)

einzelnen – ähnlich dem Zugang zu Radio und Fernsehen – auf wenige, von anderen willkürlich vorgegebene Nutzungmöglichkeiten beschränkt.

Die Formulierung des Rechtsanspruchs, des Rechts auf beziehungsweise *am* Internet, muss strukturellen Wandel mitdenken. Sie sollte dem *Anspruch auf Mitsprache bei der Gestaltung, Regelung und Verwaltung des Internets* gerecht werden. Hiermit findet sich die wesentliche Unterscheidung zu der von Matthias Kettemann in Kapitel 2.1. (*Neue Menschenrechte für das Internet?*) formulierten Position. Es genügt nicht, den bereits geltenden Menschenrechten im Internet zur Durchsetzung zu verhelfen, um das Teilhaberecht an den öffentlichen Diskursen und an politischer Meinungsbildung zu sichern. Es bedarf vielmehr *anerkannte und durchsetzbare Teilhaberechte am Internet selbst*. Nur auf dieser Basis kann, würde ich argumentieren, auf Dauer das Recht jeder und jedes Einzelnen auf Gleichberechtigung unabhängig von Merkmalen wie ethnischer, sozialer oder religiöser Zugehörigkeit, sexueller Orientierung oder Behinderung und unabhängig von Wohlstand, Status oder Weltanschauung gesichert werden. Nur durch Rechte nicht allein *auf* sondern *am* Internet, wird Schutz vor staatlicher wie auch privatwirtschaftlicher Willkür, die Abwehr von Eingriffen in den geschützten Freiheitsbereich der Einzelnen gewährleistet.

Das Internet, und hier braucht es wieder den Zusatz „*in seiner gegenwärtigen Form*“, vergrößert den Handlungsspielraum sowohl der gesellschaftlichen Starken und Mächtigen als auch der sozial Benachteiligten und Schwachen. Den Herrschenden bieten sich ungeahnte Möglichkeiten der Überwachung, Kontrolle und Disziplinierung durch das tief in die Privatsphären hinein operierende Internet. Den Unterdrückten und Ausgebeuteten bietet es Ausgrenzung, Schranken und Repression überbrückende Optionen zur Selbstorganisation, Zusammenarbeit und Organisierung.

In dieser Situation ist es offensichtlich, dass „das Internet“ zum Objekt gesellschaftlicher Kämpfe werden muss. Die asymmetrischen Macht-

verhältnisse in unseren Gesellschaften weltweit und in der Weltgesellschaft allgemein können durch gesellschaftlichen Einfluss auf „das Internet“ und auf das, was „das Internet“ in Zukunft sein wird, in die eine oder andere Richtung beeinflusst werden. Von selbst im Gleichgewicht bleiben, werden sie jedenfalls nicht (und mit Gleichgewicht sei die gegenwärtige Ausgangslage ohne Wertung in die eine oder andere Richtung definiert).

Kurz: Das Internet in zehn Jahren wird die Asymmetrie der Machtverhältnisse gemessen an heute verschärfen oder abschwächen. Hier sehe ich den Auftrag, weitergehende Teilhaberechte am Internet zu fordern, auch um die Abwehrrechte gegenüber jener Seite zu stärken, die am längeren Hebel asymmetrischer Machtverhältnisse agieren kann.

5. Abwehr- und Teilhaberechte

Es gibt ein Beispiel, wo diese Abwehr- und Teilhaberechte im Angesicht des Internets heute schon ableitbar sind. Dieses Beispiel mag ein genuin österreichisches sein und betrifft die Verfassung der Arbeitswelt:

Das Arbeitsverfassungsgesetz[10] gibt dem Betriebsrat als Vertretungsorgan Mitbestimmungsrechte für die Belegschaft und Kontrollrechte gegenüber einer Betriebs- oder Unternehmensleitung. Der Betriebsrat hat ein Verhandlungsmandat und kann Verträge mit der Unternehmensführung abschließen, die dann ein Element der Betriebsverfassung darstellen; zum Beispiel welche Regeln für die Nutzung der Telefonanlage, für den Gebrauch von E-Mails, des Internets oder des Zeiterfassungssystems gelten. Damit wird der Spielraum willkürlicher Maßnahmen, Regelungen und Forderungen des Managements eines Unternehmens gegenüber den im Unternehmen Arbeitenden be-

[10] vgl. http://de.wikipedia.org/wiki/Arbeitsverfassungsgesetz (Letzter Aufruf: 15.4.2013)

schränkt. Den Abschluss einer Betriebsvereinbarung „*Internet*“ (und „*E-Mail*“) kann der Betriebsrat fordern, weil das Internet „*zustimmungspflichtig*“ ist. Das heißt, die gesetzlich vorgesehene Körperschaft Betriebsrat hat das Recht, die Nutzung des Internets im Betrieb von der Zustimmung dieses Organs abhängig zu machen. Zustimmungspflichtig ist die Nutzung des Internets wiederum, weil jede Nutzung per se die Menschenwürde der Mitarbeiterinnen und Mitarbeiter berührt.[11]

Das bedeutet in der Praxis nun lediglich, dass eine Unternehmensführung in Österreich die Internetnutzung nicht rechtens ausgestalten kann wie es ihr beliebt, wenn ein Betriebsrat[12] konstituiert ist und die Mitbestimmungsrechte einfordert. In der Praxis gibt es nicht immer einen Betriebsrat und selbst wenn einer konstituiert ist, wird kaum irgendwo einmal per einstweiliger Verfügung in einem Betrieb das Internet abgedreht, weil dem Betriebsrat der Abschluss einer Betriebsvereinbarung „*Internet*“ verweigert wird, zu der er zustimmen kann. Die Asymmetrie der Machtverhältnisse zwischen Unternehmensführung und Mitarbeiterinnen und Mitarbeitern macht es zudem für erstere leicht, die Rechte zweiterer zu ignorieren. Es ist wahrscheinlich, dass sie bei Missachtung der Persönlichkeitsrechte ohne Konsequenzen davonkommen, weil die Kontrolle der technischen Infrastruktur in den Händen ersterer liegt. Log-Files wie E-Mails sind jederzeit und relativ einfach les- und auswertbar, ohne dass Mitarbeiterinnen und Mitarbeiter das mitbekommen könnten.

Umgekehrt ist es überall die Asymmetrie von Machtverhältnissen, die durch kodifizierte Rechte aller und also auch derer, die sich in der schwächeren Position befinden, beschränkt werden soll. Rechte von Lohnabhängigen oder Rechte von Konsumentinnen und Konsumenten, Rechte eines Vertretungsorgans wie des Betriebs- oder Gemeinde-

---

[11] Josef Cerny et al.: Arbeitsverfassungsrecht. Gesetze und Kommentare 157. Band 3, 4. Auflage, Wien: ÖGB Verlag, S. 152f.

[12] vgl. http://de.wikipedia.org/wiki/Betriebsrat (Letzter Aufruf: 15.4.2013)

oder Nationalrats, Grundrechte allgemein von Bürgerinnen und Bürgern, Menschenrechte – es geht stets um Abwehrrechte gegenüber Machtmissbrauch und um Teilhaberechte. Das konkrete Beispiel aus der Arbeitswelt ist für unsere Frage deshalb von besonderem Interesse, weil hier erstens aus den Menschenrechten etwas zur Regelung des Internets in einem Teilbereich abgeleitet wird und zweitens die Durchsetzung dieser Rechte in geregelter Art und Weise operationalisiert ist. Vor allem aber wird – drittens – aus den Grundrechten jeder und jedes einzelnen das Recht auf Mitsprache an der Regelung des Internets abgeleitet, operationalisiert hier durch die starke Verhandlungsposition der Körperschaft Betriebsrat. Dieser kann für den Geltungsbereich Betrieb die grundlegenden Regeln mitbestimmen, wie das Internet, Zugang, Nutzung, Kontrolle und so weiter im Unternehmen geregelt sind. Und er kann jede Änderung dieser Regeln mitbestimmen.

Vereinfacht können wir von diesem Beispiel aus der Arbeitswelt auf die allgemeine Ebene schließen: „das Internet" berührt sowohl als grundlegende Infrastruktur als auch durch seine technischen Eigenheiten per se mehrere Menschenrechte, weswegen Änderungen an Struktur, Regeln und Verwaltung des Internets „durch uns" zustimmungspflichtig sein müssten, da diese Änderungen wiederum automatisch in unsere Menschenrechte eingreifen und unsere durch Persönlichkeitsrechte mittelbar geschützte Grundrechtssphäre beeinträchtigen können.

Der Umstand, dass das Internet als transnationale Infrastruktur nationale Geltungsbereiche unterläuft, sollte eine weitere Motivation darstellen, den Anspruch auf Teilhaberechte am Internet auf der Ebene der Menschenrechte zu formulieren (vgl. Viktor Szabados, Kapitel 3.6. *Hassreden im Internet*). Nationale Parlamente sind nicht automatisch durch demokratische Wahlen legitimiert, zu Neuregelungen des Internets in unseren Namen zuzustimmen.

Für Teilhaberechte aller am Internet spricht außerdem und nicht zuletzt, dass wir das, was „das Internet“ gegenwärtig ist, nicht der Leistung eines Unternehmens oder dem Staat verdanken, von dem uns diese Infrastruktur zur Verfügung gestellt wird. Es ist weder das Produkt einer Firma, noch ist es natürliche Ressource oder nationalstaatlich organisiertes öffentliches Gut. „Das Internet“ geht vielmehr auf vielschichtige Prozesse gesellschaftlicher Produktion zurück als auf eine unternehmerische Leistung oder staatliche Organisation. Die Forderung auf Zugang muss dem einzelnen Staat gegenüber gestellt werden. Der Rang des Menschenrechts soll diesem Recht lediglich mehr Gewicht beimessen und alle Staaten zwingen, dieses Recht auf Zugang zu schützen. Das kann der Staat auch sehr einfach, fällt die Regulierung des Zugangs doch in seine Domäne. Ein Recht auf Teilhabe am Internet, auf gleichberechtigte Mitbestimmung bei der Regelung und Verwaltung des transnationalen Internets, das kann der einzelne Staat nicht einfach durchsetzen. Umso mehr müsste dieses Recht als universelles Menschenrecht gefordert werden.

6. Das für jeden Menschen Wesentliche am Internet

Wenn das Menschenrecht nicht am Zugang zu Internet festmachen, woran aber dann? Wenn „das Internet“ gesellschaftlich schwer zu fassen und noch schwieriger in einer Definition zu begreifen ist, die den Metamorphosen über Entwicklungszeiträume hinweg gerecht würde, wie dann die Rechte formulieren, die wir alle nur aufgrund unseres Menschseins haben? Für die Vereinten Nationen formuliert die UN-Sonderberichterstatterin Farida Shaheed, zitiert in einer Aussendung der Vereinten Nationen am 18. Mai 2012:

„Da das Internet im Wesentlichen eine globale Ressource darstellt, muss eine angemessene Regelung und Verwaltung des Internets das Recht eines jeden Menschen auf selbstbestimmten Zugang zu Infor-

mation ebenso wie auf selbstermächtigte Nutzung von Information und Kommunikationstechnologien unabdingbar unterstützen.“ [13]

Diese Formulierung geht deutlich über die Forderung eines Rechts lediglich auf Zugang hinaus. Der Zugang und die Nutzung müssen selbstbestimmt und selbstermächtigt möglich sein. Gleichzeitig kann diese Formulierung den Charakter eines Appells an die, die regeln und verwalten, nicht verbergen. Den Regelnden und Verwaltenden wird zwar eine allgemeine Schutzpflicht der Rechte eines jeden Menschen zugesprochen, aber ohne dass die Legitimation dieser unbestimmten Regelnden und Verwaltenden angesprochen oder Bedingungen unterworfen wird.

Ich habe weiter oben bereits vorgeschlagen, mehr, nämlich gleichberechtigte Mitbestimmung und Teilhaberechte am Internet zu fordern. Dazu möchte ich eine Konkretisierung versuchen, welche Aspekte „am Internet“ für jeden Menschen so wesentlich sind, dass es unserer Zustimmung und also Kontrollmöglichkeiten bedarf, wie es geregelt und verwaltet wird. Bislang bin ich der Frage ausgewichen, was das Internet sei. Ich habe es vielmehr samt vorangestelltem bestimmtem Artikel in Anführungszeichen gesetzt und als etwas schwer zu Begreifendes charakterisiert, als etwas im Rang grundlegender, obwohl in der Menschheitsgeschichte noch junger Infrastruktur, vielschichtig und komplex auf Gesellschaft wirkend, während „es“, „das Internet“, gleichzeitig gesellschaftlich produziert und durch widerstreitende gesellschaftliche Gestaltungsansprüche laufend weiter verändert wird. Mit dieser unbestimmten Benennung lässt sich freilich keine haltbare Formulierung eines sinnvollen Rechtsanspruchs gewinnen. Die Defi-

[13] Deutsche Übersetzung aus der Pressemitteilung der Vereinten Nationen vom 18. Mai 2012: „*Internet governance must ensure access for everyone*“; http://www.un.org/apps/news/story.asp?NewsID=42039&Cr=technology&Cr1 (Letzter Aufruf: 15.4.2013)

nition und Beschreibung im Wikipedia-Artikel „Internet“[14] hilft auch nicht weiter.

Ich schlage die Unterscheidung von (mindestens) vier Aspekten und Eigenschaften vor, die meines Erachtens für die Frage der Menschenrechte relevant sind:

> (1) Vermittels Internet werden Daten übertragen, Informationen übermittelt. Es ist Übertragungsmedium.
>
> (2) Im Internet werden Daten gesichert, Informationen archiviert. Es ist Speichermedium.
>
> (3) Mittels Internet kommunizieren Menschen. Es ist Kommunikationsmedium.
>
> (4) Im Internet und via Internet werden Dienste, Plattformen und Organisationen gebaut. Dienste um weitere Dienste, Organisationen, Plattformen zu bauen. Plattformen um weitere Dienste, Plattformen und Organisationen zu gründen. Organisationen um Dienste, Plattformen und Organisationen zu organisieren. Es ist grundlegende Ressource[15] und Infrastruktur[16].

All diese Eigenschaften würde ich als grundlegende bezeichnen, die als solche in einem sich laufend wandelnden Internet erhalten bleiben. Aus diesem Grund schlage ich vor, mit der Forderung von Rechten auf diese grundlegenden Eigenschaften Bezug zu nehmen. Beziehungsweise müssen sie aus der Perspektive der Menschenrechte erhalten werden, sind es doch die für jeden Menschen wesentlichen Dimensionen. Eine Transformation des Internets zum Beispiel in die Richtung, die das selbstermächtigte Bauen von Diensten, Organisationen und Plattformen einschränken oder verunmöglichen würde, käme einem willkürlichen Ausschluss von grundlegenden Ressourcen

---

[14] s. http://de.wikipedia.org/wiki/Internet (Letzter Aufruf: 15.4.2013)
[15] vgl. http://de.wikipedia.org/wiki/Ressource (Letzter Aufruf: 15.4.2013)
[16] vgl. http://de.wikipedia.org/wiki/Infrastruktur (Letzter Aufruf: 15.4.2013)

und von Infrastruktur gleich und würde Rechte wie das auf Arbeit, auf Bildung, auf Teilhabe am kulturellen Leben verletzten. Die prinzipielle Bevorzugung einzelner gegenüber anderer bei der Übertragung von Daten würde beispielsweise das Prinzip der Gleichberechtigung verletzen (siehe dazu auch Tassilo Pelligrini, Kapitel 3.2. *Netzneutralität*).

All diese Eigenschaften betreffen alle Menschen. Für alle Eigenschaften sollten die Prinzipien der Menschenrechte gelten – Universalität, Egalität, Unteilbarkeit. Und dabei ist der Gebrauch des Internets durch die oder den Einzelnen selbst nicht notwendig, um in der eigenen Menschenwürde berührt zu werden. Ähnlich dem Beispiel aus der Arbeitswelt gilt, dass wir alle per se berührt sind, weil unsere beziehungsweise uns betreffende Daten übertragen werden. Weil über uns Daten erfasst und gespeichert werden, Daten unsere Privatsphäre berühren und allzu einfach dazu eingesetzt werden können, unsere Persönlichkeits-, Freiheits- und sozialen Menschenrechte zu verletzen. Weil unsere Kommunikation gestört oder mitverfolgt oder ohne unsere Zustimmung gespeichert wird. Weil unsere Ideen, Produkte, Geschichten und Geschichte gespeichert oder verdrängt werden. Weil unsere Organisation und unsere Art uns zu organisieren ausgegrenzt, angegriffen und kriminalisiert wird.

Weil unsere Möglichkeiten der Datenübertragung, des Speicherns, des Kommunizierens, des Arbeitens, der freien Bewegung und des uns frei Organisierens durch Möglichkeiten staatlicher Repression und kapitalistischer Ausbeutung im Internet und vermittels Internet in einem Maße bedroht sind, dass wir alle – Menschen qua unserer Menschenwürde heute und in Zukunft – mitbestimmen können *müssen*, wie „das Internet" entlang der grundlegenden Eigenschaften (1) Übertragungsmedium, (2) Speichermedium, (3) Kommunikationsmedium sowie (4) Ressource und Infrastruktur geregelt und verwaltet wird.

7. Conclusio

In Abwandlung des bekannten Prinzips „*Öffentliche Daten nützen, private Daten schützen*“ würde ich im Zusammenhang von Internet und Menschenrechten für einen Zugang plädieren, der auf die Formel „*Menschenwürde schützen, Abwehrrechte zur Teilhabe nützen*“ gebracht werden könnte. Damit sei – noch einmal zusammengefasst – Folgendes gemeint:

Das Internet in seiner gegenwärtigen Form ist in komplexen und diversen Prozessen gesellschaftlicher Produktion entstanden, die mehr als zwei Jahrzehnte überspannen und weiter zurückreichen. Mit der Emergenz des sich laufend weiter entwickelnden und bisweilen strukturell wandelnden Internets ist etwas Neues in die Menschheitsgeschichte getreten, dessen globale historische Bedeutung für uns in der Gegenwart noch kaum angemessen bemessen werden kann. Internet verändert unsere Gesellschaften. Die Produktion und Reproduktion „des Internets“ passiert weiterhin in komplexen und diversen gesellschaftlichen Prozessen unter breitester Teilhabe, wird aber gleichzeitig immer mehr von Staatsapparaten und Kapitalinteressen bestimmt und eingegrenzt.

Die eminente Bedeutung des Internets macht es notwendiger Weise zum Objekt von Herrschaftsinteressen, die „das Internet“, seine Funktionen, Eigenschaften und weitreichenden Auswirkungen regulieren und beherrschen wollen (beziehungsweise aus der Perspektive der Herrschaft: müssen). In diesem Umfeld gilt es, die gesellschaftliche Teilhabe am Internet, an der Produktion und laufenden Reproduktion des Internets abzusichern. Vor diesem Hintergrund gilt es, die Rechte jeder und jedes Einzelnen in Hinblick auf das Internet und der Rechte am Internet zu schützen.

Dem Internet wohnt gleichermaßen großes emanzipatorisches wie repressives Potential inne. Angesichts der Komplexität dessen, was das Internet ist und mit Bedacht darauf, dass sich das, was es ist, ändern

und soweit geändert werden kann, dass es zu etwas im Grunde anderem transformiert würde, plädiere ich für das Menschenrecht am Internet.

Diese Forderung hat notgedrungen eine klar globale und historische Perspektive.

Ein Menschenrecht am Internet darf nicht am Zugang zum Internet allein festgemacht werden. Alle Menschen haben das Recht auf selbstermächtigenden Zugang zu Datenübertragung und ein Recht darauf, dass ihre Daten sicher übertragen werden. Alle Menschen haben das Recht auf selbstermächtigenden Zugang zu Datenspeicherung. Alle Menschen haben das Recht auf selbstermächtigende und sichere Kommunikation vermittels Internet. Alle Menschen haben das Recht, die Ressource und die Infrastruktur „Internet" zu nutzen, um im und mit dem Internet selbstermächtigt etwas zu produzieren.

Ein Menschenrecht am Internet muss die für alle Menschen wesentlichen Eigenschaften des Internets als Übertragungsmedium, Speichermedium, Kommunikationsmedium und als Ressource und Infrastruktur benennen und über den allgemeinen Zugang hinaus das Recht auf Mitbestimmung hinsichtlich Struktur, Regeln und Verwaltung für alle diese Eigenschaften festhalten. Auf Basis einer solchen Grundformulierung sollten Ableitungen für konkrete Umsetzungs-, Bemessungs- und Entscheidungsfragen sowie die Übersetzung in konkrete transnationale wie nationale Richtlinien, Gesetzestexte, Verordnungen und Verträge eindeutig operationalisierbar sein. Und eindeutig meint hier, dass in konkreten Fällen schnell klar ist, ob etwas dem Recht aller Menschen am Internet gerecht wird oder nicht.

1.3. Macht Sprache Internet? (Clara Landler)

Über die Verhexung des Verstandes mit den Mitteln der Sprache.

Keywords: Macht, Sprache, Demokratie, Gleichberechtigung

1. Die Macht der Begriffe 43
2. Menschen im Netz 44
3. Rollenspiel UserIn 46
4. Über die Notwendigkeit, mit- und umzudenken 50

1. Die Macht der Begriffe

Sprache ist das mächtigste Mittel der Verständigung zwischen Menschen. Mit ihrer Hilfe entwickeln sich Bilder und Gedanken, sie strukturiert Wissen und Annahmen, ohne sie bleibt selbst die Idee einer Verständigung unvermittelt. Auch wenn es viele Formen des Ausdrucks gibt, sind es die Wörter, die uns zur Verfügung stehen, die bestimmen, was gesagt werden kann – und was unbedacht bleibt. Angesichts des weiten Feldes der Diskurstheorien ist nicht mehr zu bestreiten, welches Gewicht Sprache für unsere Vorstellungen von Realität hat.

Begriffe sind also nie „unschuldig", sondern halten stets deutlich über ihren rein sachlichen Inhalt hinausreichend implizierte Beurteilungen bereit, die wesentlich mitverursachen, in welcher Art und Weise wir die mit ihnen bezeichneten Inhalte bewerten. So finden sich beispielsweise in den Sprach- und Kognitionswissenschaften zahlreiche Arbeiten, die sich mit der engen Verwobenheit von Denken und Sprechen befassen. Wesentlicher Begriff dabei ist die Metapher, da unsere Vorstellungen von Welt in der Regel auf Metaphern basieren, über die

sich entscheidet, wie wir Inhalte „wahr-nehmen“ und deuten. Über die gewählten Sprachbilder lässt sich wesentlich mitbeeinflussen, welche Ansichten mensch sich über Inhalte zu machen pflegt.

Die Kraft des Begriffs *Menschenrechte* lässt sich in diesem Sinne bereits aus seiner Wortzusammensetzung ableiten. *Mensch* ist, trotz seiner historisch belasteten Entwicklung bis heute, zum neutralsten Begriff geworden, den wir für „denkende Wesen“ kennen. Mensch bezeichnet in unserer aktuellen Vorstellung jede/n – egal welches Geschlecht, Alter, Vermögen oder welcher Lebensstil einem Individuum zugeschrieben wird – oder ob jemand BürgerIn eines Landes ist[1]. Rechte stehen in dieser Wortverbindung der Idee eines Naturrechts nahe[2] und sind also das, was jedem Menschen zustehen sollte, das in dieser Deutung nicht eingeschränkt werden kann, ohne die Bedeutung des Begriffs Mensch – und damit die Würde des Menschen – zu verletzen. Auch wenn ihre Durchsetzung zu gewährleisten immer wieder an deutliche Grenzen stößt und von Universalität, trotz ihres Anspruchs, keine Rede sein kann, macht bereits die eingesetzte Wortverbindung und ihre inzwischen etablierten Vorstellungen deutlich, wie unabdinglich eine Vereinbarung in dieser Form zwischen allen und für *alle Menschen* ist.

2. Menschen im Netz

Die Sprache, mit der Internet bezeichnet und im zuvor skizzierten Sinn bedacht wird, hält viele Metaphern bereit, die zwar durchaus zum Denken anregen können – als Bezeichnungen allerdings selten wirklich nutzen. Ihre Bilder sind inhaltlich häufig schlichtweg falsch,

---

[1] Die Bezeichnung BürgerIn impliziert andere Rechte und Pflichten, die unter die Regelungen der Bürgerrechte fallen.

[2] Zur Orientierung vgl. http://de.wikipedia.org/wiki/Naturrecht (Letzter Aufruf: 2.4.2013) und Christof Tschohl, 1.1. *Ethik, Recht und Menschenrechte*.

aber mächtig – man denke nur an immer wieder auftauchende Zuschreibungen wie „das Internet als rechtsfreier Raum“[3].

Einer der deutlichsten und damit vieldiskutiertesten Begriffe der letzten Jahre in diesem Kontext ist jener des *Raubkopierers*[4]. Mit den Werbespots, die diese Bezeichnung einsetzten und zunehmend verbreiteten, kam auch irgendwann zunehmender Widerspruch seitens der netzpolitisch aktiven Szene, die sich an dieser Stelle durchaus empfindsam für die Wahl von Begriffen zeigte. In deutliche Worte gefasst wurde die Problematik „des Raubkopierers“ 2012 vom Journalisten Stefan Niggemeier im deutschen Medium *Der Spiegel*:

„Metaphern sind mächtig. Sie machen einen Sachverhalt nicht nur anschaulich; sie bestimmen fundamental, wie wir ihn wahrnehmen. Bilder werden zu Rahmen, innerhalb deren(sic) wir denken. Das Bild von der Raubkopie ist falsch. Ein Raub ist im Grundsatz das gewaltsame Wegnehmen fremder Sachen. Es lässt sich schon darüber streiten, ob beim ungenehmigten Kopieren jemandem tatsächlich eine Sache weggenommen wird. Ganz sicher aber lässt sich feststellen, dass ihm dabei keine Gewalt angetan wird. Wenn wir von Raubkopieren sprechen, machen wir aus Menschen, die einen Inhalt ungenehmigt nutzen, Gewalttäter. Es wäre eine Illusion, zu glauben, dass der Begriff diese Wirkung nicht hat, nur weil wir das nicht jedes Mal bewusst mitdenken. Schon der Begriff macht die Handlung zu einem indiskutablen Akt und legitimiert drastische Schritte. Selbst das reichte der deutschen Filmindustrie nicht. Sie begann im Jahr 2003, flankiert von der Bundes-Filmförderungsanstalt, eine Kampagne ‚Raubkopierer sind Verbrecher’. ‚Raubkopierer’ wurden wie auf einem Steckbrief dargestellt.“

---

[3] Vgl. beispielsweise Lischka, Konrad: Phrasen-Kritik: Das Internet ist kein rechtsfreier Raum (2009), nachzulesen unter: http://www.spiegel.de/netzwelt/web/phrasen-kritik-das-internet-ist-kein-rechtsfreier-raum-a-632277.html (Letzter Aufruf: 14.4.2013)

[4] Hier im Sinne eines Zitates ausschließlich in seiner männlicher Form verwendet.

Aufschreie wie dieser sind wichtig und richtig, stellen sie doch klar, in welcher Form Debatten geführt werden – beziehungsweise geführt werden sollten. Eine derartig verallgemeinernde Kriminalisierung wie sie beispielsweise an dieser Stelle seitens der Verwertungsindustrie vorgenommen wurde und wird, mag zwar ein Weg sein Grenzen zu markieren und Macht an diesen Grenzen einzufordern, sie bewirkt damit aber eben auch genau das: Fronten, die gegeneinander stehen, einen Machtkampf der Interessen, die schließlich auf einer Seite mittels Rechtsprechung legitimiert werden sollen. Die Kollateralschäden solcher Kämpfe sind kaum zu überblicken und regelmäßig Gegenstand netzpolitischer Diskussionen. Der notwendigerweise mitzubedenkende Umfang solcher Verteilungskämpfe lässt sich bei Christian Voigt, Kapitel 1.2. *Rechte eines jeden Menschen _am_ Internet* nachlesen.

Als etwas weniger gewaltige Metaphern wie jene des Raubkopierers, finden die eingesetzten Begriffe allerdings eher wenig Beachtung. Im Bereich der Netzpolitik ist ein Nachdenken über Menschenrechte ob der üblicherweise verwendeten Begrifflichkeiten für *im Netz aktive Individuen* somit spürbar komplexer. Mehr oder minder „neutrale Begriffe“ wie Mensch oder auch TeilnehmerIn finden nur selten ihren Weg in den alltäglichen Sprachgebrauch, dafür spiegeln sich in den zur Anwendung kommenden Begriffen die allermeisten Probleme aktueller Netzkultur-Debatten wider. Eine Reflexion darüber, welcher Begriff welche Zuschreibungen, Bedeutungen, Rollen sowie Rechte und Pflichten impliziert, ist damit durchaus angebracht.

3. Rollenspiel UserIn

Da ein großer Teil der zur Verfügung stehenden Angebote im Netz den (Spiel-)Regeln kommerzieller Unternehmen unterliegt und daher auch von kommerziellen Interessen geleitet wird, ist nicht weiter verwunderlich, dass der am häufigsten zur Verwendung kommende Begriff für Individuen im Netz „User“ – zu deutsch „Nutzer / Inter-

netbenutzer“[5] – lautet. Die Entstehung und Etablierung des Begriffs sind nicht dokumentiert, angesichts seines semantischen Einzugsgebietes ist es jedoch nicht zu weit hergeholt, ihn auf die zu bezeichnende Rolle zurückzuführen: *Ein User oder Nutzer ist jemand, der eine im Internet bereitgestellte Infrastruktur nutzt*. In diesem Sinn ist der Begriff User(In) noch verhältnismäßig unverfänglich, da er so betrachtet in den meisten Fällen zutrifft.

Ein klein wenig zu haken beginnt diese Interpretation allerdings bereits, wenn man an die Nutzung der Kommentarfunktion klassischer Medien im Internet denkt: Auch im Falle moderierter Kommentare lässt sich die Möglichkeit als UserIn Inhalte zu ergänzen und zu erweitern (oder zu boykottieren, wofür sich die Bezeichnung *Troll* etabliert hat) nicht mehr mit der Funktion des LeserInnenbriefs vergleichen. Die Rollenverteilung AutorIn und LeserIn ist an dieser Stelle längst nicht mehr zu trennen.

Die relevante Grenzverschiebung bezieht sich somit auf das Erstellen von Inhalten, während die technische Infrastruktur dabei in den Hintergrund tritt. Genau an dieser Stelle der Verschiebung beginnt der Begriff UserIn seine Eindeutigkeit zu verlieren. Als reine NutzerIn einer technischen Infrastruktur wären die Machtverhältnisse noch relativ klar, die deutlich aktivere Rolle der inhaltlichen Mitgestaltung allerdings, findet im Begriff UserIn keine echte Referenz.

Die Frage, die sich damit aufdrängt lautet:

Kann der Einsatz eines Begriffes, der den Schwerpunkt seiner Bedeutung auf einer technischen Ebene hat, der aktuellen Entwicklung (und was fast noch wichtiger ist: der Idee) des Internets überhaupt gerecht werden?

---

[5] Das Binnen-I wird hier beabsichtigt weggelassen – da es erfahrungsgemäß im Internet kaum anzutreffen ist. Dies lässt sich als einer von vielen Hinweisen verstehen, wie männlich konnotiert das Internet ist. (Vgl. hierfür in diesem Band: 1.4. Wie männlich ist das Internet?)

Selbst alle möglichen deutschen Übersetzungen des englischen „user“ berücksichtigend, wie NutzerIn, AnwenderIn, BedienerIn, VerbraucherIn, ja sogar BetreiberIn, macht deutlich, dass wirklich aktive Rollen, wie sie beispielsweise in Konzepten wie dem der AktivbürgerIn bestehen, nicht impliziert sind. Stattdessen zeigt sich, dass die am häufigsten implizierte Bedeutung abseits der Bezeichnung der Nutzung einer Infrastruktur jene der KonsumentIn ist. Die Stärke dieser eingebürgerten Bedeutung zeigt sich durch den entsprechend gut etabliert zur Anwendung kommenden KonsumentInnenschutz. Deutlicher Nachteil allerdings ist, dass es keine ebenso etablierten Begriffe für Menschen gibt, die das Internet für zivilgesellschaftliche Interessen nutzen – um zu protestieren oder sich zu organisieren, beispielsweise.

Das zeigt sich umgekehrt betrachtet auch am Fehlen entsprechend positiv konnotierter Begriffe für im Netz (in verschiedenster Hinsicht) gestaltend aktive Menschen. Während es den technischen Bereich betreffend beispielsweise den Begriff des/der HackerIn[6] gibt, der zumindest in netzaffinen Kreisen auch positive Bilder beinhaltet, reduzieren sich die üblichen Begriffe danach rapide. In Frage kommt beispielsweise noch BloggerIn, womit aber wiederum die gesamte Umgebung anderer sozialer Medien (wie Facebook, Twitter und Co.) exkludiert ist. Gerade Soziale Medien aber „leben“ durch die vielfältige Interpretation und Gestaltung ihrer NutzerInnen – und generieren für ihre EigentümerInnen Kapital durch das Sammeln der Daten dieser ihrer „UserInnen“. Damit kommt eine weitere Dimension ins Spiel, die durch die landläufige Bedeutung von „User“ nicht abgedeckt ist und somit vor allem eine offene Frage hinterlässt: Ist der Mensch im Netz als Datenquelle *UserIn einer Infrastruktur* und hat dafür mit ebendiesen Daten als NutzerIn zu bezahlen – oder ist jede einzelne

[6] Dass der Begriff HackerIn in seiner gedenderten Form allerdings so gut wie gar keine Anwendung findet, ist auch für sich genommen bereits eine Aussage. (vgl. Leonie Tanczer, Kapitel 1.4. *Post, Gender, Internet*)

Person vielmehr EigentümerIn der eigenen Daten und kann darüber bestimmen, wieviel sie/er bereit ist, zu „verkaufen", und wo die jeweils persönlichen Grenzen liegen? Die etablierte Nutzung des Begriffs *User* macht es so betrachtet leicht, ein Machtgefälle aufrecht zu erhalten. (Vgl. Matthias C. Kettemann, Kapitel 3.4. *Ist Facebook ein neuer öffentlicher Raum?*)

Dementsprechend finden sich beispielsweise zwar Ansätze und Versuche, den Schutz von JournalistInnen und BloggerInnen zu stärken (vgl. Matthias C. Kettemann, Kapitel 5.1. *Schutz aus Straßburg*), wohingegen die verschiedenen Möglichkeiten und Formen für zivilgesellschaftliche AkteurInnen, aktiv zu werden, nur bedingt geschützt sind[7].

Ein Bewusstsein dieser Problematik findet sich im Rahmen verschiedener Konzepte, die sich in Begriffen widerspiegeln wie Netizen (zu deutsch NetzbürgerIn)[8], Cypherpunk (technikversierte Menschen, die sich für verstärkten Datenschutz einsetzen)[9], Prosument (KundenInnen, die gleichzeitig ProduzentInnen sind)[10] – oder auch dem (in dieser Aufzählung weitreichendsten) Begriff des Cyborg (in seiner Verwendung als Bezeichnung der symbiotischen Verbindung, die Menschen mit der sie umgebenden Technik eingehen)[11]. Allerdings hat sich keiner der Begriffe, die alle auf die eine oder andere Art die Vorstellung eines „aktiven Users" beinhalten, bislang als geläufig durchsetzen können.

---

[7] Vgl. Christian Möhlen, Kapitel 2.3. *Gibt es ein Recht auf politischen Online-Protest?*) sowie bspw. Pany, Thomas: *Online-Demonstranten können sich nicht aufs Demonstrationsrecht berufen*. In http://www.heise.de/tp/blogs/8/152568 (Letzter Aufruf: 14.4.2013)

[8] vgl. http://de.wikipedia.org/wiki/Netizen (Letzter Aufruf: 20.5.2013)

[9] vgl. http://de.wikipedia.org/wiki/Cypherpunk (Letzter Aufruf: 20.5.2013)

[10] vgl. http://de.wikipedia.org/wiki/Prosument (Letzter Aufruf: 20.5.2013)

[11] vgl. http://de.wikipedia.org/wiki/Cyborg (Letzter Aufruf: 20.5.2013)

4. Über die Notwendigkeit, mit- und umzudenken

So unverzichtbar zweifellos der KonsumentInnenschutz als jener Rechtsbereich ist, welcher derzeit für Individuen im Internet am besten ausgebaut ist, bleibt die begrifflich in der Form selbstverständliche Reduktion aktiver Internet-TeilnehmerInnen auf die Rolle der NutzerIn einer Infrastruktur und damit KonsumentIn ausgesprochen problematisch.

Möglich wird diese Reduktion wesentlich durch das ebenso implizite Nichtbeachten virtueller Umgebungen als Erweiterung physischer Räume. „Das Internet" ist in diesem Sinn ein längst unumgänglich gewordener, zusätzlicher „Handlungs(spiel)raum" für Individuen, um Ansichten zu entwickeln, sich auszutauschen, sich zu unterhalten, zu koordinieren oder zu organisieren – eben aktiv an einer (demokratischen) Gesellschaft teilzuhaben. Begriffe bestimmen unsere Gedankenwelt und prägen, wie eingangs erwähnt, ganz wesentlich unsere Möglichkeiten, Sachverhalte zu bedenken und Handlungsweisen zu perspektivieren. Entsprechend wichtig ist es, auch und gerade im Kontext der verschiedenen „Räume" des Internets die Rollenzuschreibungen zu beachten und zu prüfen, die den etablierten und entsprechend zur Anwendung kommenden Begriffen inhärent sind.

Pragmatische Ansätze, mit der hier angesprochenen Problematik umzugehen, werden beispielsweise seitens des *Committee on Internet User Rights* des Europarates angestrebt, wo aktuell an einem „Compendium", also einem Leitfaden für User Rechte gearbeitet wird.

Offen bleibt allerdings die Frage, warum ein weiteres Konzept, eine weitere Erklärung stärkere Durchsetzungskraft als die bisherigen entwickeln können sollte, wenn abseits „einer netzpolitisch affinen Szene" weiterhin kaum Bewusstsein für die erhebliche und vielseitige Bedeutung des Internets als Infrastruktur für Menschen besteht – und sich selbst unter den Menschen, die netzpolitisch interessiert und

engagiert sind, wenig Bewusstsein über die Macht, die auch den von ihnen (nicht) verwendeten Begriffen innewohnt, zeigt.

Erst Begriffe, die auch einer Mehrheit zu veranschaulichen in der Lage sind, warum es so wichtig ist, dass jeder Mensch Rechte am Internet haben sollte (vgl. Kapitel 1.2. *Rechte eines jeden Menschen am Internet von Hans Christian Voigt*), werden dazu beitragen können, ein breiteres Bewusstsein für ihre Bedeutung hervorrufen – und damit ein entsprechendes Verständnis als Basis für Handlungsmöglichkeiten erwirken können.

1.4. Post, Gender, Internet? (Leonie Maria Tanczer)

Wenn Post-Gender zur Utopie und das Netz zum Spiegel herrschender Geschlechterordnung wird

Keywords: Geschlecht, Gender, Sexismus, Feminismus, Männlichkeit, Gleichberechtigung

1. Das Internet ist nicht Post-Gender 53
2. Off- und Online-Sexismus 54
3. Das böse „F"-Wort 55
4. Stereotype 2.0 58
5. Männliche Netzwerke im Netzwerk Internet 63
6. Das Internet kann nicht zaubern, wir können etwas tun! 65
Online-Empfehlungen zum Weiterlesen 69

1. Das Internet ist nicht Post-Gender

Vielerorts lag die Hoffnung darin, heterosexuelle und geschlechtsspezifische Charakteristika durch die Anonymität des Netzes zu überwinden. Die Möglichkeiten die das Internet eröffnet, galten als „empowering", sprich stärkend und ermächtigend[1] und es wurde als Raum der Gleichberechtigung dargestellt[2]. Es wurde erwartet, dass gesellschaftliche Dynamiken unserer Welt damit obsolet werden. „Post-Gender" ist der Begriff, der dieses geschlechtslose Ideal abbilden sollte. Sein Ursprung findet sich in der dekonstruktivistischen Arbeit

[1] Vgl. Barak, A., Boniel-Nissim, M., & Suler, J. (2008). Fostering empowerment in online support groups. Computers in Human Behavior, 24(5), 1867–1883; Vgl. Wilding, F., & Ensemble, C. A. (1998). Notes on the political condition of cyberfeminism. Art Journal, 57(2), 46–59.

[2] Vgl. Gimmler, A. (2001). Deliberative democracy, the public sphere and the internet. Philosophy & Social Criticism, 27, 21–39.

von Donna Haraway[3]. Zentral ist dabei die Idee, dass Technologie eine neue Ontologie und damit ein neues Sein schafft.

Diesem Anspruch ist das Internet bis dato aber nicht gerecht geworden. Es ist nicht die ersehnte Utopie des geschlechtsfreien Raums. Das Internet, die IT-Branche und Technik sind stark männlich konnotiert. Diesem Umstand tragen die folgenden drei Postulate Rechnung:

Sexismus und sexistische Mechanismen finden sich auch in der Onlinewelt. Dies stellt eine neue Herausforderung für den Kampf um Gleichberechtigung und Gleichbehandlung dar.

Gesellschaftliche und damit geschlechtliche Stereotype sind auch im Internet vorhanden. Geschlechtliche Stereotype finden sich auch im Internet wieder, was der Utopie Post-Gender widerspricht.

Männliche Netzwerke und Strukturen lassen sich auf das Internet übertragen. Damit ist unter anderem gemeint, dass Frauen im Internet, aber auch in der IT-Branche marginalisiert und unterrepräsentiert sind.

2. Off- und Online-Sexismus

Sexismus kann als eine Befürwortung von benachteiligenden Vorurteilen auf Basis von Geschlecht verstanden werden[4]. Sexismus produziert damit Ausgrenzungen und Dynamiken, die die Möglichkeiten von Frauen einschränken und behindern.[5] Dies lässt sich auch auf die Onlinewelt übertragen.

---

[3] Haraway, D. (1994). A manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s. The Postmodern Turn: New Perspectives on Social Theory, 82–115.

[4] Vgl. Campbell, B., Schellenberg, E. G., & Senn, C. Y. (1997). Evaluating measures of contemporary sexism. Psychology of Women Quarterly, 21(1), 89–102.

[5] Glick und Fiske definieren 1997 in *Hostile and benevolent sexism measuring ambivalent sexist attitudes toward women*. (Psychology of Women Quarterly, 21(1), 119–135) Sexismus u.a. als eine Feindlichkeit gegen Frauen. Die Aufrechterhaltung der traditionellen Geschlechterrollen zwängt beide Geschlechter in

Aktuelle Literatur[6] definiert sexistische Online-Attacken gegen Frauen u.a. anhand von Begriffen wie *cyber stalking*, *cyber harrassment* und *cyber bullying*. Online-Sexismus ist ein weitverbreitetes Problem. Der eigentliche Umfang ist aber nur schwer abschätzbar. Eine Studie[7] geht davon aus, dass circa 40 Prozent der weiblichen Internetnutzerinnen Erfahrungen mit Online-Sexismus haben. Allerdings ist die Dunkelziffer höchstwahrscheinlich deutlich höher, da die meisten Vorfälle unangezeigt bleiben[8].

Als sexistische Angriffe können Aufrufe zu Gewalt an Frauen, die Veröffentlichung von retuschierten Bildern, die Veröffentlichung ihrer Wohnadressen sowie die Androhung von Vergewaltigung oder technische Eingriffe wie etwa die Abschaltung und Veränderung von Blogs und Webseiten von Frauen gezählt werden.

Obwohl es schon in vielen Ländern rechtliche Maßnahmen in Hinblick auf die Onlinewelt gibt, scheint es vielerorts schwer, mit diesen Online-Sexismen umzugehen[9].

3. Das böse „F"-Wort

Neben Angriffen auf individuelle Frauen, scheinen gerade Feministinnen und feministische Organisationen von diesen Feindseligkeiten

---

gesellschaftliche Rollen, wobei diese insbesondere Frauen in eine untergeordnete Position und in eine Stellung mit weniger Macht drängt, als Männer (Glick, P., Fiske, S. T., Mladinic, A., Saiz, J. L., Abrams, D., Masser, B, Alao, A. (2000). Beyond prejudice as simple antipathy: Hostile and benevolent sexism across cultures. Journal of Personality and Social Psychology, 79(5), 763.).

[6] vgl. Lipton, J. D. (2010). Combating cyber-victimization. http://works.bepress.com/jacqueline_lipton/11 (Letzter Aufruf: 23.4.2013)

[7] s. Barak, A. (2005). Sexual harassment on the internet. Social Science Computer Review, 23(1), 77–92.

[8] vgl. Citron, D. (2009b). Law's expressive value in combating cyber gender harassment. Michigan Law Review, 108, 373–416.

[9] Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the united states, the UK, and India. Victims & Offenders, 6(4), 386–398.

betroffen. Dies hat auch damit zu tun, dass Feminismus zu einem negativ behafteten Begriff geworden und ein Erstarken der maskulinistischen Bewegung online erkennbar ist[10]. Die Auffassung von Feminismus basiert innerhalb dieser Bewegung auf der verfälschten Annahme, dass Frauen Männer diskriminieren würden und Männer somit übervorteilt wären. Jegliche emanzipatorische Versuche zur Förderung von Frauen werden innerhalb dieser Bewegung als „feministisch" und damit als „unfair" oder sogar als „sexistisch" gegenüber Männern abgetan.[11]

Aufbauend auf dieser Annahme ist das böse „F"-Wort und alle mit ihm verbundenen Aspekte und progressiven Versuche, Frauen in der patriarchalen Offline- und Onlinewelt zu unterstützen, häufig Ziel von Online-Offensiven.

So wurde zum Beispiel im Juli 2012 die Seite *Feminism.org* von Teilen (der als als Wiege der „*Anonymous*"-Bewegung geltenden) *4Chan Community* gehackt, um frauenfeindliche Witze und Statements wie etwa „men are superior get over it!" zu veröffentlichen[12].

2011 wurde die Homepage des *Women's Media Center* gehackt und mit sexistischen Postings überhäuft[13]. Die Organisation bestritt zu der Zeit eine Kampagne gegen Facebook, da die Plattform nicht gegen Gruppen und Seiten vorgehen wollte, die sexuelle Gewalt gegen Frauen verharmlosen.

---

[10] vgl. Kemper, A. (2012). Die Maskulisten. Organisierter Antifeminismus im deutschsprachigen Raum. Münster: Unrast Verlag.

[11] Die Politikwissenschafterin Birgit Sauer weist in einem Interview darauf hin, dass sich Feminismus nur gegen die patriarchale Ordnung und Frauenunterdrückung, nicht jedoch gegen Männer an sich richtet. (Vgl. Schiester, A. (2012, 10.03.2012). Ohne Unterschied: Post-Gender: Was nach dem Feminismus kommt. Salzburger Nachrichten, pp. 1–2.)

[12] Reinsberg, H. (2012, 18.07.2012). 4Chan hacks feminism.org to make Rape Jokes. Buzzfeed.

[13] Bennett, J. (2011, 05.11.2011). Should facebook ban sexist pages?. The Daily Beast.

Die Feministin und Gamerin Anita Sarkeesian und ihre Kickstarter-Kampagne für das Video-Projekt *Tropes vs. Women*[14] wurden ebenfalls Ziel eines sexistischen „Shitstorms". Ihre Kritik an der Darstellung von Frauen in Videospielen und an ihrer Unterrepräsentation als Gamerinnen war der männlichen Community im Netz ein Dorn im Auge. Der Wikipedia-Eintrag von Sarkeesian wurde mit Fehlinformationen überhäuft, persönliche Attacken und Drohungen waren in ihrem Email-Account, aber auch öffentlich auf unterschiedlichsten Seiten und Boards zu finden[15].

Der Versuch, Veränderungen und Verbesserungen für Frauen im Netz zu schaffen, hat Rügen und Anfeindungen zur Folge. Nachdem der Gender Gap bei den AutorInnen der deutschen *Wikipedia*[16], aber auch das Fehlen von speziellen feministischen Artikeln und die zum Teil voreingenommene Präsentation von gewissen Themen von einigen AutorInnen kritisiert wurde, fanden sich diese plötzlich sexistischen Angriffen ausgeliefert[17]. Eine „Relevanzdiskussion" um (vor allem feministische) Themen begann.

Dies sind nur einige Beispiele, die das Bestehen von Online-Sexismus belegen. Die sexuellen Belästigungen von Gamerinnen bei Onlinespielen, die sexistischen Anmerkungen im Source-Code des Linux-Kernels (inzwischen entfernt) oder die Angriffe auf weibliche Bloggerinnen wie etwa Kathy Sierra[18] sind weitere Exempel.

---

[14] vgl. z.B. http://blog.zeit.de/netzfilmblog/2013/03/11/tropes-women-sexismus-videospiele-sarkeesian/ (Letzter Aufruf: 28.3.2013)

[15] Vgl. O'Leary, A. (2012, 01.08.2012). In virtual play, sex harassment is all too real. New York Times.

[16] Kampmann, B., Keller, B., Knippelmeyer, M., & Wagner, F. (2013). Wikipedia: Lexikon sucht frau. Die Frauen und das Netz (pp. 159-171) Springer.

[17] Kleinz, T. (2012, 31.08.2012). Sexismus bei Wikipedia. Erschreckende Aggressivität. Taz. Die Tageszeitung.

[18] Citron, D. (2009a). I. anonymous mobs of the twenty-first century. Boston University Law Review, 1–23.

Vielerorts entscheiden sich Bloggerinnen sogar dazu, ihren öffentlichen Auftritt im Internet ruhend zu stellen, nachdem der Schwall an polemischen und hasserfüllten Kommentaren im eigenen E-Mail-Account unerträglich geworden ist. Eine Studie der University of Maryland im Jahre 2005 bestätigt diesen Mechanismus. Die ForscherInnen zeigten, dass Frauen nach bedrohlichen Kommentaren z.B. in Online-Chatrooms dazu tendieren, dieses Medium nicht länger zu verwenden. Ein Einbruch von 28 zu 17 Prozent an weiblichen Nutzerinnen war dabei in der Studie erkennbar.[19]

Vorfälle und Zahlen wie diese deuten daraufhin, dass Frauen damit entmutigt werden, ihre Interessen online umzusetzen und zu verwirklichen (Citron, 2009b). Dies schließt sie von einem neuartigen Bestandteil unserer Realität aus und zeigt wie sexistische Mechanismen auch online Ausführung finden.

4. Stereotype 2.0

Ein Test: Hacker, Nerd, IT-Spezialist, Programmierer, Spieleentwickler, Web-Developer, Gamer, Internetnutzer. Welche Bilder haben wir bei diesen Begriffen im Kopf – und wie sehen die von uns vergegenwärtigten Menschen aus?

Sind sie weiß? Tragen Sie Brillen? Und: Sind sie männlich?

Technologie geht vorwiegend mit Bildern von Maskulinität und Macht einher[20]. So hält sich beispielsweise die Vorstellung, Männer

[19] Meyer, R., & Cukier, M. (2007). Assessing the attack threat due to IRC channels. University of Maryland School of Engineering, 1–6.

[20] vgl. Balsamo, A. (1995). Technologies of the gendered body: Reading cyborg women. Durham: Duke University Press Books. / Faulkner, W. (2001). The technology question in feminism: A view from feminist technology studies. Paper presented at the Women's Studies International Forum, 24(1) 79–95.

wären das technisch und mathematisch begabtere Geschlecht[21]. Die feministische Kritik des Aktiv-Passiv-Dualismus wird hier evident.[22] Frauen äußern sich in Umfragen deutlich zurückhaltender gegenüber Technologie. In vielen Studien punkten sie auch wesentlich höher auf der Computer Anxiety Rating Scale, welche einen Fragebogen darstellt der Computerangst misst[23]. Selbst die feministische Theorie schien lange Zeit Technologie kritisch gegenüber zu stehen. Entweder wurde Technologie als ein männliches Verlangen nach Kontrolle identifiziert[24] oder als getrennt von Natur und damit als problematisch betrachtet[25]. Erst mit der Idee des Cyberfeminismus in den 90er Jahren wurde begonnen, eine andere, positivere Haltung zu Technik einzunehmen[26].

Das Internet und die IT-Branche sind stark männlich dominiert. Die Ursachen hierfür sind vielschichtig. Gerade der „Stereotype threat" ist für Frauen dabei vermehrt ein Problem. Stereotype werden inter-

---

[21] Orland, B. (1996). Geschlecht als Kategorie in der Technikhistoriographie. In Meinel C., & M. Renneberg (Eds.), Geschlechterverhältnisse in Medizin, Naturwissenschaft und Technik (pp. 30-42). Stuttgart: GNT-Verlag.

[22] Frauen sind vermehrt auf der EmpfängerInnen-Seite von Technologie (Arnold, E., & Faulkner, W. (1985). Smothered by invention: Technology in women's lives. London: Pluto Press.)

[23] vgl. Durndell, A., & Haag, Z. (2002). Computer self efficacy, computer anxiety, attitudes towards the internet and reported experience with the internet, by gender, in an east European sample. Computers in Human Behavior, 18(5), 521–535. / McIlroy, D., Bunting, B., Tierney, K., & Gordon, M. (2001). The relation of gender and background experience to self-reported computing anxieties and cognitions. Computers in Human Behavior, 17(1), 21-33. / Todman, J., & Day, K. (2006). Computer anxiety: The role of psychological gender. Computers in Human Behavior, 22(5), 856-869.

[24] Stanworth, M. (1987). The deconstruction of motherhood Cambridge: Polity Press. / Wajcman, J. (1991). Feminism confronts technology. Pennsylvania: Penn State University Press.

[25] Shiva, V., & Mies, M. (1993). Ecofeminism. Atlantic Highlands, NJ: Zed,

[26] Plant, S. (1997). Zeros ones: Digital women the new technoculture. London: Fourth Estate.

nalisiert und haben Einfluss auf das Verhalten von Frauen die diese weiter perpetuieren[27].

Gruber[28] untersuchte, dass Frauen vermehrt Sexismen in stark männlich-dominierten Umgebungen ausgeliefert sind. Ähnliche Ergebnisse zeigen, dass Frauen verglichen zu ihren männlichen KlassenkollegInnen häufiger in Computerkursen in Schulen gemobbt werden[29]. Vergleichbare Muster wurden in einer Studie von Cohoon, Wu und Chao entdeckt[30]. Das ForscherInnenteam konnte zeigen, dass Frauen in Informatik-PhD-Programmen 21 Mal häufiger wegen sexistischen Vorfällen ihre Forschungsstelle verlassen, als dies Frauen u.a. wegen schlechter akademischer Leistung tun.

Tatsachen wie diese führen dazu, dass Männer tendenziell aktive Gestalter und Frauen passive Nutzerinnen der Technologie und des Internets bleiben. So sind z.B. GameentwicklerInnen primär Männer[31]

---

[27] Vgl. Barker, L. J., McDowell, C., & Kalahar, K. (2009). Exploring factors that influence computer science introductory course students to persist in the major. ACM SIGCSE Bulletin, 41(2), 282-286. Retrieved from http://www.ncwit.org/sites/default/files/legacy/pdf/Barker-McDowell-Kalahar-SIGCSE2009.pdf (Letzter Aufruf: 23.4.2013); Spencer, S. J., Steele, C. M., & Quinn, D. M. (1999). Stereotype threat and women's math performance. Journal of Experimental Social Psychology, 35(1), 4–28.

[28] Vgl. Gruber, J. E. (1998). The impact of male work environments and organizational policies on women's experiences of sexual harassment. Gender & Society, 12(3), 301–320.

[29] Gurer, D., & Camp, T. (2001). Investigating the incredible shrinking pipeline for women in computer science. (No. 9812016). National Science Foundation. Retrieved from http://women.acm.org/archives/documents/finalreport.pdf. (Letzter Aufruf: 23.4.2013)

[30] Vgl. Cohoon, J. M., Wu, Z., & Chao, J. (2009). Sexism: Toxic to women's persistence in CSE doctoral programs. ACM SIGCSE Bulletin, 41(1), 158-162. Retrieved from http://www.zuluzone.info/files/Sexism:%20toxic%20to%20women%27s%20persistence%20in%20CSE%20doctoral%20programs.pdf (Letzter Aufruf: 23.4.2013)

[31] Krotoski, A. (2004). White paper: Chicks and joysticks: An exploration of women and gaming. Entertainment & Leisure Software Publishers Association (ELSPA). http://cs.lamar.edu/faculty/osborne/COSC1172/elspawhitepaper3.pdf. (Letzter Aufruf: 23.4.2013)

und auch in der Open Source Software Erstellung nehmen Männer eine Monopolstellung ein[32]. Dieses Ungleichverhältnis von männlichen FramerInnen vs. weiblichen UserInnen ist deshalb möglich, da Männer die technischen Skills erlangen können, zu denen Frauen aus unterschiedlichen Gründen, wie etwa den Sexismen während der Ausbildung, weniger selbstverständlich Zugang finden. Technologie ist damit wortwörtlich man-made.

Betrachtet mensch direkt die Stereotype, die online anzutreffen sind, so sticht die klischeehafte Avatar-basierte Welt in Online- oder Videospielen ins Auge[33]. Dies ist abermals kein Indiz für ein vermeintlich geschlechtsloses Internet.

Auch die *Gender Bending* Möglichkeit, die durch das Internet gegeben sei[34] lässt sich selten finden. Zwar gibt es Studien, die auf Gender Performativität im Sinne Butlers hinweisen, wie etwa jene von Kelly, Pomerantz und Currie[35], jedoch werden diese Ergebnisse durch Studien rund um computer mediated communication (CMC) infrage gestellt.

---

[32] Nafus, D. (2012). Patches don't have gender: What is not open in open source software. New Media & Society, 14(4), 669-683.

[33] Bailenson, J. N., Swinth, K., Hoyt, C., Persky, S., Dimov, A., & Blascovich, J. (2005). *analysierten in* „The independent and interactive effects of embodied-agent appearance and behavior on self-report, cognitive, and behavioral markers of copresence in immersive virtual environments." (Presence: Teleoperators & Virtual Environments, 14(4), 379–393.) *die menschenähnlichen Figuren und konnten nachweisen, dass Frauen objektiviziert, stereotypisiert (z.B. Aktiv-Passiv-Dualismus: Mario rettet die hilflose Prinzessin) und stark sexualisiert werden* (vgl. auch Beasley, B., & Standley, T. C. (2002). Shirts vs. skins: Clothing as an indicator of gender role stereotyping in video games. Mass Communication & Society, 5(3), 279–293. / Burgess, M. C., Stermer, S. P., & Burgess, S. R. (2007). Sex, lies, and video games: The portrayal of male and female characters on video game covers. Sex Roles, 57(5), 419–433.)

[34] Danet, B. (1998). Text as mask: Gender, play, and performance on the internet. Cybersociety, 2, 129–158.

[35] Kelly, D. M., Pomerantz, S., & Currie, D. H. (2006). „No boundaries"?: Girls' interactive, online learning about femininities. Youth and Society, 38(1), 3–28.

Kucukyilmaz et al.[36] wiesen nach, dass unter 100 AutorInnen die geschlechtliche Identifizierung mit 99,7 Prozent Treffsicherheit ermöglicht ist. Ähnliche Ergebnisse finden sich quer durch das Forschungsfeld[37]. Douglass[38] folgert daher, dass in einem vermeintlich unidentifizierbaren Kontext und gerade in Fragen der Kommunikation das a/s/l – gemeint ist Age, Sex und Location – der UserInnen erfragt wird. Geschlechtslosigkeit im Internet ist in dieser Hinsicht pure Fiktion.

Weiters finden sich Stereotype in Online-Werbungen wieder. Frauen werden passiv und in traditionellen Rollen dargestellt[39]. Laut einer deutschen BITKOM-Studie[40] wird auch ersichtlich, dass die Verwendung des Mediums und damit auch Dynamiken, die im Internet gegeben sind, auf Stereotypen aufbauen:

Männer nehmen die öffentliche Rolle im Internet ein, posten auf Bulletin Boards oder in Foren, während Frauen eher in geschlossenen sozialen Netzwerken aktiv sind und private Kommunikation bevor-

---

[36] Kucukyilmaz, T., Cambazoglu, B. B., Aykanat, C., & Can, F. (2008). Chat mining: Predicting user and message attributes in computer-mediated communication. Information Processing & Management, 44(4), 1448-1466.

[37] Vgl. Atai, M. R., & Chahkandi, F. (2012). Democracy in computer-mediated communication: Gender, communicative style, and amount of participation in professional listservs. Computers in Human Behavior, 28(3), 881-888. / Christofides, E., Islam, T., & Desmarais, S. (2009). Gender stereotyping over instant messenger: The effects of gender and context. Computers in Human Behavior, 25(4), 897–901. / Sierpe, E. (2005). Gender distinctiveness, communicative competence, and the problem of gender judgments in computer-mediated communication. Computers in Human Behavior, 21(1), 127–145.

[38] Douglass, D. W. M. (1997). Cyberself: The emergence of self in on-line chat. The Information Society, 13(4), 375–397.

[39] Vgl. Plakoyiannaki, E., Mathioudaki, K., Dimitratos, P., & Zotos, Y. (2008). Images of women in online advertisements of global products: Does sexism exist? Journal of Business Ethics, 83(1), 101–112.

[40] Vgl. BITKOM. (2011). Das Internet ist keine Männerdomäne mehr. (Press Release). Berlin: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

zugen. Ebenso konnten Helsper[41] und Joiner et al.[42] in ihren Studien nachweisen, dass Geschlechterunterschiede in Hinblick auf die Internetnutzung eine Reflexion der Geschlechterunterschiede in unserer Gesellschaft sind. Stereotype, denen wir in unserer physischen Welt tagtäglich begegnen, ziehen sich somit bis in die digitale Welt hinein.

5. Männliche Netzwerke im Netzwerk Internet

Männliche Netzwerke und Männerbünde, wie sie u.a von feministischen ForscherInnen schon in Staatsstrukturen analysiert wurden[43], finden sich auch im Internet wieder. Was Burschenschaften, Männerrunden und Stammtische offline darstellen, ist im Netz z.B. das heitere Geplänkel, fleißige Retweeten und Favorisieren auf Twitter. Diese Schulterklopf-Mentalität konnten Ausserhofer et al.[44] durch ihre Twitterstudie nachweisen. In der „Online-Welt" sind also die selben Mechanismen am Werk, wie in der „Offline-Welt". Frauennetzwerke gibt offline wie online nur wenige.

---

[41] Helsper, E. J. (2010). Gendered internet use across generations and life stages. Communication Research, 37(3), 352–374.

[42] Joiner, R., Gavin, J., Brosnan, M., Cromby, J., Gegory, H., Guiller, J, Moon, A. (2012). Gender, internet experience internet identification and internet anxiety: A ten year follow up. Cyberpsychology, Behavior, and Social Networking, 15(7), 370–372.

[43] Kreisky, E. (1994). Das ewig Männerbündische? Zur Standardform von Staat und Politik. In C. Leggewie (Ed.), Wozu Politikwissenschaft? Über das neue in der Politik (pp. 191–208). Darmstadt: Wissenschaftliche Buchgesellschaft. und Kreisky, E. (1995). Der Stoff, aus dem die Staaten sind. zur männerbündischen Fundierung politischer Ordnung. In R. Becker-Schmidt, & G. Knapp A (Eds.), Das Geschlechterverhältnis als Gegenstand der Sozialwissenschaften, Frankfurt aM (pp. 85–124). Frankfurt: Camous.

[44] Ausserhofer, J., Kittenberger, A., & Maireder, A. (2012). Twitterpolitik: Netzwerke und Themen der politischen Twittersphäre in Österreich. (). Wien: Universität Wien.

Eine Studie von Aral und Walker[45] untermauert diese Ergebnisse der „Online-Old-Boy Networks" weiter. Sie untersuchten Facebook-UserInnen und zeigten, dass Männer mehr und viel einflussreichere Netzwerke auf der Social Media Plattform lukrieren, als Frauen. Letztgenannte bilden eher Netzwerke in ihrem Bekanntenkreis, während Männer dazu tendieren Öffentlichkeit zu schaffen, was ihnen auch umgekehrt mehr Einfluss verschafft[46].

Ersichtlich werden diese männlichen Netzwerkdynamiken auch auf Seiten wie z.B. *LAD Stories*, die vor allem in Großbritannien Popularität genießen. Dabei erzählen sich Männer u.a. gegenseitig Trinkgeschichten von letzter Nacht, heroisieren ihre Männlichkeit, während Frauen in diesen Postings objektiviert und zumal herabwürdigend präsentiert werden. Das Internet wird somit als Tool erfolgreich für männliche Netzwerkstrukturen vereinnahmt. Mann kann hier auch gerne etwas über die Stränge schlagen, spitzzüngige Kommentare formulieren und den einen oder anderen sexistischen Witz machen, den mann sich offline Auge in Auge mit seinem Gegenüber vielleicht verkniffen hätte.

Vermehrt werden diese Angriffe als schlichtes „Trollen" abgetan. Gemeint sind damit aber aggressive, online Invektive[47]. Dies sind angeblich amüsante Scherze, die durchwegs auf Kosten von schwächer gestellten Gruppen und Individuen gehen. Will frau sich gegen ebensolche Mechanismen zur Wehr setzen und spricht Ungleichheiten online gezielt an, wird z.B. gekontert: „Na und! Dann schreiben dir eben Männer Fragen zu deiner Oberweite. Ignoriere diese Postings schlichtweg." – „Das ist 4chan, da nimmt sich niemand ernst." – „Es

[45] Aral, S., & Walker, D. (2012). Identifying influential and susceptible members of social networks. Science, 337(6092), 337–341.
[46] Eagly, A. H. (1987). Sex differences in social behavior: A social-role interpretation. Hillsdale: Lawrence Erlbaum Associates. / Tannen, D. (1990). You just don't understand: Women and men in conversation. New York: Ballantine Books.
[47] Thrope, V., & Rogers, R. (2011, 06.11.2011). Women bloggers call for a stop to 'hateful' trolling by misogynist men. The Guardian.

hat ja niemand von dir verlangt, dass du einen Blog anlegst. Die Kommentare musst du dann eben in Kauf nehmen."

Hinter einer IP-Adresse versteckt lassen sich somit Ressentiments gegen Frauen leichter ausleben und finden durch das starke Kollektiv, das sich online bildet, sogar noch Zustimmung und „likes".

Ersichtlich wird dieser männliche Netzwerkmechanismus auch durch die seit 10 Jahren wachsende maskulinistische Gemeinschaft. Die Männerrechtsbewegung in der deutschsprachigen Welt nutzt hierbei gezielt das Medium Internet[48], aber auch in den USA, Kanada und Großbritannien finden sich ähnlich erstarkende Gruppierungen[49]. Frauen und Feminismus – sogenannte Feminazis – werden zum Ziel ihrer online Attacken, das Internet ermöglicht hierbei Vernetzung auf Plattformen wie *WGvdL.com*.

Die erwähnten Beispiele deuten daraufhin wie das Netzwerk Internet zu einem Männernetzwerk wird, welches sich ganz im Sinne der Netzwerktheorie um Fragen von Macht und Ressourcen dreht[50]. Abermals wird das Internet seinem geschlechtsfreiem Anspruch nicht gerecht.

6. Das Internet kann nicht zaubern, aber wir können etwas tun!

Als Haraway das Cyborgwesen konstruierte und damit den Ausdruck Post-Gender implementierte, bestand die Hoffnung darin, dass neue Technologien die Kategorie Geschlecht unwichtig und Gleichberechtigung möglich machen würden. Diese Annahme hält sich noch heute. Auf der DLD-Women-Konferenz 2012 wurden „Superfrauen" vorge-

[48] Vgl. Kemper, A. (2012). Die Maskulisten.
[49] Blais, M., & Dupuis-Déri, F. (2012). Masculinism and the antifeminist countermovement. Social Movement Studies, 11(1), 21–39.
[50] Katzmair, H., & Mahrer, H. (2011). Die Fformel der Macht. Salzburg: Ecowin Verlag.

stellt, die Karriere und Kind dank den Vorteilen des Internets managerhaft unter einen Hut bringen[51]. Das Internet ermögliche Arbeiten von zu Hause aus, Anwesenheit sei nicht mehr gefragt und Emails kann frau auch im Kinderzimmer abrufen.

Die Vorstellung, dass die „Superfrau" des Internetzeitalters mit dem Kind auf dem Schoß und dem PC vor sich CEO-Aufgaben erledigt, ist realitätsfern. – Diese „Superfrauen" haben nichts mit den Cyborgwesen von Haraway zu tun. Fragen zu Betreuungs- und Erziehungspflichten und reproduktiven Aufgaben haben sich auch durch das Internet nicht in Luft aufgelöst. Das Internet macht auch den Kampf für Gleichberechtigung nicht automatisch einfacher oder das Leben für Frauen in unserer Gesellschaft so mir nichts, dir nicht leichter.

Das Internet mag für alle Geschlechter Vorteile bringen, aber ohne die Zusatzverpflichtungen von Frauen dezidiert aufzuheben, Sexismus und Stereotype zu überwinden und Frauennetzwerke zu fördern, wird auch das Internet keine Wunder vollbringen.

Das Internet ist also weit davon entfernt, eine geschlechtsfreie Sphäre zu sein. Rollenbilder, Stereotype, Sexismus, männliche Dominanzstrukturen und Netzwerke sind online und offline vorhanden. Für Gleichberechtigung zu kämpfen heißt somit auch, diese Dynamiken im Internet kritisch zu hinterfragen. Die digitale Welt ist schlichtweg ein Spiegel der gesellschaftlichen offline Verhältnisse. Frauen in den patriarchalen Strukturen zu unterstützen und diese männlich-fixierte Konstitution der Gesellschaft zu verändern, bedeutet somit Initiativen in beiden Sphären zu schaffen.

Cyberfeministische Praxen, wie etwa die gezielte Zusammenarbeit von Frauen durch Technologie, weibliche Koalitionen online und die kritische Betrachtung des Gender Bias in der IT-Branche sind möglich[52].

---

[51] Borchardt, A. (2012, 12.07.2012). Im Wettbewerb der Superfrauen. Süddeutsche.
[52] Wilding, F. (1998). Where is feminism in cyberfeminism? N.Paradoxa, 2, 6–13.

Beispiele für dieses Empowerment ganz im Sinne von CyberfeministInnen finden sich etwa in Form von bestärkender Webseiten (z.B. *sistahspace.com*, *maedchenblog.de*, *woneedsfeminism.com*, *iholaback.org* oder *hatr.org*), aber auch in der Praxis der unzähligen weiblichen Bloggerinnen die den sexistischen Attacken stand halten. Aktuell sind Diskussionsrunden, Symposien und Konferenzen zum Thema Netzpolitik zumeist stark männlich besetzt. Aufgezeigt wird dies unter anderem auf Anne Roths blog 50 Prozent[53], dessen BetreiberInnen die Genderratio öffentlicher Events im Netz sammeln. JedeR kann dabei das Geschlechterverhältnis einer Veranstaltung veröffentlichen und die Anzahl der teilnehmenden Männern und Frauen bekannt machen. Damit wird ein kritisches Statement gesetzt und auf dieses Missverhältnis hingewiesen.

Die Antwort auf dieses Ungleichgewicht und dessen Aufhebung findet sich in aktiver Frauenförderung. Diese hat gemeinsam mit gezielter Vernetzung schon vielerorts Früchte getragen. Die Speakerinnenliste auf *Netzfeminism.org* soll hier deshalb positiv genannt werden. Dem Trend der männerbesetzten Panels entgegenwirkend, werden auf dieser Website Frauen mit entsprechendem Fachwissen in unterschiedlichen Feldern der Netzpolitik vorgestellt. Potenzielle VeranstalterInnen können diese demzufolge ansprechen und gezielt einladen. Frauenlose Panels sind damit unentschuldbar geworden.

Beispielhaft nennen lassen sich auch die Initiativen GnomeWomen und Ada Initative. Beide Projekte unterstützen Frauen bei der Ausarbeitung und Weiterentwicklung von Free und Open Source Software und motivieren diese zur Mitarbeit. Sie bieten Hilfestellung, spezielle Trainings, um Frauen in dieser stark männlich dominierten Szene zu unterstützen.

Auch auf Twitter formieren sich Bewegungen, die dazu beitragen sollen, Frauen sichtbarer zu machen. In Anlehnung an den theoretisch

[53] http://50prozent.noblogs.org

genderneutralen wöchentlichen *Follower Friday* (#ff), der dazu dient, Empfehlungen für TwitternutzerInnen auszusprechen, bietet das Hashtag #fff (*Female Follower Friday*) ein explizit weibliches Pedant dazu, das dazu dient, gezielt weibliche „Twitterinnen" zu empfehlen.

Weitere Möglichkeiten mit Sexismus off- und online umzugehen und Öffentlichkeit für dieses Problem zu schaffen zeigten unter anderem Initativen wie *#aufschrei* oder *#1ReasonWhy* auf. Der Gebrauch dieser Hashtags diente Frauen dazu, mit ihren persönlichen Erfahrungen (Alltags-)Sexismus betreffend zu Wort kommen und Unterstützung im Kollektiv finden. #aufschrei wurde in Deutschland von den Massenmedien ebenso, wie der blogospähre aufgegriffen und führte schließlich zu einer breiten gesellschaftlichen Debatte. Aktivitäten wie diese rütteln an der primären männlichen Dominanz des Internets und der IT-Branche. All das deutet daraufhin, dass Veränderungen möglich sind.

Geschlechtersensible Pädagogik bleibt angesichts der Lage weiterhin ein wichtiger Schritt, um Frauen in technischen Bereichen zu stärken und zu unterstützen.

Maßnahmen wie die hier angeführten konsequent verfolgt können helfen, Stereotype aufzuheben und aktiv-passiv Dualismen im Sinne von männlichen FramerInnen und weiblichen UserInnen zu überwinden. Es geht aber auch darum, Frauen Raum zu geben und umgekehrt, dass sich Frauen diesen Raum auch dezidiert nehmen und ihn einfordern – sowohl offline als auch online. Diese Aspekte müssen umgesetzt bzw. weitergeführt werden, damit der Gender Gap in der IT-Branche, sowie die männliche Vorherrschaft im Internet ausgeglichen – und Post-Gender keine Utopie, sondern Realität werden kann.

Online-Empfehlungen zum Weiterlesen

http://www.anschlaege.at

http://www.denkwerkstattblog.net

http://www.mzbaltazarslaboratory.org/blogDE

http://www.frauenhetz.at

http://www.ifz.tugraz.at/ger/content/view/full/6936

http://www.frauensolidaritaet.org

http://www.genderraum.at

http://netgrrrls.at

1.5. Das Internet in der arbeitsrechtlichen Kampfzone (Thomas Kreiml)

Menschenrechtliche Bruchlinien entlang der Internetnutzung im Arbeitsverhältnis

Keywords: Arbeitsverhältnisse, Arbeitsrecht, Internetnutzung

1. ArbeitnehmerInnen im Internet 71
2. Interessenkonflikt Internetnutzung 72
3. Komplexes Umfeld und rechtliche Grauzonen 73
4. Regelungen zur Kontrolle und Schutz davor 75
5. Ansprüche und (zu erkämpfende) Rechte 79
6. Gestaltungs- und Mitbestimmungsauftrag 81

1. ArbeitnehmerInnen im Internet

Technik im Allgemeinen und das Internet als technisches System im Speziellen ist mittlerweile fixer und vielfach kennzeichnender Bestandteil der Arbeitswelt. Als Betriebsmittel zur Abwicklung von Arbeitsprozessen ist das Internet nicht mehr aus den Unternehmen wegzudenken. Dementsprechend findet sich auch kaum noch ein Betrieb, in dem es keinen Internetanschluss gibt bzw. in dem komplett ohne Internetanwendungen – und sei es nur mit E-Mails – gearbeitet wird.

Während von einer sehr hohen Netzabdeckung in der Gesamtheit der Unternehmen ausgegangen werden kann, ist auch festzustellen, dass nicht alle Tätigkeitsbereiche im selben Ausmaß und nicht alle ArbeitnehmerInnen in derselben Weise von dieser Entwicklung betroffen sind. Nicht jede Tätigkeit in einem Betrieb erfordert Internetnutzung, dennoch kann davon ausgegangen werden, dass ArbeitnehmerInnen heute in hohem Grade mit dem Internet zu tun haben – und zwar

entweder beruflich oder privat. So findet sich als Beispiel aus der Praxis auf der einen Seite eine ältere Bankangestellte, „die schon lange im Geschäft ist“ und plötzlich von E-Mail-Kommunikation bis hin zum Online-Banking „Netzkompetenzen“ für ihre berufliche Tätigkeit braucht, persönlich und privat einer Internetnutzung aber kaum Bedeutung beimisst – während auf der anderen Seite eine junge HandwerkerIn (MechanikerIn, MalerIn, FriseurIn...) im Rahmen ihrer beruflichen Tätigkeit kaum bis gar nicht mit dem Internet zu tun hat, privat aber sowohl zu Hause als auch per Smartphone „Heavy UserIn“ ist.

2. Interessenkonflikt Internetnutzung

Neben solchen Kompetenzasymmetrien, die mit der Verbreitung des Internets als Betriebs- und Arbeitsmittel zu Tage treten, werden vor allem auch Interessenkonflikte hinsichtlich der Art und des Ausmaßes der Internetnutzung sowie seiner Kontrolle in der betrieblichen Praxis zur Herausforderung für alle Beteiligten. Die Konfliktfelder werden zunächst anhand recht simpel erscheinender Fragestellungen deutlich erkennbar, wie zum Beispiel: *Ist die private Internetnutzung während der Arbeitszeit erlaubt? Darf die ArbeitgeberIn das Surfverhalten ihrer MitarbeiterInnen kontrollieren? Haben ArbeitnehmerInnen bei im Internet geäußerten Meinungen mit Konsequenzen am Arbeitsplatz zu rechnen?*

Mit solchen und ähnlichen Fragen werden unterschiedliche Interessen zwischen Arbeitenden und Vorgesetzten sowie AuftraggeberInnen deutlich. Die Frage nach der privaten Nutzung von Internetdiensten etwa ist mindestens so alt wie die Verbreitung von E-Mails in Betrieben und hat ihre Vorläufer in der Nutzung von Telefonanlagen und Firmenhandys. Andere Fragen und Konfliktfelder treten hingegen erst in den letzten Jahren mit den Entwicklungen der Sozialen Medien und der vermehrten mobilen Internetnutzung auf. Möglichst kurz

zusammengefasst lassen sich die unterschiedlichen Perspektiven wie folgt auf den Punkt bringen:

> *„Unternehmen stehen in einem wirtschaftlichen Wettbewerb und haben sowohl begründetes Interesse daran, dass wichtige Informationen nicht nach außen dringen, als auch ein begründetes Interesse an einer vorteilhaften Außendarstellung. Sie wollen Informationen und Kommunikation kontrollieren und haben in einigen Bereichen und in Maßen auch das Recht dazu."*[1]

> *„Im Internet sind (auch) die bereits errungenen Menschen- und Bürgerrechte nicht außer Kraft gesetzt. Wir denken da zum Beispiel an das Briefgeheimnis, an Persönlichkeitsrechte, Meinungsfreiheit, Informationsfreiheit, durchaus aber auch an die ‚sozialen Menschenrechte'."*[2]

3. Komplexes Umfeld und rechtliche Grauzonen

ArbeitnehmerInnen finden sich damit heute grundsätzlich in einem Feld komplexer Interessenslagen und Anforderungen wieder – und das sowohl, wenn sie beruflich das Internet nutzen (müssen), als auch zunehmend, wenn sie privat online sind. Hier sind Aspekte der Datensicherheit ebenso relevant, wie jene des Datenschutzes, welche ebenso rasch miteinander in Konflikt geraten können, wie die Verschwiegenheitspflicht mit Persönlichkeits- und Menschenrechten.

Die maßgebliche Instanz zur Orientierung im Rahmen von Arbeitsverhältnissen ist das Arbeitsrecht, das einige Instrumente zur Regelung der verschiedenen Fragen beinhaltet. Was die Internetnutzung betrifft, wird in Österreich als Grundlage allerdings unter anderem die Rechtsprechung zur Nutzung von Telefonanlagen herangezogen (OGH 13.6.2002, 8 ObA 288/01p).

---

[1] Lanu / Voigt, Hans Christian (2011): Heul nicht! Sag was! Der Interessenkonflikt Arbeitgeber_innen vs. Arbeitnehmer_innen im Netz. In: Voigt, Hans Christian / Kreiml, Thomas (Hrsg.): Soziale Bewegungen und Social Media. Handbuch für den Einsatz von Web 2.0. Wien: ÖGB Verlag, S. 68.
[2] Ebd.

Auf die neueren Entwicklungen im Bereich der Internetnutzung wurde bislang – wiederum in Österreich – weder seitens der Gesetzgebung reagiert, noch gibt es dazu ausjudizierte Rechtsfälle. Das gilt sowohl für die Internetnutzung generell, als auch für Besonderheiten im Zusammenhang mit Social-Media-Plattformen. Gekennzeichnet ist die Situation folglich von erheblichen rechtlichen Grauzonen. Nicht oder nur entfernt Rechnung getragen wird unter anderem so wesentlichen Aspekten wie dem zunehmenden „Verschwimmen" von privatem und beruflichem Nutzungsverhalten oder der beschleunigten, auch öffentlichen Verbreitung von individuell erstellten Online-Inhalten durch die UserInnen selbst.

Im Zusammenhang mit dem oben genannten Interessenkonflikt spielen diese Grauzonen vorwiegend der ArbeitgeberInnenseite in die Hände. Diese ist zwar an der Nutzung des Internets als Betriebsmittel höchst interessiert, verbunden ist dieses Interesse aber auch mit der möglichst umfassenden Kontrolle der Informations- und Kommunikationsprozesse. Auf Handlungen von MitarbeiterInnen, die dieser Interessenlage widersprechen, werden gegebenenfalls auch rasch disziplinäre Maßnahmen ergriffen. So zögern ArbeitgeberInnen nicht, Dienstverhältnisse wegen Facebook-Postings zu beendigen[3], auch wenn die rechtlichen Grundlagen dafür keinesfalls eindeutig geklärt sind. Unabhängig von ungeklärten rechtlichen Verhältnissen ist zudem zu bedenken, dass die Regelungen des Arbeitsrechts schon grundsätzlich Ergebnis von Verhandlungsprozessen sind, in denen unterschiedliche Interessen aufeinander treffen. So werden beispielweise bestimmte Persönlichkeits- und Menschenrechte durch das Arbeitsrecht zwar einerseits gewahrt, allerdings nicht ohne andererseits bestimmte Rechte wie die Meinungsfreiheit den hierarchischen Bedingungen im Arbeitsverhältnis unterzuordnen.

---

[3] vgl. futurezone.at: „Österreich: Nach Facebook-Eintrag gefeuert." http://futurezone.at/digitallife/8419-oesterreich-nach-facebook-eintrag-gefeuert.php (Letzter Aufruf: 06.04.2012)

4. Regelungen zur Kontrolle und Schutz davor

Vor dem Hintergrund dieser Überlegungen stellt sich in der betrieblichen Praxis immer wieder die Frage, wie mit der Ausweitung der Internetnutzung allgemein und den neuen Möglichkeiten der einzelnen NutzerInnen umgegangen werden soll. Wie werden die unterschiedlichen Interessen organisiert oder durchgesetzt bzw. welche Basis gibt es für Vereinbarungen und Übereinkünfte?

Dass und wie von Unternehmensseite Ansprüche gestellt und bisweilen auch durchsetzt werden, ist anhand verschiedener Beispiel zu beobachten: Das reicht von Verboten der privaten Internetnutzung[4] und dem Sperren einzelner Internetseiten über die heimliche Durchsuchung von Arbeitsrechnern[5] bis hin zu ArbeitgeberInnen, die Facebook-Passwörter von BewerberInnen für Recherchen fordern[6]. Besonders zeigt es sich auch an der enormen Verbreitung von sogenannten „Social Media Guidelines“ oder „Social Media Policies“, bei denen es sich um „Codes Of Conduct“, also Verhaltenskodizes handelt, anhand derer ArbeitnehmerInnen ihr Onlineverhalten ausrichten sollen.

Aus ArbeitnehmerInnensicht betrachtet sind Überlegungen zum Schutz der Privatsphäre der Betroffenen sowie des betrieblichen Datenschutzes der Ausgangspunkt für Regelungen zum Umgang mit Internetnutzung im Arbeitsverhältnis. Verschiedene Gesetzesmaterien bieten dem Eingriff in die Privatsphäre von ArbeitnehmerInnen Einhalt bzw. setzen hier Grenzen (österreichische Rechtsmaterien):

---

[4] vgl. nachrichten.at: „Facebook während der Dienstzeit: Viele Firmen setzen sich zur Wehr” http://www.nachrichten.at/oberoesterreich/Facebook-waehrend-der-Dienstzeit-Viele-Firmen-setzen-sich-zur-Wehr;art4,371248 (Letzter Aufruf: 15.04.2010)

[5] vgl. golem.de: „Heimliche PC-Durchsuchung durch Arbeitgeber rechtswidrig” http://www.golem.de/news/persoenlichkeitsrecht-illegale-pc-durchsuchung-vom-arbeitgeber-rechtswidrig-1212-96218.html (Letzter Aufruf: 07.12.2012)

[6] vgl. welt.de: „Wenn der Arbeitgeber das Facebook-Passwort will” http://www.welt.de/wirtschaft/webwelt/article13949183/Wenn-der-Arbeitgeber-das-Facebook-Passwort-will.html (Letzter Aufruf: 27.03.2012)

- *Individualrechtliche Grenzen*

Rechtsmaterien: Allgemeines Bürgerliches Gesetzbuch (ABGB); Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG).

„*Jeder Mensch hat angeborene, schon durch die Vernunft einleuchtende Rechte, und ist daher als Person zu betrachten.*" (§ 16 ABGB) Diese Zentralnorm der Rechtsordnung beinhaltet das Recht auf Achtung des Privatlebens und der Privatsphäre, in das nur dort eingegriffen werden darf, wo das gesetzlich vorgesehen ist, wobei eine besondere Interessenabwägung vorzunehmen ist. Hier werden Grundprinzipien des Arbeitsvertrags geregelt und es wird festgelegt, dass Persönlichkeitsrechte auch im Arbeitsverhältnis gelten, allerdings werden auch für das Arbeitsverhältnis typische Kontrollrechte des Arbeitgebers bzw. der Arbeitgeberin in gewissem Umfang eingeräumt. In der Praxis zeigt sich, dass diese Rechtsgrundlagen für ArbeitnehmerInnen im Ernstfall schwer durchsetzbar sind. Es ist keine Seltenheit, dass Arbeitsverträge fragwürdige, die Beschäftigten benachteiligende Klauseln enthalten.

> *„Vielfach herrscht hier das Verständnis der Arbeitgeber vor ‚alles' kontrollieren zu dürfen. Diese Kontrolle beschränkt sich in der Regel nicht nur auf das Sperren bestimmter Internetseiten, sondern beinhaltet vielfach auch eine Auswertung des Nutzungsverhaltens."*[7]

In jedem Fall bedürfen Kontrollen in diesem Bereich der vorhergehenden Zustimmung jedes/jeder einzelnen MitarbeiterIn. (§ 10 AVRAG) Dem wird jedoch in der heutigen Arbeitswelt kaum entsprochen bzw. kann bei solchen Zustimmungserklärungen, welche die ArbeitnehmerInnen meist gleich mit dem Arbeitsvertrag vorgelegt bekommen, nicht vom Grundsatz der Freiwilligkeit ausgegangen werden. Sollte es doch zu einer Rechtsdurchsetzung seitens der Be-

---

[7] S. wienerzeitung.at: „Kontrolle des Surf-Verhaltens" http://www.wienerzeitung.at/nachrichten/wirtschaft/international/504875_Kontrolle-des-Surf-Verhaltens.html (Letzter Aufruf: 30.11.2012)

schäftigten kommen, so ist das größtenteils erst nach Konflikten und einer Beendigung des Arbeitsverhältnisses der Fall.

- *Datenschutzrechtliche Grenzen*

Rechtsmaterie: Datenschutzgesetz (DSG 2000).

Das DSG 2000 setzt die EU-Richtlinie 95/46/EG um und enthält in § 1 folgende Verfassungsbestimmung: „Jedermann hat [...] Anspruch auf Geheimhaltung seiner personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht." Als wesentliche rechtliche Instanz zum Schutz sensibler und personenbezogener Daten enthält das DSG 2000 aber kaum für das Arbeitsverhältnis relevante Regelungen. Zudem sind die aus ihm entstehenden Schutzansprüche ebenfalls nur individuell einklagbar, was seine Wirkung und Durchsetzung im Arbeitsleben stark beeinträchtigt.

- *Kollektivrechtliche Grenzen*

Rechtsmaterie: Arbeitsverfassungsgesetz (ArbVG).

Die umfassendsten Regelungen zur Internetnutzung im Arbeitsverhältnis sowie auch die in der Praxis bestmögliche Durchsetzung von Schutz- und Nutzungsansprüchen der ArbeitnehmerInnen bieten Regelungen im Rahmen von Betriebsvereinbarungen. In Betrieben in denen es einen Betriebsrat gibt, können bzw. sollten solche Vereinbarungen zwischen der betrieblichen Interessenvertretung der ArbeitnehmerInnen und der ArbeitgeberInnenseite abgeschlossen werden. Genau betrachtet dürfte das Internet in diesen Betrieben ohne die vorhergehende Zustimmung des Betriebsrats nicht als Betriebsmittel eingesetzt werden.

> *„Davon ausgehend, dass es zunächst der Arbeitgeber ist, der ein wesentliches Interesse an der Verwendung von Internet zur Geschäftsabwicklung hat, stellt § 96 Abs 1 Z 3 ArbVG die maßgebliche rechtliche Grundlage für die Einführung bzw. Nutzung von Internet und eMail am Arbeitsplatz dar. Demnach bedarf die Einführung/Nutzung von Internet im Betrieb der Zustimmung des Betriebsrats, da die Maßnahme aufgrund der intensiven Über-*

> *wachungsmöglichkeiten die Menschenwürde berührt, weshalb die Zustimmungspflicht auch nicht ersetzbar ist.*"[8]

Trotz dieser rechtlich sehr gut ausgeprägten Mitbestimmungsmöglichkeit bei Fragen der Internetnutzung ist die „Regelungsdichte" in der Praxis noch stark ausbaufähig: Betriebsvereinbarungen zu Internet/E-Mail gibt es nur in knapp der Hälfte von Betrieben, in denen es einen Betriebsrat gibt.[9]

In diesen Betriebsvereinbarungen werden üblicherweise alle Fragen der Internetnutzung im Arbeitsverhältnis möglichst umfassend geklärt. Damit lässt sich auch eine betriebliche „Netzkultur" bzw. „Netzpolitik" gestalten, bei der die ArbeitnehmerInnenseite prinzipiell eine gute Verhadlungsbasis vorfindet. Gleichwohl wird anhand der Unterschiedlichkeit, wie diese Vereinbarungen im Detail letztlich in den verschiedenen Betrieben ausgestaltet sind, bisweilen auch die jeweilige „Unternehmenskultur" sichtbar. Die Betriebsvereinbarung enthält unter anderem Regelungen zu Fragen der privaten Internetnutzung und den Voraussetzungen und Bedingungen etwaiger Kontrollen des Surfverhaltens. Aktuell finden neu auftretende Fragen bezüglich einer Nutzung Sozialer Medien (z.B. Veröffentlichungsmöglichkeiten der ArbeitnehmerInnen) in Betriebsvereinbarungen jedoch noch kaum Niederschlag. Hier bestehen derzeit erhebliche Unklarheiten und Unsicherheiten, wie und inwieweit den neuen Entwicklungen mit konkreten Regelungen entsprochen werden könnte.

---

[8] S. Kreiml, Thomas (2010): vernetzt, ver[www]irrt, verraten? Web 2.0 in der Arbeitswelt – ein Überblick für BetriebsrätInnen. Wien: GPA-djp. Online unter http://arbeitundtechnik.gpa-djp.at/2010/11/15/vernetzt-verwwwirrt-verraten-web-2-0-in-der-arbeitswelt-ein-uberblick-fur-betriebsratinnen/, S. 37 (Letzter Aufruf: 20.5.2013)

[9] Vgl. Riesenecker-Caba, Thomas / Bauernfeind, Alfons (2009): Verwendung personenbezogener Daten und Grenzen betrieblicher Mitbestimmung: Datenschutz in der Arbeitswelt. Wien: Arbeiterkammer Wien. Online verfügbar unter http://www.arbeiterkammer.at/bilder/d156/Sozialpolitik_in_Diskussion_12.pdf (Letzter Aufruf: 20.5.2013)

5. Ansprüche und (zu erkämpfende) Rechte

Die Internetnutzung in der „arbeitsrechtlichen Kampfzone" gleicht vielfach einer „Abwehrschlacht". Mit dem Eintritt in ein Arbeitsverhältnis schulden ArbeitnehmerInnen dem/der ArbeitgeberIn primär ihre Arbeitskraft und unterliegen den Interessen des Arbeitgebers, der die Betriebsmittel zur Verfügung stellt bzw. stellen muss (vgl. Arbeitnehmerschutzgesetz, § 33 Abs 2 ANSchG). Rechte der ArbeitnehmerInnen ergeben sich in erster Linie aus Schutzbestimmungen: Datenschutz, Schutz der Persönlichkeitsrechte, Schutz vor Überwachung und Verhaltenskontrolle etc.

Viel seltener als die Frage nach den Schutzansprüchen der Beschäftigten werden – bezogen auf das Thema Internet aber auch in anderen Bereichen – Fragen nach Nutzungsansprüchen und -rechten gestellt. Vereinfachend dargestellt zeigt es sich jedoch, dass technische Entwicklungen sowie Veränderungen im Kommunikations-, Konsum- und Mediennutzungsverhalten immer wieder erst zu Konfliktfällen führen müssen, bevor meist durch Rechtsprechung Grundlagen für Anspruchs- und Freiheitserweiterungen geschaffen werden. Das kann abschließend noch kurz an zwei Beispielen näher dargestellt werden.

- *Private Internetnutzung im Arbeitsverhältnis*

Die Grundlagen für die Beantwortung der Frage, ob und, wenn ja, in welcher Weise bzw. in welchem Ausmaß ArbeitnehmerInnen während der Arbeitszeit privat im Internet surfen dürfen, wurden – in Österreich – durch Judikatur zur Privatnutzung von Diensttelefonen geschaffen. Der/die ArbeitgeberIn kann als EigentümerIn der Betriebsmittel die private Nutzung untersagen. Jedoch gilt auch ein solches absolutes Verbot nicht in Notfällen (z.B. Fälle gemäß Angestelltengesetz, § 8 Abs 3 AngG). Darüberhinaus ist eine sehr eingeschränkte private Nutzung zum Beispiel zur Vereinbarung von Arzt- oder Behördenterminen (etwa per E-Mail) zulässig. De facto kann eine private Nutzung praktisch nicht komplett bzw. gänzlich verboten

werden. Besonders interessant ist weiters, dass die relativ neuen Möglichkeiten der privaten Nutzung über private internetfähige Geräte wie Smartphones oder Tablets in der Rechtsprechung noch gar nicht ausdrücklich berücksichtigt sind.

In aller Regel kann man sich an der Rechtsprechung des OGH orientieren, der eine verhältnismäßige Privatnutzung während der Arbeitszeit wiederholt als durchaus üblich erachtet hat. Eine genauere Formulierung findet sich dazu auch in der Rechtsprechung nicht, was wiederum die Regelung im Rahmen betrieblicher Vereinbarungen nahe legt.

- *Meinungsfreiheit: Veröffentlichungen durch ArbeitnehmerInnen*

Personen, die bereits in einem Arbeitsverhältnis stehen, aber auch aktuell nicht erwerbstätigen Personen, die früher oder später zu BewerberInnen werden können, wird derzeit sehr verbreitet geraten, ihre Privatsphäre bei Veröffentlichungen in Social-Media-Plattformen möglichst zu wahren und zu berücksichtigen. Bei der ersteren Gruppe der ArbeitehmerInnen kommt noch hinzu, dass sie auf persönliche Risiken von Veröffentlichungen im Zusammenhang mit beruflichen bzw. betrieblichen Informationen hingewiesen werden. ArbeitnehmerInnen bzw. AuftragnehmerInnen stehen hier tatsächlich „auf dünnem Eis“, wie anhand sich verbreitender Fälle nachzuvollziehen ist. Die rechtlichen Grundlagen für verschiedene disziplinäre Schritte, die ArbeitgeberInnen in solchen Fällen setzen sind zwar ebenso vage, die Unternehmensseite schafft hier aber zunehmend vermeintliche Tatsachen.

> *„Privatwirtschaftliche Unternehmen, aber auch Arbeitgeber_innen im öffentlichen und im Non-Profit-Sektor, [...] würden es sicherlich vorziehen, wenn Lohn- und Honorarabhängige unsichtbar beziehungsweise nur mit den Aussagen hörbar wären, die sich in die Öffentlichkeitsarbeit der Unternehmen und Organisationen einfügen. Das Internet, die Social Media-Plattformen, das ‚Mitmach-Web' geben diesem Wunsch immer weniger Chance auf Erfüllung. Immerhin gehört der größte Teil der Weltbevölkerung zur Klasse jener, die*

> *ihre Arbeitskraft verkaufen müssen, und wir alle reden irgendwann sehr wahrscheinlich über unsere Arbeit, bestimmt 'Arbeit' doch einen wesentlichen Teil unseres Lebens. Es wird schwierig bis unmöglich sein, die Masse der Menschen zum andauernden Schweigen über ihre Arbeitsbedingungen, ihre Abhängigkeiten und ihre Arbeitgeber_innen zu bewegen."*[10]

Es bedarf noch viel Aufklärungs- und Ermächtigungsarbeit, um den in der Verfassung festgeschriebenen Rechten der Meinungs- und Informationsfreiheit mehr Handlungsspielraum in der betrieblichen Praxis zu verschaffen. Rechtliche „SchützInnenhilfe" kommt hier von Entscheiden wie zum Beispiel im „Whistleblower-Fall": Der Europäische Gerichtshof für Menschenrechte (EGMR) hat im Fall einer fristlosen Kündigung einer Arbeitnehmerin festgestellt, dass dieses Vorgehen des Arbeitgebers gegen die Menschenrechtskonvention verstößt. Damit wird auch das Recht unterstützt, dass ArbeitnehmerInnen „auf Missstände in ihren Unternehmen öffentlich aufmerksam machen"[11].

6. Gestaltungs- und Mitbestimmungsauftrag

Um die weitreichende Bedeutung des Themas und den dringend nötigen Gestaltungs- und Mitbestimmungsauftrag zu betonen, schließe ich mit einem Zitat von Ulrich Klotz (2008):

> *„Technik ist Politik. Und Technikgestaltung ist Gesellschaftsgestaltung. Denn technische Entwicklungen verändern die Welt – und zwar oftmals folgenreicher und nachhaltiger als alle politischen Institutionen. Politiker und politische Organisationen, die sich nicht frühzeitig und kenntnisreich mit den Wechselwirkungen zwischen Technik und Gesellschaft befassen, verlieren allmählich den Kontakt*

[10] Lanu / Hans Christian Voigt 2011, S. 75.

[11] S. zeit.de: „Gericht schützt Meinungsfreiheit von Arbeitnehmern" http://www.zeit.de/politik/deutschland/2011-07/menschenrechte-arbeitnehmer-meinungsfreiheit (Letzter Aufruf: 21.07.2011)

zur Realität und damit auch ihren Einfluss, wenn nicht gar ihre Existenz.“[12]

[12] Klotz, Ulrich: Mit dem „Unternehmen 2.0” zur „nächsten Gesellschaft”. In: Computer und Arbeit – vernetztes Wissen für Betriebs- und Personalräte, Nr. 8-9 2008, Seite 12.

1.6. Gute Filter, böse Filter? (Julian Ausserhofer)

Algorithmen, der persönliche Informationshaushalt und digitale Öffentlichkeiten

Keywords: Filter Bubble, Social Media, Twitter, Politik, Algorithmen

1. Eifrig, parteiisch und mächtig: Algorithmen 83
2. Die Filter Bubble 84
3. Neue Filter, alter Hut? 86
4. Die Blase zerplatzen 88
5. Netzwerke und Informationsguerilla 89

1. Eifrig, parteiisch und mächtig: Algorithmen

Algorithmen sind die stillen Wegbereiter der Digitalisierung, die unsere Gesellschaft ähnlich deutlich verändert wie es die Industrialisierung im 19. Jahrhundert getan hat[1]. Ohne groß Aufsehen zu erregen, leisten Algorithmen Beachtliches: Sie wetten auf Finanzmärkten, sie schreiben Baseballberichte und helfen uns beim Finden von Spendernieren; sie recherchieren und rezensieren, sie publizieren und archivieren – ganz ohne menschliches Zutun.

Für uns sind Algorithmen Blackboxes. Erst durch ihre Nicht- oder Fehlfunktion wird klar, was ihre Leistung war: Wenn uns Facebook ein relevantes Statusupdate unterschlägt, wenn *Google Translate* Texte falsch übersetzt oder wenn der *E-Mail-Spamfilter* versagt, merken wir, welches Handlungspotenzial Algorithmen eingeschrieben ist. Wenn sie funktionieren, agieren sie jedoch fast unbemerkt. Dieser Umstand

[1] vgl. Bunz, M. (2012). Die stille Revolution: Wie Algorithmen Wissen, Arbeit, Öffentlichkeit und Politik verändern, ohne dabei viel Lärm zu machen. Berlin: Suhrkamp.

führt dazu, dass wir die Existenz von Algorithmen allzu oft ausblenden. Nicht verdrängen lässt sich jedoch die Veränderung der Wahrnehmung, die Algorithmen verursachen.

Und diese Wahrnehmungsveränderung ist beträchtlich: Im Netz entscheiden Algorithmen, welche Informationen sie uns präsentieren – und welche nicht. Manchen unserer Aktionen, die sie erfassen können, schreiben sie Relevanz zu – andere werden ignoriert. Algorithmen antizipieren unser Verhalten und wir richten unser Verhalten nach ihren Vorgaben aus[2].

All diese Tätigkeiten passieren mit dem Versprechen von Objektivität: Nicht der fehleranfällige Mensch entscheide, die vorurteilsfreie Maschine bestimme. Doch die Technologie, die das Web antreibt, ist kein neutraler Vermittler zwischen Mensch und Information. Erstens lässt sich Technik nie getrennt von ihrer Benutzung und ihren sozialen Auswirkungen beschreiben[3], zweitens basiert jeder Algorithmus auf einem Code, den eine Person geschrieben hat. Diese Person ist weder objektiv noch ideologiefrei, und ebensowenig ist es ihr Code, der im Web zum Gesetz aufsteigt[4].

2. Die Filter Bubble

Für unseren persönlichen Informationshaushalt, die Öffentlichkeit und (in weiterer Folge) die Demokratie, haben die oben beschriebenen Entwicklungen immense Auswirkungen. Pariser (The Filter Bubble, 2011) erläutert die gesellschaftlichen Konsequenzen von Per-

---

[2] vgl. Gillespie, T. (2013, forthcoming). The Relevance of Algorithms. In T. Gillespie, P. Boczkowski, & K. Foot (Eds.), Media Technologies: Paths Forward in Social Research. Cambridge, MA: MIT Press. Retrieved from http://www.tarletongillespie.org/essays/Gillespie%20-%20The%20Relevance%20of%20Algorithms.pdf (Letzter Aufruf: 15.3.2013)

[3] vgl. Latour, B. (2005). Reassembling the Social: An Introduction to Actor-Network-Theory. New York: Oxford University Press.

[4] vgl. Lessig, L. (1999). Code and other laws of cyberspace. New York: Basic Books.

sonalisierungsalgorithmen unter dem Begriff der *Filter Bubble*[5]. Die Dystopie, die er entwirft, scheint mit jeder unserer Aktionen im Web weiter Realität zu werden. Algorithmen zeichnen fast jeden unserer Schritte im Netz auf: Was wir „googlen", „liken", per E-Mail weiterleiten; wo, wann und mit wem wir online verbunden sind. All diese Daten werden gesammelt, um virtuelle „Personae" von uns zu erstellen, die wiederum als Grundlage für jegliche Informationsfilterung und -aufbereitung herangezogen werden. Komplett personalisierte Suchergebnisse, Nachrichtenseiten und Onlineshops sind die Konsequenz davon.

Diese Personalisierung unseres gesamten digitalen Informationsumfelds hat einerseits immense Vorteile: Immer schneller und leichter finden wir genau jene Informationen, Nachrichten und Produkte, die wir suchen; immer besser werden die Empfehlungen, immer angenehmer gestaltet sich das Surfen.

Andererseits bringt sie auch besorgniserregende Nachteile mit sich: Wir verlieren uns in einer Blase, in der uns unsere eigenen Vorlieben und Überzeugungen wieder und wieder vor die Nase gehalten werden. Die Folgen: Entpolitisierung, denn die politischen Menschen predigen zu den ohnehin Überzeugten – und die Unpolitischen bekommen von alledem nichts mit. Wir sehen uns in unseren Ansichten bestätigt, glauben, die Welt da draußen ticke ohnehin schon richtig.

Gegen diese sozialkonstruktivistische Anti-Utopie lassen sich natürlich einige Einwände vorbringen. Etwa, wenn wir in Sozialen Medien zufällig Inhalte entdecken, die wir zuvor nicht gesucht hatten. Wir erleben das immer wieder: In den *Social Awareness Stream*[6] eines

---

[5] vgl. Pariser, E. (2011). The Filter Bubble: What the Internet Is Hiding from You. New York: The Penguin Press.

[6] Naaman, M., Boase, J., & Lai, C.-H. (2010). Is It Really About Me? Message Content in Social Awareness Streams. In Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work (pp. 189–192). Presented at the CSCW 10, Savannah, Georgia, USA: ACM.

kunstinteressierten *Couchpotatos* schummelt sich ein Bericht über ein Fußballspiel, weil ihn einer seiner engsten Freunde für teilenswert hielt. Ein nach Restaurantempfehlungen stöbernder Gourmet stolpert über ein gesponsertes Blogpost, in dem das neueste Smartphone beworben wird. Zwei Dinge führen dazu, dass sich diese überraschenden Zufallsentdeckungen („Serendipity") minimieren. Erstens neigen wir online (ganz so wie auch offline) dazu, mit uns ähnlichen Menschen verbunden zu sein, die ähnliche Inhalte posten, wie wir selbst, zweitens lassen die Personalisierungsalgorithmen zwar Überraschungen zu – aber nur in jenem Ausmaß, das den kleinsten gemeinsamen Nenner aller UserInnen nicht befremden soll. Der Zufall wird so weit wie möglich ausgeschlossen. Dadurch versiegt eine wichtige Quelle für Kreativität, die sich aus Neuem, Fremdem und Unbekanntem speist. Im Extremfall werden uns unsere eigenen Vorstellungen wieder und wieder vorgehalten – nur immer etwas adaptiert und anders formuliert, gerade so, dass wir nicht das Interesse verlieren.

Indem sie UserInnen individualisierte Ergebnisse liefern, befördern Personalisierungsalgorithmen die Zersplitterung von Massenöffentlichkeiten. Das demontiert den Mainstream und ersetzt ihn durch Nischenöffentlichkeiten – mit allen positiven und negativen Folgen: Long Tail und Ausdifferenzierung von Interessen auf der einen Seite, Schwierigkeiten bei der breiten Mobilisierung und gesellschaftliche Zerklüftung auf der anderen.

3. Neue Filter, alter Hut?

Nun ließe sich natürlich einwenden: Diese Kritik an medialen Filtern ist nicht neu. Auch Analogmedien sind mit ähnlichen Argumenten kritisierbar. Schließlich war es immer schon die Aufgabe von Medieninstitutionen, Informationen auszuwählen – und fast nie taten sie das nach transparenten Kriterien. Jede Redaktion, vom Liechtensteiner Vaterland bis hin zu CNN, vom Dagbladet bis zur Antenne Kärnten, sie alle berichten tendenziös. Es werden Nachrichten ausgewählt, die

als wichtig erachtet werden, „nach“ denen man sich eben „richten“ sollte.

Der Unterschied zwischen filternden Redaktionen und deren algorithmischen Pendants ist fein, jedoch zentral: Zunächst einmal gab es bis zum Internet niemals individualisierte Massenmedien, bei denen jede NutzerIn etwas anderes zu Gesicht bekam. Weiters haben Redaktionen Redaktionsstatute, ethische Richtlinien und bestehen aus Menschen mit Moral, die bei Regelübertretungen zur Verantwortung gezogen werden können. Algorithmen haben (scheinbar) keine Moral, deren Selektionsregeln wirken vorurteilsfrei und unparteiisch[7]. Die PlattformbetreiberInnen wälzen die Selektionsverantwortung auf UserInnen und InhaltsproduzentInnen ab. Diese würden die Inhalte bereitstellen und verlinken, die Plattformen seien nur das neutrale Werkzeug zur Informationsfilterung. Diese Argumentationsstrategien werden sowohl gegen Zensurvorwürfe als auch gegen Klagen bei Reputationsschädigung eingesetzt – prominente Beispiele sind die Fälle des ehemaligen Formel-1-Präsidenten Max Mosley, der bei Google nicht mehr halbnackt mit Prostituierten und Peitsche gefunden werden wollte[8], und Bettina Wulff, der Ehefrau des früheren deutschen Bundespräsidenten, die ihren Ruf durch die Google-Autovervollständigung gefährdet sah[9]. Die Algorithmen vermitteln hier zwischen Persönlichkeitsschutz auf der einen und Informationsinteresse der Allgemeinheit auf der anderen Seite.

---

[7] vgl. Eisenberger, I. (2011). Die Macht der Algorithmen: Der Verlust der Öffentlichkeit durch Personalisierung im Netz. Juridikum, (4).

[8] Vgl. Hülsen, I. (2012, August 31). Max Mosley's Battle against Google Hits the Courts. Spiegel Online. Retrieved from http://www.spiegel.de/international/zeitgeist/max-mosley-sues-google-in-landmark-battle-over-digital-rights-a-853008.html (Letzter Aufruf: 15.3.2013)

[9] vgl. Niggemeier, S. (2012, September 17). Der Verleumdungs-Automat. Der Spiegel, 38. Retrieved from http://www.spiegel.de/spiegel/print/d-88656041.html (Letzter Aufruf: 15.3.2013)

4. Die Blase zerplatzen

Bei aller Kritik an Personalisierungsalgorithmen darf dennoch Folgendes nicht vergessen werden: Der eigene Informationshaushalt könnte im Social Web ohne individuelle Filter nicht bewältigt werden. Stellen Sie sich vor, Sie müssten auf Facebook jeden noch so aufwändig dekorierten Teller ansehen? Oder über jede politische Blähung in China lesen, obwohl Sie doch eigentlich Nachrichten aus Ihrem Heimatort gesucht hatten? Oder Sie bekämen ständig Justin Bieber empfohlen, obgleich Sie doch nichts außer Wagner schätzen. Personalisierungsalgorithmen sind die wichtigsten Informationsvermittler im Web – und als solche müssen wir sie sehen. *Dieses Betrachten funktioniert aber nur, wenn die Filter auch wirklich sichtbar sind.*

Aus diesem Grund verlangen AktivistInnen seit Jahren eine Offenlegung der Personalisierungsalgorithmen, wie unter anderem Eisenberger (Die Macht der Algorithmen, 2011) und Pariser (The Filter Bubble, 2011) beschreiben. Erste Forderung: Der Quellcode selbst muss einsehbar sein, damit die Auswahlentscheidungen nachvollziehbar werden.

Eine derartige Öffnung bringt indes auch einige Probleme mit sich: Allgemein bekannte einsehbare Selektionskriterien würden Manipulationen Tür und Tor öffnen. Nichts ließe sich leichter manipulieren als ein Ranking, bei dem die Kriterien bis ins letzte Detail bekannt wären.

Das allgemein noch viel gewichtigere Argument gegen die Filtertransparenz allerdings lautet: Algorithmen sind oft das Produkt vieler tausend Stunden Arbeit und die Geschäftsgrundlage zahlreicher Technologieunternehmen. Diese von einem Tag auf den anderen zu veröffentlichen, hätte unabschätzbare wirtschaftliche Folgen.

Zugleich entbehrt es nicht einer gewissen Ironie, dass viele dieser Unternehmen ihr Geschäftsmodell zwar auf dem Sammeln von UserInnendaten aufbauen, selbst aber bei der Herausgabe der eigenen Daten knausern.

Wenn schon nicht die Filter selbst offen gelegt werden, dann sollte also zumindest das Ergebnis ihrer Arbeit einsehbar sein. *Standardisierte Kennzeichen* könnten UserInnen darauf hinweisen, wenn zuvor ein Personalisierungsfilter am Werk war. Gegen eine Weigerung der Plattformen, derartige Markierungen einzuführen, könnte ein Filtermarkierendes *Browserplugin* Abhilfe schaffen.

Netzwerke wie Twitter und Facebook, bei denen Information vor allem durch Social Awareness Streams aufgenommen werden, sollten (mindestens) zwei Perspektiven auf ihre Daten anbieten: Den ungefilterten Stream, der alle geteilten Inhalte enthält – sowohl den Dreck als auch die Perlen, und einen Stream, der nach nachvollziehbaren Kriterien die Spreu vom Weizen trennt. Schalter, die Personalisierungsalgorithmen an- und abschalten, sind eine weitere Methode zur Filterbubble-Prophylaxe.

Es scheint hingegen illusorisch, an die verantwortliche Verwendung von korrekten Alternativ-Plattformen zu appellieren. Der geringe Erfolg von Diaspora und anderen Plattformen hat gezeigt, dass Kontrolle über die eigenen Daten nur ein Minderheitenmotiv ist, eine Plattform zu verwenden. Weil der Markt die Entwicklung von Informationsoligopolen nicht verhindern kann, wird der Staat mittelfristig regulatorisch eingreifen müssen und die Entwicklung von Alternativ-Plattformen fördern.

5. Netzwerke und Informationsguerilla

Alles andere als weltfremd ist hingegen die Empfehlung, in Social Networks ein großflächiges persönliches Netzwerk aufzubauen – mit möglichst vielen, unterschiedlichen AkteurInnen. Das Aufrechterhalten vieler Verbindungen, zu denen man auch nur schwachen Kontakt hat, hilft dabei, ein vollständigeres Bild von der Welt zu erlangen. Denn wer mit vielen Menschen, Dingen und Institutionen verbunden

ist, wird eher Neues erfahren als jene NutzerInnen, die wenige, starke Verbindungen pflegen[10].

Zusätzlich kann man den Personalisierungsfiltern ihre Arbeit erschweren, indem man Taktiken der Informationsguerilla einsetzt: Unterschiedliche BenutzerInnennamen, mehrere Webbrowser und Anonymisierungsdienste zu verwenden und Cookies zu löschen, sind einige der wenigen Methoden, welche die Arbeit der Algorithmen erschweren.

Kennzeichnungen und Offenlegungen, großflächige persönliche Netzwerke und Informationsguerilla, die Strategien zur Filter-Bubble-Vorbeugung müssen auf verschiedenen Ebenen greifen: Einer regulatorischen Ebene, die PlattformbetreiberInnen zu einer NutzerInnenfreundlicheren Informationspolitik zwingt, einer Community-Ebene, die kollektiv gegen Oligopole arbeitet, sowie einer individuellen Ebene, die das persönliche Informationsmanagement verbessert. Die Maßnahmen, die individuell gesetzt werden können, sind unaufwändig – auch wenn sie so manchen Schritt im Netz mühsamer machen. Die positiven Effekte sind es jedenfalls wert.

[10] vgl. Granovetter, M. (1973). The Strength of Weak Ties. American Journal of Sociology, 78(6), 1360–1380. / Granovetter, M. (1983). The Strength of Weak Ties: A Network Theory Revisited. Sociological Theory, 1(1), 201–233.

Teil 2:
Menschenrechte und neue Verantwortlichkeiten

2.1. Neue Menschenrechte für das Internet? (Matthias C. Kettemann)

Was offline gilt, muss online gelten

Keywords: Menschenrechte, Vereinte Nationen, Multistakeholder-Ansatz, Meinungsäußerungsfreiheit, Netzwerkneutralität, Zensur

1. Herausforderungen der Informationsgesellschaft 93
2. Zentrales Internet-Recht Meinungsäußerungsfreiheit 94
3. Operationalisierung statt Neudefinition 95

1. Herausforderungen der Informationsgesellschaft

Das Internet hat unsere Lebensrealitäten substanziell verändert. Es ist in den Worten von US-Außenministerin Hillary Clinton zum „öffentlichen Raum des 21. Jahrhunderts" geworden, zum „Hauptplatz der Welt, dem Klassenzimmer, dem Marktplatz, Kaffeehaus und Nachtclub". Aber es ist mehr als nur das: Das Internet ist auch zur Telefonzentrale geworden und zur Zeitungsdruckerei; zum Ort, wo sich MenschenrechtsaktivistInnen zusammenfinden, um Demonstrationen zu planen, Plakate zu gestalten, Boykottaufrufe zu formulieren und Revolutionen zu starten. Für eine ganze Generation ist das Internet heute jener Ort, wo über geografische Beschränkungen hinweg Meinungen gebildet, aggregiert und artikuliert werden. Damit ermöglicht das Internet den Userinnen und Usern viel intensiver als bisher, ihre Informations- und Kommunikationsfreiheiten auszuüben. Dies wiederum befördert die Realisierung anderer Menschenrechte und legt eine Frage nahe:

Benötigen wir im Lichte der neuen technologischen Herausforderungen auch neue Menschenrechte? Menschenrechte, die offline gelten, gelten

auch online. Das hat zuletzt der Menschenrechtsrat der Vereinten Nationen in einer am 5. Juli 2012 im Konsens angenommenen Resolution bestätigt. Doch vor welchen besonderen Herausforderungen stehen die Menschenrechte in der Informationsgesellschaft?

Natürlich stellt das Internet den Menschenrechtsschutz vor große Herausforderungen. Nur sind diese nicht konzeptioneller Natur; vielmehr ist es schwierig, die volle Anwendbarkeit der Menschenrechte auf Sachverhalte mit Internetbezug sicherzustellen. Die Herausforderung hierbei ist zweidimensional: Einerseits eröffnen Informations- und Kommunikationstechologien neue Gefährdungshorizonte (etwa durch die Kombination von sinkenden Speicherkosten und steigenden Datamining-Kapabilitäten), andererseits vertikalisiert die Vielfalt der AkteurInnen im Internet die Bedrohungsquellen für Menschenrechtsverletzungen und erweitert den Kreis der PflichtenträgerInnen auf nichtstaatliche AkteurInnen. Effektiver Menschenrechtsschutz ist äußerst komplex im normativen Mehrebenensystem internationaler Menschenrechtsverbürgungen, regionaler Schutzmechanismen, nationaler Grundrechte (und nationaler KonsumentInnenrechte) – sowie im Dickicht verschiedener AkteurInnen: InternetdiensteanbieterInnen, InternetzugangsanbieterInnen, Strafverfolgungsbehörden aber auch selbst- und fremdgefährdende UserInnen.

2. Zentrales Internet-Recht Meinungsäußerungsfreiheit

Zentrale Feststellung jeder Untersuchung der Rolle von Menschenrechten in der Online-Welt muss bleiben, dass Menschenrechte technologieneutral sind, wie schon in Artikel 19 der Allgemeinen Erklärung der Menschenrechte zu lesen ist.

Ausgehen muss jede Analyse des Schutzes von Informations- und Kommunikationsprozessen von Artikel 19 der Allgemeinen Erklärung der Menschenrechte (AEMR) von 1948. Dieser garantiert „[j]ede[m] […] das Recht auf Meinungsfreiheit und freie Meinungsäußerung;

dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten."

Der Begriff „Medien jeder Art" schließt jedenfalls das Internet mit ein; auch der Verweis auf eine Kommunikation „ohne Rücksicht auf Grenzen" ist für das grenzenlose Internet von Bedeutung.

Ein Beispiel ist die Freiheit der Meinungsäußerung: Zwar hat sich der Schutz der Informations- und Kommunikationsprozesse im Laufe der Zeit menschenrechtlich ausdifferenziert, doch bleibt die Meinungsäußerungsfreiheit ein zentrales Menschenrecht unter den Informations- und Kommunikationsfreiheiten. Sie ist ein Katalysator für andere Menschenrechte, ein „enabler". Die KommunikatorIn (UserIn), der Kommunikationsinhalt und die RezipientIn werden durch die Meinungsäußerungsfreiheit, die Meinungsfreiheit, die Informationsfreiheit, die Gedankenfreiheit, das Recht auf Achtung der Privatsphäre und der Korrespondenz geschützt.

Auch die Versammlungsfreiheit als institutionalisierte Form der Meinungsäußerungsfreiheit ist geschützt – offline wie online. Dasselbe gilt, um nur noch ein weiteres Beispiel zu nennen, für das Recht auf Teilhabe am öffentlichen Leben, das durch Zensur und Internetabschaltungen berührt ist. Einschränkungen sind möglich, nur müssen diese dem Dreistufentest von Gesetzmäßigkeit (und Vorhersehbarkeit), Legitimität (des Beschränkungsziels) und Verhältnismäßigkeit entsprechen.

3. Operationalisierung statt Neudefinition

Noch vor der Resolution des Menschenrechtsrates haben NGOs und internationale Organisationen versucht, Listen von Rechten und Prinzipien für das Internet zu entwerfen. Diese haben durchaus ihre Berechtigung, doch soll nicht die Suche nach neuen Menschenrechten

für das Internet im Mittelpunkt stehen, sondern vielmehr die Operationalisierung der bestehenden Menschenrechte. Wir brauchen keine neuen Formulierungen, sondern müssen bestehende Menschenrechte für das Internet übersetzen. Die Leitlinie ist dabei klar: Was offline gilt, muss online gelten.

Eine detaillierte Behandlung dieser Fragestellungen findet sich in Matthias C. Kettemann, Menschenrechte 2.0: UN-Menschenrechtsrat bestätigt Geltung der Menschenrechte im Internet, jusIT 3 (2012), 161–164.

2.2. Gibt es ein Recht auf politischen Online-Protest? (Christian Möhlen)

Menschenrechtlicher Schutz und digitaler ziviler Ungehorsam

Keywords: Digitaler Aktivismus, politischer Protest, Menschenrechte, ziviler Ungehorsam, Legalität, Legitimität

1. Ausgangslage 97
2. Digitale Protestmittel 98
3. Menschenrechte und digitaler Protest 101
4. digitaler Ziviler Ungehorsam 104
5. Ergebnis 108
Weiterführende Literatur 109

1. Ausgangslage

Politische AktivistInnen haben für die Verbreitung ihrer Anliegen schon immer auf neue Kommunikationsmittel zurückgegriffen, das gilt auch für das Internet. Digitaler Aktivismus tritt in unterschiedlichsten Formen auf, da AktivistInnen auf eine große Bandbreite an Methoden zurückgreifen können. Politischer Aktivismus muss dabei nicht ausschließlich in der virtuellen Sphäre stattfinden, sondern kann auch eine Verbindung von Offline- und Online-Methoden sein. Der Protest kann rechtmäßig oder illegal sein. Es ergibt sich also ein vielschichtiges, heterogenes Bild.

Aktivismus im Internet lässt sich vereinfacht, seinen unterschiedlichen Zwecken entsprechend, in drei Ebenen unterteilen:

- Informations- und Aufklärungsarbeit
- Organisation und Mobilisierung
- (Re-)Aktion und Protest

Im Folgenden wird auf die dritte Ebene genauer eingegangen. Darunter fallen neue Formen von politischem Protest, die sich im Internet entwickelt haben und als besonders öffentlichkeits- und medienwirksam gelten, wie zum Beispiel das „HackerInnenkollektiv“ Anonymous, das durch Berichte über seine Aktionen inzwischen auch abseits der „Online-Szenen“ ein Begriff ist.

Bei der Betrachtung des Umfelds elektronischer politischer Proteste von NetzbürgerInnen fällt in jüngerer Vergangenheit öfter das Schlagwort „Hacktivismus“. Dieser Begriff wird je nach Zusammenhang und NutzerIn teilweise sehr unterschiedlich verwendet: Beispielsweise wird Hacktivismus von einigen AutorInnen auf illegale Protestformen beschränkt – und so zur Abgrenzung von digitalem Aktivismus gebraucht. Andere hingegen vertreten die Auffassung, dass Hacktivismus eine Unterform von digitalem Aktivismus sei und konnotieren den Begriff wesentlich positiver. Dieser schwierige Begriff wird daher im Weiteren nicht benutzt. Digitaler Protest kann auch mit HackerInnentechniken erfolgen, doch gibt es darüber hinausgehend viele Protestformen, für die Hacken keine Rolle spielt. Im Folgenden wird digitaler Protest im Allgemeinen und digitaler ziviler Ungehorsam im Speziellen näher beleuchtet werden.

Zunächst werden dazu einzelne Beispiele für digitale Protestformen exemplarisch dargestellt, um danach auf Grundprobleme des Schutzes und der Einschränkungen digitalen politischen Protests durch die Grund- und Menschenrechte einzugehen. Schließlich wird ziviler Ungehorsam in der digitalen Sphäre beleuchtet.

2. Digitale Protestmittel

Digitale Protestmittel sind in ihren Erscheinungen sehr vielfältig, wie die folgenden Beispiele illustrieren:

Die *Distributed-Denial-of-Service-Attacke (DDoS)* ist eine Form des Protests, die sich bereits Anfang der 90er Jahre entwickelt hat. Diese

Protestform wurde von AktivistInnen wiederholt als „virtuelles Sit-in“ oder als Onlinedemonstration bezeichnet.

Bei DDoS kommt es zu verteilten Dienstangriffen mehrerer Systeme, bei der meist mit Hilfe von spezieller Software ein Internetdienst bzw. Server durch eine große Anzahl an gleichzeitigen Anfragen überflutet wird. Dadurch beantwortet der Server Anfragen nur noch stark verlangsamt oder bricht gänzlich zusammen. Daraus folgt die Unerreichbarkeit des Dienstes oder der Webseiten für Dritte.

Eine andere, weit verbreitete Form des Protests ist das *Defacement*. Dabei hackt sich ein/e AktivistIn in einen Server und übernimmt eine Zielwebseite, um eine Nachricht auf deren Startseite zu platzieren oder die ganze Seite durch eigenen Inhalt zu ersetzen. Auf diesem Weg werden politische Botschaften gegen den Willen der WebseiteninhaberInnen verbreitet.

Ein weiteres Mittel ist das Eindringen in Computersysteme und -datenbanken, um *Informationen* zu erlangen und diese anschließend *öffentlich zugänglich* zu *machen*. Beispiele hierfür sind die Veröffentlichung gestohlener KundInnendaten von Unternehmen oder die von Anonymous-Mitgliedern gehackten Daten des Sicherheitsunternehmens *Stratfor*, die später auf *WikiLeaks* veröffentlich wurden.

Ein ebenfalls in den letzten Monaten in den Medien behandeltes Phänomen ist der *Shitstorm*. Darunter versteht man die Summe meist spontaner aber geballter Reaktionen der Netzgemeinde auf aktuelle Vorkommnisse oder Erklärungen von PolitikerInnen, von in der Öffentlichkeit stehenden Personen oder Unternehmen. Die Shitstorm-TeilnehmerInnen posten Kommentare auf Webseiten, Blogs oder Social Media-Seiten von betroffenen Personen bzw. Unternehmen, um ihrer ablehnenden Haltung diesen gegenüber Ausdruck zu verleihen. Es geht vielfach nicht um eine sachliche Auseinandersetzung, sondern um die Überflutung des Zielsubjekts mit Kommentaren. Shitstorms sind meist unkontrolliert und nehmen im Verlauf

zunehmend stark emotionalisierte, beschimpfende und beleidigende Formen an.

Proteste können aber auch in wesentlich sachlicheren Formen erfolgen wie z.B. mit einem *Online-Blackout*. Bei diesem schalten die BetreiberInnen von Webseiten aus Protest ihr Angebot für einen bestimmten Zeitraum ab bzw. ersetzen die Startseite durch eine schwarze Seite mit der Erklärung, warum sie den Dienst vorübergehend nicht anbieten. Ein Beispiel war der eintägige Online-Blackout des englischen Wikipedia-Angebots aus Protest gegen die geplanten internationalen Antipiraterie-Abkommen SOPA und PIPA.

Ein weiteres, weitverbreitetes Phänomen kollektiven Protests sind *E-Mail-Kampagnen* mit Boykottaufrufen oder auch Mitteilungen über ein Social-Media-Netzwerk, um bestimmte politische Positionen zu unterstützen (beispielsweise „Liken" auf Facebook oder die Teilnahme an einem virtuellen Termin).

Kollektive Aktionen können aber auch in „Social-Media-Action-Bereiche" von NGOs eingebettet sein, die die *Meinungsäußerungen bündeln* und grafisch aufarbeiten und sie auf diese Weise für Außenstehende sichtbar machen (z.B. Online-Paraden oder virtuelle Menschenketten).

Ob diese vielen Möglichkeiten neuer Protestformen im Netz allerdings zur Demokratisierung und einer Stärkung der Zivilgesellschaft führen, wird besonders in den USA kontrovers diskutiert. Auf der einen Seite stehen BefürworterInnen, die auf die neu entstandenen Formen von Aktivismus, die gesunkenen Organisations- und Kommunikationskosten und die gestiegenen TeilnehmerInnenzahlen verweisen. Auf der anderen Seite vertreten SkeptikerInnen die Meinung, dass im Netz vielfach „zahnloses" Massenverhalten zu beobachten sei, wie das bloße Mitteilen der eigenen Meinung in sozialen Netzwerken (sog. *Slacktivism* oder *Clicktivism*). Diese Ausdrucksformen seien nicht mit nachhaltigem politischem Aktivismus vergleichbar, bei dem

sich AktivistInnen dauerhaft engagieren und gegebenenfalls auch persönliche Risiken eingehen, um eine gesellschaftliche Veränderung zu bewirken. Ein weiterer Kritikpunkt wird in der „politischen" Neutralität von technischen Entwicklungen gesehen. Das Internet und die damit vorhandenen neuen Kommunikationsmethoden könnten nicht nur von NetzbürgerInnen und AktivistInnen eingesetzt werden, sondern erleichterten gleichzeitig die Arbeit von Sicherheits- und Geheimdiensten, besonderes in repressiven Regimen zur Überwachung und Unterdrückung von politischen GegnerInnen.

Gerade vor dem Hintergrund dieser Gefahr drängt sich die Frage nach dem Schutz digitalen Protests durch die Menschenrechte auf.

3. Menschenrechte und digitaler Protest

Der Menschenrechtsschutz gilt online wie offline (s. Matthias C. Kettemann, Kapitel 2.1. *Neue Menschenrechte für das Internet?*). Grund- und Menschenrechte machen vor der virtuellen Sphäre nicht Halt. Daraus folgt, dass sich politische AktivistInnen auch im virtuellen Raum auf ihre Rechte berufen können.

Allerdings gibt es kein dezidiertes Recht auf Online-Protest. Ein Problem besteht zudem darin, dass Entscheidungen von internationalen Gerichten oder nationalen Höchstgerichten mit Bezug zu digitalen Protesten vielfach noch ausständig sind. Daraus folgt ein gewisses Maß an Rechtsunsicherheit.

Grundsätzlich müssen die rechtlichen Kriterien zu traditionellen Protestaktivitäten auf den Onlinebereich übertragen werden. Ob und wie die einzelnen Schutzbereiche der jeweiligen Menschenrechte auf digitalen Protest anwendbar sind, ist nicht nur eine Frage des Einzelfalls, sondern auch teilweise umstritten. Im Zentrum steht die Übertragungsfähigkeit und Vergleichbarkeit der Protestmittel, wobei die Eigenheiten des digitalen Protests aber nicht außer Acht gelassen

werden dürfen. Letztlich muss auch der Schutzzweck der jeweiligen Norm berücksichtigt werden.

Diese Übertragung kann im Einzelfall schwierig sein, wie aktuelle Probleme in Zusammenhang mit der Versammlungsfreiheit im Internet verdeutlichen: Allein die Bezeichnung einer DDoS durch die AktivistInnen als *Onlineversammlung* führt sicherlich nicht dazu, dass sie dem Schutzbereich der Versammlungsfreiheit unterliegt. Ist es aber überzeugend, die virtuelle Versammlungsfreiheit gänzlich abzulehnen, wie dies aktuell beispielsweise in Deutschland vielfach vertreten wird? Wie könnte der Schutzbereich der Versammlungsfreiheit im Internet definiert werden? Was bedeutet beispielsweise *friedlich* im virtuellen Raum – bzw. wann liegt bei virtuellen Protesten Gewalt vor?

Onlineproteste können je nach Art und Inhalt in den Schutzbereich verschiedener Menschenrechte fallen. Dies sind insbesondere Meinungs- und Informationsfreiheit, Versammlungs- und Vereinigungsfreiheit, Persönlichkeitsrecht und Datenschutz, Kunstfreiheit oder auch das Petitionsrecht. Auch speziellere Rechte wie Glaubens- und Religionsfreiheit oder das Recht auf Bildung können im Einzelfall Anwendung finden. Eine e-Petition als Protest gegen die Regierungspolitik unterliegt eben einem anderen Recht, als eine politische Diskussionsrunde mehrerer Personen in einem Onlineforum wie Google Hangout. Geschützt sind aber gleichwohl beide.

Auch die Form des staatlichen Eingriffs muss für die Anwendung der jeweiligen Menschenrechte berücksichtigt werden. So wird das Filtern einer Nachricht durch staatliche Behörden an der Meinungs- und Informationsfreiheit zu messen sein, wohingegen das Ausspionieren eines privaten Rechners, auf dem eine E-Mail gespeichert ist, in den Bereich des Persönlichkeits- oder Datenschutzes fällt (in Deutschland entwickelte das Bundesverfassungsgericht sogar ein eigenes Grundrecht auf digitale Intimsphäre mit der etwas sperrigen Bezeichnung „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“).

Obwohl die Menschenrechte digitalen politischen Protest durchaus erfassen, ist wesentlich zu beachten, dass diese Rechte nicht schrankenlos gewährleistet werden. Wenn die Menschenrechte offline wie online gelten, so erstreckt sich dies auch auf ihre Grenzen und Schranken.

An der Meinungsäußerung wird dies deutlich: Es mag rechtlich keinen Unterschied machen, ob diffamierende, verletzende Meinungsäußerung offline oder online getätigt wird. Unabhängig von der Verbreitungsform bleibt die Äußerung rechtswidrig.

Daher müssen die Rechte Dritter mit den Rechten der AktivistInnen abgeglichen werden. Proteste können zu Beeinträchtigungen und Verletzungen des Daten- und Eigentumsschutzes anderer führen, aber auch den Schutz der öffentlichen Sicherheit und Ordnung beeinträchtigen. Bei der Bestimmung, welche Beeinträchtigungen Dritte hinnehmen müssen, können für digitale Protestformen die Kriterien, die die internationalen Gerichte und jeweiligen nationalen Gerichte im Zusammenhang mit traditionellen Protesten entwickelt haben, eine hilfreiche Richtschnur bilden.

Ein weiteres Problem ergibt sich aus der Ubiquität des Internets. Politischer Online-Aktivismus macht vor staatlichen Grenzen nicht halt. So können die nationalen Rechtsordnungen ein unterschiedliches Maß an Schutz für politische Aktivitäten bieten; ein und dieselbe Online-Kampagne kann in Schweden geschützt sein und in Russland der Internetzensur unterliegen.

Zudem werden AktivistInnen in vielen Staaten verfolgt. Weltumspannende Online-Aktivitäten ändern nichts daran, dass sich AktivistInnen zumeist physisch weiter in ihrem Heimatland aufhalten. Daher ist hervorzuheben, dass politischer Onlineprotest jenseits der nationalen Rechtsordnungen auch durch die internationalen Menschenrechtsinstrumente (z.B. die Europäische Menschenrechtskonvention und den Zivilpakt der Vereinten Nationen) geschützt wird.

Neben den internationalen Menschenrechtsschutzmechanismen gibt es auf internationaler Ebene auch Bestrebungen zur Vereinheitlichung nationaler rechtlicher Standards in Bezug auf das Internet. Ein Beispiel ist das Übereinkommen des Europarates über Computerkriminalität aus dem Jahr 2001[1], auf dessen Grundlage die Vertragsstaaten ihre nationalen Strafrechtsregelungen angepasst haben. Auch Fälle von Online-Protest sind von diesen Regelungen erfasst. Aufgrund des Übereinkommens sind DDoS in vielen Rechtsordnungen strafbar. Auch Defacements oder der Diebstahl von Daten können strafrechtswidrig sein.

Zusammenfassend lässt sich feststellen, dass politischer Protest mit digitalen Mitteln grundsätzlich durch Grund- und Menschenrechte geschützt ist, wobei im Einzelfall nach Form und Durchführung des Protests untersucht werden muss, welches Recht einschlägig ist. Auch ist die Form des staatlichen Eingriffs für die Einordnung von Bedeutung. Die Reichweite der einzelnen Menschenrechte ist jedoch für den Online-Bereich noch nicht abschließend geklärt. Unabhängig davon gelten für politischen Protest im Internet auch Schranken und Grenzen.

4. Digitaler ziviler Ungehorsam

Die Rechtsfragen von Zulässigkeit und Grenzen digitalen Protests sind für AktivistInnen oft nicht der alleinige Maßstab bei der Auswahl von Protestmitteln: In einer Rechtsordnung kann eine bestimmte Form von politischem Aktivismus verboten sein, aber AktivistInnen können diese Protestaktion dennoch als legitim erachten. In diesen Konstellationen stehen Gerechtigkeitsbewusstsein und die tatsächlichen (rechtlichen oder sozialen) Verhältnisse in Widerspruch. Es kommt zu

[1] Vgl. conventions.coe.int/treaty/ger/treaties/html/185.htm (Letzter Aufruf: 3.4.2013)

einem Spannungsverhältnis von Recht und Moral, von Legalität und Legitimität.

Werden bewusste, öffentliche Regelverletzungen zur Aufmerksamkeitserlangung für ein Protestanliegen als Mittel eingesetzt, spricht man (auch) von zivilem Ungehorsam. Diese Proteste bewegen sich zwischen symbolischer und direkter Aktion.

Allerdings bestehen auch für den Begriff „ziviler Ungehorsam" Definitionsprobleme. Er ist ein politischer Begriff, der insbesonders in politischen Auseinandersetzungen für die Legitimation eigener Aktionen eingesetzt wird. Ziviler Ungehorsam ist begrifflich prinzipiell positiv belegt und wird daher gerne von AktivistInnen zur Selbstbeschreibung ihrer Aktionen gewählt. Grund dafür sind auch prägende Beispiele des erfolgreichen Einsatzes von zivilem Ungehorsam in politischen Bewegungen aus der jüngeren Geschichte wie durch Mahatma Gandhi oder Martin Luther King.

Aus rechtlicher Perspektive stellt ziviler Ungehorsam jedoch keinen weiteren Rechtfertigungs- oder Entschuldigungsgrund im strafrechtlichen Sinne dar. In einigen Rechtstaaten kann ziviler Ungehorsam allerdings in engen Grenzen bei der Strafbemessung Beachtung finden, indem er als Milderungsgrund berücksichtigt wird (z.B. in Deutschland oder in der Schweiz).

Wichtig ist es daher in den Vordergrund zu stellen, dass ziviler Ungehorsam weniger die rechtliche Sphäre betrifft (Legalität), als eine Frage von Ethik und Moral (Legitimität) ist.

Was als (ethisch) zulässig angesehen wird, hängt auch vom politischen Standpunkt ab. Eine radikale AnarchistIn wird ein viel weiteres Verständnis von zivilem Ungehorsam vertreten als eine gemäßigte DemokratIn, die grundsätzlich den Rechtsstaat westlicher Prägung akzeptiert. Trotz dieses Grundproblems ist der Begriff aber nicht völlig beliebig inhaltlich aufladbar oder von rein persönlicher Interpretation abhängig.

Wird ziviler Ungehorsam als Fremdbeschreibung für politische Proteste genutzt, so bedarf es objektiver Bestimmungskriterien. Wann aber ist eine Protestform ethisch vertretbar? Welche Kriterien muss politischer Protest im Internet erfüllen, um als legitimer digitaler ziviler Ungehorsam eingestuft werden zu können?

Philosophen wie John Rawls oder Jürgen Habermas haben in ihren Theorien Vorschläge für objektive Kriterien gemacht.

Rawls definiert zivilen Ungehorsam als einen „public, nonviolent, conscientious yet political act contrary to law usually done with the aim of bringing about a change in the law or the policies of the government."[2] Die AktivistIn müsse allerdings bereit sein, die rechtlichen Konsequenzen ihres Protests zu tragen.

Eine ähnliche Definition, basierend auf einem engen Verständnis des zivilen Ungehorsams, formuliert auch Habermas:

> *„Ziviler Ungehorsam ist ein moralisch begründeter Protest, dem nicht nur private Glaubensüberzeugungen oder Eigeninteressen zugrunde liegen dürfen; er ist ein öffentlicher Akt, der in der Regel angekündigt ist und von der Polizei in seinem Ablauf kalkuliert werden kann; er schließt die vorsätzliche Verletzung einzelner Rechtsnormen ein, ohne den Gehorsam gegenüber der Rechtsordnung im Ganzen zu affizieren; er verlangt die Bereitschaft, für die rechtlichen Folgen der Normverletzung einzustehen; die Regelverletzung, in der sich ziviler Ungehorsam äußert, hat ausschließlich symbolischen Charakter – daraus ergibt sich schon die Begrenzung auf gewaltfreie Mittel des Protests."*[3]

---

[2] Rawls, J. (1971). A Theory of Justice, Cambridge, Massachusetts: Belknap Press of Harvard University Press, Kapitel 6 (dt. Ausgabe (1975). Eine Theorie der Gerechtigkeit, Frankfurt: Suhrkamp), S. 364.

[3] S. Habermas, J. (1983). Ziviler Ungehorsam – Testfall für den demokratischen Rechtsstaat. Wider den autoritären Legalismus in der Bundesrepublik. In P. Glotz (Hrsg.), Ziviler Ungehorsam im Rechtsstaat, Frankfurt am Main: Suhrkamp, 29–53, S. 35.

Vier Grundelemente lassen sich für die Einstufung eines Rechtsbruchs als Akt zivilen Ungehorsams aus diesen Definitionsversuchen entnehmen:

- Öffentlichkeit (Ankündigung gegenüber den Behörden)
- Gewaltlosigkeit
- Bewusstsein (moralische, ernst gemeinte Überzeugung)
- prinzipielle Rechtstreue (grundsätzliche Akzeptanz des Systems und Bereitschaft, Konsequenzen der Aktion zu tragen)

Dennoch ist die Reichweite der einzelnen Elemente umstritten. KritikerInnen werfen Rawls oder Habermas vor, zu enge Definitionen zu wählen, die das gewünschte Ergebnis vorherbestimmen. Teilweise wird sogar vertreten, dass ein gewisses Maß an Gewalt bei zivilem Ungehorsam zulässig sein müsse, um überhaupt die nötige Aufmerksamkeit zu erlangen.

Trotz der Kritik lassen sich diese Prinzipien generell auf digitale Proteste und somit auf Formen digitalen zivilen Ungehorsams übertragen. Allerdings ergeben sich auch hier Folgefragen und Probleme. Wann ist digitaler ziviler Ungehorsam gewaltfrei? Was bedeutet Gewalt im Zeitalter der Informationsgesellschaft und Cyberattacken? Muss dafür ein physisches Element vorliegen oder reichen auch Formen von struktureller Gewalt oder psychischer Zwangswirkung aus?

An dieser Stelle schließt sich der Kreis: Die Frage der Übertragung von Begriffen oder deren Anwendung auf eine veränderte Realität stellt sich gleichermaßen im moralischen wie im rechtlichen Kontext. Definitionen haben konkrete Auswirkungen, wie ein Beispiel aus dem internationalen Recht verdeutlicht: Bricht ein Staat das allgemeine Gewaltverbot (Art. 2 IV UN-Charta) und ist die Aktion darüberhinaus als bewaffneter Angriff zu qualifizieren, so hat der angegriffene Staat das Recht zur Selbstverteidigung (Art. 51 UN-Charta). Das kann im Extremfall bedeuten, dass eine Cyberattacke – sollte diese als

bewaffneter Angriff definiert werden – rechtmäßig mit militärischer, physischer Gewalt beantwortet werden könnte.

5. Ergebnis

Die Veränderungen der (politischen) Kommunikationsmittel, welche die schnellen technischen Entwicklungen auslösen, stellen die Rechtsordnungen vor große Herausforderungen. Einige Probleme und Konflikte der digitalen Sphäre sind altbekannte Konstellationen in bloß neuem Gewand und daher mit den bestehenden Menschenrechten lösbar. In anderen Bereichen aber werden in Zukunft neue Regelungen, besonderes auf internationaler Ebene, erforderlich sein. (Vgl. Matthias C. Kettemann, Kapitel 2.1. *Neue Menschenrechte für das Internet?* bzw. als Gegenstandpunkt: Hans Christian Voigt, Kapitel 1.2. *Rechte eines jeden Menschen _am_ Internet.*)

Mit Blick auf zivilen Ungehorsam sollte man nicht vergessen, dass er Zeichen einer aktiven Zivilgesellschaft ist. AktivistInnen streben Einfluss auf Politik und Veränderungen der Rechtssysteme mit Hilfe von Methoden außerhalb der etablierten staatlichen Organe an. Für die AktivistInnen der amerikanischen Bürgerrechtsbewegung war der zivile Ungehorsam ein zentrales Mittel der politischen Auseinandersetzung zur Abschaffung der Rassentrennung in den USA. Eines der ersten Sit-ins der Geschichte wurde von vier afroamerikanischen StudentInnen initiiert, als sie sich an die Bar eines Restaurants in Greensboro (North Carolina) setzten, das ausschließlich für Weiße reserviert war. Dieser Akt zivilen Ungehorsams war ein Meilenstein für die Überwindung der US-amerikanischen Segregationspolitik.

Ziviler Ungehorsam ist immer auch mit dem Einsatz neuer, nicht etablierter Methoden in der politischen Auseinandersetzung verbunden. Er hat ein (ver)störendes Element, das für Unruhe sorgt und gesellschaftliche Spannungen sichtbar macht. Auch die neuen Erscheinungsformen digitalen zivilen Ungehorsams, die von der

Zivilgesellschaft eingesetzt werden, haben das Potential, zu einer Veränderung und Verbesserung sozialer und politischer Verhältnisse beizutragen.

Weiterführende Literatur

Gladwell, M. (2010). Small Change. Why the revolution will not be tweeted. The New Yorker (4. Oktober 2010). http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell?currentPage=all (Letzter Aufruf: 15.11.2012)

Möhlen, C. Das Recht auf Versammlungsfreiheit im Internet. Anwendbarkeit eines klassischen Menschenrechts auf neue digitale Kommunikations- und Protestformen, MMR 2013, 221–230.

Morell, A. (2001). Online-Aktivismus: Vom virtuellen Sit-In bis zur digitalen Sabotage. In com.une.farce, Zeitschrift für kritik im netz und bewegung im alltag, Nr. 5. (Letzter Aufruf: 17.11.2012)

Morozov, E. (2011). The net delusion: The dark side of Internet freedom. New York: Public Affairs.

Pabst, A. (2012). Ziviler Ungehorsam: Annäherung an einen umkämpften Begriff. In APuZ, Nr. 25/26. http://www.bpb.de/apuz/138281/ziviler-ungehorsam-annaeherung-an-einen-umkaempften-begriff?p=all (Letzter Aufruf: 18.11.2012)

Shirky, C. (2010). The Twitter Revolution: more than just a slogan. In: Prospect Magazine (6. Januar 2010). http://www.prospectmagazine.co.uk/2010/01/the-twitter-revolution-more-than-just-a-slogan/ (Letzter Aufruf: 19.11.2012)

Zuckerman, E. (2011) Cute Cats and The Arab Springs: When Social Media Meet Social Change, Vortrag vom 20. November 2011 in der Vancouver Human Rights Lecture Serie in Vancouver, CBC Radioausstrahlung (09. Dezember 2011), Podcast: http://podcast.cbc.ca/mp3/podcasts/ideas_20111209_27861.mp3 (Letzter Aufruf: 19.11.2012)

Anmerkung

Die Ausführungen in diesem Artikel stellen eines der Forschungsergebnisse des laufenden Dissertationsvorhabens dar.

2.3. Internetsperren und Menschenrechte (Eva Jana Messerschmidt)

Keywords: Internetzensur, Netzsperren, Menschenrechte

1. Internetsperren und Sperrtechnologien 111
2. Zweck von Netzsperren 113
3. Internetsperren im Lichte der EMRK[1] 119
4. Fazit 121

1. Internetsperren und Sperrtechnologien

Seit dem 1. November 2012 gilt in Russland ein neues Mediengesetz.[2] Es soll die Internetkriminalität bekämpfen, indem eine nicht öffentliche schwarze Liste von Internetseiten erstellt wird. Die betroffenen Websites sollen seitens der Zugangsprovider gesperrt werden. Obwohl die russische Regierung dieses Gesetz mit dem Kinderschutz rechtfertigt, vermuten viele KritikerInnen darin eine weitreichende Internetzensur, die sogar Sperrungen ausländischer Seiten zur Folge haben könnte. Solche Internetsperren werden schon lange weltweit zu unterschiedlichen Zwecken eingesetzt. Sie bedeuten eine inhaltliche Zensur sowie eine Verhinderung des Zugangs zu einzelnen Webseiten oder gar eine Totalabschaltung des Internets. Dabei werden diese Netzsperren nicht nur durch staatliche Institutionen bzw. auf Grund von staatlichen Verfügungen durchgeführt. Auch private Unternehmen wie beispielsweise Twitter oder Google verwenden diese Technologien, um illegale Angebote im Internet zu unterbinden.

---

[1] Europäische Menschenrechtskonvention

[2] Vgl. http://www.heise.de/tp/artikel/37/37931/1.html und en.rsf.org/russia-internet-access-barred-as-wave-of-01-11-2012,43627.html. (Letzter Aufruf: 30.5.2013)

Ein staatliches Vorgehen gegen rechtswidrige Inhalte stößt, da es über Staatsgrenzen hinausreicht, an völkerrechtliche Hindernisse. Wegen der fehlenden Gebietshoheit greifen daher zahlreiche Staaten zu Zugangssperren.[3] Da keine Möglichkeit besteht, gegen ausländische Content-Provider vorzugehen, werden die inländischen Access-Provider entsprechend in die Pflicht genommen. Tätig werden diese aber auch, um unerwünschte Seiten innerhalb des eigenen Staatsgebietes zu sperren. Solche Praktiken werden kritisiert, da Zugangsprovider dadurch zu einer Art staatlichen Werkzeugs werden.[4]

Zu den weitverbreiteten Sperrtechnologien gehören die Netzsperren am DNS-Server, Sperrungen durch Einträge in den Routing-Tabellen, Sperrungen durch einen Proxy-Server, hybride Sperransätze sowie die Technologie namens Deep Packet Inspection.[5] Nachweislich können alle Netzsperren umgangen werden. So ist es für DurchschnittssucherInnen im Internet bei einer DNS-Manipulation möglich, durch die direkte Eingabe der bekannten IP-Adresse statt des Domainnamens oder durch die Verwendung eines alternativen DNS-Servers das gewünschte Angebot doch zu erreichen.[6] Aber auch für alle anderen Technologien gibt es entsprechende Umgehungsmöglichkeiten.[7] Als

---

[3] Vgl. Sieber / Nolde, Sperrverfügungen im Internet, 2008, S. 2 f. und S. 228.

[4] Die Zugangs-Provider sollen damit „zum Büttel des Staats für dessen Absichten der Inhaltsregulierung“ werden. Vgl. Christoph Engel, Die Internet-Service-Provider als Geiseln deutscher Ordnungsbehörden, Eine Kritik an den Verfügungen der Bezirksregierung Düsseldorf, in: MMR-Beilage 4/2003, S. 1 (17).

[5] Zu den verschiedenen Sperrtechniken siehe: Sieber/ Nolde, Sperrverfügungen im Internet, 2008, S. 49 ff.; Koreng, Zensur im Internet, Der Verfassungsrechtliche Schutz der digitalen Massenkommunikation, 2010, S. 134 ff.

[6] So hat z.B. das Landgericht Hamburg einen Antrag auf einstweilige Anordnung zur Sperrung einer Webseite zurückgewiesen, da es dem Gericht selbst gelang, innerhalb einer kurzen Zeit eine DNS-Sperre zu umgehen und den gewünschten Server zu finden. Vgl. LG Hamburg, BeckRS 2009, 9535.

[7] Als ein Beispiel für die leichte Umgehung und somit die Ungeeignetheit der Netzsperren kann das Vorgehen des Torrent-Verzeichnisses The Pirate Bay genannt werden. Wegen des Verstoßes gegen das Urheberrecht wurde diese Suchmaschine per gerichtliche Anordnung z.B. in Belgien, Finnland und letztlich in

Anti-Blockade-Software wird z.B. die Hilfssoftware Psiphon eingesetzt. Die Technik ist bei solchen Programmen grundsätzlich gleich: Die Datenspur zwischen einem Rechner und einem Server wird beseitigt, indem der Datenverkehr über Umwege geleitet wird.[8]

2. Zweck von Netzsperren

Die staatlichen Netzsperren werden einerseits in einem Rechtsstaat genutzt, um rechtswidrige Inhalte wie Kinderpornographie, illegale Glückspielangebote oder Urheberrechtsverletzungen im Internet zu bekämpfen.

Auf EU-Ebene sorgte das Anti-Piraterie-Abkommen (ACTA) für Aufsehen. Die geheimen Verhandlungen zwischen der EU, den USA, Japan und vielen anderen Ländern dauerten über drei Jahre lang. Das Ziel von ACTA war die Bekämpfung von Produktpiraterie und Urheberrechtsverletzungen. Zum Schutz von Immaterialgüterrechten sollten u.a. die Überwachung des Netzwerkes durch die InternetanbieterInnen und die Weiterleitung der daraus gewonnenen Informationen an die RechtsinhaberInnen durchgeführt werden. Obwohl die umstrittenen Internetsperren nach dem „Three-Strikes" Prinzip in den Text nicht aufgenommen wurden, sollten die betreffenden Passagen nur scheinbar gestrichen werden und eine Sperrung auf Umwegen doch möglich gewesen sein.[9] Nachdem gegen das Urheberrechtsabkommen in vielen Ländern Tausende protestierten, mehrere EU-Staaten die Ratifizierung aussetzten und der EuGH eingeschaltet

---

Großbritannien gesperrt. Dies hinderte die Betreiber nicht daran, neue IP-Adressen einzurichten, so dass die Seite wieder abrufbar war. Im Übrigen zog nun The Pirate Bay – wohl um der behördlichen Verfolgung zu entgehen – in eine Cloud um.

[8] Vgl. http://www.spiegel.de/netzwelt/netzpolitik/psiphon-die-anti-zensursoftware-a-857981.html (Letzter Aufruf: 30.5.2013)

[9] Vgl. http://www.heise.de/newsticker/meldung/Gutachter-raet-zu-komplettem-Neustart-beim-Anti-Piraterie-Abkommen-ACTA-1354240.html (Letzter Aufruf: 30.5.2013)

wurde, verweigerte auch das Europaparlament im Juli 2012 dem Abkommen seine Zustimmung. Das umstrittene Vertragswerk konnte somit in Europa nicht umgesetzt werden.[10]

Im Hinblick auf den Schutz des geistigen Eigentums erregt bisweilen ein weiteres Handelsabkommen das Gemüt bürgerrechtlicher Initiativen. Durch „die kanadische Hintertür"[11] soll ACTA doch noch eingeführt werden – und zwar in der Form des CETA (Comprehensive Economic and Trade Agreement), einem Handelsabkommen zwischen der EU und Kanada, das dem abgelehnten ACTA-Abkommen „geleakten" Verhandlungsunterlagen zufolge teils wortwörtlich entsprechen soll. Dies bestreitet die EU-Kommission – allerdings ohne den Text einer Öffentlichkeit zugänglich zu machen.

Ein weiteres Beispiel für eine – zumindest zu hinterfragende – europäische Netzpolitik stellt die Richtlinie Ipred (Intellectual Property Rights Enfocement Directive)[12] dar. Diese Richtlinie zur Durchsetzung der Rechte an immateriellen Gütern, die von der EU-Kommission auf den Weg der Änderung gebracht wurde, geriet ebenfalls bereits ins Visier von NetzaktivistInnen. Die konkrete Ausgestaltung der Regelung, die vor allem die Strafmaßnahmen für die Fälle des illegalen Kopierens und Verbreitens von Inhalten im Internet regeln soll, ist noch nicht bekannt.

Obwohl vom EU-Parlament sowie vom Rat der EU bereits abgelehnt, muss hier der (nahezu „Orwellsche") Entwurf der Arbeitsgruppe für Strafverfolgung des Rats der EU vom März 2011 zur Lösung der Internetkriminalität (LEWP) Erwähnung finden. Nach diesem Vor-

---

[10] S. dazu http://www.sueddeutsche.de/digital/umstrittenes-urheberrechtsabkommen-eu-parlament-lehnt-acta-ab-1.1401319 (Letzter Aufruf: 30.5.2013)

[11] vgl. http://netzpolitik.org/2012/acta-comeback-durch-die-kanadische-hintertur-ceta/; vgl.: http://www.michaelgeist.ca/content/view/6580/135/ (Letzter Aufruf: 30.5.2013)

[12] vgl. http://www.heise.de/newsticker/meldung/Bruessel-will-schaerfer-gegen-Copyrightverstoesse-im-Web-vorgehen-1429378.html (Letzter Aufruf: 30.5.2013)

schlag sollten gesetzwidrige Webseiten im Internet europaweit gesperrt werden, um „ein sicheres und einheitliches Cyberspace in Europa“ schaffen zu können.[13]

Auch in den einzelnen EU-Ländern werden Zugangssperren eingesetzt. Die Liste der sperrungsfreudigen Länder ist lang und kann hier nicht vollständig angeführt werden, einige Beispiele sollen einen kurzen Überblick über diese Praxis geben.

Große Beachtung – nicht nur bei den NetzaktivistInnen – erfuhr das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen (ZugErschwG), das in Deutschland im Februar 2010 in Kraft getreten war. Das Bundeskriminalamt wurde damit verpflichtet, eine Sperrliste mit Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten zu führen, die kinderpornographische Inhalte i.S.d. § 184 b dStGB enthalten. Diese täglich aktualisierte Liste musste den inländischen Internetprovidern übermittelt werden. Die Provider sollten den Zugang zu den in der Sperrliste genannten Angeboten durch technische Mittel mindestens auf DNS-Ebene sperren. Dieses Gesetz wurde von Anfang an von breiten Diskussionen begleitet. Nachdem es zwischenzeitlich nicht angewendet werden durfte, um das Löschen als Alternative zu testen, wurde das Gesetz im Dezember 2011 aufgehoben.[14] Hervorgehoben werden kann in diesem Zusammenhang auch das Hadopi-Gesetz (Gesetz zur Verbreitung und zum Schutz kreativer Inhalte im Internet) in Frankreich. Das Hadopi 1-Gesetz sah vor, dass bei mehrfachen Urheberrechtsverletzungen der entsprechende Internetzugang bis zu einem Jahr zu sperren sei, wobei die gesperrten NutzerInnen die Providergebühren weiter bezahlen müssen (sog. double peine). Eine neu eingerichtete Behörde konnte bei solchen Verstößen gegen

[13] Vgl. http://www.golem.de/1104/83095.html (Letzter Aufruf: 30.5.2013)

[14] Vgl. z.B. Höhne / Dienst, Das Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen in: jurisPR-ITR 13/2009 Anm. 6, Ziff. D.

das Urheberrecht Mahnungen an die Betroffenen per Mail verschicken und bei der dritten Überschreitung eine Sperre anordnen (sog. Three-Strikes-Verfahren). Demnach war eine vorherige richterliche Anordnung nicht erforderlich, was auch der ausschlaggebende Grund war, dass dieses Gesetz durch den französischen Verfassungsrat für nicht rechtmäßig erklärt wurde. Sein Nachfolger, das Hadopi 2-Gesetz, schreibt nun vor, dass für die Sperrung sowie die weiteren Strafen ein Gericht zuständig ist. Im Herbst 2012, zwei Jahre nach dem dieses Gesetz in Kraft getreten ist, wurde in Frankreich die erste Geldstrafe wegen eines Verstoßes gegen das Urheberrecht verhängt.[15]

In Belgien endete im November 2011 ein Kampf gegen die Internetpiraterie mit einem Urteil des EuGH. Im konkreten Streit ging es um die Verpflichtung eines belgischen Providers, Urheberrechtsverstöße im Netz durch präventive Filtermaßnahmen sowie Sperren zu verhindern. Im Rahmen des Vorabentscheidungsverfahrens war insbesondere zu prüfen, ob das auf eigene Kosten einzuführende, zeitlich unbegrenzte Filter- und Sperrsystem mit der EU-Charta der Grundrechte konform ist. Das Gericht stellte fest, dass eine solche präventive Überwachung eine aktive Beobachtung sämtlicher elektronischer Kommunikation im Netz des betreffenden Providers erfordern würde. Zudem würde jede zu übermittelnde Information sowie alle das Netz nutzende KundeInnen erfasst werden. Obwohl das Recht am geistigen Eigentum in der Charta garantiert wird, gilt dieses Recht nicht schrankenlos. Das zentrale Filter- und Sperrsystem beeinträchtigt dem EuGH[16] zufolge somit unter anderem das Recht auf den Schutz personenbezogener Daten und auf Informationsfreiheit.

Diktaturen hingegen nutzen solche Zugangssperren, um demokratische Bewegungen zu untergraben, wobei nicht nur einzelne Webseiten, sondern der ganze Internetzugang gesperrt werden kann. Zu einer

---

[15] Vgl. http://www.heise.de/newsticker/meldung/Erstes-Urteil-gegen-Raubkopierer-in-Frankreich-1707909.html (Letzter Aufruf: 30.5.2013)

[16] Urteil vom 24.11.2011, Az. C-70/10.

solchen Totalabschaltung kam es beispielsweise zwischen Januar und Februar 2011 in Ägypten.[17] Diese Maßnahme wurde von der damaligen Regierung angeordnet, um die DemonstrantInnen sowohl untereinander als auch von der Außenwelt „zu trennen", indem die sog. BGP-Routen des ägyptischen Internet ins Ausland unterbrochen wurden. Als Folge konnten die ägyptischen Domain-Name-Server nicht mehr aufgerufen werden und Ägypten war tagelang offline. Auch die libysche Regierung kappte im Februar 2011 für Stunden die Internetverbindungen des Landes, um die damaligen Massenproteste zu verhindern. In Syrien erfolgte im November 2012 eine Internetblockade, bei der sämtliche Netzverbindungen ins und aus dem Land für 48 Stunden abgeschaltet wurden.[18]

Obwohl die Sperrungen bestimmter Webseiten seitens der diktatorischen Regierungen mit dem Hinweis auf die Bekämpfung von Delikten, die auch außerhalb des Internets illegal sind, gerechtfertigt wurden, dient solche Zensur vordergründig der Verhinderung regierungskritischer Online-Informationen.[19]

Zu den schärfsten weltweit zählt die Internetzensur in China. Hier hat mittlerweile ein Viertel der Gesamtbevölkerung einen Internetzugang. Es ist daher nicht verwunderlich, dass die Regierung das Netz nicht nur voll unter Kontrolle zu bekommen versucht, sondern dieses auch

---

[17] Vgl. http://www.spiegel.de/netzwelt/netzpolitik/totalabschaltung-wie-aegypten-aus-dem-internet-verschwand-a-742232.html (Letzter Aufruf: 30.5.2013)

[18] Vgl. http://www.zeit.de/digital/internet/2012-11/syrien-internet-blackout; http://www.heise.de/newsticker/meldung/Syrische-Netzblockade-hatte-fast-keine-Luecken-1763939.html (Letzter Aufruf: 30.5.2013)

[19] Nach einem Bericht der Organisation „Reporter ohne Grenzen" gehören zu den sogenannten „Feinden des Internets 2012" folgende Länder: Bahrein, Belarus, Birma, China, Kuba, Iran, Nordkorea, Saudi Arabien, Syrien, Turkmenistan, Usbekistan und Vietnam. Hier kommt es nicht nur zu einer ständigen Internetüberwachung und -zensur, sondern werden auch unliebsame Blogger systematisch verfolgt, wobei Iran und China ihre Internetüberwachungsmaßnahmen im Vergleich zum Vorjahr verstärkt haben sollen. Vgl. http://www.reporter-ohne-grenzen.de/presse/pressemitteilungen/meldung-im-detail/artikel/rog-bericht-feinde-des-internets-2012/ (Letzter Aufruf: 30.5.2013)

zur Selbstpropaganda nutzen will. Die Internetzensur in China hat eine lange „Tradition". Hier wurde bereits 1998 mit dem sogenannten Golden Shield Projekt begonnen, das sich mit der Überwachung und Inhaltszensur des Internets befasst.[20] Die „Chinesische Mauer 2.0 (Great Firewall)"[21] wird durch die dortige Regierung mit dem Gesetz über Staatsgeheimnisse sowie dem Parteienprinzip gerechtfertigt. Letzteres soll die Gefährdung der Herrschaft der Kommunistischen Partei Chinas, wozu auch die Forderung nach Menschenrechten zählt, verhindern. Den Höhepunkt des Versuchs einer staatlichen Machtübernahme des Internets stellt die Sperrung des Zugangs zu den Google-Diensten im Oktober 2012 dar.[22]

Internetsperrungen erfolgen mittlerweile auch durch Private, und zwar entweder auf freiwilliger Basis oder aufgrund von behördlichen Hinweisen und gerichtlichen Beschlüssen. Sie werden beispielsweise wegen Copyright-Ansprüchen oder des Vorwurfs von *hate speech* durchgeführt. Google sperrte vor einiger Zeit in manchen Staaten – ohne richterliche Anordnung – den Film *The Innocence of Muslims*. Als aktuelles Beispiel für eine solche Blockierung[23] einer Webseite durch ein privates Unternehmen kann auch die Sperrung des Accounts einer verbotenen Neonazi-Gruppe für deutsche NutzerInnen durch Twitter genannt werden. Der Kurznachrichtendienst

---

[20] Vgl. Clayton / Murdoch / Watson, Ignoring the Great Firewall of China: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf (Letzter Aufruf: 30.5.2013)

[21] Vgl. http://www.faz.net/aktuell/politik/ausland/internetzensur-chinesische-mauer-2-0-1991259.html (Letzter Aufruf: 30.5.2013)

[22] Vgl. http://www.heise.de/newsticker/meldung/China-sperrt-waehrend-des-Parteitags-den-Zugang-zu-Google-1747841.html (Letzter Aufruf: 30.5.2013)

[23] Twitter wurde von der Polizeidirektion Hannover aufgefordert, das Twitterkonto der verbotenen Neonazi-Gruppe „umgehend und ersatzlos zu schließen". Solche landesspezifischen Sperren sind bei Twitter neu, bis jetzt betrafen durchgeführte Sperrungen die gesamte Plattform. Vgl. http://www.spiegel.de/netzwelt/netzpolitik/laendersperre-twitter-unterdrueckt-neonazis-in-deutschland-a-861982.html und http://netzpolitik.org/2012/dieser-tweet-ist-in-deinem-land-nicht-verfugbar-twitter-fuhrt-offenbar-landerspezifische-zensur-ein/ (Letzter Aufruf: 30.5.2013)

scheint damit einen Strategiewechsel durchzuführen und sperrt so bestimmte Inhalte nur in den Ländern, in denen diese illegal sind. Der Zugriff auf die betroffene Webseite bleibt ansonsten gewährt.[24]

3. Internetsperren im Lichte der EMRK

Die Konventionsrechte sind auch auf das Internet anwendbar. Dies wurde zum Beispiel in Bezug auf die Meinungsfreiheit nach Art. 10 EMRK im Urteil *Times Newspapers Ltd. gegen Großbritannien* entschieden:

> *„The Court has consistently emphasised that Article 10 guarantees not only the right to impart information but also the right of the public to receive it (see Observer and Guardian v. the United Kingdom, 26 November 1991, § 59(b), Series A no. 216; Guerra and Others v. Italy, 19 February 1998, § 53, Reports of Judgments and Decisions 1998-I). In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10."*[25]

Der EGMR beschäftigte sich auch bereits mit dem Einsatz von Internetsperren.[26] In dem betreffenden Fall ging es um die Verhinderung des Zugangs zu einer persönlichen Webseite. Die türkischen Behörden ließen die Seiten im Netzwerk Google.com sperren, um den Abruf einer ganz bestimmten Seite zu unterbinden. Dadurch wurde jedoch nicht nur eine einzelne, gesetzeswidrige Webseite gesperrt, sondern

---

[24] Auf der Seite http://www.chillingeffects.org können die betroffenen Tweets und Accounts sowie die Gründe für die Sperrung nachgelesen werden. Auch Google veröffentlicht auf: http://www.google.com/transparencyreport/ einen entsprechenden Bericht. Aus diesem ergibt sich u.a., dass Deutschland weltweit an der Spitze der Löschanträge steht. (Letzter Aufruf: 30.5.2013)

[25] EGMR 10.3.2009, Nr. 3002/03, 23676/03, Ziff. 27.

[26] EGMR 18.12.2012, Yildirim gegen Türkei, Nr. 3111/10.

der Zugang zu Google-Webseiten insgesamt. Dabei handelte es sich hier um den sog. Kollateralschaden, also um eine an sich unbeabsichtigte Folge der vorgenommenen Netzsperre. Der Beschwerdeführer rügte die Verletzung des Rechts auf freie Meinungsäußerung gemäß Art. 10 EMRK, da er auf Grund dieser staatlichen Maßnahme auf seine persönliche Webseite, die in keinem Zusammenhang mit der betroffenen Seite stand, nicht zugreifen konnte. Der EGMR stellte eine Verletzung des Rechts aus Art. 10 EMRK fest. In seiner Begründung betonte der Gerichtshof u.a. die Bedeutung des Internets für das Recht auf Meinungsäußerungs- und Informationsfreiheit als eines der wichtigsten Mittel des/der Einzelnen zur Wahrnehmung dieser Konventionsrechte.

Was den Einsatz der Netzsperren in einem Rechtsstaat angeht, kann durch diese sowohl die Informationsfreiheit der RezipientInnen als auch die Meinungs- bzw. Medienfreiheit der InhaltsanbieterInnen beeinträchtigt werden. Die Access-Provider können sich demgegenüber auf die Berufsfreiheit berufen. Diese wird in der EMRK zwar nicht ausdrücklich gewährleistet, entsprechende wirtschaftsrechtliche Bezüge werden allerdings anderen Konventionsrechten zugeschrieben, wodurch neben der Eigentumsgarantie gemäß Art. 1 des 1. ZP EMRK auch die übrigen wirtschaftlichen Grundrechte durch andere Garantien miterfasst werden.[27] Je nach angewandter Sperrtechnologie steckt in der Filterung zusätzlich ein hohes Überwachungspotential, was wiederum die Rechte der InternetnutzerInnen im Hinblick auf Art. 8 (Fernmeldegeheimnis und Datenschutz) verletzen kann. In Diktaturen geht es vordergründig um die Verhinderung der Verbreitung unerwünschter regimekritischer Informationen, so dass hier insbesondere das Recht auf freie Meinungsäußerung bereits durch den Einsatz der Sperren selbst tangiert wird. Durch die Überwachung des Internets liegt außerdem eine zusätzliche Beeinträchtigung vor,

[27] Vgl. Grabenwarter / Pabel, EMRK, 5. Auflage, 2012, S. 516, Rz. 27.

beispielsweise des Rechts auf Freiheit und Sicherheit nach Art. 5 EMRK, sowie des Rechts auf Achtung des Privatlebens aus Art. 8 EMRK oder der Religionsfreiheit nach Art. 9 EMRK. Dies ist nur eine knappe Aufzählung der möglichen Eingriffe in die – durch die EMRK geschützten – Rechte. Es muss immer im Einzelfall geprüft werden, welche Garantien im konkreten Fall tatsächlich betroffen sind.

Naheliegend und höchst interessant im Rahmen der Verwendung der Netzsperren ist auch die Diskussion hinsichtlich der Frage, ob Internetzugang an sich als eigenes Menschenrecht gewährleistet werden soll.[28] (vgl. Matthias C. Kettemann, Kapitel 2.1. *Neue Menschenrechte für das Internet?* und Hans Christian Voigt, Kapitel 1.2. *Rechte eines jeden Menschen _am_ Internet*)

4. Fazit

Dem Äußerungsweg im Internet kommt in der heutigen „On-line-Welt" eine besondere Stellung zu. Die Möglichkeit einer grenzenlosen und kostengünstigen Vernetzung muss als große Chance für die Verwirklichung der Grund- und Menschenrechte angesehen werden. Daneben müssen jedoch auch rechtswidrige Inhalte im Netz verhindert werden. Aufgrund der Tatsache, dass Internetsperren – und sei es auch zum legitimen Zweck – immer mehr zum Einsatz kommen, müssen diese als ultima ratio betrachtet werden. Deren Verwendung setzt also voraus, dass eine Löschung der illegalen Seite oder eine andere Vorgehensweise[29] nicht möglich ist. Um eventuelle Kollateral-

---

[28] http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf / http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html sowie http://www.libelle.me/ausgaben/juni-2012/das-internet-als-menschenrecht/ (Letzter Aufruf: 30.5.2013)

[29] In Dänemark soll neuerdings ein Sperrgesetz aufgrund der mangelnden Wirkung von Netzsperrung außer Kraft gesetzt werden. Im Kampf gegen ein bestimmtes illegales Angebot im Internet soll nun verstärkt internationale Koopera-

schäden durch das Over-Blocking zu vermeiden, sollten die entsprechenden Sperrtechnologien weiter erforscht werden. Dabei muss allerdings neben der zielgenaueren Sperrung auch das damit verbundene Überwachungspotential möglichst niedrig gehalten werden. Die Transparenz des staatlichen wie des privaten Einsatzes solcher Zugangssperren muss gewährleistet werden, da der Missbrauch von Sperren evident ist und die Gefahr einer übermäßigen Kontrolle oder gar eines Versuchs einer Internetreglementierung besteht – nicht nur in Diktaturen. Unumgänglich ist ebenfalls eine diesbezügliche genaue gesetzliche Vorgabe, insbesondere im Hinblick darauf, dass Internetsperren nicht durch eine staatliche Behörde erfolgen können, sondern Access-Provider als entsprechende Werkzeuge benutzt werden. Auch die Selbstzensur der Privaten sollte nicht unterschätzt werden. Trotz der ursprünglichen Ideale zahlreicher Plattformen oder Suchmaschinen absolute Meinungsfreiheit und völlige Transparenz herstellen zu wollen, ist ein Voranschreiten kommerzieller Interessen zu beobachten. Menschen haben durch das Internet fast unbegrenzte Möglichkeiten, sich aus verschiedensten Quellen zu unterrichten, eigene Kommentare abzugeben, oder sich zu einer Versammlung zu verabreden. Dadurch ist es jedoch für staatliche Behörden auch viel einfacher geworden, BürgerInnen zu überwachen, zu verfolgen und durch die vorgenommene Filterung der Internetinhalte eigene „Empfehlungen“ vorzuschreiben.[30] (vgl. Julian Ausserhofer, Kapitel 1.6. *Gute Filter, böse Filter*)

---

tion genutzt werden. Vgl. http://www.heise.de/newsticker/meldung/Daenisches-Parlament-rueckt-von-Websperren-ab-1758768.html (Letzter Aufruf: 30.5.2013)

[30] S. http://netzpolitik.org/2012/das-internet-im-burgerkrieg-in-syrien-uberwachungstechnologien-als-waffen-und-staatliche-hacker/ (Letzter Aufruf: 30.5.2013)

2.4. Paradigmenwechsel Vorratsdatenspeicherung im EU-Datenschutzrecht (Christof Tschohl)

Keywords: Menschenrechte, Datenschutz, Vorratsdatenspeicherung, Unschuldsvermutung, Rechtsstaatsprinzip, Überwachung, Freiheit, Kommunikation, Verkehrsdaten, Grundsatz der Verhältnismäßigkeit

1. Die VDS[1] nach der Richtlinie 2006/24/EG 123
2. VDS als Abschied von anonymen Online-Räumen 126
3. Grundrechtswidrigkeit der Vorratsdatenspeicherung 127
4. Die betroffenen Grundrechte im Detail 128
5. VDS und der Grundsatz der Verhältnismäßigkeit 132
6. Gesellschaftliche Veränderungen durch VDS 134
7. Conclusio 136
Weiterführende Literatur 137

1. Die VDS nach der Richtlinie 2006/24/EG

Bei jeder elektronischen Kommunikation werden bestimmte Daten verarbeitet bzw. erzeugt. Diese Daten werden von den Netz- bzw. DienstanbieterInnen häufig schon zu Betriebszwecken gespeichert, zum Teil aus technischen Gründen, zum Teil für die Rechnungslegung bzw. Vertragsabwicklung. Die Daten müssen nach dem datenschutzrechtlichen Grundsatz der Zweckbindung gelöscht werden, sobald sie für Zwecke der Entgeltverrechnung oder des technischen Betriebes nicht mehr notwendig sind. Die Dauer der Aufbewahrung hängt davon ab, welchem Zweck die Daten dienen. Ausschließlich technisch bedingte Speicherung ist zumeist nur für eher kurze Zeiträume (einige Stunden oder Tage) notwendig, während eine Speicherung verrechnungsrelevanter Daten je nach Geschäftsbedin-

[1] Vorratsdatenspeicherung

gungen der AnbieterInnen üblicherweise bis zu 3 Monaten durchaus gerechtfertigt sein kann. Die Zeiträume unterscheiden sich je nach System und Tarifmodell der AnbieterInnen. Diese Daten werden in der Diskussion oft salopp als *Billing-Daten* bezeichnet, obwohl diese Bezeichnung zu kurz greift, weil nicht nur Daten davon umfasst sind, die zum *Billing* (= Verrechnung) notwendig sind, sondern Daten für alle betriebsnotwendigen, insbesondere für technische Zwecke.

Aufgrund der im Jahr 2006 verabschiedeten Richtlinie 2006/24/EG (Vorratsdatenspeicherungs-Richtlinie) sind sämtliche AnbieterInnen öffentlich zugänglicher Telekommunikationsdienste und AnbieterInnen öffentlicher Kommunikationsnetze (nachfolgend kurz „*AnbieterInnen*“) verpflichtet, das gesamte Kommunikationsverhalten ihrer NutzerInnen für mindestens sechs Monate bis maximal zwei Jahre zu protokollieren. Die EU-Mitgliedstaaten müssen ihren heimischen AnbieterInnen diese Datenspeicherung auf Vorrat gesetzlich vorschreiben, damit die Daten zur Verfolgung schwerer Straftaten europaweit zur Verfügung stehen. Die Speicherung betrifft alle NutzerInnen, unabhängig von einem konkreten Verdacht.

Die von den AnbieterInnen vorrätig gespeicherten Daten sollen entsprechend der Vorratsdatenspeicherungs-Richtlinie dem Zweck der Verfolgung schwerer Straftaten, insbesondere Terrorismus und organisierter Kriminalität, dienen. Allerdings ist den Mitgliedstaaten bewusst die Regelung überlassen, was unter „schweren Straftaten“ zu verstehen ist bzw. ob die Daten auch für präventive Gefahrenabwehr, für Zwecke der Nachrichtendienste oder für völlig andere Interessen verfügbar sein sollen, etwa für die Verfolgung von Urheberrechtsverletzungen oder anderen zivilrechtlichen Streitigkeiten. Die Aufklärung schwerer Straftaten dient damit bloß als Argument, den „Bauchladen“ mit Daten zu füllen; wer sich daraus bedienen darf, können sich die Mitgliedsstaaten aussuchen. Die Erfahrung lehrt, dass mit der Sammlung umfassender und aufschlussreicher Datenbestände die Flut an Begehrlichkeiten nicht lange auf sich warten lässt. Durchsetzen

wird sich wohl, wer im Heimatstaat die stärkste Lobby hat. Dass Regierungen von EU-Staaten Maßnahmen, die in der eigenen Bevölkerung unpopulär sind, wenn möglich gerne auf EU-Ebene beschließen, um den „Schwarzen Peter" dann nach Brüssel zu schieben, ist ebenfalls ein bekanntes Phänomen.

Erstaunlicherweise wird die Richtlinie auf EU-Ebene als reine Maßnahme der Harmonisierung des europäischen Binnenmarkts und nicht einmal teilweise als Maßnahme der „Polizeilichen und Justiziellen Zusammenarbeit in Strafsachen", der vormals sogenannten dritten Säule der EU, gehandelt. Dadurch konnte die Richtlinie praktischerweise mit Mehrheitsbeschluss durch den Rat und das Parlament verabschiedet werden, denn eine (für die damalige dritte Säule notwendige) Einstimmigkeit im Rat wäre politisch nicht zu erreichen gewesen. Der EuGH hat die wettbewerbsrechtliche Natur der Richtlinie anlässlich einer Nichtigkeitsklage der Republik Irland, unterstützt durch die Slowakei, allerdings in einer vielfach kritisierten Entscheidung bestätigt (10.2.2009, C-301/06).[2] Der Europäische Datenschutzbeauftragte Peter Hustinx erklärte in seiner im Rahmen der Konferenz *Taking on the Data Retention Directive* (3. Dezember 2010) gehaltenen Rede, die Richtlinie habe „die Harmonisierung der nationalen Rechtsvorschriften verfehlt."[3] Selbst die EU Kommission hat mittlerweile zugestanden, dass „der Beitrag der Richtlinie zur Harmonisierung der Vorratsdatenspeicherung (…) begrenzt" war.[4]

---

[2] Der Vollständigkeit halber sei angemerkt, dass der irischen Regierung seinerzeit die EU-Regelung zur Vorratsdatenspeicherung zu wenig weit ging und nicht etwa Grundrechtsbedenken diese Klage motiviert haben.

[3] Die Behörde nennt sich auch wörtlich tatsächlich „Der Europäische Datenschutzbeauftragte (EDSB)", s. http://www.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS (Letzter Aufruf: 2.3.2013)

[4] KOM (2011) 225 endgültig, Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), Brüssel 18.4.2011; Online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:DE:PDF (Letzter Aufruf: 2.3.2013)

2. VDS als Abschied von anonymen Online-Räumen

Zu den Begehrtesten unter den Vorratsdaten zählt die Information, welcher TeilnehmerIn eine bestimmte (dynamische) IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Nun besteht das Interesse der Sicherheitsbehörden an einer Auskunft über eine hinter einer IP-Adresse stehende TeilnehmerIn überhaupt nur darin, einen bereits bekannten Inhalt (beispielsweise die Nutzung eines Online-Dienstes, den Zugriff auf eine Website oder den Eintrag in einem Online-Forum) einer bestimmten Person zuordnen zu können. Der Inhalt ist also schon vorher bekannt, bleibt aber ohne die Verkehrsdatenauskunft, die erst den Personenbezug herstellt, anonym. Die Information darüber, welcher TeilnehmerIn eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, stellt sozusagen den *missing link* her, um öffentlich bekannte oder bei einem DienstanbieterInnen ausgeforschte Kommunikationsinhalte mit einer bestimmten Person zu verbinden. Zwar dürfen Internet-ZugangsanbieterInnen nicht aufzeichnen, welche Internetseiten von TeilnehmerInnen aufgerufen wurden. Allerdings sind viele Internetseiten bzw. -dienste technisch derart konzipiert, dass bei Zugriffen auf diese Seiten oder Dienste die IP-Adresse der TeilnehmerInnen sowie der Zeitpunkt des Zugriffs durch den Host-Provider protokolliert und bei manchen Anwendungen auch mit bestimmten Inhalten verknüpft wird (z.B. bei Einträgen in einem Online-Forum). Bei vielen Online-Diensten existieren auch Aufzeichnungen über das konkrete Nutzungsverhalten (z.B. Einkäufe bei Amazon.com, EBay, Suchanfragen bei Google, …).

Gleichzeitig lässt sich daraus noch nicht ableiten, ob die AnschlussinhaberInnen auch mit den UrheberInnen der Kommunikation ident sind. Die Information ist vielmehr bloß ein erster Ermittlungsansatz. Die Zuordnung von Verbindungsdaten (insbesondere IP-Adressen) zu einer bestimmten Person lässt selbst keine Rückschlüsse darüber zu, ob diese Person auch tatsächlich am fraglichen Kommunikationsvorgang beteiligt war. Hierzu bedarf es weiterer konkretisierender Erhe-

bungen, welche gerade bei der Erforschung von Kommunikationsvorgängen im Internet häufig schwer fassbar sind.

Anschaulich lässt sich eine IP-Adresse als eine Art KFZ-Kennzeichen auf dem „Datenhighway" beschreiben. Vielfach wird daher eine Art „IT-LenkerInnenerhebung" erforderlich sein, um Aussagekraft und Zuverlässigkeit der ermittelten Daten beurteilen zu können; denn eine reine Gefährdungshaftung für InhaberInnen von Internet- oder Telefonanschlüssen ist zumindest der österreichischen Rechtsordnung bislang nicht bekannt. Der Aussagekraft und, mit ihr verbunden, dem tatsächlich Nutzen der Daten für den angestrebten Zweck kommt für die Verhältnismäßigkeit der behördlichen Befugnisse entscheidende Bedeutung zu, die bereits abstrakt in jeden Abwägungsvorgang miteinzubeziehen ist. Die Praxis wird dieser Anforderung nicht zuletzt aufgrund des meist nur mäßig entwickelten technischen Verständnisses der RechtsanwenderInnen nicht gerecht.

3. Grundrechtswidrigkeit der Vorratsdatenspeicherung

Grundsätzlich sollte das Verhältnis zwischen einem demokratischen Verfassungsstaat und seinen BürgerInnen bzw. allen in seinem Machtbereich lebenden Menschen von Vertrauen geprägt sein. Jede/r Einzelne soll darauf vertrauen können, dass in ihre/seine grundrechtlich geschützten Positionen im Zuge von Ermittlungstätigkeiten bzw. Strafverfolgungsmaßnahmen grundsätzlich nur bei Vorliegen entsprechender Verdachtsmomente, also als *ultima ratio*, unter Wahrung der rechtstaatlichen Prinzipien, insbesondere unter Beachtung des Verhältnismäßigkeitsprinzips eingegriffen wird. Der Grundsatz, dass gegen eine bestimmte Person ausschließlich bei Vorliegen von Verdachtsmomenten Ermittlungs- bzw. Verfolgungsmaßnahmen gesetzt werden, zieht sich gleich einem roten Faden durch alle rechtsstaatlichen Gesetzgebungen moderner demokratischer Prägung.

Die Vorratsdatenspeicherungs-Richtlinie geht von diesem Grundsatz ab, indem sie eine verdachtsunabhängige, gleichsam antizipierte *Sicherung von Beweismitteln* vorschreibt. Die Grundidee dabei ist simpel: Potenziell ist jede/r verdächtig.

Die Vorratsdatenspeicherung unterminiert aber nicht nur den Schutz der Privatsphäre völlig, Sie bewirkt auch eine nachhaltige Erosion von demokratischen Grundpfeilern wie der Meinungs- und Medienfreiheit, dem Schutz von Berufsgeheimnissen und schließlich der Unschuldsvermutung.

4. Die betroffenen Grundrechte im Detail

Im Einzelnen stellt die Vorratsdatenspeicherung einen – unverhältnismäßigen und daher nicht gerechtfertigten Eingriff in die nachfolgend aufgelisteten Grundrechte dar:

- Art. 8 Europäische Menschenrechtskonvention (EMRK) / Art 7 EU Grundrechte-Charta (GRC) (Privatleben und Familienleben, Schutz der Kommunikation)
- Art. 1 § 1 Datenschutzgesetz (DSG 2000) / Art 8 GRC (Grundrecht auf Datenschutz)
- Art. 10 EMRK / Art 11 GRC (Meinungs- und Informationsfreiheit, Redaktionsgeheimnis)
- Art. 11 EMRK / Art 12 GRC (Versammlungs- und Vereinigungsfreiheit)
- Art 10a Staatsgrundgesetz 1867 (StGG) (Fernmeldegeheimnis)
- Art 6 EMRK / Art 48 GRC (Unschuldsvermutung im Strafverfahren)

Zwar wurden schon bisher vielfältig personenbezogene Daten ermittelt und verarbeitet. Diese Datenanwendungen erfolgen in aller Regel

aber entweder zur individuellen Aufklärung und Verfolgung konkret begangener Straftaten, zur Erfüllung eines Vertrages und somit zumindest mittelbar auf Wunsch bzw. mit Zustimmung der datenschutzrechtlich Betroffenen, oder aber mit dem Ziel, der Gesellschaft die unterschiedlichsten Leistungen der öffentlichen Daseinsversorgung zur Verfügung zu stellen.

Davon unterscheidet sich die Vorratsdatenspeicherung im Sinne der Richtlinie schon durch ihre Zielsetzung in fundamentaler Weise, da personenbezogene Telekommunikations- und Geo-Daten aller KundInnen, die Dienste eines Telekommunikationsunternehmens in Anspruch nehmen, präventiv zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten ohne irgendeinen konkreten Tatverdacht gesammelt und verarbeitet werden.

Die Richtlinie bricht mit dem rechtsstaatlichen Gebot der bestmöglichen Minimierung von Eingriffen in Grundrechte nach dem Grundsatz der Verhältnismäßigkeit. Mussten verarbeitete Verkehrs- und Standortdaten bisher teilweise sofort, grundsätzlich aber jedenfalls dann gelöscht werden, wenn und soweit sie etwa für die Bereitstellung von Telekommunikationsdiensten und in weiterer Folge für die Abrechnung nicht mehr erforderlich waren, wurde diese im Sinne eines effektiven und grundrechtskonformen Datenschutzes normierte Löschungsverpflichtung durch die Richtlinie 2006/24/EG in eine verdachtsunabhängige, flächendeckende Speicherungspflicht verkehrt, um „schwere Straftaten“, insbesondere Terrorakte und organisierte Kriminalität, bekämpfen zu können. Eine vergleichbare Maßnahme in der „analogen Welt“ wäre, wenn künftig gesetzlich vorgeschrieben würde, alle AbsenderInnen und AdressatInnen jedweden Briefes durch die Post dokumentieren zu lassen, weil potentiell jeder Briefkontakt ermittlungsrelevante Information liefern könnte.

Die garantierte Unschuldsvermutung ist eine wesentliche Voraussetzung einer auf angstfreier Kommunikation basierenden Gesellschaft freier Menschen. Der EGMR hat zur Bedeutung der Unschuldsvermu-

tung im Zusammenhang mit der Speicherung von DNA-Profilen und Fingerabdrücken im Fall „S. und Marper vs UK“ (2008) klargestellt:

> *„Im vorliegenden Zusammenhang kommt der Gefahr der Stigmatisierung besondere Bedeutung zu. Diese ergibt sich aus der Tatsache, dass Personen in der Situation der Bf., die nicht verurteilt wurden und für die daher die Unschuldsvermutung gilt, gleich behandelt werden wie verurteilte Personen. Zwar kann die Speicherung der privaten Daten der Bf. nicht mit der Äußerung eines Verdachts gleichgesetzt werden. Ihre Wahrnehmung, nicht als unschuldig behandelt zu werden, wird aber dadurch verdeutlicht, dass ihre Daten ebenso wie die von verurteilten Personen unbeschränkt gespeichert werden, während die Daten von nie verdächtigten Personen vernichtet werden müssen. Die Regierung bringt dazu vor, der einzige Grund für die Speicherung der Daten bestehe in der Steigerung der Größe und damit der Nutzbarkeit der Datenbank zur künftigen Identifizierung von Straftätern. Der GH hält dieses Argument jedoch für schwer vereinbar mit der gesetzlichen Verpflichtung zur Vernichtung der Fingerabdrücke und Proben von Freiwilligen, hätte dieses Material doch ähnlichen Wert für die Vergrößerung der Datenbank.“*[5]

Die flächendeckende Speicherung erhöht zwingend und logisch die Wahrscheinlichkeit, dass sich auch unbescholtene und unschuldige Menschen in einem Ermittlungsverfahren rechtfertigen müssen, warum sie in einer bestimmten Weise zu einer bestimmten Zeit mit einem bestimmten Anschluss in Kontakt standen. Allein in solche Ermittlungen zu geraten – auch wenn sich später herausstellt, dass es rein zufällig war und keine rechtlichen Konsequenzen folgen – kann bereits zu erheblich nachteiligen privaten oder beruflichen Konsequenzen führen. Die Vorratsdatenspeicherung ist jedenfalls geeignet, den Kreis der Verdächtigen immens zu vergrößern, weil die Zahl der auswertbaren Kommunikationsverbindungen größer und umfassender wird.

---

[5] EGMR, S. und Marper vs UK, Urteil vom 4.12.2008, Große Kammer, Bsw. Nr. 30.562/04 und 30.566/04, zitiert aus NL Menschenrechte, http://www.menschenrechte.ac.at/docs/08_6/08_6_14 (Letzter Aufruf: 30.5.2013)

Nicht mit Art. 8 EMRK bzw. Art. 7 GRC vereinbar ist auch die grundsätzliche Gefahr, die aus der systemimmanenten unzuverlässigen Aussagekraft riesiger Datenmengen resultiert, die durch die Vorratsspeicherung von Telekommunikations- und Internetzugangsdaten in allen EU Mitgliedsstaaten angesammelt werden. Die – jedenfalls unter Technikern – „goldene Regel zur Optimierung von Datensicherheit" ist das Prinzip der Datensparsamkeit. Das Risiko steigt exponentiell zur Menge der gesammelten Informationen. Auch der Schaden, der an der Informationsfreiheit durch die permanente Aufzeichnung des Kommunikationsverhaltens der gesamten europäischen Gesellschaft entsteht, lässt sich mit gleichwohl notwendigen „Safeguards" nicht beheben.

Der EGMR wertete im Fall „Segerstedt-Wiberg u.a. v. Schweden"[6] die Sammlung und Aufbewahrung allgemein zugänglicher Quellen wie Artikel in Zeitschriften als Eingriff in das Privatleben, sofern sie systematisch durch Behörden (Geheimdienste, Verfassungsschutz) erfolgt. Revolutionär war in diesem Urteil aber die Feststellung, dass allein schon die (überschießende bzw. nicht gerechtfertigte) Speicherung von Daten einerseits Art. 8 EMRK, andererseits aber auch Art. 10 und 11 EMRK, also die Rechte auf Meinungs- und Versammlungsfreiheit verletzt. Der Gerichtshof stellte fest, dass eine Speicherung von Daten zu politischen Überzeugungen, Tätigkeiten und Parteizugehörigkeiten, die nicht nach Art. 8 Abs. 2 gerechtfertigt werden kann, ipso facto auch eine Verletzung der politischen Rechte aus Art. 10 und 11 EMRK bedeute.[7]

---

[6] EGMR Segerstedt-Wiberg u.a. v. Schweden, Urteil vom 06.06.2006, Bsw. Nr. 62332/00.

[7] Siehe § 107 des Urteils.

5. VDS und der Grundsatz der Verhältnismäßigkeit

Die Vorratsdatenspeicherung (VDS) betrifft alle NutzerInnen von Kommunikationsdiensten aktuell, unmittelbar und nachteilig in ihrer Grundrechtssphäre. Schon die Speicherung der Verbindungsdaten ist ein Grundrechtseingriff, nicht erst eine allfällige Auskunft an die Behörden – diese aber natürlich auch. Im System der Europäischen Menschenrechtskonvention muss jeder Grundrechtseingriff *notwendig in einer demokratischen Gesellschaft* erscheinen, um gerechtfertigt zu sein. Der EGMR hat dazu über Jahrzehnte hinweg ein Schema zur Prüfung entwickelt, ob ein Eingriff in diesem Sinne verhältnismäßig ist. Demnach ist ein Grundrechtseingriff nur zulässig, wenn er auf einem Gesetz beruht und solche Ziele verfolgt, die in der EMRK relativ abstrakt materiell determiniert sind, wie etwa der Schutz der öffentlichen Ordnung und Sicherheit. Außerdem muss der Eingriff überhaupt geeignet sein, diese Zwecke zu erreichen. Dabei muss der Eingriff auch das gelindeste noch zum Ziel führende Mittel sein. Schließlich muss eine angemessene Balance zwischen den Nachteilen für die vom Eingriff Betroffenen und den erhofften Vorteilen bestehen, also die sogenannte Adäquanz oder Verhältnismäßigkeit im engeren Sinn. Im Folgenden soll jeder dieser gedanklichen Schritte konkret auf die VDS angewendet werden:

Die VDS ist gar nicht geeignet, die vorgeblichen Zwecke zu erreichen. Die von der zugrundeliegenden Richtlinie vorgegebene Bekämpfung schwerer Kriminalität wird durch die VDS nicht merkbar gefördert. Beispielsweise fasst eine aktuelle Studie des deutschen Max-Planck-Instituts für Strafrecht und Kriminologie als Ergebnis ihrer Untersuchung zu den deliktsspezifischen Aufklärungsquoten für den Zeitraum 1987 bis 2010 in Deutschland zusammen, dass der Wegfall der Vorratsdatenspeicherung nicht als Ursache für Bewegungen in der Aufklärungsquote herangezogen werden kann. Dieser Befund gilt insbesondere für die Bereiche der Computerkriminalität sowie der so genannten Internetkriminalität. Die Studie selbst liefert die Zahlen

deliktsspezifisch und stellt fest, dass sich keine Bewegung durch den Wegfall der VDS ergibt. Bislang gibt es keine Gegenstudien dazu, die politische Rechtfertigung besteht stets nur aus emotional überhöhten Einzelfällen.

Ein „Ausweichen" ist dabei in vielen Fällen trivial, Untersuchungen zeigten auch, dass TerroristInnen bereits jetzt so kommunizieren, dass sie von der VDS nicht erfasst werden. Die häufig zur Rechtfertigung der VDS angeführten Einzeltäter (wie der norwegische rechtsextremistische Massenmörder Anders Behring Breivik) kommunizieren überdies häufig mit gar niemandem (über die geplante Tat) und wären daher von der VDS gar nicht erfasst. Selbst Breiviks Suche nach Bombenbauanleitungen wäre mit der VDS nach aktueller Rechtslage nicht erfassbar, da die Speicherung von Inhaltsdaten ausdrücklich ausgeschlossen ist.

Selbst für den mittelschweren Bereich – z.B. Straftaten mit knapp über einem Jahr Strafrahmen – konnte kein Anstieg der Aufklärungsquote in jenen Mitgliedsstaaten belegt werden, in denen die VDS bereits umgesetzt wurde. Gerade durch die Umsetzung könnte in diesem Bereich die Aufklärung sogar erschwert werden, da das Problem auch bei Kriminellen ins Blickfeld gerät und diese aktiv Gegenmaßnahmen ergreifen. Umgehungsmöglichkeiten werden immer allgemeiner bekannt. Beachtenswert sind in diesem Zusammenhang insbesondere die Pläne in Großbritannien, die VDS auf Facebook, Twitter und Online-Spiel-Kommunikation auszuweiten – also sind die bisherigen Mittel der VDS offensichtlich nicht ausreichend oder nicht geeignet.

Zusammenfassend lässt sich festhalten:

- Die VDS ist selbst dort, wo sie möglicherweise in manchen Einzelfällen die Ermittlungen unterstützt, nicht das schonendste Mittel, den Zweck zu erreichen.

In den meisten Fällen würden schon betrieblich notwendig vorhandene Daten ausreichen, wenn die Investitionen zur VDS besser in

mehr Personal der Exekutive investiert und Ermittlungen beschleunigt würden. In den übrigen Fällen würde ein abgekürztes Verfahren genügen, bei dem ein Gericht bei entsprechender Verdachtslage anordnet, bestimmte Daten von bestimmten TeilnehmerInnen „einzufrieren" (sog. *Quick-Freeze*).

- Die VDS steht selbst dann, wenn man sie als das gelindeste noch zum Ziel der Kriminalitätsbekämpfung führende Mittel ansieht, in keinem angemessenen Verhältnis zum Nachteil für die Einzelnen sowie die Gesellschaft.

Je fragwürdiger die Eignung und die Notwendigkeit (im Sinne des gelindesten Mittels) erscheinen, desto höher sind die Anforderungen an die Verhältnismäßigkeit des Eingriffs. Die Güterabwägung zeigt – wenn überhaupt – nur einen geringen positiven Effekt in wenigen Einzelfällen gegenüber einem schweren Eingriff in die Privatsphäre praktisch der gesamten Bevölkerung. Die Unverhältnismäßigkeit der VDS ergibt sich schließlich auch daraus, dass die Verwendungszwecke viel zu weit gefasst sind und keine ausreichenden Rechtsschutzmöglichkeiten zur Verfügung stehen.

6. Gesellschaftliche Veränderungen durch VDS

Die Intensität des Eingriffs für die GrundrechtsträgerIn wird davon beeinflusst, welche über die Informationserhebung hinausgehenden Nachteile ihr aufgrund der Maßnahme drohen oder von ihr nicht ohne Grund befürchtet werden. Die Schwere des Eingriffs nimmt mit der Möglichkeit der Nutzung der Daten für Folgeeingriffe in Grundrechte der Betroffenen zu, sowie mit der Möglichkeit der Verknüpfung mit anderen Daten, die wiederum andere Folgemaßnahmen auslösen können[8]. Zu bedenken ist auch, dass im Fall einer konkreten Datenverwendung durch Strafverfolgungsbehörden nicht nur in die

[8] vgl. dazu die Judikatur des deutschen Bundesverfassungsgerichts: BVerfGE 100, 313 (376); 113, 348 (382); 115, 320 (347 f); BVerfG, NJW 2007, 2464 (2469).

Rechtssphäre etwa einer möglichen StraftäterIn oder deren KomplizInnen eingegriffen wird, sondern auch in die Rechtssphäre derjenigen Personen, die mit den AdressatInnen der Maßnahme über Telekommunikationseinrichtungen nur zufällig in Verbindung standen oder stehen. Dies schafft ein System der Überwachung zum Schutz der Sicherheit des Staates und der Gesellschaft, das die Demokratie bzw. die Rechtsstaatlichkeit, die es schützen soll, aushöhlen bzw. umgehen könnte.

Vor allem aber verlieren die Menschen das Gefühl, frei, selbstbestimmt und unbeobachtet leben zu können und nicht behelligt zu werden, soweit und solange sie die Gesetze des Staates und der Gesellschaft achten und befolgen und nicht delinquent werden. Das Verhalten der Menschen wird sich unter der verdachtsunabhängigen Erfassung alltäglicher Lebensäußerungen schleichend verändern, wo Vertrauen die Basis zwischenmenschlicher Kommunikation war, wird Misstrauen herrschen.

Anhand einiger weniger Beispiele soll verdeutlicht werden, inwieweit Menschen durch die Vorratsdatenspeicherung in der angstfreien Inanspruchnahme ihrer Grundrechte eingeschränkt oder verunsichert werden können:

- Inanspruchnahme von Aidsberatungsstellen, psychologischen Diensten, Seelsorgern, Kontakt zu Rechtsanwälten, Ärzten generell, Kontakt zu diskriminierten bzw. unter Generalverdacht stehenden Gruppen usw. (Art. 8 EMRK);
- Mitteilungen an Medien/Redaktionen im öffentlichen Interesse (Stichwort „whistleblowing“), öffentliche Meinungsäußerung in Blogs, Foren etc. (Art. 10 EMRK);
- Beitritt oder auch nur Besuch von oder Kontaktnahme zu politischen Parteien, Religionsgemeinschaften, Vereinigungen (z.B. unbequeme BürgerInneninitiativen), Teilnahme an Demonstrationen etc. (Art. 11 EMRK).

Überall dort, wo Personen befürchten müssen, aufgrund der Vorratsdatenspeicherung bei der Inanspruchnahme von Grundrechten eventuell Nachteile zu erleiden, beeinträchtigt die Vorratsdatenspeicherung diese Grundrechte.

Oft trifft man in diesem Zusammenhang auf das Argument: „Wer nichts zu verbergen hat, hat auch nichts zu befürchten". Der grundsätzliche Fehler in dieser Argumentation besteht vor allem darin, dass im liberalen Rechtsstaat nicht die Menschen rechtfertigen müssen, warum sie einen Eingriff in ihre Grundrechte nicht hinnehmen wollen, sondern die Rechtfertigungslast für einen Grundrechtseingriff beim Staat liegt.

7. Conclusio

Die Umsetzung der Richtlinie 2006/24/EG stellt einen Dammbruch dar, eine Art Quantensprung in den „Überwachungsstaat". Setzen sich diese Prinzipien durch und fort, ist die auf individueller Freiheit basierende Ordnung westlicher Demokratien am Ende – unabhängig davon, wie das Staatswesen formal organisiert und verwaltet wird.

Die vollständige Erfassung des Kommunikationsverhaltens mit dem Argument, (weitgehende) Sicherheit in einer unsicheren Welt zum Preis der Aufgabe der bürgerlichen Privatsphäre schaffen zu können, stellt das Konzept der „unveräußerlichen Rechte", das seit der Amerikanischen und Französischen Revolution das geistige Fundament der freiheitlich geprägten westlichen Gesellschaften darstellt, gleichsam auf den Kopf. Die legalisierte präventive Überwachung des Kommunikationsverhaltens aller in Europa lebender und elektronisch kommunizierender Menschen stellt einen unumkehrbaren Paradigmenwechsel dar, der mit dem Konzept eines von Grund- und Freiheitsrechten geprägten Rechtsstaates unvereinbar ist.

Weiterführende Literatur

Joe McNamee (2011), Vorratsdaten: Zehn irreführende Behauptungen der Europäischen Kommission, EDRi-gram Nr. 9.8, 20. April 2011, online: http://www.unwatched.org/EDRigram_9.8_Vorratsdaten_Die_zehn%20irrefuehrendsten_Behauptungen_der_EU-Kommission (Letzter Aufruf: 30.5.2013)

European Digital Rights – EDRi (2011), Shadow evaluation report on the Data Retention Directive (2006/24/EC), online: http://www.edri.org/files/shadow_drd_report_110417.pdf (Letzter Aufruf: 30.5.2013)

Christof Tschohl (2011), Der Europäische Vorrat an Daten über Kommunikationsverhalten, in: Bielefeld ua. (Hrsg.), Jahrbuch Menschenrechte (2011), Nothing to hide – nothing to fear? Datenschutz – Transparenz – Solidarität, Wien/Köln/Weimar, 74ff.

Christof Tschohl (2011), Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich, Dissertation, approbiert im Dezember 2011 an der Universität Wien, rechtswissenschaftliche Fakultät.

Christof Tschohl (2011), Die Anonymität im Internet – Umsetzung der Vorratsdatenspeicher-RL im österreichischen Telekom-, Strafprozess- und Sicherheitspolizeirecht, in: Jaksch-Ratajczak/Stadler (Hg.), Aktuelle Rechtsfragen der Internetnutzung, Band 2, Wien, S 341–359.

Anmerkung

In diesem Beitrag wurden einige Passagen aus dem Individualantrag verarbeitet, der vom AKVorrat.at organisiert und im Juni 2012 im Namen von 11.139 AntragstellerInnen beim österreichischen Verfassungsgericht eingebracht wurde (s. http://www.verfassungsklage.at). Dieser Antrag wurde vom Autor dieses Beitrags gemeinsam mit Rechtsanwalt Ewald Scheucher und Philipp Schmuck verfasst. Den beiden Co-Autoren sei an dieser Stelle auch für ihre indirekte Mit-Urheberschaft an diesem Beitrag gedankt.

2.5 Die Reform des EU Datenschutzrechts (Andreas Krisch)

Keywords: Datenschutz, Zentrale Datenverarbeitung, Privatsphäre, Datenschutzverordnung

1. Allgegenwärtige Datenverarbeitung 139
2. Der Grundrechtsschutz hinkt hinterher 141
3. Wesentliche Aspekte der EU Datenschutzreform 143
4. Eine Verordnung ersetzt die Richtlinie 145
5. Betriebliche Datenschutzbeauftragte 147
6. Datentransfer in Drittstaaten 149
7. Stärkung der Datenschutzbehörden 150
8. Datenschutz in Strafverfolgung und Justiz 151
9. Die Richtung stimmt, aber es gibt noch viel zu tun 152

1. Allgegenwärtige Datenverarbeitung

Aktuelle Trends der Informationstechnologie weisen deutlich in die Richtung, dass das Volumen der verarbeiteten (personenbezogenen) Daten in nächster Zukunft rapide zunehmen wird. Gleichzeitig nehmen die Re-Zentralisierung der Datenverarbeitung sowie die Miniaturisierung der Computer weiter zu. Ohne effektiven Datenschutz wird diese Entwicklung ernsthafte Folgen für unsere Privatsphäre haben, denn die Zukunft der massenhaften Datenverarbeitung hat bereits begonnen.[1]

Europaweit wird unter dem Stichwort „Smart Grids“ daran gearbeitet, unsere Energieversorgung „intelligenter“ zu gestalten. Im Zuge dessen sollen sogenannte „Smart Meter“ unseren Verbrauch an Strom, Gas

[1] Vgl. bspw. http://www.zeit.de/digital/datenschutz/2013-02/stellungnahme-datenschutz-professoren bzw. http://www.dataprotectioneu.eu/index_de.html (Letzter Aufruf: 30.5.2013)

und Wärme minutiös aufzeichnen. Die jährliche Zählerablesung soll durch eine Verbrauchsmessung im 15-Minuten-Takt abgelöst werden. An die Stelle eines einzelnen jährlichen Messwertes sollen mehr als 35.000 Messwerte pro Jahr treten. Wie Forschungsergebnisse zeigen, lassen Messungen dieser Häufigkeit sehr genaue Rückschlüsse darauf zu, welche Verhaltensmuster und Handlungen den gemessenen Energieverbrauch verursacht haben. Das Privatleben in unseren Wohnungen wird auf diese Art und Weise aus der Ferne nachvollziehbar und beobachtbar.

Doch das ist nur eine der aktuellen Entwicklungen. Intelligente Transportsysteme sollen helfen, die Verkehrsströme besser zu steuern. An die jeweilige Verkehrs- und Wettersituation angepasste automatische Regelungen der zulässigen Höchstgeschwindigkeit, Fahrzeuge, die Gefahrenmeldungen automatisch an nachfolgende Fahrzeuge weitermelden und die automatisierte gezielte Umleitung von Verkehrsströmen sind nur einige wenige Beispiele dieses Bereichs. Die Auswertung meist personenbezogener Daten über unser Verkehrs- und Transportverhalten sind die Grundlage dafür.

Mit dem Einsatz der RFID-Technologie (Stichwort: Funkchips) im Einzelhandel hat auch die „Computerisierung" alltäglicher Gegenstände bereits begonnen. Während diese RFID-Tags derzeit „nur" eine eindeutige Kennung (wiederum ein personenbezogenes Datum) speichern und auf Anfrage wiedergeben, ist ein deutlicher Ausbau der Funktionalitäten bereits weit fortgeschritten und damit absehbar. Sensoren der unterschiedlichsten Art sollen dazu eingesetzt werden, diverse Umweltzustände und Gegebenheiten automatisch zu erkennen, aufzuzeichnen und weiterzuverarbeiten. Diese Sensoren können in weiterer Folge zu Sensor-Netzwerken ausgebaut werden, deren Daten zentral gesammelt, verarbeitet und analysiert werden.

Schlussendlich spricht man bereits von einem *Internet der Dinge* – und arbeitet an dessen Realisierung. Dabei sollen alltägliche Gegenstände und Maschinen mit dem Internet verbunden und somit unter-

einander vernetzt werden. Die bereits angeführten Beispiele sind erste Anwendungen davon. Mark Weiser, der am XEROX PARC im Bereich des Ubiquitous Computing forschte, fasste diese Entwicklung bereits im Jahr 1991 mit den Worten *The most profound technologies are those that disappear* zusammen. Genau diese Entwicklung findet derzeit statt. Informationstechnologie „verschwindet" in Gegenständen und Maschinen des täglichen Gebrauchs und werden von uns genutzt, ohne dass uns überhaupt noch auffällt, dass wir es mit datenverarbeitenden Computern zu tun haben.

Gleichzeitig zeichnet sich im Bereich der alltäglichen Computernutzung ein Trend zur Re-Zentralisierung der Datenverarbeitung ab. Hinter dem Begriff Cloud Computing verbirgt sich schlussendlich nichts anderes als eine Verlagerung der Rechenleistung weg vom einzelnen Computer der BenutzerInnen, hin zu einem Rechnerverbund in verteilten Rechenzentren eines zentralen Anbieters. Ebenso werden Computerprogramme „in der Cloud" angeboten. Das jeweiligen Programm ist also nicht mehr am Computer der NutzerInnen installiert, sondern diese nutzen lediglich ein Programm im Internet, das bei einem externen Anbieter installiert ist. Dieser Trend kann im Laufe der Zeit zu einer starken Abhängigkeit von externen Anbietern führen. Vertrauen in die Zuverlässigkeit dieser Anbieter ist daher besonders wichtig – sofern man sich auf derartige Angebote einlassen möchte.

2. Der Grundrechtsschutz hinkt hinterher

Technischer Fortschritt – insbesondere auch im Bereich der Datenverarbeitung und Kommunikationstechnik – ist zweifellos von großer Bedeutung für unsere Gesellschaft. Eine Welt ohne der Errungenschaften der letzten zehn bis zwanzig Jahre (Mobiltelefonie, großflächige Verfügbarkeit des Internets, …) ist heute kaum mehr vorstellbar. Genau dieser Fortschritt der letzten Jahre hatte jedoch sehr starken experimentellen Charakter und war hauptsächlich von technischen Fragestellungen getrieben. Gesellschaftliche Fragestellungen und der

Schutz von Grundrechten wurden dabei weitgehend außer Acht gelassen.

Gesetze zum Schutz personenbezogener Daten waren zwar die meiste Zeit über vorhanden, jedoch ist die Rechtsdurchsetzung in diesem Bereich EU-weit bis heute mehr als mangelhaft. So zeigt beispielsweise eine Studie der Grundrechtsagentur der Europäischen Union[2] aus dem Jahr 2010, dass kaum eine der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten über alle Befugnisse und Mittel verfügt, über die sie gemäß den Bestimmungen der EU Datenschutzrichtlinie verfügen sollte.

Diese mangelhafte nationale Umsetzung der Datenschutzrichtlinie (deren Durchsetzung im Übrigen die Aufgabe der Europäischen Kommission wäre) führt in weiterer Folge dazu, dass in den einzelnen Mitgliedstaaten eine sehr unterschiedliche Durchsetzung des Datenschutzrechts besteht. Insgesamt betrachtet ist die Rechtsdurchsetzung in diesem Bereich als sehr mangelhaft zu bezeichnen. Dieser Mangel an Rechtsdurchsetzung führt wiederum dazu, dass Datenschutz in der Gestaltung und Entwicklung von Informationstechnologien und -systemen noch nicht den Stellenwert einnimmt, den er einnehmen müsste, um einen zufriedenstellenden Schutz unserer Grundrechte auf Datenschutz und Schutz der Privatsphäre zu gewährleisten. Darüber hinaus hat dieser Mangel auch negative Auswirkungen auf die wirtschaftliche Entwicklung Europas und der digitalen Wirtschaft ganz allgemein. Der Mangel an Datenschutz führt nämlich zunehmend zu einem Vertrauensverlust gegenüber den Anbietern digitaler Produkte und Services.

Darüber hinaus entsteht durch den Mangel an Rechtsdurchsetzung gegenüber Anbietern aus Drittstaaten ein Marktungleichgewicht zum

---

[2] Data Protection in the European Union: the role of National Data Protection Authorities, European Union Agency for Fundamental Rights, 2010, http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf (Letzter Aufruf: 14.4.2013)

Nachteil europäischer Anbieter, die sich an geltende Datenschutzgesetze halten. Datenschutz kann in diesem Zusammenhang tatsächlich zum wirtschaftlichen Nachteil werden. Weiters behindert die mangelnde Rechtsdurchsetzung den technischen Fortschritt. Erst die tatsächliche Durchsetzung der Datenschutzbestimmungen setzt eine Nachfrage nach datenschutzfreundlichen Technologien in Gang. Erst wenn es diese Nachfrage gibt, werden sich innovative Unternehmen auf diesen Aspekt der technischen Entwicklung konzentrieren und für die Entwicklung und Verbreitung datenschutzfreundlicher Informationstechnik sorgen.

Schlussendlich nimmt durch die mangelnde Rechtsdurchsetzung auch unsere Gesellschaft Schaden. Abgesehen von den unmittelbaren Auswirkungen des mangelnden Datenschutzes, ist es für eine demokratische Gesellschaft abträglich, wenn die Einhaltung geltender Gesetze als optional erlebt wird. Ist dies der Fall, verliert das gesamte Rechtssystem an Glaubwürdigkeit.

3. Wesentliche Aspekte der EU Datenschutzreform

Die Grundrechte auf Datenschutz und den Schutz der Privatsphäre sind sowohl in der Europäischen Menschenrechtskonvention als auch der Charta der Grundrechte[3] der Europäischen Union verankert. Die Charta ist sozusagen *das* zentrale Versprechen der Europäischen Union an ihre EinwohnerInnen. Die beiden genannten Grundrechte sollen durch das EU Datenschutzrecht geschützt werden. Derzeit wird daran gearbeitet, dieses Datenschutzrecht zu erneuern und an die geänderten Rahmenbedingungen anzupassen.

Wie die eingangs erwähnten Beispiele zeigen, ist es im Rahmen dieser Erneuerung besonders wichtig, bereits jetzt auf absehbare Entwick-

[3] Charta der Grundrechte der Europäischen Union, Amtsblatt der Europäischen Union, C 303, 14.12.2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:DE:PDF (Letzter Aufruf: 14.4.2013)

lungen einzugehen und sicherzustellen, dass geeignete rechtliche Rahmenbedingungen geschaffen werden, um den technischen Fortschritt in die richtige Richtung zu lenken. Wenn wir weiterhin vom technischen Fortschritt im Bereich der Informations- und Kommunikationstechnik profitieren wollen, müssen wir sicherstellen, dass die Menschen den angebotenen Informationstechnologien, intelligenten Produkten und innovativen Services vertrauen können und diese in weiterer Folge gerne nutzen. Die grundlegenden wirtschaftlichen Zusammenhänge haben auch im Internet und im Bereich der Informations- und Kommunikationstechnik ihre Gültigkeit. KundInnenzufriedenheit und KundInnenbindung sind auch hier der Schlüssel zu langfristigem Erfolg. Vertrauen – und damit hochwertiger Datenschutz – ist eine Grundvoraussetzung für erfolgreiches Wirtschaften. Grundrechte sind die Basis für das Funktionieren unserer Gesellschaft. Hier sollten wir uns keinen Vertrauensverlust leisten.

Es ist daher an der Zeit, dass wir die experimentelle Phase der IT-Entwicklung verlassen und die Geschäftsmodelle und Technologien zur Reife führen und in Einklang mit den bestehenden Grundrechten bringen.

Ähnlich den Bemühungen um einen möglichst sparsamen und effizienten Einsatz von Energie müssen wir unsere Innovationsanstrengungen auch im Bereich der Datenverarbeitung darauf richten, mit möglichst geringem Einsatz personenbezogener Daten die jeweils angestrebten Ziele zu erreichen. An die Stelle einer massiven Ausbeutung personenbezogener Daten muss daher das Konzept der Datenminimierung treten. Der Schutz der Grundrechte muss in allen Mitgliedsstaaten der Europäischen Union (und darüber hinaus) auf einem hohen Niveau sichergestellt werden – und zwar in allen Branchen und Bereichen, einschließlich der Strafverfolgung und Justiz sowie der öffentlichen Verwaltung und ähnlichen Bereichen.

Im Jänner 2012 hat die Europäische Kommission einen Reformvorschlag für das EU Datenschutzrecht vorgestellt[4]. Eine allgemeine Datenschutzverordnung und eine Richtlinie für den Datenschutz im Bereich Strafverfolgung und Justiz sollen das bestehende Datenschutzrecht ersetzen. Grundlage für das derzeitige Datenschutzrecht der EU Mitgliedsstaaten ist die Datenschutzrichtlinie aus dem Jahr 1995[5]. Diese Richtlinie gibt den groben Rahmen für das Datenschutzrecht der Mitgliedsstaaten vor, und musste von den Mitgliedstaaten jeweils in nationales Recht umgesetzt werden. Bei dieser Umsetzung hatten die Mitgliedstaaten einigen Ermessensspielraum, was dazu geführt hat, dass in den einzelnen Ländern inzwischen sehr unterschiedliche Regeln für den Datenschutz gelten. Die ursprünglich angestrebte Vereinheitlichung des Datenschutzrechts ist bisher also nur bedingt eingetreten.

4. Eine Verordnung ersetzt die Richtlinie

Die EU-Kommission schlägt daher anstelle der bisherigen Richtlinie nun eine Datenschutzverordnung vor. Diese hätte den Vorteil, dass sie unmittelbar in allen Mitgliedstaaten der Europäischen Union gültig ist und nicht mehr in nationales Recht umgesetzt werden muss. Damit wäre erreicht, dass in allen Mitgliedstaaten dasselbe Datenschutzrecht wortgetreu zur Anwendung kommt. Das reduziert den administrativen Aufwand für Unternehmen und kann für Betroffene die Rechtsdurchsetzung erleichtern. Darüber hinaus sieht der Vorschlag der Kommission auch eine Ausweitung des Gültigkeitsbereichs der

---

[4] Commission Proposals on the data protection reform, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.html (Letzter Aufruf: 14.4.2013)

[5] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:DE:PDF (Letzter Aufruf: 14.4.2013)

Datenschutzverordnung vor. So sollen künftig auch Unternehmen, deren Sitz sich außerhalb der EU befindet, dem europäischen Datenschutzrecht unterliegen, wenn deren Angebote sich an Menschen innerhalb der Europäischen Union richten. Unmittelbar davon betroffen wären beispielsweise Unternehmen wie Google oder Facebook, die derzeit für eine europäische Datenschutzbehörden nur schwer greifbar sind, wie der aktuelle Fall der Initiative Europe vs. Facebook[6] deutlich vor Augen führt.

Hinsichtlich einer datenschutzfreundlichen technischen Entwicklung sieht das EU Reformpaket zwei wesentliche Konzepte vor. Einerseits soll das Prinzip des eingebauten Datenschutzes (*Privacy by Design*) künftig Grundlage der technischen Entwicklung werden. Dies bezweckt nichts anderes, als dass künftig bereits bei der Planung neuer Angebote sowie der Entwicklung von Software und Services der Datenschutz als technische Anforderung mitberücksichtigt werden soll. Systeme sollen so implementiert werden, dass sie von Haus aus mit möglichst wenigen personenbezogenen Daten auskommen, diese nur so lange wie unbedingt erforderlich verarbeiten und den NutzerInnen immer die datenschutzfreundlichsten Einstellungen als Grundeinstellungen präsentieren.

Um eingebauten Datenschutz in der Praxis umsetzen zu können, bedarf es eines weiteren Instruments, das ebenfalls Bestandteil des Reformpaketes ist. Datenschutz-Folgenabschätzungen (*Data Protection Impact Assessments*) sollen künftig dabei helfen, die Auswirkungen konkreter Datenverarbeitungen auf die Datenschutzsituation der Betroffenen zu analysieren und bewerten. In einem weiteren Schritt können auf Basis dieser Erkenntnisse Problembereiche entschärft und geeignete Maßnahmen zur Risikominimierung getroffen werden.

---

[6] Europe vs Facebook http://europe-v-facebook.org/ (Letzter Aufruf: 14.4.2013)

5. Betriebliche Datenschutzbeauftragte

Direkt in den Unternehmen und Behörden soll der Datenschutz künftig durch die Einsetzung von Datenschutzbeauftragten verankert werden. Aufgabe dieser Personen ist es dafür zu sorgen, dass die Datenverarbeitung der jeweiligen Organisation im Einklang mit den Datenschutzanforderungen erfolgt. Sie sind im Unternehmen beratend tätig, führen Schulungen von MitarbeiterInnen durch und halten Kontakt mit den Datenschutzbehörden. Für KundInnen sind sie die AnsprechpartnerInnen in Datenschutzfragen und sorgen dafür, dass diese ihr Recht auf Auskunft, Richtigstellung und Löschung tatsächlich wahrnehmen können. Gemäß den Plänen der Kommission sollen die Datenschutzbeauftragten in Zukunft die in manchen Mitgliedstaaten wie beispielsweise Österreich bestehenden Datenverarbeitungsregister ersetzen. Anstatt aus dem zentralen Register kann der/die Einzelne dann direkt von den Datenschutzbeauftragten eines Unternehmens erfahren, welche Daten das Unternehmen verarbeitet.

Eine bedeutende Schwachstelle dieses an sich sehr begrüßenswerten Vorschlags ist, dass Datenschutzbeauftragte erst ab einer Unternehmensgröße von 250 Mitarbeitern verpflichtend vorgeschrieben werden sollen. Ebenso sollen sich Unternehmen erst ab dieser Größe strukturiert mit dem Thema Datenschutz auseinandersetzen müssen. Für Behörden ist diese größenmäßige Einschränkung nicht vorgesehen. Die Grenze von 250 MitarbeiterInnen ist bei weitem zu hoch angesetzt und beinhaltet auch einen strukturellen Fehler. Es hängt heutzutage nicht mehr von der Anzahl der MitarbeiterInnen ab, ob ein Unternehmen viele und sensible Daten verarbeitet oder nicht. Je nach Branche können Großbetriebe unter Umständen mit sehr geringen Mengen an personenbezogen Daten auskommen, während kleine Unternehmen anderer Branchen mit großen Datenmengen hantieren. Um nur ein Beispiel zu nennen: Das Foto-Netzwerk *Instagram* verfügte lediglich über zehn MitarbeiterInnen, als es um eine Milliarde US-Dollar verkauft wurde.

Privacy by Design und *Privacy Impact Assessments* stellen die Softwareentwicklung vor neue – aber durchaus lösbare – Herausforderungen. Hier wird es nötig sein mit entsprechenden Schulungs- und Ausbildungsmaßnahmen bereits bestehende Datenschutzkonzepte zu vermitteln und neue innovative Gestaltungsmöglichkeiten zu entwickeln.

Ausbildung ist jedoch auch in anderen Bereichen ein wesentlicher Aspekt künftigen Datenschutzes. So wird auch in Zukunft jede/r Einzelne für sich selbst darüber entscheiden müssen, welche Informationen sie/er preisgibt und welche nicht. Der bewusste und kritische Umgang mit datenverarbeitenden Systemen muss verstärkt in allen Bereichen unseres Bildungssystems verankert werden. Auch dazu will das Reformpaket einen Beitrag leisten.

Für den – leider gar nicht unwahrscheinlichen – Fall, dass personenbezogene Daten einmal verloren gehen, sieht das Reformpaket eine Informationspflicht für Datenverarbeiter vor. Diese sollen bei einer Datenpanne innerhalb kurzer Zeit die zuständige Datenschutzaufsichtsbehörde über das Datenleck informieren und – sofern nachteilige Folgen zu erwarten sind – auch die Betroffenen.

Diese Regelung ist speziell für die Betroffenen von Bedeutung. Schließlich sind sie es, die einerseits unmittelbar von der Panne betroffen sind, andererseits kann nur jede/r für sich entscheiden, wie wichtig oder vernachlässigbar das Bekanntwerden einer bestimmten Information für eine/n selbst ist. Entsprechend wären in diesen Bereich eine noch weitergehende Informationspflicht und ein zentrales öffentliches Register der Datenpannen wünschenswert, in dem man sich über Datenschutzverletzungen und die von den DatenverarbeiterInnen eingeleiteten Schutzmaßnahmen informieren kann.

6. Datentransfer in Drittstaaten

Klar kritikwürdig sind die Bestimmungen des Reformentwurfs zum Datentransfer in Drittstaaten außerhalb der Europäischen Union. Zwar fordert der Verordnungsentwurf weiterhin, dass in dem jeweiligen Drittstaat ein angemessenes Datenschutzniveau sichergestellt sein muss. Jedoch wurden bereits in der Entwurfsphase des Textes entscheidende Passagen wieder entfernt.

So war ursprünglich vorgesehen, dass die Datenweitergabe an Behörden von Drittstaaten – wie sie etwa durch US-amerikanische Unternehmen auf Basis des *PATRIOT Act* und des *Foreign Intelligence Surveillance Act* (FISA) erfolgen – nur nach vorheriger Genehmigung der lokalen Aufsichtsbehörde erfolgen darf. Ersetzt wurde diese Genehmigungspflicht durch einen Passus, der lediglich fordert, dass der Drittstaat angemessene Datenschutzvorkehrungen rechtsverbindlich vorgesehen hat. Eine Datenübermittlung in Drittstaaten soll künftig auch auf Basis von sogenannten *Binding Corporate Rules* (BCR), also rechtsverbindlichen Unternehmensregeln, erfolgen. Sofern sich ein Unternehmen solche Regeln auferlegt und diese mit den Datenschutzaufsichtsbehörden vereinbart, dürfte es beispielsweise personenbezogene Daten aus der EU nach China oder Indien übermitteln, wo Datenverarbeitung zu deutlich günstigeren Preisen angeboten wird als in der EU.

Diese Datenverarbeitung im Ausland unterliegt dann – so die Theorie – immer noch dem europäischen Datenschutzrecht und das Unternehmen ist verpflichtet dieses Schutzniveau aufrecht zu erhalten. In der Praxis ist dies jedoch nicht kontrollierbar. Es ist im Gegenteil sogar vollkommen unvorstellbar, dass sich MitarbeiterInnen einer europäischen Datenschutzbehörde auf Dienstreise nach China oder Indien begeben, um sich dort persönlich von der Einhaltung der BCR zu überzeugen. Sollten sich eines Tages doch ein paar wackere DatenschützerInnen finden, die eine solche Reise unternehmen, werden sie

vor Ort schnell feststellen, dass ihre diesbezüglichen Rechte und Möglichkeiten an den Grenzen der EU rasch ein Ende finden.

7. Stärkung der Datenschutzbehörden

Innerhalb der Grenzen der Europäischen Union sieht der Entwurf für die Datenschutzaufsichtsbehörden eine deutliche Stärkung vor. Die Möglichkeiten zur Zusammenarbeit der nationalen Aufsichtsbehörden sollen gestärkt werden. Ebenso sollen deutlich höhere Sanktionsmöglichkeiten dabei helfen, den Forderungen nach ordnungsgemäßem Datenschutz mehr Nachdruck zu verleihen. Die Betroffenen sollen sich – im Sinne eines One-Stop-Shops – mit allen Anliegen an eine Aufsichtsbehörde ihrer Wahl (z.B. die im eigenen Land) wenden können, auch wenn die betreffende Datenverarbeitung im Zuständigkeitsbereich einer anderen Aufsichtsbehörde erfolgt.

Ebenso soll für Unternehmen mit Niederlassungen in mehreren Mitgliedsstaaten diejenige Aufsichtsbehörde zuständig sein, in deren Land das Unternehmen seine Hauptniederlassung hat. Hierbei zeigt sich jedoch wiederum eine Schwachstelle des Entwurfs: Bei allen Bemühungen um eine Harmonisierung des Datenschutzrechts wird man auch in Zukunft davon ausgehen müssen, dass nicht jede Datenschutzbehörde gleich effektiv und konsequent bei der Durchsetzung des Datenschutzrechts vorgehen wird. Die Ursache dafür ist unter anderem auch im unterschiedlichen Verfahrensrecht der Mitgliedsstaaten zu finden. So ist das Verwaltungsverfahren in Österreich offenbar deutlich anders geregelt als in Irland. Wie sich im bereits erwähnten Fall von Europe vs. Facebook zeigt, ist die irische Aufsichtsbehörde beispielsweise der Ansicht, dass die Beschwerdeführer kein Recht hätten, die von Facebook vorgebrachten Rechtfertigungen einzusehen. Ein in Österreich – zumindest formal – undenkbarer Zustand.

In diesem Sinne wäre es daher sinnvoll, den Reformvorschlag der EU-Kommission in diesem Punkt zu ergänzen. Es sollte sichergestellt werden, dass bei Fällen von grenzüberschreitender Bedeutung auch die Aufsichtsbehörden der anderen betroffenen Mitgliedsstaaten mitentscheiden. Diesen sollte also nicht nur eine beratende Funktion zukommen, sondern die Entscheidung sollte tatsächlich gemeinsam erfolgen. Derartige gemeinsame Entscheidungen der Aufsichtsbehörden funktionieren auch bisher schon sehr gut. So werden die Arbeitspapiere der Artikel 29 Datenschutzgruppe, dem EU-Gremium der nationalen Aufsichtsbehörden, gemeinsam verabschiedet. Die fachliche Qualität dieser Dokumente ist hervorragend und ein exzellentes Beispiel für eine fruchtbringende europäische Kooperation.

8. Datenschutz in Strafverfolgung und Justiz

In einem weiteren Punkt von höchster grundrechtlicher Relevanz bleibt das Reformpaket der EU-Kommission klar hinter den Erwartungen zurück. Während das Grundrecht auf Schutz des Privat- und Familienlebens sowie das Grundrecht auf Datenschutz den Menschen in der EU grundsätzlich in allen Lebensbereichen zusteht, unterscheidet der Vorschlag der Kommission zwischen einer allgemeinen Datenschutzverordnung und einer – nicht unmittelbar gültigen – Richtlinie für den Datenschutz im Bereich der Strafverfolgung und Justiz.

Diese Trennung sollte aufgehoben werden. In den Fällen, wo für die Zwecke der Strafverfolgung und Justiz begründete Ausnahmen vom allgemeinen Datenschutzrecht erforderlich sind, sollten diese klar abgegrenzt in die Verordnung aufgenommen werden. Darüber hinaus sollte aber auch in diesen besonders sensiblen Bereichen dasselbe Datenschutzniveau erreicht werden, wie es zurecht in allen übrigen Bereichen unseres Lebens erwartet wird.

9. Die Richtung stimmt, aber es gibt noch viel zu tun

Zusammenfassend kann gesagt werden, dass das von der EU-Kommission im Jänner 2012 vorgelegte Datenschutz-Reformpaket eine ganze Reihe sehr guter und wichtiger Vorschläge zur Verbesserung des Datenschutzes in Europa enthält. In manchen Bereichen sind noch wesentliche Anpassungen erforderlich, der Vorschlag geht jedoch grundlegend in die richtige Richtung. Es wird nun auf die laufenden Verhandlungen zwischen der EU-Kommission, dem Europäischen Parlament und dem EU-Ministerrat ankommen, in welche Richtung sich das Reformvorhaben bewegt. Eines steht jedoch jetzt bereits fest: Es handelt sich um eines der aktuell wichtigsten Reformvorhaben der Europäischen Union. Entsprechend hoch ist der Druck, dem die europäischen Institutionen durch allerlei inner- und außereuropäische LobbyistInnen ausgesetzt sind.

Die Zivilgesellschaft ist hier zahlen- und ressourcenmäßig klar unterlegen. Das bedeutet aber nicht, dass wir uns nicht Gehör verschaffen können. So hat European Digital Rights[7], der Dachverband von derzeit 32 Datenschutz- und Menschenrechtsorganisationen aus 20 europäischen Ländern, eine der ausführlichsten Analysen der Datenschutzverordnung vorgelegt und online gestellt[8], in der Artikel für Artikel, Absatz für Absatz konkrete Verbesserungsvorschläge angeführt und begründet werden. Damit gibt es nun eine solide Argumentationsbasis, die in den weiteren Verhandlungen ausgiebig genutzt werden wird.

---

[7] European Digital Rights (EDRi) http://www.edri.org/ (Letzter Aufruf: 14.4.2013)
[8] EDRi Informationsseite zur Datenschutzreform, Protect My Data: http://protectmydata.eu (Letzter Aufruf: 14.4.2013)

Teil 3:
Governance und Netzpolitik

3.1. Grenzen staatlicher Internetpolitik (Matthias C. Kettemann)

Ein Leitfaden für Gesetzgeber

Keywords: Internetzugang, Zensur, Menschenrechte, Vorsorgeprinzip, Nichteingriffsprinzip, Rücksichtnahmeprinzip

1. Recht zur Regulierung? 155
2. Schranken für staatliches Handeln 156
3. Zentrale Rolle der Menschenrechte 158
4. Die Zukunft der Internetregulierung 158

1. Recht zur Regulierung?

Das Internet ist ein Forum und eine Arena der menschlichen Emanzipation. Es stellt einen Katalysator für die Menschenrechte dar und eröffnet durch den Zugang zu Information und vereinfachter Kommunikation wertvolle Perspektiven der individuellen und gesellschaftlichen Entwicklung. Gleichzeitig dynamisiert das Internet auch Prozesse gesellschaftlichen Wandels. Darauf reagieren autoritäre Staaten mit intensivierter Überwachung, Zensur, physischer Gewalt gegen InternetnutzerInnen und sogar mit Internetabschaltung. *Reporters without Borders*[1] hat Staaten wie Bahrain, Belarus, Burma, China, Kuba, Iran, Nordkorea, Saudi-Arabien, Syrien, Turkmenistan, Usbekistan und Vietnam in ihrem Bericht von 2012 als „Feinde des Internets" bezeichnet. Doch auch europäische Staaten intensivieren Angriffe auf die Internetfreiheit. Die gute Nachricht dabei: Das Völkerrecht und insbesondere die Menschenrechte setzen staatlichen Angriffen auf die Internetfreiheit klare Grenzen.

[1] s. http://rsf.org

Während Online-Aktivist John Perry Barlow 1996 am Rednerpult des Weltwirtschaftsforums in seiner Erklärung über die Unabhängigkeit des Cyberspace den Regierungen der Welt das Recht absprach, das Internet regulieren zu dürfen, wird hier davon ausgegangen, dass Staaten nicht nur das *Recht*, sondern sogar die *Pflicht* haben, Regeln für den Cyberspace zu entwerfen. Diese Pflicht ergibt sich aus der staatlichen Aufgabe, die Rechte der Bevölkerung zu schützen. Allerdings fehlt häufig das entsprechende legistische Fingerspitzengefühl (Bsp. „Bundestrojaner"), weiters verkennen Staaten die legitimitätsstiftende Funktion von Multi-Stakeholder-Prozessen, durch die auf eine Einbeziehung von Wirtschaft und Zivilgesellschaft gesetzt wird. Regelmäßig werden dabei Menschenrechte berührt, oft sogar verletzt.

Daher stellt sich die Frage: Welche Schranken existieren für staatliches Handeln?

2. Schranken für staatliches Handeln

Das Völkerrecht ist ein kraftvolles Instrument der internationalen Gemeinschaft zur Regelung von zur Gegenständen von international-öffentlichem Interesse zum Schutz globaler Allgemeingüter und Begrenzung der Rechte und Pflichten von Staaten.

Das Internet und sein Schutz haben sich zu einem Gegenstand international-öffentlichen Interesses entwickelt: Hintergrund dieser Entwicklung ist die Vision einer durch Informations- und Kommunikationstechnologie gerechter werdenden Welt. Zu dieser haben sich alle teilnehmenden Staaten anlässlich des Weltgipfels zur Informationsgesellschaft 2005 in der *Verpflichtungserklärung von Tunis* bekannt. Sie bestätigten, eine „den Menschen in den Mittelpunkt stellende, inklusive und entwicklungsorientierte Informationsgesellschaft" bauen zu wollen, die „gestützt auf die Ziele und Grundsätze der Charta der Vereinten Nationen, das Völkerrecht und den Multilateralismus" sei und in der die volle „Achtung und Einhaltung der Allgemeinen Erklä-

rung der Menschenrechte“ sichergestellt sei. In der zeitgleich beschlossenen *Tunis Agenda* wiederum schrieben die Staaten ihr Bekenntnis zu einem stabilen und sicheren Internet als globale Einrichtung nieder.

Vor diesem Hintergrund ist staatliches Handeln zu bewerten; auf diese Vision hin müssen Staaten ihre gesetzgeberischen Aktivitäten hin ausrichten. Operationalisiert wird diese Verwendungszusage mittels völkerrechtlicher Prinzipien. Einschlägig sind vor allem die Rücksichtnahmepflicht, die Kooperationspflicht, das Nichteingriffsprinzip, das Vorsorgeprinzip und das internationale Regime des Menschenrechtsschutzes.

Die Rücksichtnahmepflicht und das Vorsorgeprinzip bestehen nicht nur hinsichtlich des Nachbarstaates, da angesichts der technischen Realitäten des Internets kaum je nur einzelne Staaten durch – zumindest besonders intensive – Eingriffe wie Internetabschaltungen betroffen sein können. Staaten dürfen nicht ohne Berücksichtigung der Folgen nationale Internetpolitik gestalten.

Darüber hinaus kann das Prinzip der zwischenstaatlichen Zusammenarbeit dergestalt weiterentwickelt werden, dass Staaten sich in der Ausgestaltung ihrer nationalen Internetpolitik der internationalen Dimension bewusst sein und sich absprechen müssen. Staaten, die sich der Kooperationspflicht verweigern und Internetpolitik als arbiträres Machtinstrument benutzen, verletzen das Völkerrecht.

Auch das Nichteingriffsprinzip ist einschlägig: Eine intensive Beeinträchtigung des Internets durch das Regime eines Staates mit Kaskadenfolgen auf die Nutzbarkeit von Internetservices in anderen Staaten könnte bei einer substanziellen Beeinträchtigung eine Intervention darstellen, und somit wieder – eine Verletzung des Völkerrechts.

3. Zentrale Rolle der Menschenrechte

Eine zentrale Rolle in der Beschränkung staatlicher Regulierungsautonomie spielen die Menschenrechte. Das Internet verdient aufgrund der vielen verschiedenen Rollen, die es zu den Bedingungen des Informations- und Kommunikationszeitalters ausfüllt, einen besonderen Schutz. Dieser wird durch die informations- und kommunikationsbezogenen Menschenrechte geleistet, die – fußend auf den Artikeln 19 der Allgemeinen Erklärung für Menschenrechte und des Zivilpaktes und den entsprechenden regionalen Menschenrechtsschutzsystemen – einen umfassenden Schutz garantieren, der in seinem Kerngehalt gewohnheitsrechtlich abgesichert ist.

Natürlich: Die Meinungsäußerungsfreiheit im Internet ist nicht grenzenlos. Beschränkungen sind rechtmäßig, wenn sie gesetzlich vorgesehen sind, ein legitimes Ziel verfolgen und verhältnismäßig sind (vgl. Eva Jana Messerschmidt, Kapitel 2.3. *Internetsperren und Menschenrechte*). Aus Gründen der nationalen Sicherheit etwa kann die Veröffentlichung eines Aufrufs zu politischer Gewalt verboten werden. „Nationale Sicherheit" darf aber nicht als Vorwand für willkürliche Beschränkungen verwendet werden.

4. Die Zukunft der Internetregulierung

Jeder Staat hat gegenüber der internationalen Gemeinschaft (also allen anderen Staaten) die Pflicht, Gefahren von der Integrität und Funktionalität des Internets abzuwenden und den globalen, unbeschränkten, grenzübergreifenden Internetverkehr nicht negativ zu beeinflussen. Gleichzeitig bestehen globale positive Schutzpflichten aller Staaten hinsichtlich des Internets, die sich unter anderem aus der Pflicht der Staaten zur Gewährleistung der Kommunikations- und Informationsrechte ergeben.

Nun ist es leicht, Schranken-Schranken[2] für staatliches Handeln aufzuzeigen, aber schwierig, diese auch durchzusetzen. Zu viele Staaten verweisen auf das Argument der staatlichen Souveränität, um Einmischungen in die nationale Politikgestaltung abzuwehren. Sie haben Unrecht: Dem Völkerrecht und dem Regime des internationalen Menschenrechtsschutz lassen sich klare rote Linien für staatliche Internetpolitik entnehmen.

Die Feinde des Internets müssen die Menschenrechte ihrer Bevölkerung akzeptieren und die Attacken auf die Internetfreiheit unterlassen. Doch auch dem Internet gegenüber offener eingestellte Staaten wie Österreich müssen bei der Regulierung internetbezogener Sachverhalte sensibler vorgehen, in der Bevölkerung Bewusstsein für die Chancen und Gefahren des Internets schaffen, außenpolitisch mehr Freiheit für das Internet fordern und sich auf internationalen Foren verstärkt für den Multistakeholder-Ansatz einsetzen.

[2] Jedes Recht stößt an eine Grenze oder Schranke. Diese wiederum hat eine Grenze oder Schranke. Redefreiheit darf nicht als Völkermordsaufforderung missbraucht werden (Schranke), diese darf nicht so ausgelegt werden, dass sie den Kerngehalt des rechts berührt (Schranken-Schranke).

3.2. Netzneutralität (Tassilo Pellegrini)

Das Internet im Spannungsfeld von Public Service und Kommerzialisierung

Keywords: Netzneutralität, Internet Governance, Traffic Management, Internet Access, Medienvielfalt, Meinungsvielfalt

1. Meinungsfreiheit und kommerzieller Datentransport 161
2. Definitionsansätze für Netzneutralität 162
3. Argumente für und wider die Netzneutralität 164
4. Netzneutralität in der Europäischen Union 167
5. Schlussbetrachtung 168
Weiterführende Literatur 170

1. Meinungsfreiheit und kommerzieller Datentransport

Die demokratisierende Funktion des Internets bestand bisher in den offenen Standards, den geringen Kosten und dem gleichberechtigten Zugang zur Netzinfrastruktur mit ihren unzähligen Services und Anwendungen. Grundlage dafür bildete die sogenannte *Netzneutralität*, eine historisch gewachsene *technische Konvention*, die alle Datenpakete im Netz gleichberechtigt behandelt. Die Netzneutralität diente ursprünglich der verrechnungstechnischen Komplexitätsreduktion unter Telekommunikationsanbietern und stellte sicher, dass Netzwerke auf globalem Niveau interoperabel sind. Mit der Nachrüstung der Telekommunikationsinfrastrukturen um leistungsfähigere *Routing*- und *Monitoringtechnologien* sind Telekommunikationsbetreiber seit wenigen Jahren in der Lage komplexere Transport- und Verrechnungsdienste anzubieten. Dies kommt vor allem in der aktuellen Debatte um *Quality of Service* (QoS) bzw. *Managed Services* zum Aus-

druck und hat weitreichende Folgen für die Funktionsweise und den gleichberechtigten Zugang zur Netzinfrastruktur.

Die Netzneutralität ist sowohl Bedingung als auch Ursache für inhaltliche Vielfalt, niedrige Markteintrittsbarrieren und relativ geringe Partizipationskosten – sowohl auf SenderInnen- wie auf NutzerInnenseite. Mit der zunehmenden multimedialen und damit bandbreitenintensiven Anreicherung des Internets kristallisieren sich neue Verteilungs- und Verfügungskonflikte über Zugang und Vertrieb zu bzw. von multimedialen Inhalten heraus. Gerade die datenintensiven Angebote audiovisueller Medien, die heute in Form von Mediatheken, Streaming-Diensten, IP-TV oder VoIP daherkommen und wesentlicher Bestandteil des „Netz" als offenem Kommunikations- und Informationsraum sind, veranlassen daher eine Diskussion um gesellschaftliche Bedeutung und strukturelle Abhängigkeiten zwischen der Telekommunikationsindustrie (als Gatekeeper zur Infrastruktur) und den ErzeugerInnen publizistischer Angebote im Internet. Demnach ist das Bestreben der großen Telekommunikationsunternehmen künftig nicht zur den Zugang zur Netzinfrastruktur stärker zu regulieren, sondern auch deren Nutzung und diese – vor allem – differenziert zu bepreisen. Damit verbunden sind neue Wertschöpfungsszenarien der Infrastrukturbetreiber, die das Internet, wie wir es bisher kannten, maßgeblich verändern.

2. Definitionsansätze für Netzneutralität

In der idealtypischen Definition bezeichnet Netzneutralität die Gleichbehandlung (Parität) der physikalischen Einheiten (bits) im Datentransport mittels des TCP/IP-Protokolls (Internet). Daraus ergeben sich folgende Bedingungen:

- Diskriminierungsfreier Datentransport (Routing) in Bezug auf
  – EigentümerIn, UrheberIn, Dienst-Typ, Endgerät der Datenpakete
  – Volumen, Herkunft, Zielort der Datenpakete

- Stärkung der KonsumentInnen bei Wahlfreiheit und Kontrolle von Inhalten, Diensten und Service-Levels (NUI – Network-User Interconnection)
- Stärkung von InnovatorInnen neue Dienste und Protokolle zu entwickeln und zu nutzen ohne Eingriffe der NetzbetreiberInnen
- Nicht-diskriminierende Zusammenschaltung von Backbone-Netzen (NNI – Network-Network Interconnection) auf globalem Niveau („Best-Effort-Prinzip" im Routing/„End-to-End")

Eine realtypische Betrachtung zeigt, dass NetzbetreiberInnen seit Jahren ein sogenanntes *Traffic Management* anwenden, um die Auslastungseffizienz der Netze zu optimieren. Dazu werden zeit- und qualitätskritische Datenpakete gegenüber anderen bevorzugt, um so ein möglichst effektives Service-Niveau sicher zu stellen und die Netzlast zu minimieren. Entsprechend kann von einem *wirtschaftlich diskriminierungsfreien Traffic Management* gesprochen werden, welches keine NutzerInnengruppen bevorzugt, benachteiligt oder strukturell ausschließt.

Zunehmend halten jedoch – insbesondere in Mobilfunknetzen – wirtschaftlich motivierte Diskriminierungspraktiken Einzug, bei denen als Bestandteil des Geschäftsmodells gezielt gegen bestimmte Dienste, Anwendungen oder Protokolle (wie etwa VoIP, P2P oder Streaming) vorgegangen wird. Diese Form des Traffic Managements birgt Problematiken in Bezug auf Wettbewerb und KonsumentInnenschutz. So zeigt ein aktueller BEREC-Report[1] zur Neutralitätsgebarung der europäischen Telekommunikationsanbieter, dass etwa *25% der Mobilfunk- und Festnetz-Carrier* aktiv und regelmäßig gegen bestimmte Dienstearten (vornehmlich P2P und VoIP) entweder als Bestandteil ihrer Geschäftsbedingungen und/oder zu Zwecken des Managements von Lastspitzen diskriminieren. Vor dem Hintergrund des in manchen EU-Ländern unzureichend ausgeprägten Wettbe-

werbs sind dadurch bis zu *50% der europäischen Internet-UserInnen* betroffen.

In anderen Worten: Diese NutzerInnen können gar nicht, nur zeitweise oder nur gegen Aufpreis auf bestimmte Dienste bzw. Inhalte des Internets zugreifen.

3. Argumente für und wider die Netzneutralität

Die aktuelle Debatte zur Netzneutralität kristallisiert an der Frage, nach welchen Kriterien die Telekommunikationsbetreiber das Wirtschaftsgut *Datentransport* diversifizieren dürfen und können, um neue Erlöskanäle zu erschließen. In der klassischen Rolle als *Common Carrier* sind Telekommunikationsanbieter verpflichtet, einspeisungswilligen KundInnen einen Zugang zu ihren Netzen zu ermöglichen, ohne dabei auf Art, Herkunft, Zielort des Dienstes oder die übertragenen Inhalte Einfluss zu nehmen (sofern keine strafrechtlichen Belange vorliegen). Der Netzzugang *muss* hierbei *zu vernünftigen Preisen* gewährt werden. Ziel der aktuellen Entwicklungen ist es jedoch, einen zweiseitigen Markt zu etablieren, der es den Carriern ermöglicht, sowohl von NetzeinspeiserInnen als auch von EndkundInnen Entgelte für den dienste- und inhaltsspezifischen Datentransport zu verlangen.

Vor diesem Hintergrund ist die Ausgestaltung der Netzneutralität seit einigen Jahren Gegenstand von Gesetzgebungsverfahren in den USA und seit spätestens 2009 auch in der Europäischen Union. Telekommunikationsanbieter argumentieren, dass eine *Diversifikation im Datentransport* eine wirtschaftliche Notwendigkeit darstellt, um zukünftige *Kosten des Netzausbaus* finanzieren und über entsprechende Mehreinnahmen die bei der Einspeisung erzielt werden, amortisieren zu können. Entsprechend sollen Content und Service Provider, die hohe Datenvolumina generieren (u.a. deshalb, weil sie eine hohe Popularität bei den NutzerInnen genießen), stärker zur Kasse gebeten werden. Weiters erhoffen TelekommunikationsanbieterInnen Mehr-

einnahmen auf KonsumentInnenseite, wenn es etwa darum geht Dienste wie VoD, VoIP, Hochsicherheits-Dienste bzw. bevorzugtes Routing als Mehrwertpakete an die EndkonsumentInnen weiterzuverkaufen. Der Wettbewerb soll hierbei sicherstellen, dass es zu keinem Machtmissbrauch und ergo zu einem *erhofften Wohlfahrtsgewinn* aller am Wertschöpfungsprozess beteiligten AkteurInnen kommt.

KritikerInnen der Telekommunikationsbetreiber argumentieren, dass mit der Einführung eines Quality-of-Service (QoS) Modells in den Datentransport die Netzneutralität weitgehend ausgehebelt wird. Ohne Netzneutralität kommt es zu einer *technischen Fragmentierung* des Internets in regionale Netz-Cluster, die nicht nur kartellrechtlich problematisch sind, sondern weiters zu einer Erhöhung der Markteintrittsbarrieren für *Content und Service Provider* führen, sowie auch die Kosten für die EndkonsumentInnen steigern. Entsprechend würde eine Abschaffung bzw. eine Einschränkung der Netzneutralität zu einer ungebührlichen Stärkung der Marktmacht von TelekommunikationsbetreiberInnen, aber auch marktdominierenden Inhalte- und DienstanbieterInnen führen und – wie empirisch vielfach nachgewiesen – auch zu Missbrauch verleiten. Weiters verlieren Telekommunikationsbetreiber ihren Common Carrier-Charakter, da sie implizit und explizit Inhaltanbieter zu Gunsten eigener Angebote (vor allem kostentechnisch) diskriminieren können. Der Public Service Charakter des Internets kann dadurch mit weitreichenden negativen Folgen für die publizistische Vielfalt, die Innovationsdynamik und die KonsumentInnensouveränität zerstört werden.

Folgende Szenarien illustrieren unterschiedliche Effekte auf *Content Provider* (CPs) und *Enduser* (EUs):

Szenario	Beschreibung	Effekte auf CPs	Effekte auf EUs	Regulierung
QoS-based Competition (Wettbewerb auf Basis der Service-Qualität)	Bepreisung unterschiedlicher Service-Levels nach funktionalen Kriterien	Effizientere Netzauslastung, Qualitätsgarantien	Preiselastizität, Qualitätsgarantien	Markt
Negative Effekte				
Tiered Access (Abgestufter Zugang)	Verlagerung der Investitionen vom neutralen in den nicht-neutralen Bereich der Infrastruktur	Erhöhung der Markteintrittsbarrieren	Vertiefung der digitalen Kluft	Markt
Corporate Bureaucracy (Zugangsschranken durch Verwertungspolitik)	Exklusive Bereitstellung innovationskritischer technischer Funktionalitäten im nicht-neutralen Bereich der Infrastruktur	Verlangsamte Innovation	Verringertes Angebot / Lock Out	Wettbewerbsrecht Marktaufsicht
Bad Incentive (Diskriminierung von Konkurrenzangeboten)	Bevorzugung eigener Services gegenüber jenen von FremdanbieterInnen	Lock-Out-Mechanismen durch Diskriminierung	Verringerung der KonsumentInnen-Souveränität	Wettbewerbsrecht Marktaufsicht

Blocking (Ausschluss von Konkurrenz-angeboten)	Verringerung der Content- und Dienste-Vielfalt durch Ausschluss fremder Dienste	Markt-abschottung	Verringerung der kulturel-len und publizisti-schen Vielfalt	Wettbe-werbsrecht Marktauf-sicht

Quelle: Krone und Pellegrini (2012)

4. Netzneutralität in der Europäischen Union

In der Regulierungsgebarung der EU-Mitgliedsstaaten zur Netzneutralität droht eine *Fragmentierung des europäischen Telekommunikationsmarktes* durch abweichende nationale Regulierungspraktiken und Gesetzgebungen. Während etwa Frankreich, Spanien und Großbritannien durch Maßnahmen wie „Sperren statt Löschen", die in Gesetzen wie dem britischen *Digital Economy Act*[1] oder dem französischen *Hadopi Gesetz*[2] festgeschrieben sind, bereits weitgehend von der Netzneutralität abgerückt sind, haben die Niederlande, Luxemburg und der wallonische Teil Belgiens die Netzneutralität de facto gesetzlich verankert. Zwischen diesen beiden Extrempositionen finden sich die restlichen Länder der EU 27, die mit unterschiedlichen Regulierungsansätzen, vor allem aber in sehr unterschiedlich ausgereiften politischen Diskursen den Regulierungsgegenstand behandeln. Innerhalb dieser Gruppe der „Unentschlossenen" reicht das Spektrum von einer intensiven Diskussion (z.B. in Deutschland, Österreich, Polen, Schweden), über einen schwach ausgeprägten Diskurs (z.B. Belgien [Flandern], Griechenland, Zypern, Irland, Slowakei, Slowenien, Tschechien, Ungarn, Bulgarien), bis hin zum kompletten Fehlen des Themas auf den nationalen politischen Agenden (z.B. Estland, Lettland, Litauen, Finnland).

[1] s. http://erg.eu.int/doc/consult/bor12_30.pdf (Letzter Aufruf: 01.06.2012)
[2] s. http://www.legislation.gov.uk/ukpga/2010/24/section/47 (Letzter Aufruf: 10.11.2012)

Auf Ebene der EU kreist der Diskurs vornehmlich um die Definition von *Transparenzrichtlinien und -vorgaben*, die im Sinne des *KonsumentInnenschutzes* die KonsumentInnensouveränität stärken und so (indirekt) den Wettbewerb stützen. Dieser Transparenzansatz greift jedoch zu kurz und blendet die *Marktmacht- und Konzentrationsproblematik* auf Seite der Carrier und Einspeiser weitgehend aus. Es ist nachweislich bekannt, dass Carrier durch *vertikale Integration* zunehmend selbst Content-Services anbieten und diese zu Lasten von konkurrenzierenden Angeboten bevorzugen. Hier bedarf es im Sinne einer *Entbündelung von Infrastruktur und Inhalten* einer klaren gesetzlichen Regelung, in welchem Ausmaß und zu welchen Bedingungen Carrier in der Lage sein dürfen, Content-Dienste über hauseigene Netze anzubieten.

Wie auch der Dachverband der europäischen Telekommunikationsregulierungsbehörden *BEREC*[3] in ihrer Untersuchung thematisiert, ist weitgehend offen, inwieweit wirtschaftliche Diskriminierungspraktiken und die dazu nötigen technischen Maßnahmen in die *bürgerlichen Grundrechte* – allen voran Briefgeheimnis, Rede- und Versammlungsfreiheit – eingreifen. Eine differenzierte Analyse steht hierzu aus.

5. Schlussbetrachtung

Der Regulierungsgegenstand Netzneutralität ist abstrakt und komplex, jedoch in seinen Folgewirkungen – insbesondere gesellschaftspolitisch – weitreichend. Die unterschiedlichen Positionen in der EU bergen die Gefahr der Herausbildung eines fragmentierten europäischen Telekommunikationsmarktes. Entsprechend kann nur eine gesamteuropäische Lösung als sinnvoll und erstrebenswert angesehen werden.

---

[3] s. http://www.senat.fr/dossier-legislatif/pjl07-405.html (Letzter Aufruf: 10.11.2012)

Eine rein wirtschaftlich geführte Diskussion verkennt den öffentlichen Charakter des Internets sowie den öffentlichen Auftrag der Telekommunikationsanbieter als Common Carrier. Ein Bekenntnis zur Netzneutralität trägt dem öffentlichen Charakter des Internets Rechnung und ist gleichzeitig ein Bekenntnis zur Kommunikations- und Meinungsfreiheit und damit zur Sicherung der bürgerlichen Grundrechte.

Entsprechend findet sich der politische Diskurs mit folgenden *Spannungsfeldern* konfrontiert:

- Telekommunikations- und Medienregulierung (Wirtschafts- vs. Kulturgut)
- Zugangsfreiheit und Verfügungsgewalt über Eigentum (Wegerecht vs. Diskriminierung)
- Netzneutralität und Diversifikationspotentiale im TK-Sektor (Durchleitungsentgelte für Netzeinspeiser und Premiumdienste wie IPTV für Internetuser)

Aus wettbewerbspolitischer Dimension lässt sich festhalten:

- Breitband-Dienste sind in einem nicht-neutralen Internet stärker betroffen als Schmalband, aber schmalbandige Datenlast ist schwer prognostizierbar (kumulative Effekte)
- QoS-Prinzip hebt die Trennung zwischen Infrastruktur und Content auf
- Marktmachtproblematik und Lock-In Effekte werden in einem nicht-neutralen Internet verschärft und begünstigen bereits dominante Infrastruktur- und Content-Anbieter
- Regulative Korrektive (z.B. Marktaufsicht, Wettbewerbsrecht) eignen sich nur bedingt für dynamische, innovations- und diffusionskritische Märkte, da zu behäbig, teuer und langwierig

Adverse redistributive Wohlfahrtseffekte auf Content Provider und End User sind im Falle eines unzureichenden politischen Ordnungsrahmens für zweiseitige Märkte absehbar.

Weiterführende Literatur

Krone, Jan / Pellegrini, Tassilo (2012). Netzneutralität und Netzbewirtschaftung. Baden-Baden: Nomos Verlag.

Pellegrini, Tassilo (2012). Quality-of-Service in der Netzbewirtschaftung – Effekte einer eingeschränkten Netzneutralität auf Cloud-basierte Geschäftsmodelle. In: Krone, Jan / Pellegrini, Tassilo (Hg.). Netzneutralität und Netzbewirtschaftung. Baden-Baden: Nomos Verlag, S. 117–137.

Waltner, Katharina / Pellegrini, Tassilo (2012). Die Netzneutralität aus wettbewerbsökonomischer Sicht. Eine Argumentationsanalyse der EU-Konsultation zu „Offenes Internet und Netzneutralität". In: Krone, Jan; Pellegrini, Tassilo (Hg.). Netzneutralität und Netzbewirtschaftung. Baden-Baden: Nomos Verlag, S. 97–116.

3.3. Menschenrechte und OGD (Christof Tschohl)

Open Government Data aus der Perspektive der Grund- und Menschenrechte

Keywords: Menschenrechte, Gewährleistungspflichten, Open Government Data (OGD), Digital Rights, Good Governance, Transparenz, Informationsfreiheit, Datenschutz

1. Funktionen der Grund- und Menschenrechte 171
2. Information im Netz – Serviceleistung oder Gebot? 172
3. Anhaltspunkte für Veröffentlichungspflichten in der EMRK 174
4. Grundrechte für eine Veröffentlichungspflicht 175
5. „Digital Rights" im modernen Grundrechtsbestand 177
6. Transparente Verwaltung und Datenschutz 180
7. Schlussfolgerungen 181
Weiterführende Literatur 182

1. Funktionen der Grund- und Menschenrechte

Grund- und Menschenrechte sind die Eckpfeiler einer offenen demokratischen Gesellschaft, über die sich auch der Gesetzgeber nicht einfach hinwegsetzen darf. Den Grundrechten kommt dabei mehrfache Bedeutung zu, oder anders gesagt, sie erfüllen mehrere Funktionen. Im Zentrum der juristischen Arbeitspraxis steht dabei zumeist ihre Eigenschaft als subjektive Rechte, die dem oder der Einzelnen zustehen und die letztlich einklagbar sind. In Verfahren vor Gerichten und Verwaltungsbehörden sollen sie jedem Individuum die gleiche Freiheit und Fairness garantieren, hier entfalten die Grundrechte ihre konkrete Rechtsschutzfunktion. In ihrer institutionellen Funktion repräsentieren die Menschenrechte zugleich grundlegende Wertvor-

stellungen und sind damit Orientierungsnormen, die den Gesetzgeber in seinem Gestaltungsspielraum anleiten sollen.

In Europa kommt der Europäischen Menschenrechtskonvention (EMRK) herausragende Bedeutung zu. Als internationale Konvention mit 47 Mitgliedsstaaten, das sind alle europäischen Staaten außer Weißrussland, eröffnet sie für alle Menschen im Jurisdiktionsbereich der Mitgliedsstaaten den Weg einer Individualbeschwerde an den Europäischen Gerichtshof für Menschenrechte (EGMR) in Straßburg. In Österreich steht die EMRK seit 1964 im Verfassungsrang und die Einhaltung ihrer Garantien sind daher innerstaatlich letztlich beim Verfassungsgerichtshof (VfGH) einklagbar.

Der EGMR zieht in ständiger Rechtsprechung die Mitgliedsstaaten der Konvention nicht nur aufgrund eines unmittelbaren Eingriffs durch staatliches Handeln zur Verantwortung, sondern auch dann, wenn sie es unterlassen haben, eine wirksame Ausgestaltung der Konventionsrechte vorzunehmen. Den Staat trifft eine umfassende Gewährleistungspflicht, den Garantien in der Konvention zu effektiver Wirksamkeit zu verhelfen. Diese Gewährleistungspflicht kann etwa bedeuten, dass der Staat in der Verantwortung steht, Institutionen zur Verfügung zu stellen, etwa Gerichte, und auch entsprechende Verfahren vorsehen muss, innerhalb derer der Schutz von Grund- und Menschenrechten wirksam betrieben werden kann.

Die Gewährleistungspflicht kann aber auch darin liegen, dass der Staat für die Öffentlichkeit oder einen eingeschränkten Kreis (sog. Parteienöffentlichkeit) Informationen zur Verfügung stellen muss, über die er bereits verfügt, oder die er unter Umständen sogar erheben oder zumindest aufbereiten muss, was zum Thema dieses Beitrags führt.

2. Information im Netz – Serviceleistung oder Gebot?

Die Zugänglichkeit von Informationen für die Menschen in einer staatlich organisierten demokratischen Gesellschaft ist in manchen

Bereichen fundamental für ein gleichberechtigtes Zusammenleben. Beispielsweise stellt die Kundmachung eines Gesetzes im Bundesgesetzblatt überhaupt die Bedingung für dessen Geltung dar. Es sei vorerst dahingestellt, ob damit ein normativer Zwang einhergehen kann, dass diese Kundmachung über eine Online-Datenbank zugänglich sein soll. Tatsächlich besteht in Österreich mit dem Rechtsinformationssystem des Bundes (RIS) eine umfassende Datenbank aller Gesetze und Verordnungen. Aus dem juristischen Arbeitsalltag wegzudenken ist diese jedenfalls kaum mehr.

Ähnliches gilt für die Sammlung der Entscheidungen der österreichischen Höchstgerichte, die ebenfalls im RIS auffindbar sind. Anders als zur Kundmachung von Gesetzen findet sich hierfür zwar keine Veröffentlichungspflicht in der Österreichischen Bundesverfassung (nicht zu verwechseln mit dem Öffentlichkeitsgrundsatz von Gerichtsverfahren), Anhaltspunkte für einen solchen Zwang ergeben sich jedoch aus der Rechtsprechung des EGMR. Grundrechtseingriffe sind nach der EMRK nämlich generell nur auf Basis einer gesetzlichen Grundlage zulässig, wobei als solche auch eine gefestigte Rechtsprechung in einem Land dienen kann, was jedenfalls eine gewisse Vorhersehbarkeit der Judikatur voraussetzt, die ohne Veröffentlichung von Entscheidungssammlungen kaum gegeben ist.

In anderen Bereichen erkennt die Rechtsordnung die grundlegende Notwendigkeit einer allgemeinen Veröffentlichung bestimmter Informationen an, indem sie beispielsweise das Vertrauen in die Richtigkeit bestimmter Register schützt und daran bestimmte Rechtsfolgen knüpft. Als eines der wichtigsten Beispiele sie in diesem Zusammenhang das Grundbuch genannt. Die Zivilrechtsordnung lässt dabei den gutgläubigen Erwerb von Rechten im Vertrauen auf den aktuellen Grundbuchstand zu, selbst wenn dieser von den tatsächlichen rechtlichen Verhältnissen abweichen sollte. Nicht weniger wichtig für ein funktionierendes Wirtschaftsleben, um ein anderes Beispiel zu nennen, ist etwa die Ediktsdatei zu Insolvenzen, Zwangsverwaltungen

und Versteigerungen. Dieses Beispiel unterstreicht die Bedeutung des Internets als Medium für die Zugänglichkeit wesentlicher Informationen des Wirtschaftslebens. Daraus ist natürlich nicht automatisch zu schließen, dass für den Staat auch ein grundrechtlicher Zwang besteht, dieses Medium dafür zu nützen.

3. Anhaltspunkte für Veröffentlichungspflichten in der Europäischen Menschenrechtskonvention

Die erste Norm im Gefüge der EMRK (Europäischen Menschenrechtskonvention), die in diesem Zusammenhang zunächst die Aufmerksamkeit auf sich zieht, ist Artikel 10 EMRK, der den Titel *Meinungs- und Informationsfreiheit* trägt. Diese Norm beinhaltet in ihrem Kern, dass der Staat für eine pluralistische Medienlandschaft und einen indoktrinierungsfreien Raum zu sorgen hat. Die Zugänglichkeit zu bereits bestehenden Medien und öffentlichen Informationskanälen darf nur unter engen Voraussetzungen auf der Basis gesetzlicher Grundlagen zur Erreichung bestimmter, eindeutig genannter höherwertiger Ziele beschränkt werden. Diese Ziele werden abstrakt in Artikel 10 Absatz 2 EMRK aufgezählt.

In den Schutzbereich dieses Grundrechts fallen auch das Verbot der Zensur sowie der Schutz des Redaktionsgeheimnisses. Aufgrund der Rechtssprechung des EGMR zu dieser Norm wurde in den 90er Jahren etwa das ORF-Monopol zu Fall gebracht.

Auch bestimmte Gewährleistungspflichten, also positive Verpflichtungen des Staates, hat der EGMR aus dieser Bestimmung bereits abgeleitet. So wurde zum Beispiel der Ausschluss einer kritischen Soldatenzeitung (*Der Igel*) aus dem Verteilersystem im österreichischen Bundesheer im Fall EGMR 1994, *Vereinigung Demokratischer Soldaten Österreichs* und *Gubi gg. Österreich*, als Verletzung des Art 10 EMRK angesehen. Das österreichische Bundesheer musste daher auch diese aufgrund ihrer kritischen Inhalte in „Ungnade“ gefallene

Zeitung wie alle anderen Zeitschriften über das bestehende Verteilersystem allen Soldaten zugänglich machen.

Davon zu trennen ist jedoch die Frage, ob aus dieser Grundrechtsgarantie auch die Pflicht des Staates ableitbar ist, bestimmte Inhalte der Öffentlichkeit zur Information zugänglich zu machen. Die bisherige Leitentscheidung zu dieser Frage wurde vom EGMR 1984 im Fall Guerra gg. Italien gefällt. Es ging in diesem Fall darum, dass die AnrainerInnen forderten, dass ihnen Daten über die Emissionen dieser Industrieanlage zugänglich gemacht werden sollen. Nachdem die innerstaatlichen Instanzen in Italien ihnen diesen Anspruch verwehrten, führten die Anrainer dagegen Beschwerde vor dem EGMR und stützten sich dabei auf Art 10 EMRK. Der EGMR hielt in seinem Urteil zunächst fest, dass ein solcher Anspruch auf Veröffentlichung bestimmter Informationen nicht allgemein aus der Informationsfreiheit des Art 10 EMRK ableitbar sei. Bemerkenswert ist, dass der Gerichtshof das Bestehen dieser Informationspflicht aber aus dem Anspruch auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK ableitet[1]. Der EGMR hielt dabei fest, dass dem materiellen Anspruch gewisse Verfahrens- und Informationsrechte immanent sind, die eine Bedingung zur effektiven Gewährleistung dieses Anspruchs darstellen.

4. Grundrechte für eine Veröffentlichungspflicht

Aus der Informationsfreiheit im klassischen Sinn des Art 10 EMRK lässt sich also keine allgemeine Pflicht zur aktiven Veröffentlichung von Informationen durch den Staat ableiten. Wenn die Veröffentlichung von bestimmten Informationen in begründetem Zusammenhang konkret dem effektiven Schutz bestimmter Grundrechtsgaran-

[1] Diese Norm wird in der Rechtsprechung des Gerichtshofs traditionell sehr weit ausgelegt und umfasst auch den Schutz der Gesundheit als notwendige Voraussetzung für die Verwirklichung des Privat- und Familienlebens.

tien dient, trifft den Staat die Pflicht, Informationen auch zu erheben und für deren Veröffentlichung in angemessener Form zu sorgen. Dabei hat er als Kriterien die Auffindbarkeit, die Zugänglichkeit und Datenbankqualität zu berücksichtigen. Diese Konstellation wird vor allem im Umwelt- und Gesundheitsbereich häufig anzutreffen sein. Je stärker der Zusammenhang zwischen der begehrten Information und dem Schutz fundamentaler Rechtsgüter ausgeprägt ist, desto höher die Anforderungen an Qualität und Aktualität der Informationen (Stichwort: Fukushima).

Eigenständig ist die Frage, über welches Medium der Zugang zu öffentlichen Informationen hergestellt werden soll und ob die Veröffentlichung im Internet allgemein zugänglich sein soll. Dabei ist die Art des öffentlichen Interesses ausschlaggebend bei der Abwägung, inwieweit der Aufwand in einem vertretbaren Verhältnis zum Nutzen steht. Welche Informationen via Open Government Data proaktiv zur Verfügung gestellt werden sollen, lässt sich abstrakt schwer definieren, sondern hängt vom Thema ab. Mögliche Beispiele wären Materialien über Gesetzesentwürfe oder Informationen zum Haushalt eines Ministeriums.[2]

Sind die Informationen „im Netz", wird der Zugang zum *Digital Right*. Zu beachten sind die Bedingungen für den Zugang zur Information. Ist nachvollziehbar, welche NutzerInnen sich wann welche Informationen einholen? Werden IP-Adressen beim Zugriff auf die Informationen gespeichert? Welches Maß an Kontrolle besteht im Hinblick auf das NutzerInnenverhalten?

Besonders indiziert ist die Klärung dieser Fragen, wenn es um politische Grundrechte und die Wahrung der demokratischen Mitbestimmung der Menschen geht. Die Digital Rights erhalten an dieser Stelle eine neue Dimension. Das Grundrecht auf Datenschutz dient hier

[2] Welche Beamten zuständig sind, muss beispielsweise nicht unbedingt generell öffentlich sein, sondern nur auf Anfrage. Die Notwendigkeit solcher Informationen kann aber ebenfalls je nach der interessierenden Materie unterschiedlich sein.

ebenfalls der Wahrung der politischen Grundfreiheiten in einer demokratischen Gesellschaft. Wenn nur „Parteienöffentlichkeit" gemeint ist, kommen weitere Regelungsfragen hinzu: Zum Beispiel Registrierungspflichten, Zugriffsprotokollierung, Integritätsgewährleistung, NutzerInnen-Authentifizierung, etc.

5. „Digital Rights" im modernen Grundrechtsbestand

Das Konzept der *Digital Rights* basiert auf der Annahme, dass die universell geltenden Menschenrechte nicht nur *offline* sondern auch *online* zu respektieren sind. Dies hat der Menschenrechtsrat der Vereinten Nationen hat im Juli 2012 durch eine Resolution (A/HRC/20/L.13) in Bezug auf die Allgemeine Erklärung der Menschenrechte aus 1948 klargestellt. Der Begriff *Digital Rights*, wie er hier verstanden wird, bezieht sich auf die Anwendung des Schutzbereichs bestehender Menschenrechte auf jene Phänomene, die durch den besonderen Bezug zur „digitalen Welt" die Zusammenfassung zu einer Gruppe rechtfertigen. Die Überlegung dahinter ist, dass in der digitalen Welt nicht zuletzt aufgrund der oft komplexen technischen Zusammenhänge die Beurteilung alles andere als trivial ist, welche (klassischen) Menschenrechte durch einen Sachverhalt berührt oder gar verletzt sind. Als Beispiel sei an den Höhepunkt des „Arabischen Frühlings" erinnert, als das Regime in Ägypten den Zugang zum Internet weitgehend abschaltete. Diese Maßnahme lässt sich nur schwer den Garantien der Privatsphäre oder des davon abgeleiteten Datenschutzes zuordnen, weil es sich kaum um eine „Verarbeitung" personenbezogener Daten handelt. Allerdings sollte mit dieser Aktion verhindert werden, dass die Menschen Informationen erhalten und politische Aktionen und Demonstrationen online organisieren. Über die moderne grundrechtsdogmatische Figur umfassender Gewährleistungspflichten gelangt man zum Ergebnis, dass ein Eingriff in die demokratischen Grundpfeiler der Informations-, Meinungs- und Versammlungsungsfreiheit vorlag. Diese Konstellation ist noch

verhältnismäßig einfach zu fassen, viel schwieriger wird es, wenn Eingriffe über „mehrere Ecken" technischer Zusammenhänge stattfinden. Wie ist beispielsweise der Einsatz sogenannter *Spyware* zu beurteilen, die zunächst nur Informationen über sämtliche Nutzer-Inneneinstellungen eines Computersystems sammelt und weiterleitet, ohne sogleich einen Bezug zu einer bestimmten Person herstellen zu können? Dies könnte etwa der Vorbereitung dienen, Schwachstellen im System zu finden, um später unbemerkt Zugang zu diesem System zu erlangen. Immer häufiger wird in jüngster Zeit in dieser Hinsicht diskutiert, ob gar die Schaffung neuer Grundrechtsgarantien notwendig ist, um die besonderen Schutzbedürfnisse in der IT-Welt angemessen zu erfassen. Diesen Ansatz wählte etwa das Deutsche Bundesverfassungsgericht, als es mit dem Urteil vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07) ein neues *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität Informationstechnischer Systeme* schuf, das vielfach als „Computer-Grundrecht" bezeichnet wurde und international Aufsehen erregte. Auch die eigenständige Verankerung des Grundrechts auf Datenschutz in Artikel 8 der Grundrechte-Charta der EU geht in diese Richtung. Die Debatte um die Formulierung und Verankerung neuer Rechte ist aber lediglich eine Begleiterscheinung einer intensiveren Befassung mit digitalen Phänomenen, die mit dem Konzept der Digital Rights einhergeht. Der Mehrwert des Konzepts liegt vielmehr darin, durch eine Risikobewertung aus einer technischen Perspektive in Relation zu den Schutzzwecken des etablierten Bestands an Menschenrechten zu erkennen, ob und inwiefern eine Bedrohung aus der virtuellen Welt ihr schädliches Potential in der realen Welt zu entfalten vermag.

Die EMRK entstand im Jahr 1948 und die VerfasserInnen haben die besonderen Fragestellungen einer digitalen Informationsgesellschaft wohl kaum bedacht. Der EGMR folgt dazu bis heute seinem Grundsatz, den er im Jahr 1978 in der Rechtssache *Tyrer gg. U.K.* aufgestellt

hatte (EGMR 25.4.1978, 5856/72, Tyrer gg. Vereinigtes Königreich, Serie A 26 = EuGRZ 1979, 162 = NJW 1979, 1089): „The Convention is a living instrument wich has to be interpreted in the light of present-day conditions." Grundrechtsschutz ist stets modern.

Seit 1. Dezember 2009 ist die Charta der Grundrechte der Europäischen Union als Teil des Primärrechts verbindlich für die Europäische Union. Die Grundrechte-Charta enthält als moderner Menschenrechts-Katalog in Art 41 ein *Recht auf eine gute Verwaltung* und in Art 42 ein *Recht auf Zugang zu Dokumenten*. Das Schlagwort in der internationalen Entwicklungszusammenarbeit zu diesem Ansatz ist *Good Governance*. Im Zusammenhang mit Open Government Data geht es dabei auch um die Nachvollziehbarkeit von wesentlichen Entscheidungen (Verwaltungsbehörden, Gerichte, Regierung) und um die Frage, wie weit Entscheidungsprozesse generell transparent sein müssen, beispielsweise im Hinblick auf die Veröffentlichung von Beratungsprotokollen eines gerichtlichen Senats oder die Veröffentlichung von Dissenting- oder Concouring Opinions.

Der Begriff Good Governance ist auslegungsbedürftig und muss in Zukunft erst noch mit mehr Gehalt durch die Rechtsprechung erfüllte werden. Jedenfalls aber ist anzunehmen, dass damit gewisse Mindestanforderungen an eine transparente Verwaltung einhergehen, die auch die Zugänglichkeit von Informationen im öffentlichen Interesse umfassten. Im Hinblick auf die Bekämpfung und Verhütung von Korruption und Missständen innerhalb der Verwaltung besteht ein enger Zusammenhang mit der Wahrung des rechtsstaatlichen Prinzips. Das noch relativ junge Feld des E-Government bietet nun die große Chance, die tragenden Grundsätze einer transparenten Verwaltung bereits in der Konzeption neuer Anwendungen zu implementieren. Ähnlich dem modernen Datenschutzkonzept *Privacy by Design* sollte das Leitmotiv hier *Transparency by Design* lauten.

6. Transparente Verwaltung und Datenschutz

Transparenz im Staat ist ohne Zweifel zu begrüßen und stets zu fordern. Gleichzeitig ist darauf Bedacht zu nehmen, dass durch die Offenlegung von Daten im Rahmen der öffentlichen Verwaltung nicht eine Verletzung der Privatsphäre einzelner Menschen resultiert. Dort wo die Gefahr einer Kollision mit dem Grundrecht auf Datenschutz (Art 8 Grundrechte-Charta, § 1 DSG 2000) besteht, ist eine Abwägung nach dem Grundsatz der Verhältnismäßigkeit vorzunehmen. Der Zweck der Offenlegung im öffentlichen Interesse muss in einem angemessenen Verhältnis zur möglichen Beeinträchtigung betroffener Personen stehen. Insbesondere ist zu bedenken, in welchem Umfang personenbezogene Daten zur Erreichung des Zwecks veröffentlicht werden sollen. Öffentlich Bedienstete in bestimmten Zusammenhängen namentlich zu nennen kann angemessen sein, während die Veröffentlichung von deren Privatanschrift oder ihrer Sozialversicherungsnummer kaum gerechtfertigt sein wird. Dabei kann die konkrete politische Situation in einem bestimmten Land durchaus unterschiedliche Maßstäbe bei der Abwägung sachlich rechtfertigen. Als Beispiel kann hier etwa die junge Republik Montenegro genannt werden, wo zur Bekämpfung des immensen Korruptionsproblems vor nicht allzu langer Zeit beschlossen wurde, eine Spendenliste für politische Parteien mit *personal-ID* der SpenderInnen zu veröffentlichen. Inwiefern es zur Erreichung des Zwecks tatsächlich notwendig ist, auch die Personal-Identifikationsnummer zu veröffentlichen, sollte freilich in Frage gestellt werden.

Das Datenschutzgrundrecht ist seinerseits nicht Selbstzweck, sondern hat vielmehr „Katalysatorfunktion“ für den Schutz anderer Grundrechtsgarantien. Am häufigsten dient es dem Schutz der Privatsphäre, häufig aber auch dem Schutz vor Diskriminierung. In etwas anderer Konstellation dient es gerade dem Schutz der politischen Grundrechte wie der Meinungsfreiheit oder der Vereinigungs- und Versammlungsfreiheit.

Der Grundsatz der Transparenz und der Datenschutz stehen sich aus der Perspektive der Grundrechtswissenschaften jedenfalls nicht im Weg, die Balance ist aber mit Sorgfalt zu suchen.

7. Schlussfolgerungen

Die Betrachtung des Themas Open Government Data (OGD) aus der speziellen Perspektive der Grund- und Menschenrechte soll in diesem weiten Feld eine Orientierung bei der Suche nach den Prioritäten bieten. Neben ihrem Charakter als subjektive Gewährleistungen erfüllen die Menschenrechte auch die objektivierte Funktion von Orientierungsnormen und reflektieren als solche Wertvorstellungen, allen voran das Bekenntnis zur unantastbaren Menschenwürde. Obwohl praktisch jedes Thema letztlich mit mehr oder weniger Umwegen auf eine menschenrechtliche Frage zurückgeführt werden kann, sollte man nicht übersehen, dass bei weitem nicht jedes Problem rechtlich gelöst werden kann. Die Systematik der Menschenrechte vermag aber gerade bei schwierigen Abwägungsproblemen oft einen wertvollen Beitrag zu leisten, insbesondere zur Wahrung der Sachlichkeit und zur Transparenz der Argumente. Als lebendiges Instrument am Puls der Zeit verstanden, gebieten Grund- und Menschenrechtsgarantien meines Erachtens aber vor allem, den Grundgedanken der OGD, also die freie und elektronisch standardisierte Verfügbarkeit staatlich gesammelter Informationen, im modernen demokratischen Staat als grundsätzliche rechtliche Garantie anstatt als freiwillige Serviceleistung zu verstehen.

Weiterführende Literatur

10 Prinzipien offener Regierungsinformationen, englische Fassung, Sunlight Foundation: http://sunlightfoundation.com/policy/documents/ten-open-data-principles/ (Letzter Aufruf: 29.03.2013)

Deutsche Fassung, OGD WEISSBUCH, online: http://open.semanticweb.at/display/OGDW/6.2+Die+zehn+Prinzipien+offener+Regierungsinformationen (Letzter Aufruf: 29.03.2013)

Wolfgang Benedek / Catrin Pekari (Hrsg.), Menschenrechte in der Informationsgesellschaft, 2007.

3.4. Ist Facebook ein neuer öffentlicher Raum? (Matthias C. Kettemann)

Keywords: Öffentlicher Raum, Privatsphäre, Facebook

1. Die alten öffentlichen und die neuen privaten Räume 183
2. Zwischen NutzerInnenglück und Regierungszensur 184
3. Die Einschränkung des Hausrechts 185
4. Facebook – der neue „Uhu"? 187

1. Die alten öffentlichen und die neuen privaten Räume

Was den Griechen die Agora und den Römern das Forum war, ist für die politisch Aktiven unserer Zeit (aber nicht nur für diese) das Internet. Eine der zentralen Rollen des Internets ist es, Resonanzraum zu sein, in dem neue Ideen ventiliert, Meinungen gesammelt und artikuliert werden. Das Internet ist die am schnellsten wachsende Diskurssphäre des 21. Jahrhunderts mit substanziellem Einfluss auf soziale und politische Entscheidungsfindungsprozesse. Von seinem Potenzial her ist das Internet daher ein genuin öffentlicher Raum. Nur wurde dieser öffentliche Raum seit Beginn der Kommerzialisierung des Internets zunehmend in private Räume und Räumlichkeiten aufgesplittet. Die Geschichte des Internets ist daher auch eine Geschichte der Privatisierung. Diese ist nicht nur negativ zu sehen: Die Privatisierung des Netz ging Hand in Hand mit einer Professionalisierung; ohne kommerzielle Anreize wäre die Entwicklung nicht so schnell (wenn überhaupt) fortgeschritten. Doch der Prozess verlief nicht ohne Opfer und ist durchaus in wichtigen Teilen konzeptuell reversibel.

Was macht einen öffentlichen Raum aus? In einem öffentlichen Raum können BürgerInnen „truth to power" sagen. Doch in zunehmenden Maße können sie dies nur, nachdem sie sich Allgemeinen Geschäfts-

bedingungen unterworfen haben, die große Teile des öffentlichen Raums des Internets zu einem de jure privaten Ort machen.

Da der dort geführte Diskurs aber dennoch genuin öffentlich ist, können sie als halböffentlich-halbprivate Orte bezeichnet werden. So sieht es auch die *OpenNet Initiative* in einem 2010 veröffentlichten Bericht: „Instead of an unregulated, decentralized Internet, we have centralized platforms serving as public spaces: a quasi-public sphere. This quasi-public sphere is subject to both public and private content controls spanning multiple jurisdictions and differing social mores. "

Der Europarat hat sich dieser Herausforderung angenommen. In seiner Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated internet platforms and online service providers von 2011[1] unterstrich das Ministerkomitee des Europarates, dass soziale Netzwerke und Blogging-Seiten wichtige Rollen für die Kommunikation der Zivilgesellschaft einnehmen und es Whistleblowern und MenschenrechtsverteidigerInnen ermöglichen, Informationen auszutauschen. Aus dieser Rolle, dieser Verantwortlichkeit, folgen Pflichten.

2. Zwischen NutzerInnenglück und Regierungszensur

Nun verwenden viele Unternehmen allerdings Allgemeine Geschäftsbedingungen (AGBs) (terms of service), die Menschenrechte (insbesondere jene, die die Privatsphäre schützen) verletzten. Soziale Netzwerke stehen vor dem Dilemma, „NutzerInnen glücklich zu machen" und „Regierungszensur zu vermeiden, um ihr Service in möglichst vielen Ländern anbieten zu können", wie Jillian C. York

[1] s. https://wcd.coe.int/ViewDoc.jsp?id=1883671&Site=CM (Letzter Aufruf: 4.4.2013)

schreibt[2]. Zu oft zensieren die Anbieter sozialer Netzwerke daher lieber mehr als weniger.

Die Nutzung eines Bildes, das ein Tier bei der Schlachtung zeigt, würde als legitime Meinungsäußerung im Rahmen einer Kampagne für eine vegetarische Lebensweise im öffentlichen Raum (etwa während einer Demonstration) als unproblematisch wahrgenommen werden. In vielen der – sonst so offenen – sozialen Netzwerke würde ein derartiges Bild aber zensiert werden. Nicht, weil der Staat dies verlangte, sondern weil das soziale Netzwerk die Inhalte als Teil ihres Verwaltungsraums begreift, im Rahmen ihres Hausrechts regulieren möchte, und „ihr" Netzwerk möglichst „sauber" zu halten bestrebt ist. Denn unproblematische Meinungen, also jene, die nicht „offend, shock and disturb" (also beleidigen, schockieren und stören), wie es der Europäische Gerichtshof für Menschenrechte im Fall *Handyside* formulierte, sind sozialen Netzwerken viel eher willkommen als Herausforderungen des Meinungsmainstreams. Denn diese könnten UserInnen abschrecken; und abgeschreckte UserInnen besuchen keine sozialen Netzwerke. Damit gingen diesen aber ihre Ware verloren: die Aufmerksamkeit der UserInnen, die von sozialen Netzwerken an WerbekundInnen verkauft wird.

Wie kann die Gestaltungsfreiheit sozialer Netzwerke hinsichtlich ihrer Allgemeinen Geschäftsbedingungen eingeschränkt werden? Wie kann dem Argument, dass UserInnen ja nicht verpflichtet seien, gerade in diesem Netzwerk ihre Meinung äußern zu wollen, effektiv entgegnet werden?

3. Die Einschränkung des Hausrechts

Auf beiden Seiten des Atlantiks lassen sich Gerichtsentscheidungen Hinweise entnehmen, wie soziale Netzwerke zu semi-öffentlichen,

[2] s. https://opennet.net/policing-content-quasi-public-sphere (Letzter Aufruf: 4.4.2013)

semi-privaten Räumen werden können – mit eingeschränktem „Hausrecht“ für die BetreiberInnen.

In *New Jersey Coalition Against War in the Middle East v. J.M.B. Realty Corp.* (1994) arbeitete der Supreme Court von New Jersey das Recht von Individuen heraus, Protestliteratur in privaten Shopping Malls zu verteilen. Wenn nämlich die EigentümerInnen von Shopping Malls diese zu de facto öffentlichen Foren gemacht hätten (etwa durch die Aufstellung von Bühnen und die Erlaubnis für High School-Gruppen, dort aufzutreten), gebe es kein Zurück. Wer zu *Cheerleaders* Ja sagt, muss auch Demonstrationen erlauben. Unter welchen Umständen die Eigentumsrechte der Mall-BetreiberInnen gegenüber der Meinungsäußerungsfreiheit zurücktreten müssen, hat das Gericht dann 2000 im Fall *The Green Party of New Jersey v. Hartz Mountain Industries, Inc.* entwickelt.

Der einzig relevante vergleichbare Fall des Europäischen Gerichtshofs für Menschenrechte folgte im Wesentlichen den amerikanischen Urteilen, gestattete Staaten aber einen weiten Ermessensspielraum. In der 2003 ergangenen Entscheidung in *Appleby gegen Vereinigtes Könrigreich* musste der Gerichtshof die Rechte von Shopping Mall-EigentümerInnen gegen die Meinungsäußerungsfreiheit einer Gruppe abwägen, die in der Mall Unterschriften für eine Petition sammeln wollte. Straßburg betonte, dass in diesem Fall eine Vielzahl von alternativen Möglichkeiten bestanden habe, Unterschriften einzuholen und die Meinung der Gruppe zu äußern: Die erfolglosen KlägerInnen hätten „alternative means, such as calling door-to-door or seeking exposure in the local press, radio and television“ verwenden können, um auf sich aufmerksam zu machen.

Dieser Entscheidung können wir entnehmen, dass der Gerichtshof bereit ist zu akzeptieren, dass unter bestimmten Umständen (wenn keine Alternative besteht), die Eigentumsrechte der ManagerInnen von privaten Orten (wie es soziale Netzwerke formal sind) gegen das Recht auf Meinungsfreiheit zurückstehen müssen. Denn dieses ist

Voraussetzung für jenen öffentlichen Diskurs, der einer Demokratie wesenseigen ist.

4. Facebook – der neue „Uhu“?

Je erfolgreicher soziale Netzwerke also werden (und je weniger Alternativen sie zulassen, um erfolgreich andere Menschen zu kontaktieren), desto eher werden sie zu halb-öffentlich, halb-privaten Räumen. Dieser Prozess erinnert an die generischen Produktbezeichnung: An einst geschützte Begriffe, die ob ihres Erfolges in das öffentliche Sprachgut übergingen und Gattungsnamen wurden. Die RechteinhaberInnen von Tesa, Tixo, Uhu und Walkman beraubten sich, qua Erfolg, ihres eigenen Copyrights. Dieses Schicksal kann auch sehr erfolgreichen sozialen Netzwerken drohen.

Doch schon bevor soziale Netzwerke auf dem Wege des Rechts dazu gezwungen werden, auch Meinungen zuzulassen, die „shocking, disturbing and offending“ sind, sollten sie sich den Mehrwert eines menschenrechtssensibleren Ansatzes vor Augen führen.

Unabhängig ihrer Klassifikation als private, halb-private oder öffentliche Räume ergeben sich aus der Funktion von sozialen Netzwerken für den öffentlichen Diskurs schon jetzt zwei Folgen: Eine Verpflichtung zumindest der Meinungsmonopolen nahe kommenden Netzwerke, die öffentliche Debatte zu fördern (auch wenn dies mit ihren kurzfristigen wirtschaftlichen Zielen in einem gewissen Konflikt stehen könnte) und eine Verpflichtung für Staaten, keinen politisch motivierten Druck auf privat organisierte Internetplattformen auszuüben, sondern sich ihrer Verantwortung für die Einhaltung bzw. Gewährleistung aller Menschenrechte, insbesondere jenem der Meinungsfreiheit, bewusst zu werden.

3.5. Weltöffentlichkeit (Stephan Schlögl)

Ein Fallbeispiel zu Rio+20 auf Twitter

Keywords: Öffentlichkeit, Habermas, Twitter, Rio+20, Globalisierung

1. Öffentlichkeit – wozu? 190
2. Globalisierte Öffentlichkeit 193
3. Rio+20 auf Twitter 196
4. Zugang 196
5. Ebenbürtigkeit 198
6. Ungleichverteilung 200
7. Zersplitterter Diskurs 202
8. Schlussfolgerungen 205

WWW meint world wide web. Diesen drei Buchstaben hängt die Vorstellung an, das Internet würde uns in ein globales Netzwerk einflechten, in dem informiert, debattiert und zunehmend auch revoltiert wird, Diskussionsprozesse hätten sich internationalisiert und die GesprächsteilnehmerInnen seien heute über den ganze Erdball verteilt. Diese Idee einer Weltöffentlichkeit geistert vermutlich durch viele Köpfe, und zwar nicht nur durch jene der sogenannten „digital natives".

Auf welchen Prämissen eine solche Idee aufbaut, welche Voraussetzungen sie zu erfüllen hätte und inwiefern sich letztere im Netz bereits umgesetzt sehen, soll hier anhand der Ergebnisse einer Fallstudie zu Twitter und der Kommunikation rund um die „Konferenz der Vereinten Nationen über Nachhaltige Entwicklung" 2012 (kurz Rio+20) aufgezeigt werden.

1. Öffentlichkeit – wozu?

Die wissenschaftliche Konzeption des Öffentlichkeitsbegriffs geht zu weiten Teilen auf die Arbeit Jürgen Habermas' zurück, der 1962 mit seiner Habilitationsschrift „Strukturwandel der Öffentlichkeit" einen ersten Grundstein gelegt hat. Es handelt sich dabei um eine historisch-soziologische Aufarbeitung der Öffentlichkeitsstrukturen seit dem 15. Jahrhundert. Seinen normativen Ansatz illustriert Habermas am Bild des Kaffeehauses des 17. und 18 Jahrhunderts, wo sich „die zum Publikum versammelten Privatleute […] anschickten, die öffentliche Gewalt zur Legitimation vor der öffentlichen Meinung zu zwingen"[1]. Die Öffentlichkeit beansprucht als Forum die Arbeit der EntscheidungsträgerInnen zu legitimieren – oder eben nicht. Dieser Anspruch impliziert jedoch, dass es sich hier nicht um ein direktes Herrschaftsbestreben handelt, sondern vielmehr ist es deklariertes Ziel der Sache, Herrschaft aufzulösen[2].

Habermas' Habilitationsschrift hieße wohl nicht „Strukturwandel", wenn sie sich nicht mit Veränderungen beschäftigen würde. Jene Öffentlichkeit, die in den Kaffeehäusern und Salons des 17. und 18. Jahrhunderts dem normativen Konzept noch nahe genug kam, um sie zur Verbildlichung des Ideals zu benutzen, verfällt im 19. und 20. Jahrhundert zusehends. Diesen komplexen Prozess analysiert Habermas als sozialen Strukturwandel und politischen Funktionswandel. Ersterer manifestiere sich als Wandel, von einem „kulturräsonierenden" zu einem „kulturkonsumierenden" Publikum, der wie folgt beschrieben wird.

> *„Funk, Film und Fernsehen bringen den Abstand, den der Leser zum gedruckten Buchstaben einhalten muß, gradweise zum Verschwinden – eine Distanz, die die Privatheit der Aneignung ebenso*

---

[1] vgl. Habermas, Jürgen (1990). Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Öffentlichkeit. Frankfurt am Main: Suhrkamp, S. 84.
[2] vgl. ebd. S. 153

> *verlangen, wie sie die Öffentlichkeit eines räsonierenden Austausches über das Gelesene erst ermöglichte. Mit den neuen Medien ändert sich die Kommunikationsform als solche; sie wirken darum, in des Wortes strikter Bedeutung, penetranter als die Presse je es vermochte. Das Verhalten des Publikums nimmt unter dem Zwang des Don't talk back eine andere Gestalt an. Die Sendungen, die die neuen Medien ausstrahlen, beschneiden, im Vergleich zu gedruckten Mitteilungen, eigentümlich die Reaktion des Empfängers. Sie ziehen das Publikum als Hörende und Sehende in ihren Bann, nehmen ihm aber zugleich die Distanz der Mündigkeit , die Chance nämlich, sprechen und widersprechen zu können.*"[3]

„Strukturwandel der Öffentlichkeit" erschien erstmals 1962. Ins Englische übersetzt wurde das Buch jedoch erst 1990 und schließlich in den USA neuerlich stark rezipiert. Dies hat nicht zuletzt damit zu tun, dass in den 90er Jahren jenes Medium aufkam, dem diese Publikation gewidmet ist, das Internet. Die Faszination, die dem Web zukam, lässt sich mitunter dadurch erklären, dass es den BenutzerInnen, zumindest in technischer Hinsicht, jene Mündigkeit zurückgibt, die Habermas 30 Jahre zuvor im obigen Zitat ansprach. KonsumentInnen werden zu engagierten NutzerInnen, sie werden in diesem Sinn erneut zu ProduzentInnen von Information und Argumentation. (Vgl. Clara Landler, Kapitel 1.3. *Macht Sprache Internet?*)

Die Vorstellung, reziproke Kommunikationskanäle stellten eine Notwendigkeit dar, um der Demokratie den notwendigen Schub zu versetzen, stammt jedoch schon aus den dreißiger Jahren des vergangenen Jahrhunderts. Schon Berthold Brecht forderte, den Rundfunk von einem „Distributionsapparat in einen Kommunikationsapparat" zu verwandeln, um die NutzerInnen aus ihrer Isolation zu befreien[4]. Dass diese Forderung im Netz und insbesondere in Sozialen Medien nun

---

[3] ebd. S. 260f

[4] vgl. Brecht, Bertold (2002). Der Rundfunk als Kommunikationsapparat – Rede über die Funktion des Rundfunk (1932). In: Kursbuch Medienkultur: Die maßgeblichen Theorien von Brecht bis Baudrillard. Hrsg. von Claus Pias. Stuttgart: DVA, S. 260.

seine Umsetzung gefunden hat, ist vielleicht der zentralste Grund dafür, dass viele BeobachterInnen im Internet einen potentiellen Aktionsraum einer neuen Öffentlichkeit im Sinne Habermas' sehen.

Erst 2006 äußert sich der Sozialwissenschaftler dann persönlich zu jenem vermeintlichen Potential des nun gar nicht mehr so neuen Mediums. Er tat dies entgegen aller Erwartung mit vernichtenden Worten und setzte das Web dem Vorwurf aus, es würde den Diskurs in Millionen Einzelteile zersplittern und stünde auf diese Weise der Verdichtung und Synthetisierung von Argumenten entgegen[5]. Dass diese Einschätzung in der politischen Blogosphäre zu großem Unmut führte, war voraus zu sehen. Howard Rheingold, Netzenthusiast der ersten Stunde, warf dem Theoretiker vor, das Internet nicht zu verstehen und wünschte sich, Habermas hätte es bei einem „I leave that work to younger scholars, who can build contemporary theories on the foundations of my earlier work about the role of the public sphere in an infosphere dominated by mass media"[6] belassen. Rheingold war jedoch nicht der einzige, der in dieses Horn stieß[7]. Zur Frage, ob es legitim ist, den Theoretiker zu enteignen und sich seines Werkes nach eigenem Sinn und Zweck und Anwendungsgebiet zu bedienen, kann man stehen, wie man will. Habermas' Kritikpunkt allzu unreflektiert im Raum stehen zu lassen, ist jedoch verfehlt. Es mag sein, dass Habermas die Funktionsweisen neuer Medien tatsächlich nicht zu überblicken vermag, mit seiner Kritik der Zersplitterung schlägt er jedoch ein Thema an, welches auch jüngere und sicherlich technik-

---

[5] vgl. Habermas, Jürgen (2008). Ach, Europa. Frankfurt am Main: Suhrkamp, S. 161f.

[6] s. Rheingold, Howard (2007). Habermas blows off question about the Internet and the Public Sphere. Weblog url: http://www.smartmobs.com/2007/11/05/habermas-blows-off-question-about-the-internet-and-the-public-sphere/ (Letzter Aufruf: 19.11.2012), vorletzter Absatz.

[7] Stuart Geiger (2009) fasst in *Does Habermas Understand the Internet? The Algorithmic Construction of the Blogo/Public Sphere* diese Debatte anschaulich zusammen. (In: Gnovis 10.1, S. 1–29.)

affinere BeobachterInnen thematisieren. Eli Pariser schlägt mit seinem Begriff der „Filterbubble“ in genau die selbe Kerbe[8]. Die Filterbubble ist schlussendlich nichts anderes, als eine Zersplitterung in unverbundene Teilöffentlichkeiten (vgl. Julian Ausserhofer, Kapitel 1.6. *Gute Filter, böse Filter?*). Diese Problematik sollte also nicht außer Acht gelassen werden, wenn man sich mit potentiellen virtuellen Öffentlichkeiten auseinandersetzt.

2. Globalisierte Öffentlichkeit

In seiner Habilitationsschrift behandelt Habermas Öffentlichkeit im gesicherten Rahmen des Nationalstaates. Wenn er von öffentlicher Gewalt spricht, denkt er an Regierungen, die in Parlamenten Gesetze verabschieden. Die bürgerliche Öffentlichkeit sieht er im Kaffeehaus versammelt vor sich.

Wenn man heute von virtuellen Öffentlichkeiten spricht und den Versuch unternimmt, dieses Theoriegebäude dem Internet gefügig zu machen, denkt man an Foren und Soziale Medien, man denkt an AkteurInnen, die losgelöst und unabhängig von nationalstaatlichen Grenzen agieren und somit im besten Fall in einen internationalen Dialog treten. Gleichzeitig haben sich in unserer globalisierten Welt auch die Problemstellungen verändert und den begrenzten nationalstaatlichen Rahmen gesprengt. Die neuen Herausforderungen unserer Zeit, allen voran sei hier der Klimawandel zu nennen, sind zweifellos nur über gemeinsame, international koordinierte Anstrengungen in den Griff zu bekommen.

James Bohman (Professor für Philosophie an der Saint Louis University, USA) versuchte bereits 2004, die Idee der Öffentlichkeit auf das Internet anzuwenden und sie gleichzeitig in den transnationalen

[8] vgl. Pariser, Eli (2012). Filter Bubble: Wie wir im Internet entmündigt werden. Carl Hanser Verlag GmbH & CO. KG.

Raum zu heben[9]. Er setzt sich dabei mit zwei Einwänden des kanadischen Politikwissenschaftlers und Philosophen Will Kymlickas auseinander.

Kymlicka hält der globalen Öffentlichkeit erstens entgegen, dass sich die Problematik der Elitenbildung bei räumlicher Ausdehnung geradewegs verschärft und mit dem Ideal der Gleichheit unter den DiskursteilnehmerInnen endgültig brechen würde.

Bohman widerspricht dieser Kritik insofern, als dass eine verstärkte Elitenbildung seiner Ansicht nach nur dann zum Tragen käme, wenn man transnationale Öffentlichkeit als ein aufgeblasenes Abbild nationaler Öffentlichkeiten verstehe. In diesem Fall ließe sich die Kritik als reiner Skaleneffekt formulieren. Tatsächlich müsste eine transnationale Öffentlichkeit jedoch weit flexibler und vielschichtiger an die Arbeit der EntscheidungsträgerInnen andocken[10] und schließlich sei die Kompetenz letzterer auf Grund ihrer Dezentralität nicht mit nationalstaatlichen Systemen vergleichbar. Diese Argumentation deckt sich mit jener der *Global-Governance* Forschung, derzufolge:

> *„Governance keine Staatstätigkeit ist und somit begrifflich nicht mehr in ein hierarchisches System eingebettet. Mit Governance werden hier horizontale (verschiedene Akteure) sowie vertikale (verschiedene Ebenen) Formen der Koordination bezeichnet. Es gibt keinen zentralen Akteur mehr, dem allein eine Steuerungs- und Kontrollfähigkeit zugesprochen wird, sondern Entscheidungsprozesse finden interaktiv zwischen staatlichen wie nichtstaatlichen Akteuren statt".*[11]

---

[9] vgl. Bohman, James (2004). Expanding Dialogue: the Internet, the public sphere and prospects for transnational democracy. In: After Habermas: New Perspectives on the Public Sphere. Hrsg. von Nick Crossley und John Michael Roberts. Oxford, Blackwell Publishing/The Sociological Review, S. 131–155.

[10] vgl. ebd., S.147f

[11] s. Behrens, Maria (2005). Global Governance – Eine Einführung. In: Globalisierung als politische Herausforderung. Global Governance zwischen Utopie und Realität. Hrsg. von Maria Behrens. Bd. 3. Governance. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 18.

Zweitens wirft Kymlicka ein, dass Öffentlichkeit stets einen gemeinsamen kulturellen und politischen Verständigungsraum voraussetze, der auf globaler Ebene nicht gegeben sei[12]. Diese Problemstellung ist jedoch keineswegs neu. In gewisser Weise ähnelt sie dem Übergang von archaischen, zu modernen Gesellschaften, wie ihn Habermas selbst analysiert. In archaischen Gesellschaften sind die drei lebensweltlichen Elemente Kultur, Gesellschaft und Identität zu einer Einheit verschmolzen und erklären sich demnach gegenseitig. In modernen Gesellschaften differenziert sich diese Einheit aus – und die Regeln des Zusammenlebens lassen sich immer weniger auf Basis gemeinsamer traditioneller Weltbilder legitimieren. Sie müssen deshalb diskursiv stabilisiert werden[13]. In anderen Worten: Legitimität muss kommunikativ erzeugt werden und Kommunikation wird damit gleichsam zum Ziel und zur Voraussetzung einer funktionierenden Öffentlichkeit.

Neue Medien bieten die technischen Instrumentarien um global zu kommunizieren, Solidarität und letztlich Legimtität herzustellen. Ob diese Kommunikation den Idealen einer politischen Öffentlichkeit gemäß der Habermas'schen Konzeption entspricht, soll nun anhand eines Fallbeispiels hinterfragt werden, welches passender kaum sein könnte. Die *Konferenz der Vereinten Nationen über Nachhaltige Entwicklung*, abgehalten im Juni 2012 in Rio de Janeiro, bot ein Forum, um sowohl die sozialen, als auch ökologischen Herausforderungen zu diskutieren, die eine globalisierte Weltwirtschaft mit sich bringt. Welche Kommunikationsstrukturen sich rund um dieses Ereignis auf der Microbloggingplattform Twitter entwickelt haben, möchte ich im Folgenden kurz beleuchten.

---

[12] vgl. Bohman 2004, S. 147

[13] vgl. Palazzo, Guido (2002). Die Mitte der Demokratie. 1. Auflage. Baden-Baden: Nomos Verlagsgesellschaft, S. 30f.

3. Rio+20 auf Twitter

Jürgen Habermas hat ein normatives Öffentlichkeitskonzept geschaffen. Seine Ausführungen beschreiben einen Sollzustand, dem zumindest drei Voraussetzungen zu Grunde liegen. Es handelt sich dabei um die grundsätzliche Unabgeschlossenheit des Publikums, die Ebenbürtigkeit der TeilnehmerInnen und die uneingeschränkte Problematisierbarkeit aller Themenbereiche[14]. Weil mir die ersten beiden Kriterien Zugang und Ebenbürtigkeit im Zusammenhang mit einer ausgedehnten transnationalen Öffentlichkeit besonders zentral erscheinen, werde ich nun versuchen, sie einigen empirischen Daten gegenüberzustellen und mich zusätzlich mit dem Einwand der Zersplitterung des Diskurses im Netz auseinandersetzen.

Rio+20 fand zwischen dem 20. und 22. Juni 2012 statt. Ich habe den Untersuchungszeitraum auf eine Woche vor und eine Woche nach der Konferenz eingeschränkt und anhand verschiedener Schlagwörter[15] Statusupdates auf Twitter gefiltert. Daraus ergab sich eine Gesamtsumme von knapp über 717.000 Tweets, die wiederum von knapp 240.000 verschiedenen BenutzerInnen verfasst wurden. Anschließend wurden über die Twitter-API bzw. Entwicklerschnittstelle noch zusätzliche Profilinformationen zu den einzelnen BenutzerInnen erhoben.

4. Zugang

> *„Die bürgerliche Öffentlichkeit steht und fällt mit dem Prinzip des allgemeinen Zugangs. Eine Öffentlichkeit, von der angebbare Gruppen eo ipso ausgeschlossen wären, ist nicht etwa nur unvollständig, sie ist vielmehr gar keine Öffentlichkeit.“* [16]

---

[14] vgl. Habermas 1990, S. 97f.

[15] Gesucht wurde nach den Schlagwörtern RIO20, RIO+20, Rioplus20 und futurewewant.

[16] S. Habermas 1990, S. 156.

Die Zentralität dieses Kriteriums liegt also auf der Hand. Aus empirischer Sicht lässt sich die Frage des grundsätzlich möglichen Zugangs, der hier angedeutet wird, nur aus einem Rückschluss des tatsächlichen Zugangs beantworten. Natürlich ließe sich im Fall von Twitter auch argumentieren, jeder Mensch könne sich problemlos ein Twitterkonto einrichten, womit dieses Kriterium ohnehin gegeben sei. Spätestens seit Michel Castells acht verschiedene *digital gaps* identifiziert hat[17], wissen wir jedoch, wie vielfältig Zugangsbeschränkungen wirken können. Für die vorliegende Fragestellung ist der sogenannte *global divide* am wichtigsten, also die Frage, aus welchen Weltregionen Menschen am Diskurs teilnehmen (können).

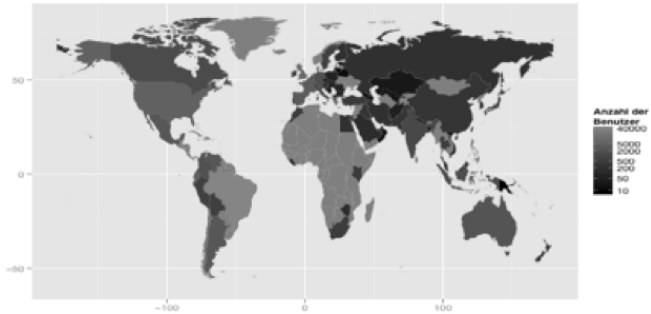


Abbildung 1: Herkunft der Twitter-UserInnen[18]

Abbildung 1 zeigt, aus welchen Ländern zu Rio+20 getwittert wurde. Wie sich unschwer erkennen lässt, dominieren die beiden Amerikas und Europa. Wäre Südamerika nicht so stark vertreten, würde sich dieses Bild perfekt mit jenem decken, das Castells beschreibt, wenn er

[17] vgl. Castells, Manuel (2008). Die Internet-Galaxie: Internet, Wirtschaft und Gesellschaft. 1. Auflage der deutschen Übersetzung von Reinhart Kößler. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 261ff.

[18] Die Daten beziehen sich auf das Feld Timezone in den Benutzereinstellungen, die in den meisten Fällen mit einem englischen Städtenamen versehen sind. Über einen automatisierten Abgleich mit einer Städtedatenbank konnten 145.720 Benutzer eindeutig einem Staat zugeordnet werden. Die Farbskala dieser Weltkarte wurde logarithmiert, um auch die feineren Abstufungen vor allem im unteren Bereich der Skala sichtbar zu machen.

vom Global Divide des Digital Gaps spricht. Afrika ist der sprichwörtliche graue Fleck auf der Landkarte und die Tatsache, dass insgesamt nicht einmal 2% aller UserInnen von diesem Kontinent aus twitterten, lässt außer Zweifel, dass es sich hier nicht um einen Zufall handelt. AfrikanerInnen werden damit zur „angebbaren Gruppe" in den Worten Habermas' und die NutzerInnenzahlen lassen mehr als nur die bloße Vermutung zu, dass ökonomische und soziale Strukturen in den jeweiligen Ländern mitverantwortlich für die fehlende afrikanische Präsenz in diesem Diskurs sind.

Für die Frage der Öffentlichkeit bedeutet dies, dass ein konstitutives Kriterium nicht gegeben ist, was in diesem Fall besonders schwer wiegt. Entscheidungen, die auf Konferenzen wie Rio+20 getroffen oder eben nicht getroffen werden, können besonders für afrikanische Länder schwerwiegende Konsequenzen haben, da Themen mit spezifischer Relevanz auch für Afrika (allen voran nachhaltige Entwicklung) hier auf globaler Ebene verhandelt werden.

5. Ebenbürtigkeit

> *„Die Parität, auf deren Basis allein die Autorität des Arguments gegen die der sozialen Hierarchie sich behaupten und am Ende auch durchsetzten kann, meint im Selbstverständnis der Zeit die Parität des »bloß Menschlichen«. Les hommes, private gentleman, die Privatleute bilden das Publikum nicht nur in dem Sinne, daß Macht und Ansehen der öffentlichen Ämter außer Kraft gesetzt sind; auch wirtschaftliche Abhängigkeiten dürfen im Prinzip nicht wirksam sein; Gesetze des Marktes sind ebenso suspendiert wie die des Staates."*[19]

Um die Frage der Ebenbürtigkeit bzw. Gleichheit der AkteurInnen zu operationalisieren, macht es Sinn, sich das Bild des Kaffeehauses in Erinnerung zu rufen. Der bedeutende Unterschied zu Sozialen Medien liegt hier in der absoluten Gleichverteilung der Reichweite.

[19] S. Habermas 1990, S. 97.

Die physischen Begebenheiten des Gesprächs versammelter Personen haben den egalitären Nebeneffekt, dass jedes Wort von jedem/jeder anderen gehört werden kann bzw. muss. Demgegenüber wird mit dem Followerprinzip auf Twitter die Ungleichverteilung der Reichweite geradezu institutionalisiert und technisch integriert. Wie stark drückt sich diese strukturelle Ungleichheit tatsächlich aus?

Ein klassisches, aus der Statistik stammendes Maß zur Bestimmung von Ungleichverteilungen, ist der sogenannte Gini-Koeffizient. Dieser kann zwischen null und eins schwanken, wobei null absolute Gleichverteilung bedeuten würde (jedeR bekommt exakt gleich viel) und eins dementsprechend absolute Ungleichverteilung (eineR bekommt alles und alle anderen nichts). Darstellen und gleichzeitig graphisch definieren, lässt sich dies anhand der Lorenzkurve, bei der man auf der y-Achse bspw. das kumulierte Einkommen aufträgt und auf der x-Achse die Gesamtbevölkerung in aufsteigender Reihenfolge gemäß dem Einkommen listet. Eine 45° Gerade würde demnach Gleichverteilung darstellen, denn 20% der Bevölkerung hätten dann 20% des Einkommens zur Verfügung, 50% hätten 50% usw. Umso weiter sich die reale Kurve von dieser Geraden entfernt, umso ungleicher verteilt wären die unterschiedlichen Einkommen – und genau das misst der Gini-Koeffizient[20].

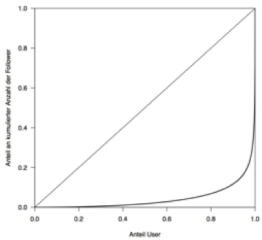


Abbildung 2: Lorenzkurve

Legt man dieses Analyseinstrument auf die Followerzahlen der TwitteruserInnen um, die zu Rio+20 getweetet haben, ergibt sich die in Abbildung 2 dargestellte Lorenzkurve. Wie sich unschwer erkennen lässt, haben wir es hier mit einer enormen Ungleichverteilung, bzw. einem Gini-Koeffizienten von 0,913, zu tun. 80% der NutzerInnen

[20] vgl. Cowell, Frank A (2009). Measuring Inequality. Oxford University Press. url: http://darp.lse.ac.uk/pap ersDB/Cowell_measuringinequality3.pdf (Letzter Aufruf: 19.11.2012), S. 22, 26f.

erreichen gemeinsam nicht einmal 10% der kumulierten Reichweite. Um der LeserIn eine Orientierung zu geben, sei hier angemerkt, dass die Vereinten Nationen die weltweite Verteilung von Reichtum auf einen Gini-Koeffizienten von 0,892 schätzt[21].

Inwieweit dieser Vergleich zulässig ist, lässt sich natürlich anzweifeln. Man könnte argumentieren, dass die Ökonomie mit knappen Ressourcen rechnet und ihre Instrumente auf der Prämisse aufbauen, dass kein Dollar gleichzeitig von mehreren Personen besessen werden kann. Demgegenüber könnte man behaupten, Twitter biete einen Kontext, in welchem jede BenutzerIn mit einem unerschöpflichen Investitionspotenzial an Aufmerksamkeit ausgestattet ist und so vielen anderen UserInnen folgen kann, wie ihr oder ihm beliebt. Ich möchte dem jedoch entgegnen, dass Aufmerksamkeit ein ebenso beschränktes Gut ist, welches im Informationszeitalter besonders stark umkämpft ist. Niemand, der Twitter ernsthaft benutzt, kann einer unbeschränkten Anzahl an Personen folgen[22].

6. Ungleichverteilung

Wie lässt sich diese Ungleichverteilung nun erklären? Der Verdacht liegt nahe, dass jenes Ideal, demzufolge „Macht und Ansehen der öffentlichen Ämter außer Kraft gesetzt sind“[23], hier verletzt wird. Natürlich sind hier nicht Ämter im klassischen Sinne gemeint, sondern jede Art von Ansehen und Reputation, die von außerhalb des Mediums (Twitter) in dieses hineingetragen wird. In anderen Worten: Prominente jeder Art verzerren die Ebenbürtigkeit innerhalb von Twitter aufs Gröbste. Ein Indiz dafür ist, dass die *verifizierten*

---

[21] vgl. Davies, James B. u. a. (2008). The World Distribution of Household Wealth. In: WIDER Discusion Paper, S. 10.

[22] Selbst wenn die Daten durch Bots und Spam Accounts stark verfälscht wären, sprechen die Zahlen so eindeutige Worte, dass man ohne Weiteres von einer stark ausgeprägten Ungleichheit sprechen kann.

[23] vgl. Habermas 1990, S. 97.

Accounts[24] im Datensatz durchschnittlich fast 150-mal so viele *Follower* haben, wie „normale NutzerInnen" und die Wahrscheinlichkeit, dass eine ihrer Statusmeldungen „geretweetet" (also von anderen NutzerInnen weitergeleitet) wird, ist über 50 mal so groß wie bei letzteren. Es ist weder Sinn und Zweck, noch entspricht es dem Geschäftsmodell von Twitter, Gleichheit unter den TeilnehmerInnen herzustellen. Viele der NutzerInnen würden dies wohl auch gar nicht gutheißen, denn schließlich ermöglicht das System „auch normalen NutzerInnen" politischen RepräsentantInnen und anderen „Prominenten" in gewisser Weise nahe zu sein. Gleichzeitig vermittelt diese Nähe jedoch ein falsches Gefühl von Gleichheit, dass auf wundersame Weise den Eindruck entstehen lässt, Kommunikation funktioniere hier auf gleicher Augenhöhe.

Vorstellungen wie jene von Howard Rheingold, der 1994 noch davon sprach „daß virtuelle Gemeinschaft [sic!] sie [die Menschen; Anm. d. Verf.] so behandeln, wie sie sich das immer gewünscht haben: als Denker, als Übermittler von Ideen, als Wesen mit Gefühlen, nicht als bloße Körper mit einem bestimmten Aussehen und einer bestimmten Art zu gehen und zu sprechen"[25], müssen heute als romantische Utopie eines frühen Netz-Enthusiasmus verstanden werden. Die „Autorität des besseren Argumentes" wird von der faktischen Abschaffung der Anonymität (allen voran in sozialen Netzwerken) untergraben. Hierarchien werden gemeinsam mit Stereotypen und Sexismen ins Netz übertragen und Wege hin zu einem adäquaten Umgang damit, geschweige denn einer Überwindung davon, müssen,

---

[24] Verifizierte Accounts sind solche, bei denen Twitter die Authentizität der BenutzerInnen überprüft. Laut eigenen Angaben konzentriert man sich dabei auf Prominente aus den Bereichen Musik, Film, Mode, Regierung, Politik, Religion, Journalismus, Medien, Werbung, Business. Die Verifizierung von Accounts stellt damit den legitimierten Brückenschlag zwischen Twitter-interner und Twitter-externer Identität dar.

[25] vgl. Rheingold, Howard (1994). Virtuelle Gemeinschaft. 1. Auflage der deutschen Übersetzung. Addison-Wesley, S. 41.

genauso wie in allen anderen Diskursräumen, erst gefunden werden. (Vgl. Leonie Tanczer, Kapitel 1.4. *Post, Gender, Internet?*)

7. Zersplitterter Diskurs

Übrig bleibt Habermas' eigene Kritik am Internet als Aktionsraum einer funktionierenden Öffentlichkeit. Das „Publikum zerfällt im virtuellen Raum in eine riesige Anzahl von zersplitterten, durch Spezialinteressen zusammengehaltenen Zufallsgruppen" sagt Habermas 2008 (S. 161). Inwiefern diese Aussage auch auf den Twitterdiskurs um Rio+20 zutrifft, möchte ich nun kurz anhand meiner empirischen Daten beleuchten.

Grundsätzlich entsprechen die Daten den klassischen Voraussagen für moderne Onlinekommunikation. Ein großer Teil der BenutzerInnen beteiligt sich nur marginal an der Diskussion, während der größte Teil der Inhalte von einigen wenigen generiert wird[26]. Konkret heißt das in diesem Fall, dass 64% der NutzerInnen nur einen einzigen Tweet zu den definierten Schlagwörtern verfasst haben und nur knappe 20% häufiger als 5-mal getweetet haben. Diese Tatsache dafür zu missbrauchen, den Diskurs als zersplittert zu verdammen, wäre jedoch allzu einfach und wenig zielführend. Bestimmt ist es wahr, dass große Teile nur kurz an der Diskussion teilnehmen und wenig dazu beitragen, dies ist jedoch nicht viel mehr als ein Resultat der Technik, die es erlaubt, auch ohne tiefer gehendes Engagement schnell seine Meinung oder eine bestimmte Information zu einem Thema los zu werden. Interessant sind aber, wie in jedem Diskurs, die TeilnehmerInnen, die sich intensiv mit einem Thema auseinander setzen und dementsprechend kommunikativ engagiert sind. Wie stark diese NutzerInnen

[26] vgl. Stegbauer, Christian (2012). Strukturelle Ursachen der Entstehung von Ungleichheit in Beziehungsmedien. In: Ungleichheit – Medien- und kommunikationssoziologische Perspektiven. Hrsg. von Christian Stegbauer. Wiesbaden: Springer VS, S. 301–322.

vernetzt sind, ist schlussendlich für die Konsistenz eines Diskurses ausschlaggebend.

Abbildung 3: Followernetzwerk der UserInnen mit über 50 Tweets zu Rio+2027

Abbildung 3 stellt das Netzwerk der Followerbeziehungen jener NutzerInnen dar, die zumindest 50-mal etwas zu Rio+20 getweetet haben. Insgesamt trifft das auf 1213 NutzerInnen zu, die wiederum ein Netzwerk aus 1081 Knoten bilden[28]. Jede NutzerIn wird in der Abbildung

[27] Für eine genauer Betrachtung in Farbe kann diese Visualisierung online unter http://homepage.univie.ac.at/stephan.schloegl/rio20 abgerufen werden.
[28] Für die restlichen Accounts konnten die Informationen zu Followern entweder nicht abgerufen werden oder sie stellen sogenannte Isolate dar, also Knoten die zu keinem einzigen der anderen Knoten Verbindungen eingehen.

durch einen Kreis (Knoten) dargestellt, dessen Farbe[29] Auskunft darüber gibt, welche Spracheinstellung das Konto hat. Die Größe gibt an, wieviele Follower die NutzerIn innerhalb des Netzwerkes hat. Die Linien zwischen diesen Knoten stellen die Followerbeziehungen zwischen ihnen dar. Jene Knoten, die zueinander Verbindungen haben bzw. Verbindungen zu den gleichen Knoten haben, werden möglichst nahe beieinander dargestellt.

Auf den ersten Blick fällt auf, dass sich das Netzwerk in Sprachgruppen gliedert, wobei einerseits eine portugiesischsprachige bzw. brasilianische Gruppe identifizierbar ist und andererseits eine englischsprachige Gruppe, die stark von den offiziellen Twitteraccounts der Vereinten Nationen dominiert und zusammengehalten wird.

Das soll nicht darüber hinwegtäuschen, dass das Netzwerk insgesamt überaus gut integriert ist. Alleine die Tatsache, dass weniger als 10% aller NutzerInnen, welche zumindest 50-mal zu Rio+20 getweetet haben, in irgendeiner Weise in das Netzwerk eingebunden sind, spricht gegen die Kritik Habermas'. Durchschnittlich hat jeder Knoten des Netzwerkes 30 Verbindungen zu anderen TeilnehmerInnen. Bedenkt man nun, dass die hier abgebildeten NutzerInnen laut Profilinformationen aus insgesamt über 50 verschiedenen Ländern der ganzen Welt stammen, ist dies besonders bemerkenswert. Würde man den englischsprachigen Teil des Netzwerkes nach Herkunft einfärben, könnte man sehen, dass hier NutzerInnen aus den verschiedensten Weltregionen teilnehmen.

Insgesamt lässt sich deshalb nur noch einmal wiederholen, dass diese Gruppe der Engagierten überaus eng vernetzt ist und sich Informationsaustausch bzw. Diskussion hier scheinbar tatsächlich auf globalem Niveau abspielt. Von einer Zersplitterung kann demnach kaum die Rede sein.

---

[29] Die Wichtigsten sind Blau: Englisch, Grün: Portugiesisch, Gelb: Französisch, Rosarot: Spanisch.

8. Schlussfolgerungen

Normative Konzepte wie jenes der Öffentlichkeit von Jürgen Habermas eignen sich hervorragend dafür, Fragestellungen zu formulieren und Kriterien für empirische Untersuchungen zu operationalisieren. Schwierig wird es allerdings dann, wenn es darum gehen soll, die Resultate zu bewerten, weil Ideale besonders unbarmherzige Maßstäbe sind und es in ihrer Natur liegt, dass sie unerreichbar bleiben.

Aus diesem Grund mögen auch viele der hier vorgestellten Ergebnisse ein vernichtend negatives Bild auf das Netz als Diskursraum im Habermas'schen Sinne geworfen haben. Wir haben gesehen, dass mit Afrika ein ganzer Kontinent an den vermeintlich globalen Kommunikationsprozessen, die unseren Alltag in nördlichen Industrieländern so maßgeblich prägen, kaum Anteil hat. Es konnte gezeigt werden, wie ungleichverteilt die Reichweite unserer geschriebenen Worte zumindest auf der Plattform Twitter ist.

Gleichzeitig hätte man den Fokus aber auch auf die positiven Ergebnisse richten können. Man hätte unterstreichen können, dass bereits heute breite Teile der Weltbevölkerung (mit der empfindlichen Ausnahme von Afrika) stärker oder schwächer in diesen Diskurs integriert sind. Man hätte die Aufmerksamkeit auch darauf lenken können, dass der Median der Followerzahlen bei 189 liegt und darauf hinweisen, dass dies eine beachtliche Reichweite ist und es ohne Twitter sehr schwierig wäre, die eigenen Anliegen und Informationen ähnlich breit diffundieren zu können.

Darin liegt jedoch nicht der Sinn dieses Artikels. Auch heute überwiegt meiner Wahrnehmung zufolge die Euphorie darüber, welche deliberativen Möglichkeiten uns das Netz bietet. Gerade deshalb ist es wichtig, auch die Schwächen dieser Systeme zu beleuchten. Erst wenn wir Kenntnisse darüber haben, welche Stimmen im Netz unter- oder gar nicht repräsentiert sind und wir uns bewusst werden, dass wir trotz aller vermeintlichen Nähe innerhalb der Sozialen Medien nicht

immer auf gleicher Augenhöhe kommunizieren, können wir diese Instrumente sinnvoll und mit Bedacht nutzen und die Aussagekraft des Kommunizierten richtig einschätzen. Der Netzenthusiasmus soll keineswegs getrübt werden, schließlich scheint er das Interesse junger Generationen an deliberativen Prozessen neu geweckt zu haben. Es ist jedoch von äußerster Wichtigkeit, über die Kommunikationsstrukturen, in denen wir uns hier bewegen, Bescheid zu wissen, um diese sinnvoll nutzen zu können.

3.6. Hassreden im Internet (Viktor Szabados)

Über die Grenzen der juristischen Verfolgung von Hassreden im Internet

Keywords: Hassreden, geographische Grenzen, globales Internet, juristische Verfolgung

1. Grenzenloses Internet 207
2. Grenzen der Meinungsfreiheit 208
3. Grenzen der juristischen Verfolgung 211
4. Ausblick 214
Weiterführende Informationen 216

1. Grenzenloses Internet

Das Internet hat unser Leben verändert. Es bietet vieles, angefangen von der Verbreitung und dem Austausch von Informationen über den Erwerb von Produkten und Dienstleistungen bis hin zur persönlichen Entfaltung von Meinungsfreiheit. Die Ausübung der Menschenrechte wird durch das Internet unterstützt und deren Wirkungsbereich insbesondere durch den so geschaffenen Raum erweitert. (Vgl. Hans Christian Voigt, Kapitel 1.2. *Rechte eines jeden Menschen _am_ Internet*; Matthias C. Kettemann, Kapitel 2.1. *Neue Menschenrechte für das Internet?*)

Meinungen über die Unterschiede oder Koexistenz der offline sowie der online Welt können auseinandergehen. Aber eines scheint sicher zu sein: Diese Fragenstellung bringt mehrere Herausforderungen mit sich. Mit Blick auf die Staatsbürgerschaft sind wir zum Beispiel alle zumindest einem Staat zugehörig, der sowohl geographisch als auch juristisch gesehen Grenzen und Regeln aufweist. Das Internet hinge-

gen kennt üblicherweise keine Grenzen. Digitale BürgerInnen bilden ein Netzwerk, das über Staatsgrenzen hinausgeht und sehr unterschiedliche Aspekte umfasst. Zu glauben, dass weltweit dieselben Umstände und Einschätzungen zur Offenheit und Neutralität des Internet verbreitet werden können, wäre daher sehr optimistisch (vgl. Eva Jana Messerschmidt, Kapitel 2.3. *Internetsperren und Menschenrechte*). Was sich aber feststellen lässt, ist, dass sich Staaten sowie unterschiedliche Interessenvertretungen aller Art immer mehr und zunehmend global mit diesen Fragen beschäftigen.

Die globale Sicht wird durch die globale Beschaffenheit des Internet notwendig. Wenn man eine Webseite aus einem bestimmten Gebiet der Welt (wie beispielsweise den USA) betreibt, muss man sich vor Augen halten, dass die Meinungsfreiheit auch online gilt. Dabei besteht kein Unterschied, ob eine deutsche oder ungarische Seite – den BesucherInnen wenig auffallend – aus den USA geladen wird. So entstehen in diesem Fall amerikanische Webseiten mit deutschem sowie ungarischem Inhalt. Aus einem anderen Staat heraus kann man deswegen nur schwer gefährliche, insbesondere Hass beladene Inhalte bekämpfen. Eine eventuell gerichtlich bestellte Blockierung einer bestimmten Webseite oder Link bietet aus einem geographisch und juristisch begrenzten Gebiet wie Österreich oder Ungarn somit nur wenig Schutz. Applikationen sind in der Lage, im Bruchteil einer Sekunde mit diesen Regelungen umzugehen und Inhalte weiterhin oder erneuert erreichbar zu machen. Online Hassreden so wie die Bekämpfung und Verfolgung solcher Inhalte müssen durch diese Komplexität verstanden werden.

2. Grenzen der Meinungsfreiheit

Der Zugang zum globalen Netzwerk ist entscheidend. Wer ihn nicht hat, kann mit den Entwicklungen schwer mithalten. Der Zugriff ermöglicht uns – im Gegensatz zum Zugriff zu Massenmedien – die selbstständige Kreation und Veröffentlichung von Inhalten. Durch

den Online-Austausch in Form von Interaktion zwischen BenutzerInnen und Gruppierungen zu verschiedenen Themen bekam die Ausübung von Meinungsfreiheit und Versammlungsfreiheit eine neue Dimension. Noch nie war es einfacher, Proteste der Zivilgesellschaft wie eine Versammlung oder eine Veranstaltung zu organisieren, im Vorfeld Informationen auszutauschen und in Echtzeit sowie im Nachhinein zu berichten. (Vgl. Christian Möhlen, Kapitel 2.2. *Gibt es ein Recht auf politischen Online-Protest?*) Bisherige Freigabe-Methoden wie das vergleichsweise kostenaufwendige Plakatieren auf den Straßen treten in den Hintergrund. Das Internet ersetzt diese Wege, es bietet einen neuartigen öffentlichen Raum. (Vgl. Matthias C. Kettemann, Kapitel 3.4. *Ist Facebook ein neuer öffentlicher Raum?*) Wie dieser Raum gestaltet oder kontrolliert werden kann oder soll, wirft weitere interessante Fragen auf.

Die Grenze zwischen Meinungsfreiheit und Hassrede – sowie die Anstiftung zu Hassverbrechen – klar zu definieren, ist gar nicht so einfach. Der Europäische Gerichthof für Menschenrechte identifiziert Äußerungen, die beispielsweise durch Rassismus, Xenophobie, Antisemitismus, aggressiven Nationalismus, Diskriminierung von Minderheiten und MigrantInnen gegen die Europäische Menschenrechtskonvention verstoßen und somit vor Gericht anfechtbar sind. Dabei muss aber von Fall zu Fall untersucht werden, in welchem Verhältnis das Recht jedes Individuums, seine Meinung frei zu äußern (und damit eventuell auch zu schockierend, zu beunruhigend oder beleidigend zu wirken), und die Gefahr, ernsthaft zu Verbrechen anzustiften, stehen.

Es existiert keine allgemein anerkannte Definition von Hassreden. Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte macht einige Parameter deutlich, die helfen, die Grenzen des Schutzes der Freiheit der Meinungsäußerung (Artikel 10) oder der Versammlungs- und Vereinigungsfreiheit (Artikel 11) zu erkennen. Zusätzlich findet man in den Empfehlungen des Ministerrates des Europarates

eine kurze Definition, die sich auf die Verbreitung, Anstiftung, Promotion oder Rechtfertigung sowie mit Hass beladener Intoleranz bezieht:

> *„The term »hate speech« shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.“*[1]

Folgende zwei Fälle des Europäischen Gerichtshofs für Menschenrechte geben ein Beispiel für die Unterscheidung zwischen Anstiftung bzw. Diskriminierung und Meinungsfreiheit unter offline Umständen.

Der erste Fall hat mit einer oppositionellen Politikerrede aus der Türkei zu tun (*Faruk Temel v. Turkey no. 16853/05 2011*): Faruk Temel verlas bei einer Parteiveranstaltung eine Pressemitteilung, worin er unter anderem die Vereinigten Staaten wegen bevorstehender Intervention im Irak, der Einzelhaft von PKK-Führer Abdullah Öcalan und dem Verschwinden von Personen in Polizeigewahrsam kritisierte[2]. Nach seiner Rede wurde Temel wegen Verbreitung von Propaganda verurteilt, da er öffentlich die Anwendung von Gewalt oder anderen terroristischen Methoden verteidigt haben soll. Der EMRK entschied, dass die Rede allgemein nicht zur Gewalttätigkeit wie bewaffnetem Widerstand oder Aufstand angestiftet habe und nicht als Hassrede zu beurteilen sei. Die türkischen Behörden verletzten jedenfalls die Meinungsfreiheit des Politikers durch die Verurteilung.

Im zweiten Fall (*Vejdeland and Others v. Sweden no. 1813/07 2012*) hatten VertreterInnen einer Jugendorganisation in einer Mittelschule Flugzettel verteilt, auf denen Homosexualität als abweichende sexuelle

---

[1] S. Appendix to Recommendation No. R (97) 20 of the Committee of Ministers on „Hate Speech“, Council of Europe.

[2] vgl. http://blog.lehofer.at/p/egmr-rechtsprechung-zu-art-10-emrk.html (Letzter Aufruf: 6.4.2013)

Neigung beschrieben wurde. Sie soll eine moralisch zerstörerische Wirkung auf die Substanz der Gesellschaft haben sowie für die Entwicklung von HIV und AIDS verantwortlich sein. Die AntragstellerInnen gaben an, sie hätten nicht aus Verachtung gegenüber Homosexuellen gehandelt. Zweck ihrer Aktivität wäre vielmehr gewesen, eine Debatte über den Mangel an Objektivität in der Ausbildung in Schweden anzuregen. Auch wenn keine direkte Anstiftung zur Gewalttätigkeit stattfand, befand der EMRK dennoch, dass Diskriminierung aufgrund sexueller Orientierung vorlag. Die Reaktion der schwedischen Behörden, derzufolge diese Aktion für Homosexuelle diskriminierend und beleidigend wirkte, wurde damit gerechtfertigt. In einer demokratischen Gesellschaft – so die Begründung – ist der Schutz der Rechte von anderen notwendig. Somit lag keine Verletzung des Rechts auf Meinungsfreiheit vor (Artikel 10 EMRK), da sich bereits ein Hassverbrechen ereignete.[3]

Diese Fälle zeigen, dass auch extrem denkende Personen in ihren Rechten nicht verletzt werden sollen. Doch nicht alle Äußerungen fallen unter den Schutz der Meinungsfreiheit.

3. Grenzen der juristischen Verfolgung

Wenn Hassreden online stattfindet, ist die Verfolgung von den TäterInnen und AutorInnen schwieriger, die Verbreitung der Inhalte hingegen deutlich einfacher. Wie bereits erwähnt wurde, können durch die weltweite Vernetzung über das Internet Inhalte aus Gebieten veröffentlicht werden, die juristisch gesehen außerhalb des eigenen Gebietes liegen.

Ein Beispiel aus Ungarn zeigt, wie in einem Mitgliedsstaat der EU die juristische Verfolgung von Hassreden vorgeht und an welche Grenzen

[3] Nachzulesen beispielsweise unter http://www.queernews.at/archives/2899 (Letzter Aufruf: 6.4.2013) sowie http://blog.lehofer.at/2012/02/egmr-einstimmig-aber-mit-einigem-zogern.html (Letzter Aufruf: 6.4.2013)

sie stoßen muss. Im Juni 2012 fanden die internationalen Euro Games 2012, die LGBTQ-Spiele mit 3.000 SportlerInnen aus aller Welt in Budapest statt. Diese Spiele wurden zum ersten Mal in einem mitteleuropäischen Land organisiert. Die OrganisatorInnen mussten das Event ohne öffentliche Unterstützung organisieren, da sogar der inzwischen gewählte konservative Bürgermeister von Budapest die durch den vormaligen Amtsinhaber während der Antragsstellung zugesprochene Unterstützung zurückzog.

Direkt nach den Euro Games-Tagen wurde auch die alljährliche Budapest Pride mit viel Kulturangeboten und dem Pride-Marsch veranstaltet. Von der Bekanntgabe der Veranstaltung der Euro Games 2012 bis zu den Wochen vor dem Beginn der Euro Games wurden mehrere Hass beladene Inhalte online veröffentlicht. Es existierten etliche Webseiten auf Ungarisch mit Hassreden, die von einem außereuropäischen Gebiet aus betrieben wurden (den USA und anderen Gebieten). In der Vorwoche dieser zwei wichtigen LGBTQ- Veranstaltungen befassten sich die Hassreden mit den Einzelheiten der Spiele und der Frage, an welchen Orten in der Stadt sie stattfinden. Wie für Hassrede-Artikel üblich wurden diese auch deswegen radikal geschrieben, damit sie so viel öffentliches Interesse wie möglich bekommen. Nichtdestotrotz haben auch die Polizei und die OrganisatorInnen viele Vorbereitungen hinsichtlich der Sicherheit vornehmen müssen.

Einer der Artikel ging dann über alle anderen veröffentlichten Inhalte hinaus. Zwei Dutzend der OrganisatorInnen von Euro Games Budapest und Budapest Pride wurden Ziele einer „Menschenjagd“. Der Artikel hatte das Ziel, die Erkennung der Personen zu ermöglichen, die mit diesen LGBTQ-Veranstaltungen öffentlich oder als Freiwillige im Hintergrund zu tun haben. Durch direkte Verlinkung zu ihren persönlichen Facebook-Profilen sowie durch Verwendung und mittels Kommentierung ihrer Fotos wurden alle einzeln und namentlich zur Schau gestellt und zum Gegenstand von Hassreden gemacht. Der

Domain-Name der Webseite ist in der Konstitutionellen Monarchie Tuvalu registriert (.tv), die ein Inselstaat im Stillen Ozean und Mitglied des Commonwealth of Nations ist.

Ein Dutzend der angesprochenen Personen haben eine Sammelklage wegen Vorbereitung einer Gewalttat an Mitglieder einer Gemeinschaft (Ungarisches Strafgesetzbuch Btk. 174/B., 3) durch die rechtliche Vertretung der LGBTQ-Organisation „Hintergrund für Homosexuelle in Ungarn" (Háttér Társaság a Melegekért) eingereicht. Nach der Veröffentlichung dieses Artikels wurde auch eine Aktion zur Meldung des Inhaltes an die Nationale Medienaufsicht (NMHH) sowie an die Polizei gestartet. Die Medienaufsicht hat eine eigene Kategorie für rassistische, gefährliche Inhalte in ihrem Online-Formular. Hunderte meldeten binnen weniger Tage den Artikel wegen Rassismus an beide Behörden. Die Antwort der Medienaufsicht basierte aber auf einer Erklärung, dass diese Webseite wegen des Domain-Namens und ihrer Ansiedelung in einem außereuropäischen Gebiet und daher außerhalb der Reichweite der Aufsicht liege.

Andere Anklagen wegen Hetze gegen eine Gemeinschaft oder Missbrauch von persönlichen Daten haben keinen Erfolg gezeigt, die Ermittlungen wurden nicht einmal aufgenommen. In diesem Fall nahm die Polizei zumindest die Ermittlungen auf aber Anfang August 2012 wurden sie wegen mangelnder Straftat eingestellt. Die rechtliche Vertretung der betroffenen Personen hat eine Beschwerde gegen diesen Beschluss eingereicht, der von der Staatsanwaltschaft Ende Oktober 2012 akzeptiert wurde und gleichzeitig die Polizei zur Fortsetzung der Ermittlungen veranlasste. In der Begründung des Staatsanwaltes hieß es, dass der indirekte Aufruf zur Gewalttätigkeit, der über eine Bedrohung hinausgeht und mit der Veröffentlichung von persönlichen Daten der Zielpersonen zur Erleichterung von Gewalttätigkeit einhergeht den Tatbestand der Vorbereitung einer Gewalttat an Mitgliedern einer Gemeinschaft laut Ungarischem Strafgesetzbuch erfüllt.

Inzwischen wurde der Artikel von der Webseite entfernt, wie auch der früher aktive Link zum Artikel. Hier handelte es sich vermutlich um Selbstzensur als Versuch zur Schadensbegrenzung durch die BetreiberInnen der Webseite. Das ändert aber an der Tatsache der früheren Veröffentlichung nicht viel.

Obwohl die Ermittlungen – wie von der Staatsanwaltschaft begründet – theoretisch auch zeigen, dass mit der online Veröffentlichung des Artikels eine Straftat begangen wurde, werden weitere Fragen aufgeworfen. Wer soll für den Artikel haften und wie kann man diese Personen identifizieren sowie juristisch verfolgen? Sollen die BetreiberInnen, RedakteurInnen und VerfasserInnen der Webseite aufgesucht werden, auch wenn der Domain-Name (im angeführten Beispiel: .tv) und der Server (Speicherung der Inhalte zu einer www-Adresse) im außereuropäischen Gebiet liegen und es daher schwierig zu bewerkstelligen sein wird? Oder soll durch Identifizierung des Content Management Systems der Webseite der/die ProgrammiererIn herangezogen werden? Fragen, welche die derzeitigen Grenzen der juristischen Verfolgung von online Hassreden und somit die Notwendigkeit diesbezüglicher öffentlicher Diskussionen aufzeigen.

Februar 2013 wurde auch aufgrund dieser offenen Fragen die Ermittlung durch die Polizei wieder eingestellt. Dagegen hat wiederum die rechtliche Vertretung eines Kreises der Betroffenen, die Organisation Háttér, Einspruch erhoben. Ein Tauziehen, dessen Ende noch ungewiss ist, aber auf dem Weg stets durch behördliche Unfähigkeit, Absagen oder mangelnde Ermittlungsmethoden im Internet begleitet wird.

4. Ausblick

Noch im Dezember 2012 verabschiedete der ungarische Nationalrat eine Ergänzung zum Ungarischen Strafgesetzbuch, die es ermöglichen soll, Inhalte online mittels amtlicher Verfügung blockieren zu können, sofern ein Verdacht wegen Kinderpornografie, einer Straftat gegen

den Staat oder der Gefahr von Terrorismus besteht. Dieses und andere Beispiele weltweit zeigen, dass GesetzgeberInnen immer mehr versuchen, die im– meist durch private Anbieter angebotenen Internet weltweit veröffentlichten Inhalte unter einer gewissen Kontrolle zu bekommen. Die Effizienz dieser Maßnahmen stoßt aber an ihre Grenzen. Wenn wir die globalen Umstände und die Existenz von Umgehungsmechanismen online bedenken, erscheinen geographisch begrenzte Blockaden als sehr schwach. Wir sehen eine geographisch begrenzte rechtliche Zuständigkeit auf der einen und das globale Internet auf der anderen Seite.

Nach der Auffassung der ungarischen „Gesellschaft für Bürgerrechte" (TASZ), die sowohl jene, die nur innerhalb der persönlichen Meinungsfreiheit extreme Gedanken verbreiten, als auch Opfer von Hassreden und Verbrechen berät, sind Gesetze gegen Diskriminierung jeglicher Art in Ungarn bereits Grundbestandteil der geltenden Rechtslage. Es kommt aber darauf an, wie sensibel Behörden in solchen Fällen handeln. Junge TeilnehmerInnen des Europarat-Trainings „Bekämpfung von Hassreden online" hoben auch in einer ihrer Arbeitsgruppen hervor, dass entsprechende Mittel für die Prävention, die Schulung von Fachpersonal und für Betroffene und Gefährdete sowie für Öffentlichkeitsarbeit bereitgestellt werden sollten (vgl. Julian Ausserhofer/Heinz Wittenbrink, Kapitel 4.2 *Web Literacies und Offene Bildung*). Gesetze allein sind oft wenig effizient. Internationale Zusammenarbeit sollte auch die Verfolgung und das Monitoring von online Hassreden im globalen Kontext sichern. (vgl. Eva Jana Messerschmidt, Kapitel 2.3. *Internetsperren und Menschenrechte*)

Hoffentlich werden zumindest auf unserem europäischen Gebiet mehr Diskussionen, Aufklärung und Austausch initiiert. Einen Beitrag soll auch der Europarat setzen, der für 2013 die Bekämpfung von online Hassreden in den Mittelpunkt stellt.

Weiterführende Informationen

Council of Europe

No Hate Speech Movement – Young People Combating Hate Speech Online
http://www.nohatespeechmovement.org (Letzter Aufruf: 05.04.2013)
http://www.facebook.com/nohatespeech (Letzter Aufruf: 05.04.2013)
http://act4hre.coe.int (Letzter Aufruf: 05.04.2013)

Starting Points for Combating Hate Speech Online – 3 studies
http://goo.gl/7dh6h (Letzter Aufruf: 05.04.2013)

Combating Hate Speech facebook group
http://www.facebook.com/groups/combatinghatespeech (Letzter Aufruf: 05.04.2013)

European Dialogue on Internet Governance
http://www.eurodig.org (Letzter Aufruf: 05.04.2013)

European Court of Human Rights, Hate speech factsheet
http://goo.gl/h1QNz, http://www.echr.coe.int (Letzter Aufruf: 05.04.2013)

United Nations

World Summit on Information Society
http://www.itu.int/wsis (Letzter Aufruf: 05.04.2013)

Internet Governance Forum
http://www.intgovforum.org (Letzter Aufruf: 05.04.2013)

World Conference on International Telecommunications
http://www.itu.int/en/wcit-12 (Letzter Aufruf: 05.04.2013)

Cyberspace Conference 2012
http://www.cyberbudapest2012.hu (Letzter Aufruf: 05.04.2013)

Teil 4:
Bildung und Emanzipation

4.1. Digitale Technologien und Partizipation (Mihi Bauer)

Keywords: Partizipation, Technologie, Gesellschaft

EINLEITUNG 219
1. MEDIALE ENTWICKLUNGEN 220
2. DIE ROLLE VON BLOGS UND SOZIALEN MEDIEN 221
3. POLITISCHE PARTIZIPATION UND NEUE MEDIEN 222
4. MANGELNDE „DIGITALE ALPHABETISIERUNG“ 224

Einleitung

Die Anteilnahme an politischen und gesellschaftlichen Entscheidungen ist ein hart erkämpftes oder teuer erkauftes Recht (vgl. Christof Tschohl, 1.1. *Ethik, Recht und Menschenrechte*) und immer wieder aufs Neue nicht als gesichert zu betrachten (vgl. Hans Christian Voigt, Kapitel 1.2. *Rechte eines jeden Menschen _am_ Internet*). In den meisten Hochkulturen versuchte eine kleine Elite, politische Partizipation auf ihre Kreise zu beschränken. Im 20. Jahrhundert wurde durch das zunehmende demokratische Grundverständnis und die Anerkennung der allgemeinen Deklaration der Menschenrechte die Hürde, Teil dieser Elite zu werden, deutlich gesenkt. Digitale Technologie, ihre Kultur und ihre Kommunikation werden spätestens seit dem „Arabischen Frühling“[1] als neues Mittel dargestellt, diese Eliten aufzubrechen. Die Prämisse: Durch digitale Kommunikation kann jede/r Ein-

[1] Als Arabischer Frühling wird eine Serie von Protesten, Aufständen und Revolutionen in den arabischen Ländern bezeichnet, die im Dezember 2010 in Tunesien begann. Für die Bedeutung Sozialer Medien während des Arabischen Frühlings vgl. bspw. Die Erfahrungsberichte von BloggerInnen aus sechs arabischen Ländern in: http://politik-digital.de/social-media-und-die-arabische-revolution/ (Letzter Aufruf: 31.5.2013)

zelne gehört und wahrgenommen werden. Schafft die digitale Zeit neue Möglichkeiten für eine breitere politische Partizipation – oder sehen wir vor allem, was wir sehen wollen?

Um diese Frage zu beantworten, gehören vor allem zwei Aspekte näher betrachtet: Die Möglichkeiten zur politischen Partizipation durch Digitalisierung und Vernetzung der Gesellschaft einerseits, sowie andererseits die Frage, ob die Nutzung digitaler Technologien tatsächlich eine Begünstigung von Eliten verringert.

1. Mediale Entwicklungen

In den letzten 20 Jahren des 20. Jahrhunderts war gesellschaftliche und politische Partizipation in Österreich stark von großen Medien abhängig. Ein staatliches Monopol auf TV und Rundfunk ließ de facto einzig die Printmedien als nicht-staatliche Medien zu. Dadurch waren Printmedien, allen voran einflussreiche Boulevard-Zeitungen, der nahezu einzige alternative Weg politisch auf die Öffentlichkeit Einfluss zu nehmen. Die Aufhebung des staatlichen Rundfunkmonopols veränderte daran kaum etwas. Wollten BürgerInnen etwas erreichen, mussten sie Redaktionen und JournalistInnen möglichst einflussreicher Medienhäuser für ihre Sache gewinnen.

Die seit den 90er Jahren sprunghaft ansteigende Zahl der NutzerInnen der Infrastruktur Internet änderte ursprünglich nicht viel an der Situation: Es wurde von wenigen Portalen beherrscht und es waren weiterhin KuratorInnen, die entschieden, welche Inhalte publiziert und damit „gehört“ werden sollten.

Abseits dieser großen Webportale (wie u.a. Yahoo, Altavista oder AOL) entstanden allerdings zunehmend viele kleine Interessensgruppen und Gemeinschaften, die sich jener Themen annahmen, die in den Massenmedien ebenso wie auf Online-Portalen vernachlässigt wurden. Die zunehmende Vernetzung von AkteureInnen und Interessensgruppen untereinander ermöglichte es, auch abseits der durch

GatekeeperInnen aufbereiteten Inhalte Informationen zu finden: Das klassische Internetsurfen war geboren. Wer einmal eine Webseite gefunden hatte, die das Thema behandelte, zu dem es sonst wenige Informationen gab, folgte (oft stundenlang) weiteren Links zu weiteren Webseiten, um dennoch mehr zu erfahren.

Ende der 90er Jahre begann schließlich eine kleines Unternehmen die Art und Weise zu revolutionieren, wie und was im Internet gesucht und gefunden wird: *Google*. Anstatt wie frühere Suchmaschinen auf aktive Einreichungen und Schlüsselwörter zu bauen, wurden Volltextsuche und jene Linksammlungen, die abseits von Portalen Webseiten vernetzten, zu Indikatoren für Inhalt und Bedeutung. Die Macht der großen Portale wurde durch die effektive Suche abgelöst. (Vgl. Julian Ausserhofer, Kapitel 1.6. *Gute Filter, böse Filter?*)

2. Die Rolle von Blogs und Sozialen Medien

Die Tatsache, dass Inhalte von BenutzerInnen nun leichter gefunden werden konnten, vereinfachte es, eine eigene Meinung kund zu tun. Damit entwickelte sich das, was wenig später als die „Blogosphäre“ bekannt wurde: Individuen hatten nun die Möglichkeit, ohne den Umweg über GatekeeperInnen, ihre Ansichten zu auszutauschen. Mehr und mehr Plattformen bauten auf Inhalte, die durch BenutzerInnen generiert werden – und Soziale Medien entstanden. Diese ermöglichen NutzerInnen, eigene Inhalte rasch an einen Kreis von Interessierten zu verbreiten. Durch klassische Netzwerkeffekte breitet sich so Information rasant fort. Plattformen wie Twitter überholten klassische Medienhäuser, wenn es darum ging, möglichst schnell an Information zu kommen.

Soziale Medien ermöglichten Interessensgruppen, mit wenig Aufwand ihre Anliegen zu verbreiten. Flashmobs zeigten wie einfach es sein konnte, mit dieser Technologie viele Menschen zu mobilisieren. Im Rahmen der Studierendenproteste (#unibrennt) in Österreich ließ sich

beobachten, dass Soziale Medien dazu geeignet sind, Massenmedien zu umgehen. Obwohl die Proteste zu Beginn von großen Medienhäusern ignoriert wurden, wuchs die Bewegung trotzdem – bis sie nicht mehr ignoriert werden konnte.

Auch während der Proteste in Tunesien, Ägypten und Libyen wurde seitens der Protestierenden auf Soziale Netzwerke zurückgegriffen, um unabhängig von staatlichen Medien Nachrichten in die Welt zu bringen. Der Einfluss von Sozialen Medien auf die Organisation der Proteste ist jedoch kaum belegt – klar ist aber: Soziale Medien halfen, Europa und Nordamerika in das Geschehen einzubeziehen.

Die Möglichkeit zur direkten Kommunikation zwischen Individuen mittels Sozialer Medien wird als Indikator dafür zu gesehen, dass politische Partizipation breiter und einfacher geworden ist. PolitikerInnen und JournalistInnen können über diese Plattformen verhältnismäßig leicht erreicht werden und Debatten entstehen, die ohne die neuen Kommunikationsmöglichkeiten wenig Beachtung gefunden hätten.

3. Politische Partizipation und Neue Medien

Ermöglichen diese neuen Technologien aber tatsächlich bessere Möglichkeiten für eine breitere Teilnahme an politischen Prozessen? Gerade in Sozialen Medien wie Twitter wird politischen Fragen viel Aufmerksamkeit gewidmet. Allerdings benutzt nur ein Bruchteil der österreichischen Bevölkerung diese Plattform – und von diesem kleinen Teil wiederum beteiligt sich nur eine sehr überschaubare Menge der NutzerInnen aktiv an den politischen und gesellschaftlichen Diskussionen. (Vgl. Stephan Schlögl, Kapitel 3.5. *Weltöffentlichkeit*)

Eine Studie zur politischen Teilnahme der österreichischen TwitterbenutzerInnen [2] identifizierte zentrale Twitter-AkteurInnen und konnte zeigen, dass es sich bei den im Kern des Netzwerks befindlichen TeilnehmerInnen insbesondere um JournalistInnen, einige PolitikerInnen und Politik-ExpertInnen handelt. Etwa ein Sechstel aller Adressierungen durch JournalistInnen und PolitikerInnen gilt BürgerInnen – die zu einem Gutteil ein „Early-Adopter-Netzwerk" ausmachen. Außerhalb dieser schon etablierten Personengruppen bleiben nur sehr wenige, die Einfluss auf die Diskussion zu nehmen in der Lage sind. NutzerInnen im Netzwerk-Kern stehen zwar mit einer Reihe von Menschen in Kontakt, die nicht Teil des engen Netzwerkes sind, die Politik-Profis werden aber sehr viel stärker von NutzerInnen außerhalb des Netzwerks erwähnt, als sie selber ebensolche adressieren. Dennoch gibt es Kontakte „nach außen", was für eine Erweiterung politischer Partizipationsmöglichkeiten durch Twitter spricht. Allerdings beschränkt sich die Interaktion mit NutzerInnen von außerhalb des Netzwerks bei Politik-Profis oftmals auf kurze Frage-&-Antwort-Dialoge. Deutlich wurde bei der Untersuchung vor allem, dass ein massiv ungleiches Geschlechterverhältnis unter den NutzerInnen des Samples besteht, das auch in anderen Untersuchungen bestätigt wird (vgl. Leonie Tanczer, Kapitel 1.4. *Post, Gender, Internet?*). Vermutungen für mögliche Ursachen diesbezüglich reichen laut den AutorInnen je nach Perspektive von fehlender Technologieaffinitat, schwächer ausgeprägtem politischem Interesse, geringerem Sendungsbewusstsein bis hin zu allgemeinen gesellschaftlichen Machtstrukturen. In jedem Fall zeigt sich ein Ungleichgewicht an Möglichkeiten, Neue Medien – in diesem Fall Twitter – zur politischen Partizipation zu nutzen.

---

[2] Vgl. Ausserhofer, Julian / Kittenberger, Axel / Maireder, Axel (2012). Twitterpolitik. Netzwerke und Themen der politischen Twittersphäre in Österreich. Nachzulesen unter: http://twitterpolitik.net (Letzter Aufruf: 31.5.2013)

4. Mangelnde „digitale Alphabetisierung“

Es scheint sich also vielmehr um eine neue Form der kommunikativen Elite zu handeln, nämlich digital und technisch versierte AkteurInnen, die sich auf diesem Wege informieren und austauschen und in der Art Einfluss nehmen. Für sie stellen die Möglichkeiten der Plattformen vor allem eine Erweiterung an nützlichen Werkzeugen dar. Die Verbreitung digitaler Technologie vereinfacht es also vor allem, versierten, gut vernetzten Individuen ihre Nachrichten einfacher zu vermitteln – und senkt für diese Personengruppen die Schwelle für eine aktive Teilnahme.

Das gilt jedoch weiterhin und bei weitem nicht für die gesamte Bevölkerung: Um am Diskurs teilzunehmen, gibt es weiterhin eine Vielzahl an Barrieren und Beschränkungen, sie verändern sich im jeweiligen Kontext nur. Durch den Einfluss dieser neuen digitalen Eliten, die ihre Möglichkeiten zur Partizipation zunehmend realisieren, entsteht der Eindruck, digitale Technologie könne für sich genommen bereits breite Partizipation fördern und ermöglichen. Dieser Eindruck sollte jedoch angezweifelt werden.

Technologie selbst hilft nur weiter, wenn Individuen diese zu nutzen verstehen. Um breite gesellschaftliche und politische Partizipation technologisch vermittelt zu ermöglichen, braucht es zum einen die möglichst weitläufige Verbreitung eines technischen Verständnisses (und viele weitere Fähigkeiten), zum anderen ist ein politischer Wille nötig, mehr Partizipation zuzulassen sowie die Akzeptanz, dass gesellschaftliche Prozesse unvorhersehbar sein können. Eine möglichst umfassende „digitale Alphabetisierung“ in einem möglichst großen Teil der Bevölkerung ist somit als eine Grundvoraussetzung zur Partizipation zu verstehen. (S. Julian Ausserhofer und Heinz Wittenbrink, Kapitel 4.2 *Web Literacies und Offene Bildung*)

4.2. Web Literacies und Offene Bildung (Heinz Wittenbrink, Julian Ausserhofer)

Von Medienkompetenz zu Web Literacies

Keywords: Medienkompetenz, Web Literacy, Bildung, Öffentlichkeit, Konnektivismus

EINLEITUNG 225
1. SCHRIFTLICHKEIT UND LITERACIES 227
2. MODELLE FÜR WEB LITERACIES 229
3. WEB LITERACIES ERLERNEN 233
4. SCHLUSSFOLGERUNG 235

Einleitung

Im Zuge des Aufstiegs des World Wide Web zum gesellschaftlichen Leitmedium haben sich in den letzten Jahren auch neue Formen der asynchronen, schriftartigen Kommunikation entwickelt. Insbesondere weil sich der Charakter von Öffentlichkeit veränderte, entstanden Praktiken, die wiederum neue Kommunikationskompetenzen voraussetzen. In diesem Beitrag erläutern wir, wie diese Kompetenzen aussehen und unter welchen Bedingungen sie sich vermitteln lassen.

Wer aktiv am World Wide Web teilnehmen will, braucht Fähigkeiten auf den Gebieten (1) des Informationsmanagements, (2) der Medienproduktion und (3) des Identitäts- und Netzwerkmanagements, die von mehreren der vorliegenden Kompetenzmodelle mit unterschiedlichen Akzentsetzungen beschrieben werden. Wie sich diese Fähigkeiten erwerben lassen, beschreibt das konnektivistische Lernkonzept, auf das wir im letzten Abschnitt eingehen.

Für das, was wir im Folgenden als Web Literacies bezeichnen, werden auch Ausdrücke wie Digital Literacy, Network Literacy oder schlicht Medienkompetenz[1] verwendet – im Singular wie auch im Plural. Wir ziehen den Ausdruck Web Literacies vor, weil die Fähigkeiten, um die es geht, an die spezifischen Eigenschaften des World Wide Web gebunden sind: an seine Offenheit, seine Universalität und seinen hypermedialen Charakter[2].

Web Literacies bezeichnen das Wissen und die praktischen Fähigkeiten, die man benötigt, um mit den Mitteln des Web zu kommunizieren. Sie sind Begleiterscheinungen der Entwicklung des World Wide Webs: Ohne die Dynamik, die dieses Medium entfaltet, bräuchte es auch keine Web Literacies. Die Form, in der Web Literacies - vermittelt werden, muss zu ihrem Inhalt passen. Gelehrt und gelernt werden Web Literacies deshalb im Netz: Wer sich diese Kompetenzen aneignen will, muss sich selbst vernetzen und auch den eigenen Lernprozess assoziativ und interaktiv organisieren. Offene Bildungsressourcen sind eine zentrale Voraussetzung für Web Literacies. Das Web dient nicht nur dazu, Netzwerke zu bilden und vernetzte Praktiken zu unterstützen, es vernetzt auch diese Praktiken und Netzwerke wieder untereinander.

---

[1] Der nicht unproblematische Begriff der „Kompetenz“ wird in Ausführungen über „Medienkompetenz“ zumeist gar nicht hinterfragt. Korrekter, jedoch auch umständlich, wäre es, von „Performanzorientierung“ zu sprechen, die nüchtern auf das „Ausführen von Handlungen“ rekurriert. Vgl. Reischmann, J. (2004). Kompetenz lehren? Kompetenz- und Performanz- Orientierung in der Andragogik zwischen Didaktik und Organisationsentwicklung. Online unter: http://www.uni-bamberg.de/fileadmin/andragogik/publi/Reischmann2004-Kompetenz.pdf (Letzter Aufruf: 31.5.2013)

[2] Wittenbrink, H., & Ausserhofer, J. (2011). Social Media-Kompetenz im Kontext des E-Learning. In J. Pauschenwein (Ed.), Innovative Lern- und Trainingsszenarien mit Social Media: Tagungsband Zum 10. eLearning-Tag Der FH Joanneum (pp. 5–27). Presented at the 10. eLearning-Tag der FH Joanneum, Graz.

1. Schriftlichkeit und Literacies

Der Begriff der Literacy ist an die Schrift, ihre Geschichte und Kultur gebunden. Im Anschluss an Ong[3] lässt sich zwischen einer handschriftlichen („chirographic literacy"), einer an den Druck gebundenen („typographic literacy") und einer an vernetzte, digitale Medien gebundenen Literacy unterscheiden.

Zur Literacy gehört immer auch die Fähigkeit zur Übersetzung von Äußerungen in verschiedene Nutzungsformate. In Bezug auf mündliche Kommunikation kann das beispielsweise eine Verschriftlichung bedeuten, bei handschriftlichen Texten die Umwandlung in druckfähige Formulierungen oder in Bezug auf gedruckte Texte, die digitalisiert und im Netz publiziert werden sollen. Zur Literacy gehört aber auch die Kompetenz zur Übersetzung in umgekehrter Richtung, zum Beispiel die Umformung eines geschriebenen Textes für einen mündlichen Vortrag.

Diese Übersetzungsleistungen wurden theoretisch unterschiedlich erfasst: Lotman[4] spricht in Bezug auf die typografische und handschriftliche Literacy von „sekundären modellierenden Systemen", Heritage[5] in der Gesprächsanalyse von „institutional talk" oder Goffman[6] in der Beobachtung von Interaktionen von „Framing".

Was die typographische, also die an den Druck gebundene Literacy von Web Literacies unterscheidet, ist vor allem deren Verhältnis zu Öffentlichkeit. Während bei ersterer LeserIn und AutorIn von der

---

[3] vgl. Ong, W. J. (2002). Orality and Literacy: The Technologizing of the Word (2nd ed.). London, New York: Taylor & Francis. (Original work published 1982)

[4] vgl. Lotman, J. M. (1993). Die Struktur literarischer Texte (4th ed.). Stuttgart: UTB. (Original work published 1972)

[5] vgl. Heritage, J. (1998). Conversation Analysis and Institutional Talk: Analyzing Distinctive Turn-Taking Systems. In S. Cmejrková, J. Hoffmannová, O. Müllerová, & J. Svetlá (Eds.), Proceedings of the 6th International Congresss of IADA (International Association for Dialog Analysis) (pp. 3–17). Tübingen: Niemeyer.

[6] Goffman, E. (1974). Frame Analysis: An Essay on the Organization of Experience. New York: Harper Colophon Books.

Mündlichkeit abgeschnitten sind, verändert sich bei Web Literacies die Beziehung zwischen Lernen und Publizieren. Vor dem Web drehte sich Bildung um gedrucktes Material, z.B. Lehr- und Schulbücher, um mündliche Äußerungen von Lehrenden und Lernenden sowie um private, oft handschriftliche Texte. Im (Social) Web ist das private Material potenziell auch öffentlich, weil es leicht geteilt werden kann; das offizielle Lernmaterial kann bearbeitet, ergänzt und weitergegeben werden. Und nicht zuletzt ändert sich auch die Struktur des Lernmaterials, weil sich die Rezeptionspraktiken der (sozialen) Technologie anpassen[7].

Lernen vollzieht sich heute in Schule, Hochschule und Weiterbildung noch weitgehend in den Formen, die vor dem Web entwickelt wurden – und in denen der Gegensatz von dauerhaftem, in Buchform verfasstem Wissen und den vorübergehenden, meist nicht öffentlichen mündlichen Äußerungen eine entscheidende Rolle spielt. Die Produktion von Wissen selbst vollzieht sich dagegen heute oft schon in nur im Web möglichen Formen[8].

---

[7] Man kann diese Veränderungen mithilfe von allgemeinen medientheoretischen Kategorien erfassen, wie es Ong (1982/2002) selbst tut, der sich in vielem auf Marshall McLuhan stützt. Als Alternative zu diesem Verfahren gehen wir, aufbauend auf Schmidt (2012), von lokalen und für die TeilnehmerInnen verständlichen öffentlichen Praktiken aus, in die mediale Kommunikation, auch die über das Web, jeweils eingebunden ist. Bei diesem „praxeologischen" Zugang werden Web Literacies nicht normativ von AkteurInnen der Wissenschaft oder der Theorie postuliert und der Praxis gegenübergestellt. Sie werden als „2nd order"-Begriffe verstanden, die das Wissen der praktisch Handelnden interpretieren und es explizit machen. Die Praxis wird dabei nie nur als Realisierung von Regeln oder Verwirklichung von Kompetenzen begriffen. Vgl. Schmidt, R. (2012). Soziologie der Praktiken: Konzeptionelle Studien und empirische Analysen. Berlin: Suhrkamp.

[8] Siemens' (2004, 2006) konnektivistische Lerntheorie geht von seinem Verständnis des zeitgenössischen Wissens aus. Für ihn ist das Wissen netzwerkartig, nicht mehr hierarchisch organisiert. Es ist dynamisch und selbstgesteuert. Lernen vollzieht sich als Vernetzung und ist in Netzwerke eingebunden, jede TeilnehmerIn hat als Knoten im Netz dabei eine eigene Position und von dieser Position abhängige eigene Lernwege.

Einen Platz für mehr Web Literacies im Bildungssystem einzufordern, bedeutet damit die Forderung, sich vom Paradigma des Gedruckten als kanonisierter Form des Wissens zu lösen.

2. Modelle für Web Literacies

Wir haben oben vorgeschlagen, Web Literacies immer im Zusammenhang mit öffentlichen, vernetzten Praktiken zu diskutieren und auch ihre Vermittlung innerhalb von Netzwerken zu denken. Bei diesem Ansatz tritt die Bedeutung eines systematischen Modells von Kompetenzen zurück. Allerdings ist es aus heuristischen Gründen sinnvoll mit Kompetenzmodellen zu arbeiten, um Lernprozesse zu strukturieren. In den vergangenen Jahren wurden verschiedene Konzeptionen von Webkompetenz entworfen. Herausragend sind die Kompetenzmodelle von *Jenkins*, *Rheingold* und der *Mozilla Foundation*, die in diesem Abschnitt kurz diskutiert werden, bevor wir ein weiteres Modell von Web Literacies darlegen.

Jenkins' (2009)[9] Modell von New Media Literacies ist sehr umfassend und breit angelegt. Er entwirft darüber hinaus Szenarien für die konkrete Vermittlung dieser Kompetenzbündel in der Ausbildung. Das unterscheidet seinen Ansatz von anderen, die zwar ein profundes Modell liefern, die Umsetzung jedoch vernachlässigen. Er nennt insgesamt 12 unterschiedliche Teilkompetenzen, die er in der Arbeit mit Jugendlichen identifiziert hat:

- Play
- Performance
- Simulation
- Appropriation
- Multitasking
- Collective Intelligence
- Judgment
- Transmedia Navigation
- Networking
- Negotiation

[9] vgl. Jenkins, H. (2009). Confronting the Challenges of Participatory Culture: Media Education for the 21st Century. Cambridge, London: MIT Press.

- Distributed Cognition
- Visualization

Rheingold (2012)[10] spricht von Network Literacies und definiert fünf Teilkompetenzen:

- Attention
- Participation
- Collaboration
- Critical consumption of information
- Network smarts

„Attention" meint Aufmerksamkeit, die effizient verteilt werden muss. Sie hängt eng mit kritischem Informationskonsum zusammen, auch „crap detection" genannt, was bedeutet, Sinnvolles von Schwachsinn und Zeitraubendem unterscheiden zu können. „Participation" bezeichnet bei Rheingold die Fähigkeit, sich an Kommunikationsprozessen zu beteiligen – sowie diese zu steuern. Schließlich bezieht sich „Collaboration" auf das Vermögen zur Zusammenarbeit mit anderen Individuen mit dem Ziel, Inhalte zu produzieren. Dies alles in einem Netzwerk zu schaffen („Network smarts"), stellt eine große Herausforderung dar, denn für erfolgreiche Kollaboration müssen Voraussetzungen wie Gruppenfindung oder Einigung auf Ziele erfüllt sein[11].

Die Mozilla Foundation (2012) begreift Web Literacies als ein Bündel von Fähigkeiten und ihre Reflexion als Schnittmenge aus media literacies, digital literacies und Informatik:

[10] vgl. Rheingold, H. (2012). Net Smart: How to Thrive Online. Cambridge, London: The MIT Press.
[11] vgl. Shirky, C. (2008). Here Comes Everybody: The Power of Organizing Without Organizations. New York: Penguin Press.

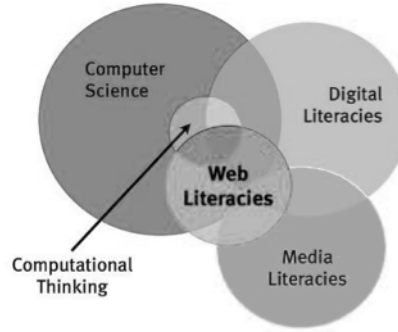


Abbildung: Web Literacies aus Sicht der Mozilla Foundation.[12]

Kernbereiche der Web Literacies sind das Finden von Informationen, das Schaffen von Inhalten und der Austausch mit anderen TeilnehmerInnen. Hinzu kommen als vierte Gruppe von Literacies das Wissen und die Fähigkeiten, die nötig sind, um das Web und seine TeilnehmerInnen zu schützen und die Besonderheiten des Web zu verteidigen. Wie bei Jenkins und Rheingold geht es in diesem Modell darum, dass Web Literacies dazu befähigen, das Web zu gestalten und es nicht nur zu konsumieren.[13]

Kondensiert man die Modelle von Jenkins, Rheingold und der Mozilla Foundation, dann kristallisieren sich drei Komponenten heraus, die Web Literacies ausmachen:

- *Informationsmanagement* (Rezeption und Organisation von Information)
- *Medienproduktion*
- *Identitäts- und Netzwerkmanagement* (Interaktionen, die mit der Produktion und dem Austausch von Texten verbunden

[12] S. Mozilla Foundation. (2012). Web Literacies White Paper. Online unter: https://wiki.mozilla.org/Learning/WebLiteraciesWhitePaper (Letzter Aufruf: 31.5.2013)

[13] Für Praxisbeispiele für Web Literacies, s. ebd. Tabelle unter „Web Skills / Competencies / Literacies grid“

sind und diese einerseits steuern, andererseits von ihnen beeinflusst werden)

Wie diese Ebenen bei „typographischer Schriftlichkeit" im Sinne Ongs zusammenwirken, lässt sich am Beispiel eines LeserInnenbriefs für eine Zeitschrift erklären:

Es gehört zur ersten Ebene, (1) LeserInnenbriefe in der Zeitschrift zu finden und zu wissen, was sie von Artikeln unterscheidet, zur (2) Medienproduktionsebene, selbst einen Brief zu verfassen, und zur dritten (3) Ebene, einen Dialog mit der AutorIn eines Artikels zu führen, auf den man mit dem LeserInnenbrief antwortet, und die Wirkung des LeserInnenbriefs auf andere LeserInnen einzuschätzen. Von Medienkompetenz oder eben Literacy würde man dann sprechen, wenn die Fähigkeit besteht, allen drei Ebenen zu erfüllen.

Im Web ist das ähnlich:

Wer beispielsweise Twitter erfolgreich verwenden will, muss (1) die eigene Timeline organisieren und nach Tweets suchen können, „Twitterer", denen man folgt, zu Listen zusammenfassen und Twitter mit anderen Tools wie beispielsweise persönlichen Nachrichtendiensten verbinden können. Auf dieser Ebene wird Twitter als *Werkzeug zum Informationsmanagement* benutzt.

Das Abfassen von Tweets – die zweite Ebene (2) – schließt die Kenntnis der Syntax von Twitter mit ein. Zu dieser Ebene gehört auch der Gebrauch von Twitter-Clients. Neben diesen eher technischen Kompetenzen sind auch inhaltliche Fähigkeiten essenziell, etwa die, in einer 140-Zeichen kurzen Nachricht relevante oder interessante Informationen weiterzugeben.

Auf einer dritten Ebene (3) erfordert es die Kommunikation mit Twitter, sich ein Netzwerk aus Followern und Followees aufzubauen und in diesem Netzwerk eine eigene, erkennbare Identität zu besitzen. Ist ein solches Netzwerk nicht vorhanden, scheitern Tweets als Kommunikationsakte. Zur Literacy auf dieser Ebene gehört es, die

Regeln und Praktiken zu beherrschen, die für die Interaktion bei Twitter gelten. Diese dritte Ebene inkludiert das Verständnis von Twitter-Communities als spezifische Teil-Öffentlichkeiten.

3. Web Literacies erlernen

Bisher wurde dargelegt, was Web Literacies sind und wie sie beschrieben werden können. Dass Web Literacies zu den Kompetenzen gehören, die für vernetzte Praktiken nötig sind, bedeutet aber auch, dass Vernetzung in Lernöffentlichkeiten auch für die Methode ihrer Vermittlung von größter Bedeutung ist. Bereits vor O'Reillys Beschreibung des Web 2.0[14] konzipierte Siemens[15] mit dem Konnektivismus eine Theorie des Lernens, die sich auf Erfahrungen mit Social Media stützte. Siemens forderte für die Pädagogik ähnliche Konsequenzen aus der Verwendung von Social Media wie Gillmor[16] für den Journalismus und McAfee[17] für die Unternehmensorganisation.

Wer Web Literacies erwirbt, eignet sich praktische Fähigkeiten an. Da Praktiken nie in ihren verschiedenen Repräsentationen (z.B. durch Regeln oder Theorien der Handelnden über das, was sie tun) aufgehen, lassen sich Web Literacies nur in „Communities of Practice"[18] erwerben, die vernetzt arbeiten und kommunizieren. Zu den Voraussetzungen für die Vermittlung von Web Literacies gehört auch, dass sich bei

---

[14] O'Reilly, T. (2005, September 30). What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software. Online unter: http://oreilly.com/web2/archive/what-is-web-20.html (Letzter Aufruf: 31.5.2013)

[15] Siemens, G. (2004, December 12). Connectivism: A Learning Theory for the Digital Age. Elearnspace. Retrieved December 28, 2011. Online unter: http://www.elearnspace.org/Articles/connectivism.htm (Letzter Aufruf: 31.5.2013)

[16] vgl. Gillmor, D. (2004). We the Media: Grassroots Journalism by the People, for the People. Sebastopol: O'Reilly Media.

[17] McAfee, A. (2009). Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges. Boston: Harvard Business School Press.

[18] vgl. Wenger, E. (1999). Communities of Practice: Learning, Meaning, and Identity. Cambridge & New York: Cambridge University Press.

ihnen nur sehr beschränkt zwischen Grundlagen und Anwendung sowie zwischen festen, geronnenen Wissensbestandteilen und flüssigen, sich laufend verändernden Inhalten unterscheiden lässt. Es ist also nicht oder kaum möglich „Basics" zu vermitteln, auf denen die Lernenden dann aufbauen können[19].

Webkommunikation ist komplex. In ihr spielen Hardware, Software und Algorithmen, Standards und Protokolle, Applikationen, Inhaltsformate und vernetzte Öffentlichkeiten eine wichtige Rolle. Im Web kommunizieren zu können bedeutet, mit diesen Faktoren umzugehen und das Wissen über diese Faktoren wieder in das Netzwerk zu delegieren – aber auch damit interagieren zu können, wo es notwendig ist. Damit sind diese Praktiken des Lernens zugleich Praktiken einer öffentlichen oder teilöffentlichen, auf Dokumente bezogenen Interaktion. Lernen ist eine Tätigkeit, von der Rechenschaft abgelegt wird. Die Reflexion des Lernens findet dabei im Web statt, sie benutzt webtypische Publikationsformen.

Dabei ist das Netzwerk dafür zuständig, dass das Wissen, das die Lernenden erwerben, aktuell ist. Der Lernweg jedes Individuums ist nicht vorab determiniert, sondern von den Interaktionen im Netzwerk abhängig. Die Lernumgebung ist ein offener Raum (keine „Klasse"), die unterschiedliche Lernwege ermöglicht, sie aber nicht vorschreibt. Ein großer Teil des – ohnehin schnell veraltenden – Faktenwissens ist an das Netzwerk delegiert. Nicht „wissen was" steht im Mittelpunkt, sondern

- zu wissen, wie und wo man etwas findet,
- zu wissen, wie man etwas *ist*, also seine eigene Rolle im Netzwerk gestaltet
- und zu wissen, wie man das Netzwerk verändert.

Für netzwerkorientiertes, „konnektivistisches" Lernen ist Web Literacy als Basis- oder Metakompetenz erforderlich; umgekehrt wird

[19] vgl. Siemens, G. (2006). Knowing Knowledge. Lulu.com.

erfolgreiches Lernen mit Webmedien immer auch zu einer Steigerung der Kompetenz im Umgang mit diesen Medien führen. Web Literacy ist überdies immer dort gefordert, wo mit Sozialen Medien kommuniziert wird, also in immer mehr Bereichen des beruflichen und privaten Lebens.

4. Schlussfolgerung

Dieser Aufsatz beschäftigte sich mit verschiedenen Aspekten von Web Literacies: ihrer Beziehung zu älteren Formen von Literacy, ihrer Bezogenheit auf öffentliche/soziale Praktiken, mit Möglichkeiten sie zu klassifizieren sowie mit ihrem Naheverhältnis zum vernetzten Lernen. Web Literacies sind nicht nur ein deskriptives Konzept, sondern sie formulieren einen Anspruch: Es ist eine der wichtigsten Aufgaben des Bildungssystems, diese Kompetenzen zu vermitteln. Web Literacies sind die Voraussetzung dafür, an der Netzkultur teilzunehmen, zu der unsere Kultur geworden ist – so wie niemand ohne eine auf gedruckte Bücher bezogene Bildung an der Kultur der Gutenberg-Epoche teilnehmen konnte.

Unsere bisherigen Vorstellungen von Bildung hängen eng mit älteren Literacy-Konzepten zusammen. Bei der Entwicklung von Leitvorstellungen für die Literacy in einer digitalen Kultur stehen wir noch am Anfang. Erfahrungen mit sozialen Medien und Erfahrungen mit sozialem Lernen im Web sind die Basis dafür, Bildungskonzepte zu entwerfen, die auch in einer nicht mehr von gedruckten und handgeschriebenen Texten bestimmten Öffentlichkeit funktionieren.

4.3. Zu viel im Netz? (Judith Schoßböck)

Digital inclusion als netzpolitisches Konzept

Keywords: Medienkompetenz, Bildung, Öffentlichkeit

1. „Wired by nature“ 237
2. Gefahren im Netz und Regeln für junge Menschen 239
3. Neue Nutzungsarten, neue Risiken 242
4. Exzessive vs. sichere Online-Nutzung 243
5. „Digital inclusion“ als netzpolitisches Konzept 245

1. „Wired by nature“

Verbringt die junge Generation zu viel Zeit im Netz? Sicher ist: Die Integration technischer Geräte in unsere unmittelbare Lebenswelt (augmented reality), die Vermischung von bisher getrennten Online-Kommunikationsräumen und die zunehmende Mobilisierung über Smartphones tragen dazu bei, dass wir häufiger erreichbar sind. Mediennutzungskompetenz ist das Schlagwort, wenn es um die sinnvolle Nutzung von Online-Welten geht, sodass andere Lebensbereiche davon keinen Nachteil erhalten. Wenn diese anderen Bereiche aber zunehmend digitalisiert sind, inwiefern gilt dann noch das Prinzip „Weniger ist mehr“? Wann macht es Sinn, sich selbst zu beschränken – und noch schwieriger – bis zu welchem Ausmaß ist die Internetnutzung von Kindern und Jugendlichen als gesund anzusehen?

William Powers schlägt 2010 in seinem Buch „Hamlet's Blackberry“ ein Internet-freies Wochenende als Lösungsansatz und Reaktion auf den Druck, ständig erreichbar zu sein, vor[1]. Seine Ausführun-

[1] vgl. Powers, William (2010): Hamlet's BlackBerry: A Practical Philosophy for Building a Good Life in the Digital Age. Harper Collins: New York.

gen sind insofern interessant, als sie mediengeschichtlich belegen, wie neue Medien immer zuerst mit Befürchtungen behaftet sind, bevor sie schließlich in unseren Lebensalltag integriert werden. So folgt die Bewertung von Medien historisch einem bestimmten Muster, an dessen Beginn zumeist Angst und Ablehnung zu finden sind, was mit zunehmender Verbreitung schließlich in Akzeptanz übergeht.

Doch mobile Geräte und vernetzte Kommunikation können auch zu einer Last werden, die es erschweren kann, sich auf eine Sache zu konzentrieren. Für den Drang, ständig unsere digitalen Bildschirme zu kontrollieren, macht Powers unsere evolutionäre Programmierung mitverantwortlich. Wir sind also „wired by nature" – und schenken neuen Stimuli Aufmerksamkeit, um schnell auf potentielle Gefahren oder Vorteile reagieren zu können. Dieser biochemische Effekt würde in unserem Gehirn einen Dopaminschub auslösen, gleichzeitig liefen wir durch diesen „alert modus" aber Gefahr, zu verlernen, uns langfristig auf andere Dinge als diese Stimuli zu konzentrieren – unsere Familie, Gedanken, Bücher etc.

Powers stellt die Frage, wie eine Mediennutzungskompetenz aussehen könnte, die dazu befähigt, mit dieser ständigen Erreichbarkeit umzugehen. Zeitliche Beschränkungen sind nur eine Möglichkeit, der eigenen, exzessiven Nutzung Einhalt zu gebieten.

Aber ist eine exzessive Nutzung immer automatisch schlecht? Könnte der Begriff auch positiv interpretiert werden? Oder stehen häufige und lange Online-Zeiten eines Kindes tendenziell mit einem problematischen Nutzungsverhalten in Zusammenhang?

Dieser Beitrag versucht auf Basis der Forschung zum Thema Internetnutzung von Kindern und Jugendlichen zwischen exzessiver und problematischer Internetnutzung abzugrenzen bzw. exzessive Nutzung als weniger problematisches Konzept zu denken. Auf Basis ausgewählter Ergebnisse von Studien zur Internetnutzung und zu

Online-Risiken werden für Österreich gültige Spezifika vorgestellt und deren Relevanz für das Bildungswesen reflektiert.

Vor der zunehmenden Verfügbarkeit des Internets waren vor allem zeitliche Beschränkungen der Mediennutzung verbreitet. Erziehungsberechtigte legten zum Beispiel eine maximale Dauer, die junge Menschen vor dem Fernsehgerät verbringen durften, fest – eine Kontrollmöglichkeit war klar gegeben. Mit der zunehmenden Verbreitung von Smartphones auch für junge KonsumentInnen und der permanent vorhandenen Möglichkeit „online zu gehen", ändern sich jedoch die Spielregeln.

2. Gefahren im Netz und Regeln für junge Menschen

Die JIKS-Studie in Kooperation der Donau-Universität Krems, des ICT&S-Centers der Universität Salzburg und des Demokratiezentrums Wien zum Thema Internetkompetenz von 14-jährigen SchülerInnen in Österreich[2] hat gezeigt, dass österreichische Jugendliche im europäischen Vergleich mit weniger Regelungen in Bezug auf ihre Internet-Nutzung konfrontiert sind, als beispielsweise Jugendliche in nordeuropäischen Länder. Die Studie zeigte, dass es nur bei 34,8% überhaupt Regeln gibt (am häufigsten bezüglich der Zeit), während 62,2% explizit angeben, dass es zu Hause keine Internetregeln gibt, wobei sich hier ein Geschlechtsunterschied (p=.038) dahingehend zeigte, dass es bei Mädchen häufiger keine Regeln gibt und bei Burschen überproportional viele inhaltsbezogene Regelungen.

Die große Mehrheit der SchülerInnen (90,5%) wurden über gefährliche Inhalte im Internet informiert (Stand 2010). Dennoch kommt der Risk and Safety Report der EUKidsOnline-Studie der School of Economics and Political Science (LSE) zu dem Schluss, dass junge

[2] vgl. Parycek, Peter, Maier-Rabler, Ursula und Diendorfer, Gertraud (Hg.) (2010): Internetkompetenz von SchülerInnen. Themeninteressen, Aktivitätsstufen und Rechercheverhalten in der 8. Schulstufe in Österreich. Studienbericht. Wien/Salzburg/Krems.

ÖsterreicherInnen die Risiken im Netz im Vergleich zu anderen europäischen Ländern mehr unterschätzen: „It appears that Austrian children tend to underestimate risks on the internet more than children from other European countries.“[3] Zudem geben im europäischen Durchschnitt mehr Kinder an, online oder offline mit „bullying“ konfrontiert zu sein.

Im Vergleich zum europäischen Durchschnitt lässt sich festhalten, dass Österreichs Eltern häufiger die Wahrscheinlichkeit unterschätzen, dass ihr Kind pornografischen Inhalten online ausgesetzt war. Im EU-Vergleich glauben 56% der Eltern, deren Kinder verletzende oder hässliche Nachrichten bekommen haben, dass dem nicht der Fall war[4]. Die geringe Besorgnis der ÖsterreicherInnen steht auch in Zusammenhang mit einem Vertrauen in den Nachwuchs: 66% der österreichischen Eltern nehmen an, ihr Kind wisse, was in problematischen Situationen zu tun ist[5].

Positiv schneidet Österreich hinsichtlich der Frage ab, inwieweit sich Kinder durch die Online-Risiken belästigt oder gestört fühlen – trotz des relativ hohen Risikos, dem österreichische Kinder im Vergleich ausgesetzt sind, fühlen sich diese wenig davon gestört. Dies deutet drauf hin, dass Risiken nicht unbedingt zu negativen Erfahrungen führen müssen. Dennoch gilt es zu berücksichtigen, dass österreichische Eltern die Risiken, denen ihre Kinder im Netz ausgesetzt sein

---

[3] S. Livingstone, Sonia and Haddon, Leslie and Görzig, Anke and Ólafsson, Kjartan (2011) Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9–16 year olds and their parents in 25 countries. EU Kids Online, Deliverable D4. EU Kids Online Network, London, UK. http://eprints.lse.ac.uk/33731/ (Letzter Aufruf: 28.01.2011).

[4] vgl. Livingstone et al. (2011)

[5] Hasebrink, Uwe; Livingstone, Sonia; Haddon, Leslie & Ólafsson, Kjartan (2009): Comparing children's online. opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. Second edition. LSE, London: EU Kids, S. 33. Online unter: http://www2.lse.ac.uk/newsletters/EUKidsOnline/EUKidsOnlineAlert7.htm (Letzter Aufruf: 30.10.2012).

könnten, tendenziell unterschätzen. Zudem zählt Österreich bei mittlerer Nutzungshäufigkeit des Internets laut „EU Kids Online" zu den Ländern mit immerhin mittlerem Online-Risiko. Im Nachfolgeprojekt „EU Kids Online II" steht der Bereich dieser Online-Risiken im Mittelpunkt einer europaweiten Befragung junger NutzerInnen.

In Ländern, in denen die Eltern weniger über die Risiko-Erfahrungen ihrer Kinder Bescheid wissen (neben Österreich sind das noch Länder wie Rumänien, Estland oder Litauen), sollten sich nationale Empfehlungen daher auch auf Bewusstseinsbildung und Kommunikation zwischen Eltern und Kindern konzentrieren. Spezifische Länder erfordern spezifische Empfehlungen für das Bildungswesen und dementsprechend angepasste Schulprogramme. Da es sich beim Thema Medienkompetenz aber um ein besonders schnelllebiges Gebiet handelt, hinkt die Umsetzung oft hinter derartigen Empfehlungen her.

Bis zum Alter von 10 Jahren steigt das Setzen von Regeln für Kinder und Jugendliche europaweit an, ab dann werden Limits und Regulationen weniger[6]. Wie in den meisten europäischen Ländern wurden in der Vergangenheit auch in Österreich mehr Regeln in Bezug auf das Fernsehen als auf das Internet aufgestellt (43% Fernsehen vs. 35% Internet). In Schweden, Dänemark und den Niederlanden war dies 2009 jedoch umgekehrt. In Schweden stehen 33% Regeln beim Fernsehen 58% Regeln bei der Internetnutzung gegenüber. Bis zum Alter von 12 bis 14 ist auch EU-weit das Fernsehen das am meisten regulierte Medium. Ab 12 bis 13 Jahren werden aber im EU-Durchschnitt mehr Regeln für das Internet als für das Fernsehen aufgestellt.

[6] vgl. Hasebrink et al (2009), S. 38.

3. Neue Nutzungsarten, neue Risiken

Der hohe Grad an mobilem Internet-Zugang in einigen EU-Ländern führt zu neuen Herausforderungen hinsichtlich der empfohlenen Nutzungsintensität für Jugendliche und entsprechenden Schutzbestrebungen. Gerade in Ländern wie Norwegen, Großbritannien oder Deutschland ist der Zugang über Smartphones besonders verbreitet, während in Griechenland, Bulgarien, Zypern und Österreich der Zugang über gewöhnliche Mobiltelefone besonders hoch ist[7]. Andererseits: Im Vergleich zum europäischen Durchschnitt (34%) nutzt in Österreich eine relativ hohe Anzahl an Kindern (53%) das Internet mobil (entweder über Handies oder über „handheld devices" wie Smartphones).

Auch das Alter, mit dem Österreichs junge Generation ins Netz einsteigt, ist mit zehn Jahren vergleichsweise über dem europäischen Durchschnitt. Der Report von EU Kids Online betont, dass in Zukunft besonders die Tatsache im Mittelpunkt stehen sollte, dass eine steigende Anzahl von Kindern das Internet unabhängig von der Aufsicht Erwachsener nutzt, insbesondere eben über mobilen Zugang[8]. 87% der Kinder nutzen demnach das Netz zu Hause, 49% in ihrem Zimmer und 38% irgendwo anders zu Hause. Interessant ist zudem, dass mehr junge ÖsterreicherInnen als der EU-Durchschnitt einen *social media*-Zugang besitzen.

Eines ist evident: In Zukunft kann es – nicht nur mangels umfassender Kontrollmöglichkeiten – nicht mehr ausschließlich darum gehen, die Menge der im Internet verbrachten Zeit zu begrenzen bzw. dies als Maßstab für einen gesunden Umgang mit dem Medium anzunehmen. Die im Internet verbrachte Zeit ist von vielen Faktoren abhängig, und die Forschung hat bestätigt, dass gesteigerte Internet-Nutzung sowohl

[7] vgl. Livingstone et al. (2011)
[8] vgl. Livingstone et al. (2011)

Risiken als auch Chancen bergen kann. Die Entwicklung von Online-Medienkompetenz wird also umso wichtiger.

Österreich zählt hier im europäischen Vergleich eher zu jenen Ländern, die zwar eine vergleichsweise weniger intensive Nutzung, aber auch weniger Risiko aufweisen – das Gegenteil zu jenen Ländern, die durch die intensivere Nutzung neuer Kommunikationsformen auch mit mehr neuartigen Risiken konfrontiert sind. In der Folge soll ein Blick auf jenen Teil des Reports geworfen werden, der sich mit der besonders starken, exzessiven Nutzungsdauer des Internets von Kindern beschäftigt. Er kommt zu dem Schluss, dass unter den 25 untersuchten Ländern 29% der Kinder eine von fünf Komponenten, die man mit exzessivem Internetkonsum in Verbindung bringen kann (s.u.), erfahren haben.

4. Exzessive vs. sichere Online-Nutzung

Besonders lange oder exzessive Nutzungsdauer ist nicht unbedingt ein Zeichen für eine problematische Nutzung. In der Forschung wird der Begriff der exzessiven Nutzung oft zur Beschreibung eines Musters gewählt, das sich auf wiederholte, und manchmal auch zwangshafte und unkontrollierte Verwendung bezieht. Das muss jedoch nicht unbedingt so sein. Die Ergebnisse des dritten Reports zeigen, dass Zeit auch kontra-indikativ für eine problematische Nutzung sein kann. Jene Kinder, die am anfälligsten für negative Konsequenzen einer exzessiven Nutzung sind, scheinen jene zu sein, die älter sind, emotionale Probleme haben oder einen hohen Grad an Sensationsgier besitzen[9]. Nach Mark Griffith, der sich die Frage gestellt hat, ob Internet- und Computersucht überhaupt existiert, ist ebenso nicht Zeit der kritische Faktor – das „Wie“ der Internet-Nutzung muss im Vorder-

[9] vgl. Smahel, David, Ellen Helsper, Lelia Green, Veronika Kalmus, Lukas Blinka and Kjartan Ólafsson (2012): Excessive Internet Use among European Children. http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/ExcessiveUse.pdf (Letzter Aufruf: 28.01.2013).

grund stehen. Er schlägt ein Modell mit sechs Levels vor. Damit man von Abhängigkeit bzw. Sucht sprechen kann, müssen alle Komponenten dieser Levels präsent sein[10].

Die sechs Levels sind:

- *Salienz* (ein Begriff aus der Psychologie, der besagt, dass ein Reiz aus seinem Kontext hervorgehoben und daher dem Bewusstsein leichter zugänglich ist[11], also in welchem Ausmaß Gedanken an das Internet das Leben einer Person bestimmen),
- *Stimmungseinfluss* (inwieweit subjektive Erfahrungen durch die Aktivität bestimmt werden),
- *Toleranzsymptome* (ähnlich wie bei Suchtsymptomen braucht ein Individuum dann mehr Zeit im Internet, um dieselben Effekte hervorzurufen),
- *Entzugserscheinungen* (negative Gefühle und Emotionen, die mit dem Ende des Online-Seins einhergehen),
- *interpersonelle Konflikte* (bezogen auf enge soziale Beziehungen) oder
- *intrapersonelle Konflikte* (bezogen auf die eigenen Gefühle des Individuums) sowie
- *Rückfälle* (ein Individuum versucht, die Online-Präsenz zu beschränken und scheitert).

Bei diesem Konzept stehen die negativen Konsequenzen der Nutzung und die Gefühle des Individuums statt der Nutzungsdauer im Vordergrund. Sehr wenige Kinder der Studie (1%) konnten sich mit allen Komponenten des Modells identifizieren[12]. Kinder, die alle fünf Komponenten erfahren haben, gaben außerdem an, mit einer Reihe von psychologischen bzw. emotionalen Herausforderungen konfrontiert

[10] vgl. Griffiths, Mark (2000): Does internet and computer „addiction“ exist? Some case study evidence. CyberPsychology and Behavior vol. 3, no 2, S. 211–218.
[11] vgl. http://de.wikipedia.org/wiki/Salienz (Letzter Aufruf: 28.01.2013)
[12] Die europaweite Studie zieht nur 5 der 6 Levels in Betracht.

zu sein, die sich auf ihr online-, aber auch offline-Verhalten auswirken. Die Studie EU Kinds empfiehlt daher, das gesamte Verhalten des Kindes im Off- und Online-Spektrum für Auffälligkeiten heranzuziehen. Das Online-Verhalten müsse also mit dem breiteren sozialen und psychologischen Kontext und dem generellen Nutzungsverhalten des Kindes in Beziehung gesetzt werden.

5. „Digital inclusion" als netzpolitisches Konzept

Das Konzept der „digital inclusion" (digitale Inklusion) bietet die Möglichkeit, lange Internet-Zeiten auch produktiv zu betrachten. Es birgt dabei die Gefahr, exzessiven Internet-Konsum zu beschönigen. Als Ausgangspunkt dient das Argument, dass exzessive Nutzung des Internets auch positiv betrachtet werden kann. ForscherInnen möchten dabei aufzeigen, dass jene Menschen, welche über gute Offline-Ressourcen und soziale Vorteile verfügen, auch die nötigen Fähigkeiten aufweisen, Technologien häufiger, breiter und kompetenter zu nutzen[13]. Das bedeutet, dass Kinder aus einem Haushalt mit höherem Bildungsgrad tendenziell auch besseren Zugang zu neuen Technologien haben, tendenziell über höhere Medienkompetenzen verfügen und daher das Internet auch meist intensiver nutzen. Gleichzeitig könnten diese Kinder aber durch den höheren Nutzungsgrad und trotz ihrer sozio-ökonomischen Vorteilspalette mit mehr Risiken konfrontiert sein. Daher sollten Maßnahmen zur Prävention hier bereits sehr früh und offline ansetzen – im sozialen und psychologischen Bereich. Klar ist: Zeitliche Beschränkungen sind hier kontraproduktiv, da sie nicht die Ursache des Problems bekämpfen und zudem auch die mit einer kompetenten Mediennutzung verbundenen Vorteile minimieren können. Dass Österreichs Eltern aber weniger zeitliche Beschränkungen vorgeben als die Eltern in anderen

[13] vgl. Helsper, E. J. (2012). A corresponding fields model of the links between social and digital exclusion, Communication Theory, vol 22, no 4.

Ländern, bedeutet in diesem Fall aber noch nicht eine Einsicht in diese Problematik[14] – vielmehr kann es sich um einen ersten Reflex auf Basis von Überforderung bzw. Unsicherheit im Umgang mit der Thematik handeln.

Mit der Allgegenwart des Netzes sollten pädagogische Strukturen und Prinzipien jedenfalls angepasst werden. Strategien für Online-Aktivitäten und digitale Kompetenzen müssen eine stärkere Rolle in der Schulbildung spielen. Dazu gehören beispielsweise Bewertungskompetenzen in Bezug auf Online-Inhalte, Suchstrategien oder Sicherheits-Strategien vom Schutz der persönlichen Daten bis hin zur Cybermobbing-Thematik. Livingstone et al. (2011) empfehlen in dieser Hinsicht, Strategien bereits im jungen Alter (11 bis 12 Jahre) zu vermitteln. Bezüglich Sicherheitsstrategien gaben die meisten der 11- bis 16-Jährigen an, dass sie Nachrichten von unwillkommenen Kontakten blocken (64%) oder Sicherheitsempfehlungen online finden können (64%). Etwas mehr als die Hälfte kann Privatsphäre-Einstellungen ändern (56%), die Qualität einer Website mit anderen vergleichen (56%) oder Spam blockieren (51%). Hier zeigt sich deutliches Potential für die Vermittlung von Strategien für Internet-Sicherheit, möglicherweise bereits im Vorschulalter, vor allem, weil in der Altersgruppe der Jüngeren (11 bis 12 Jahre) weniger als die Hälfte angaben, dass sie die grundsätzlichen Fähigkeiten in Bezug auf Online-Sicherheit besitzen würden. Netzpolitik kann daher bereits ab der ersten Schulstufe ein Themenschwerpunkt sein.

Aber auch pädagogische Initiativen und Veranstaltungen für Eltern können einen großen Beitrag leisten. Es geht nicht darum, die Kontrolle kindlicher Aktivitäten auszubauen – vielmehr sollte die realistische Einschätzung der im Internet vorhandenen Gefahren Schwerpunkt sein, da die Forschungsergebnisse zeigen, dass Eltern diese häufig unterschätzen. Kinder empfinden Hilfe und Mediation von

[14] vgl. Parycek et al. (2010)

Eltern mehrheitlich als sehr positiv – 70% der befragten Kinder der EU Kids Online-Studie gaben an, dass dies sehr helfe (9 bis 12-Jährige bewerten dies noch positiver[15]).

Trotz und aufgrund der notwendigen Neudefinition einer problematischen Internetnutzung und deren Faktoren und Ursachen mag es sein, dass Eltern und Kinder eine unterschiedliche Auffassung darüber haben, was denn nun zu viel ist. Auch dürften sich die Ansichten von Erziehungsberechtigten in dieser Hinsicht unterscheiden, und Kinder sind gemeinhin sensibel, wenn es um Vergleiche zwischen verschiedenen Familien geht. Empfehlenswert ist diesbezüglich, sich in der Diskussion und im Verhandeln von Grenzen nicht auf zeitliche Vorgaben, sondern auf den Erfolg bzw. die Resultate der Nutzung zu konzentrieren. Wenn sich negative Konsequenzen zeigen, speziell wenn die Internetnutzung stark mit anderen Aspekten des Lebens in Konflikt steht, sind Eltern und PädagogInnen gefragt, die dahinter liegenden Gründe (sowohl on- als auch offline) der Situation aufzudecken und gegebenenfalls Hilfe heranzuziehen.

Es besteht, obwohl der Thematik Online-Nutzung ein hoher Stellenwert in der Öffentlichkeit zugeschrieben wird, nach wie vor ein Defizit an spezifischer Forschung. Obwohl in Österreich Ende 2009 insgesamt 28 Studien mit Daten zur Online-Nutzung österreichischer Kinder und Jugendlicher identifiziert werden konnten, gibt es immer noch vergleichsweise wenig spezifischere Daten. Einen positiven Schwerpunkt bietet die EU-Initiative *Saferinternet*.at, die bei der sicheren Nutzung von Internet, Handy & Co. durch die Förderung von Medienkompetenz unterstützt. Bereits identifizierte Defizite, zum Beispiel der Mangel an Langzeitstudien, die Vernachlässigung von Alltagskontexten, der eingeschränkte Zugang zu Ergebnissen (Stichwort *open access*) und das Forschungsdefizit zu Risiken, besonders hinsichtlich jener Probleme, die sich nicht nur auf gefährliche Inhalte

[15] Livingstone et al. (2011)

beziehen (wie beispielsweise Datenmissbrauch, kommerzielle Fallen oder Cybermobbing[16]), sollten jedoch weiter ausgeglichen werden.

[16] vgl. Paus-Hasebrink, Ingri und Rathmoser, Manfred (2007): Kinder, Jugendliche und Internet: Ein europäisches Forschungsprojekt gibt Aufschluss. In: MEDIENIMPULSE 60, S. 12–16. / vgl. weiters Paus-Hasebrink, Ingrid & Ortner, Christina (2008): Online-Risiken und Chancen für Kinder und Jugendliche: Österreich im europäischen Vergleich. Bericht zum österreichischen EU Kids Online-Projekt. Url: http://www.bka.gv.at/Docs/2008/11/6/kids_online.pdf und http://www.bmukk.gv.at/medienpool/17370/eukidsonlineabschlussbericht.pdf (Letzter Aufruf: 28.01.2013).

4.4. „Subscribe NoW!“ (Joachim Losehand)

Fallstricke und Hindernisse für Archive, Bibliotheken und Bildungseinrichtungen durch digitale Geschäftsmodelle

Keywords: Zugang, Wissen, Bildung, Kultur, Urheberrecht, Digitale Medien

1. Das Recht auf Wissen 249
2. Zugang zu Bildung 250
3. Eigentumsverhältnisse in der Wissensgesellschaft 251
4. Zugang zu Wissen und Kultur 252

1. Das Recht auf Wissen

Vor etwas über dreißig Jahren machte sich Umberto Eco ironisch darüber Gedanken, „wie man eine öffentliche Bibliothek organisiert“[1]; abschließend formuliert er:

> *„Ideal wäre es schließlich, wenn der Benutzer die Bibliothek gar nicht erst betreten könnte; betritt er sie aber doch, stur und pedantisch auf einem Recht beharrend, das ihm aufgrund der Prinzipien von 1789 zugestanden worden ist, aber noch nicht Eingang ins kollektive Bewusstsein gefunden hat, so darf er auf keinen Fall, nie und nimmer, außer bei seinen kurzen Besuchen im Lesesaal, Zugang zu den Bücherregalen selbst haben“. (Punkt 18)*

Das Recht auf Bildung erschöpft sich nicht im Recht auf staatlich organisierte oder beaufsichtigte „Beschulung“ der jungen Menschen, in einem garantierten Kindergartenplatz oder dem flächendeckenden Angebot von Ganztagsschulen. Es umfasst ganz allgemein das Recht auf Wissen, das heißt: den Zugang zu Wissen.

[1] S. Eco, U. (1981): Wie man eine öffentliche Bibliothek organisiert.

Im kontinentalen Europa haben seit Anfang des 19. Jahrhunderts öffentliche Bibliotheken zur so genannten „Volksbildung“ beigetragen – in Wien wurde 1887 der „Wiener Volksbildungsverein“ zu diesem Zweck gegründet – und der Öffentlichkeit jegliche Druckerzeugnisse und später auch audiovisuelle Medien zugänglich gemacht. Mit dem Medienwandel, der letztendlich weg vom einzelnen physischen Datenträger hin zur immateriellen Datei führt, ergeben sich neue Herausforderungen – nicht nur für die Aufbewahrung, also die Speicherung der Medien, sondern auch für den Zugang und die Benutzung dieser „neuen“ Medien, die Text, Bild, Ton, Bewegtbilder (Film) oder eine multimediale Mischung aus allen beinhalten.

2. Zugang zu Bildung

Das Internet und seine Möglichkeiten hat uns Menschen ungeduldiger gemacht; was wir suchen, darf im Idealfall nur *one click* weit entfernt sein. „Ich will alles, und zwar sofort, jederzeit, überall und kostenlos zur Verfügung haben“ forderte 2001 Martin Grötschel, Präsident des Konrad-Zuse-Zentrums für Informationstechnik in Berlin (ZIB).

Es ist vornehmlich eine politische Frage, ob das (Menschen-)Recht auf Bildung auch das Recht des kostenlosen Zugangs zu Bildung und Wissen inkludiert – oder ob die eigene Fort- und Weiterbildung den Menschen etwas wert sein soll und damit etwas kosten darf.

Jedoch wird in den nächsten Jahren und Jahrzehnten nicht die Frage der persönlichen oder gesellschaftlichen Finanzierung des Zugangs zu Bildung von eminenter Bedeutung in der digitalen Wissensgesellschaft sein, wiewohl der effiziente und zielgerichtete Einsatz von Geldmitteln eine der Grundlagen der Bildungspolitik ist.

Weitaus grundsätzlicher und bedeutsamer wird das Thema der kommerzialisierten Kontrolle des Zugangs zu Wissen und Bildung

sein. Dieses wachsende Problem allein als das Problem der Finanzierung des kontrollierten Zugangs wahrzunehmen, greift zu kurz.

3. Eigentumsverhältnisse in der Wissensgesellschaft

In der vor-digitalen Ära waren Nutzungsrechte an immateriellen Gütern immer auch mit Eigentumsrechten an den materiellen Trägermedien verbunden. Wer ein Buch käuflich erwarb, erwarb und zahlte nicht alleine dafür, den darin abgedruckten Text lesen zu dürfen, sondern zahlte auch für das Buch in seiner physischen Gestalt, das in das uneingeschränkte Eigentum überging, unbeschadet von eingeschränkten Nutzungsrechten am Text. Ein Buch darf man ohne Einschränkung verleihen, verschenken oder verkaufen (jedoch nicht den Text alleine oder in neuer Ausstattung verbreiten) – oder es jeder anderen individuellen Verwendung zuführen.

Medien in digitaler „Gestalt“ benötigen zwar immer auch einen Datenträger wie beispielsweise eine Festplatte, das einzelne Medium aber ist „frei“ von physischen Beschränkungen und kann paradoxerweise gerade deshalb in seiner Benutzung kontrolliert und damit eingeschränkt werden.

Der technische Fortschritt ermöglicht es heute Verlagen, mittels *digitalem Rechtemanagement* (*DRM*, Digital Rights Management) die digitalen Medien vor nicht intendierten, unerwünschten und unautorisierten Zugriffen und Nutzungen zu schützen. Das kann bedeuten, dass Filme oder Musik nur in bestimmten geographischen Regionen oder auf bestimmten Geräten („devices“) genutzt werden können, dass man für ein Computerspiel eine aufrechte Internet-Anbindung benötigt oder dass digitale Texte nicht ausgedruckt, nicht gespeichert und nicht per copy-’n-paste in eigene Texte eingefügt werden können.

Alle diese Elemente digitaler Zugriffsverwaltung können technisch und praktisch mit einem kostenpflichtigen Abonnement kombiniert werden, das die Datei in dem Moment unbenutzbar und zu

„totem“ Ballast auf der Festplatte macht, sobald man keine Subskription mehr hält.

DRM geht also schon heute, am Anfang des 21. Jahrhunderts, weit über den bloßen Schutz vor illegalem Kopieren und Verbreiten hinaus. Wer sich DRM-geschützte *E-Books* auf einen proprietären *E-Reader* erwirbt, erwirbt keinen zeitlich unbegrenzten und garantierten Zugang, sondern muss jederzeit damit rechnen, dass das Portal oder die Internet-Buchhandlung das Zugangskonto ohne Angabe von Gründen sperren oder einzelne erworbene Titel beispielsweise bei Urheberrechts- oder auch Persönlichkeitsrechts-Streitigkeiten löschen kann.

Physische Bücher und Medien sind – gleich ob sie legal (durch einen Kauf in einer Buchhandlung) oder illegal (durch das bewusste Überschreiten der Leihfrist) im eigenen Verfügungsbereich sind – vor derartigen Zugriffen durch Dritte geschützt: Weder wird die Buchhändlerin Ihres Vertrauens noch der Bibliothekar Ihrer Institutsbibliothek sich nächtens Zugang zu Ihrer Wohnung verschaffen, um dort „Ihre“ Bücher aus dem Regal zu holen.

4. Zugang zu Wissen und Kultur

Juristische Gegenwehr Einzelner bei derartigen (und üblicherweise mit *Allgemeinen Geschäfts- und Nutzungsbedingen* begründeten) Eingriffen in die eigenen digitalen Bestände ist in der globalisierten Internet-Ökonomie zusehends schwieriger geworden. Die einseitigen Durchgriffe der Unternehmen schaffen „vollendete Tatsachen“, die erst im Nachhinein juristisch überprüft werden können. Diese Privatisierung der Rechtsdurchsetzung schafft ein „Recht des Stärkeren“, das sich faktisch juristischer Kontrolle entzieht, da die Rechtsdurchsetzung auf dem Klageweg mit großem Aufwand verbunden ist.

Gesetzliche Rahmenbedingungen wie Schutzfristen, die über eine Menschen-Generation hinausreichen, tun ein weiteres, den Zugang zu

Wissen und Kultur der Kontrolle einiger weniger zu überlassen, die die Verwertungsrechte innehaben. Sie handeln wesentlich nach ökonomischen Prinzipien und nicht unter gesellschaftlichen oder sozialen Gesichtspunkten (was man nicht apriori kritikwürdig finden muss). Das kulturelle Erbe der Menschen ist unter dem Paradigma der Verwertung ein Produkt, der Zugang dazu eine Dienstleistung, die bezahlt werden will.

Die Konsequenz ist, dass alle von einer Schutzfrist betroffenen Werke, die nicht kommerzialisiert werden, wirtschaftlich verwertbar sind oder deren Zugänglichmachung nach einer Kosten-Nutzen-Rechnung unrentabel ist, auch nicht zugänglich gemacht werden und von Dritten selbst aus altruistischen Gründen nicht zugänglich gemacht werden dürfen.

Auch öffentliche Einrichtungen wie Bibliotheken und Archive sind von diesen einseitig formulierten und durchgesetzten Restriktionen betroffen, wie in Deutschland die Auseinandersetzung um die „Bildungs- und Wissenschaftsschranke“ (UrhG § 52a)[2] und um den Zugriff auf Digitalisate oder digitale Medien in Lesesälen zeigen (vgl. die Auseinandersetzung des Ulmer-Verlages gegen die TU Darmstadt seit 2009)[3]. Gerade im Bildungs- und Wissenschaftsbereich muss man das Urheberrecht einen Hemmschuh nennen, der vieles, was im schulischen und universitären Alltag technisch möglich wäre (Stichwort: „digitaler Semesterapparat“), schlichtweg verunmöglicht.

---

[2] vgl. Stadler, Th. (2012): Gesetzgeber kann sich im Bereich des E-Learnings nicht zu urheberrechtlichen Neureglungen durchringen, lawblog vom 10.11.2012, http://www.internet-law.de/2012/11/gesetzgeber-kann-sich-im-bereich-des-e-learnings-nicht-zu-urheberrechtlichen-neureglungen-durchringen.html (Letzter Aufruf: 19.11.2012)

[3] Urheberrechtstreit: TU Darmstadt erreicht Vorlage beim Europäischen Gerichtshof, Echo online vom 26.09.2012, http://www.echo-online.de/region/darmstadt/studienortdarmstadt/technischeuniversitaet/Urheberrechtstreit-TU-Darmstadt-erreicht-Vorlage-beim-Europaeischen-Gerichtshof;art477,3252612 (Letzter Aufruf: 19.11.2012)

Natürlich: Wo „brachliegende“, also ungenutzte Verwertungsrechte neu monetarisiert werden können, werden sich vertragliche Vereinbarungen treffen lassen, die eine allgemeine Nutzung und auch den Kontrollverlust über die geschützten Werke finanziell kompensieren können. Den Wert und den Preis allerdings bestimmt nicht die Gesellschaft.

Diese dystopisch anmutenden Aussichten sollen zwar zum Vorausdenken anregen, dürfen jedoch nicht allgemein kulturpessimistisch und speziell kapitalismuskritisch verstanden werden.

Unser Nutzungsverhalten wird sich in den nächsten Jahrzehnten mit jeder Generation weiter entwickeln und wir werden sicherlich legalistische Grundlagen und gesellschaftliche Mechanismen entwickeln, die unser originäres Bedürfnis nach Kunst und Kultur, Unterhaltung und Bildung stillen. Vielleicht wird weniger das konstante „Haben“ und mehr das flüchtige „Sein“ eines vermehrt kontextbezogenen Gebrauchs unseren Umgang mit immateriellen Gütern bestimmen.

In jedem Fall müssen wir als Gesellschaft und am Diskurs Beteiligte dafür Sorge tragen, dass der Wunsch nach einem „gerechten Interessenausgleich“ auch umgesetzt wird, damit das Recht auf Bildung auch weiterhin ein Recht auf den Zugang zu Bildung, Wissen und unserem kulturellen Erbe bleibt.

Teil 5:
Aktivität und Engagement

5.1. Schutz aus Straßburg (Matthias C. Kettemann)

Wie der Europäische Gerichtshof für Menschenrechte die Meinungsäußerungsfreiheit im Internet garantiert

Keywords: Europäischer Gerichtshof für Menschenrechte, Meinungsäußerungsfreiheit, JournalistInnen, BloggerInnen, Kinder, Internet

1. Offline ist online 257
2. Staaten müssen handeln 258
3. Straßburg geht ins Netz 259
4. Schutz für JournalistInnen 261
5. Schlechte Nachrichten für „PiratInnen“ 262
6. Keine Verantwortung für Kommentare 262

1. Offline ist online

Das Internet wurde im Laufe der Zeit immer wieder als „rechtsfreier Raum“ bezeichnet. Der Europäische Gerichtshof für Menschenrechte hat allerdings – ganz im Gegensatz zu dieser Behauptung – eine ausführliche Judikatur zum Schutz der Menschenrechte im Internet entwickelt, die im Folgenden überblicksweise dargestellt wird. Besonders angetan haben es dabei den Straßburger Richtern JournalistInnen, BloggerInnen und Kinder. Deutlich schwächer ausgeprägt ist hingegen der Schutz beispielsweise für politischen Online-Protest (vgl. Christian Möhlen, Kapitel 2.2. *Gibt es ein Recht auf politischen Online-Protest?*)[1].

[1] vgl. auch bspw. „Online-Demonstranten können sich nicht aufs Demonstrationsrecht berufen“ unter:
http://www.heise.de/tp/blogs/8/152568 (Letzter Aufruf: 31.5.2013)

Grundsätzlich gilt: Was offline verboten ist, ist es auch online. Doch Online-Menschenrechtsverstöße können eine stärkere Wirkung entfalten, weshalb besondere Sorgfalt geboten ist. So lassen sich die jüngsten Urteile des Europäischen Gerichtshofs für Menschenrechte (EGMR) zu Menschenrechten im Internet in einem Satz fassen. Mit drei wichtigen Fällen mit Onlinebezug tat der EGMR 2012 einen großen Schritt nach vorne: In *Yildirim gegen Türkei* verbot er Staaten Internzensur ohne Abwägung der Rechte Betroffener; in *Mouvement Raëlien Suisse gegen die Schweiz* unterstrich er, dass die Abrufbarkeit problematischer Inhalte im Internet durch Kinder die Abwägung zuungunsten der Meinungsäußerungsfreiheiten ausgehen lassen kann; und in *Stoll gegen die Schweiz* betonte der Gerichtshof, dass Informationsvielfalt im Netz die Anforderungen an die journalistische Sorgfalt wachsen lässt.

Damit plüschten die Straßburger Richter den Judikaturpolster, der BloggerInnen und JournalistInnen eine weiche Landung im Netz garantiert, behutsam auf. Staaten hingegen nimmt er zunehmend in die Pflicht. Zuletzt war mit der Türkei ein Land im Visier der Richter, das sich schon länger einen Namen als Verfechter einer offensiven und nicht allzu feinfühligen Internetzensur gemacht hat. In *Yildirim gegen Türkei* (2012) bestätigte der EGMR, dass sich der Schutz der Meinungsäußerungsfreiheit nach Artikel 10 der EMRK auch auf das Internet erstreckt und daher unvorhersehbare Blankett-Sperren von ganzen Internetangeboten nicht dem stringenten Ausnahmekatalog genügen.

2. Staaten müssen handeln

Doch der EGMR hat Staaten schon anderes ins Hausaufgabenheft geschrieben: Seiner Judikaturlinie zu positiven Pflichten folgend urteilte der Gerichtshof, dass Staaten neuen Informations- und Kommunikationstechnologien nicht mit legislativer Ignoranz begegnen können. In *K.U. gegen Finnland* (2008) war es den finnischen

Behörden aufgrund der Gesetzeslage unmöglich herauszufinden, wer die Kontaktdaten eines 12-Jährigen auf eine Dating-Webseite gestellt hatte. Dadurch, so urteilte der EGMR, hatte der Staat seine Pflicht verletzt, das Kind und sein Recht auf Privatsphäre zu schützen. Diese Schutzpflicht erstreckt sich auch auf JournalistInnen, wie der 2011 entschiedene Fall *Pravoye Delo und Shtekel g. Ukraine* bestätigt: Staaten sind verpflichtet, ihr Rechtssystem so einzurichten, dass der effektive Schutz von journalistischer Arbeit auch und gerade im Internet gesichert ist.

Überhaupt sind die Gefahren für Kinder im Netz und die Verfolgung von JournalistInnen ein zentraler Motor des Judikaturzuges zu Privatsphäre und Meinungsfreiheit im Netz. Im Fall *Perrin* entschied der EGMR schon 2005, dass der Betreiber einer Online-Porno-Seite bereits bei seiner Gratis-Vorschau Altersüberprüfungen einführen muss, um Minderjährige zu schützen. 2012 fügten die Straßburger Richter hinzu, dass der Abwägungsprozess zugunsten einer Einschränkung der Meinungsäußerungsfreiheit auch durch die Abrufbarkeit problematischer Inhalte im Netz durch Kinder beeinflusst werden kann (*Mouvement Raëlien Suisse gegen Schweiz*).

3. Straßburg geht ins Netz

Judikate zu Offline-Sachverhalten behalten natürlich ihre Relevanz – und nicht immer nimmt der EGMR jede Möglichkeit wahr, auf das Internet einzugehen. So etwa in *Féret gegen Belgien* (2009), in dem er die Verurteilung eines belgischen Rechtsaußen-Politikers wegen anstößiger Flugblätter zwar bestätigte, nicht aber deren Veröffentlichung im Internet, auch wenn die Parolen dadurch zweifellos eine viel weitere Verbreitung genossen.[2]

[2] Nachzulesen bspw. unter http://merlin.obs.coe.int/iris/2009/8/article1.de.html (Letzter Aufruf: 6.4.2013)

Dennoch ist gut, dass der EGMR die Erstreckung seiner Judikatur auf Online-Sachverhalte recht unaufgeregt vollzieht. So kommen KommentatorInnen gar nicht erst in Versuchung, die ausgefeilte Rechtsprechung zu Hassreden zu hinterfragen. Denn klar ist: Auch online darf nicht alles gesagt werden, was man möchte. Die 1976 in *Handyside* gefundene Wendung, nach der auch Meinungen, die schockieren, beleidigen, verstören, zu schützen sind, gilt zwar nach wie vor; Toleranz und Menschenwürde als Grundlagen des europäischen Menschenrechtsschutzsystem sind indes stets im Auge zu behalten, wenn Hassrede vor den Kadi kommt. (Vgl. Viktor Szabados, Kapitel 3.6. *Hassreden im Internet*)

Auch online gilt, dass Hassrede selbst nicht geschützt wird, die Berichterstattung über sie aber schon (vgl. *Jersild g. Dänemark* (1994)). Die Funktion der Medien als Wachhunde in demokratischen Gesellschaften überwog den negativen Einfluss der Äußerungen. Im Internet darf wie auch offline nicht zu religiös motiviertem Hass aufgerufen werden (*Norwood v. Vereinigtes Königreich* (2004)) und Holocaust-Leugnung ist in allen Medien verboten (*Honsik gegen Austria* (1995)). Dies lässt sich unter anderem daraus ableiten, dass der Gerichtshof in *Karatas gegen Türkei* (1999) die korrodierende Wirkung einer Aussage auf die öffentliche Ordnung in direktem Verhältnis zu deren Verbreitung wachsen sieht. Eine Zeitung findet stärkere Verbreitung als ein Flugblatt, ein Blog wird häufiger gelesen als so manche Zeitung.

Auch Luxemburg äußerte sich schützend zur schönen neuen Onlinewelt: In *Scarlet Extended* (2011) beschied der Europäische Gerichtshof, dass ein Gesetz, das Internetdiensteanbieter dazu verpflichtet, Filtersoftware zu installieren, um damit illegale Inhalte aufzuspüren, gegen europäisches Datenschutzrecht und die Meinungsäußerungsfreiheit verstößt. In *SABAM* (2012) unterstrich der EuGH, dass auch soziale Netzwerke nicht gezwungen werden können, Filtersoftware zum Aufspüren von Copyrightverstößen zu einzubauen.

4. Schutz für JournalistInnen

JournalistInnen fanden in Straßburg auch 2012 einen Freund. In *Stoll gegen die Schweiz* (2012) betonte die Große Kammer, das die Beachtung journalistischer Sorgfalt gerade in einer Zeit des Austausches riesiger Informationsmengen im Netz und außerhalb stark zunimmt. Diese Sorgfalt umfasst auch Internetarchive, die vom Schutzumfang des Artikel 10 EMRK umfasst sind. In Folge von *Times Newspapers Ltd egen. Vereinigtes Königreich* (2009) sind Zeitungen verpflichtet, gedruckte Korrekturen auch bei archivierten Artikeln ohne Zeitlimit anzufügen.

Was für Zeitungen gilt, ist auch auf Blogs anwendbar und was für JournalistInnen gilt, müssen sich in Zeiten der „citizen journalists" auch BloggerInnen vor Augen führen. In *Ovchinnikov gegen Russland* urteilte der Gerichtshof etwa, dass eine vorangegangene Veröffentlichung im Internet nicht gegen eine Verurteilung wegen einer Wiederveröffentlichung immunisiert. Aber wenn eine Information einmal im Netz ist, wie er in *Editions Plon gegen Frankreich* (2004) ausführte, sei sie jedenfalls weniger schutzwürdig. In *Fatullayev gegen Aserbaidschan* (2010) betonte Straßburg, dass jeder Vorwurf eines Fehlverhaltens die Pflicht mit sich zieht, eine faktische Grundlage nachzuweisen. Dies gilt auch, wenn eine JournalistIn „privat" bloggt.

Schließlich erinnerte der EGMR in *Polanco Torres und Movilla Polanco gegen Spanien* (2010) daran, dass sich journalistische Sorgfalt nicht darin erschöpft, einen Artikel aus einer Zeitung nachzudrucken, wenn dieser Anschuldigung der Geldwäsche enthält. In diesem bemerkenswerten Fall fand der Gerichtshof nichts dabei, dass sich die AutorInnen des Originalartikels freibeweisen konnten und im nationalen Verfahren freigesprochen wurden, während die HerausgeberInnen der Zeitung, in welcher der Nachdruck erschien, verurteilt wurden. Die Anschuldigungen hatten zwar eine entsprechende

Tatsachenbasis, aber diese hatten sie nicht überprüft, weshalb die unterschiedliche Behandlung gerechtfertigt war.

5. Schlechte Nachrichten für „PiratInnen“

Schlechte Nachrichten gibt es für „PiratInnen“: 2013 bestätigte der EGMR in *Neij und Sunde Kolmisoppi gegen Schweden*, dass eine strafrechtliche Verurteilung und hoher Schadenersatz für Verstöße gegen nationale Schutzgesetze für geistiges Eigentum durch die Gründer der Filesharing-Plattform „The Pirate Bay“ in einer demokratischen Gesellschaft zum Schutz der Eigentumsrechte anderer und zur Verhinderung von Kriminalität notwendig sind.

6. Keine Verantwortung für Kommentare

BetreiberInnen von Seiten mit Kommentarfunktion können übrigens aufatmen. Während der Gerichtshof noch in *Sürek gegen Türkei* (1999) die Verantwortung für LeserInnenbriefe durch die Auswahl und Aufnahme durch die Redaktion begründet sah, lehnte er in *Renaud gegen France* (2010) die Verurteilung eines Webmasters für Kommentare auf dessen Seite im Rahmen einer emotional geführten öffentlichen Debatte ab. Ob dies auch für die BetreiberInnen eines Online-Nachrichtenportals in Hinblick auf anonyme Anschuldigung gilt, wird Straßburg in dem seit 2011 anhängigen Fall *Delfi AS gegen Estland* entscheiden müssen. Eingeweihte Auguren tippen auf Ja.

Sollten die SeitenbetreiberInnen aber doch verurteilt werden und sich im Gefängnis wiederfinden, bleibt ihnen gleich wieder die Hoffnung auf den EGMR. In *Jankovskis gegen Litauen* (anhängig seit 2010) werden die Richter entscheiden müssen, ob GefängnisinsassInnen ein Recht auf Internetzugang haben.

5.2. Wie können wir die Privatsphäre schützen? (Markus Sabadello)

Keywords: Privatsphäre, Datenschutz, Technologie, Privacy-By-Design, FreedomBox

EINLEITUNG 263
1. KOMMERZIELLE DATENSAMMLUNG 264
2. POLITISCHE ÜBERWACHUNG 265
3. ZENTRALISIERTE DIENSTE 268
4. SCHUTZ DER PRIVATSPHÄRE FÜR ALLE 269
ZUSAMMENFASSUNG 270

Einleitung

Wenn man über die Interpretation, Bedeutung und Verteidigung von Menschenrechten im Internet diskutiert, dann geht es meist um verschiedene Ansätze in politischen Bereichen wie Datenschutz, Netzneutralität oder Internet Governance. Während solche Diskussionen stattfinden, gibt es jedoch auch jede Menge technischer Überlegungen und Entwicklungen, um Rechte wie die freie Meinungsäußerung und den Schutz der Privatsphäre zu stärken. Da das Ausmaß von Bedrohungen für diese Rechte durch Maßnahmen wie Überwachung und Zensur stark von der technischen Natur der verschiedenen Schichten und Protokolle des Internet abhängt, macht es Sinn, diesen Aspekt näher zu beleuchten. Dabei kann Technologie einerseits punktuell verwendet werden, um beispielsweise Überwachungsmaßnahmen in konkreten Situationen zu umgehen, andererseits stellen sich auch grundlegendere Fragen nach der technischen Architektur des Internet und danach, wie diese aussehen sollte, um Menschenrechte möglichst gut zu schützen.

Die konkret möglichen Technologien für eine bessere Durchsetzung von Menschenrechten hängen von der jeweiligen Bedrohungslage ab. Im Englischen hat sich hier der Begriff *threat modelling* durchgesetzt, womit eine Methodik bezeichnet wird, um Gefahrenquellen systematisch zu beschreiben – mit dem Ziel, geeignete Gegenmaßnahmen ergreifen zu können.

Ein solches Modell hängt einerseits von den verwendeten Technologien ab, hat aber anderseits auch mit der gesellschaftlichen Stellung und dem politischen Umfeld der sich im Internet bewegenden Individuen zu tun. Beispielsweise könnte Twitter für einen syrischen Dissidenten ein nützliches und vertrauenswürdiges Werkzeug sein, während eine amerikanische Occupy-Aktivistin Twitter aufgrund eines möglichen Zugriffs durch die US-Regierung womöglich meiden wird.

1. Kommerzielle Datensammlung

Eine für viele Menschen im Alltag bedeutsame Bedrohung der Privatsphäre im Internet ergibt sich aus dem Sammeln, Speichern und Auswerten von persönlichen Daten („Data Mining"). Mit dem Siegeszug von stark zentralisierten Internetdiensten wie Facebook, Twitter, YouTube oder Gmail, sowie mit dem Aufstieg des „Cloud"-Paradigmas wird immer klarer, dass persönliche Daten im Internet oft gegen die eigenen Erwartungen oder sogar ohne Wissen der Betroffenen für kommerzielle Zwecke genutzt werden, hauptsächlich um Werbungen zu schalten, aber teils auch, um einzelne Individuen basierend auf ihren persönlichen Profilen nachteilig zu behandeln. Persönliche Daten wurden vom Weltwirtschaftsforum inzwischen als „neues Öl" und von der EU als „Währung im digitalen Zeitalter" bezeichnet. Um sich diesem blühenden Wirtschaftszweig, dessen Methoden wohl nicht immer mit dem Recht auf Privatsphäre vereinbar sind, zu entziehen, hilft als Gegenmaßnahme oft nur der Verzicht oder zumindest eine entsprechende Zurückhaltung beim Verwenden datenhungriger Webanwendungen.

Hierbei geht es allerdings nicht nur um die kommerzielle Nutzung von freiwillig ins Internet gestellten persönlichen Daten. Oft werden nämlich detaillierte Interessens- und Verhaltensprofile auch unfreiwillig angelegt. Dies geschieht hauptsächlich mittels klassischer Methoden wie Cookies oder JavaScript, aber auch mit neueren Technologien wie Bestandteilen des HTML5 Standards, oder durch sogenanntes „Fingerprinting", also der Identifikation durch Eigenschaften des benutzten Webbrowsers und Betriebssystems. Einige einfache Softwaretools zur Vermeidung von allzu starker Überwachung dieser Art haben sich bereits in großem Stil durchgesetzt, beispielsweise Browser-Plugins wie „Adblock Plus" zum Blockieren von Werbung, oder „NoScript" zum Unterbinden von aktivem Code (Scripts) innerhalb des Webbrowsers. Tools dieser Art erfreuen sich seit Jahren steigender Beliebtheit.

2. Politische Überwachung

Neben dem Sammeln von Daten für kommerzielle Zwecke stellen politische Einflussnahmen auf das Internet eine weitere Gefahr für Menschenrechte dar. Seit in den sogenannten „Twitter-Revolutionen" („Arabischer Frühling") das Potential von Internettechnologien für politische Bewegungen detailliert erörtert wurde, hat eine Art Wettrüsten eingesetzt. Während repressive Regimes Mittel wie Zensur und Überwachung einsetzen, um ihre Interessen zu verteidigen und ihre Gegner zu schwächen, wird auf der anderen Seite an Technologien gearbeitet, die vor solchen Maßnahmen schützen und freie Kommunikation ermöglichen sollen. Dies geschieht nicht selten mit Unterstützung aus westlichen Staaten, beispielsweise durch die amerikanische „New America Foundation" oder die europäische „No Disconnect Strategy", die politische AktivistInnen mit geeigneten Internettechnologien sowie mit Trainings unterstützen. Solche Hilfestellungen mögen allerdings manchmal etwas zynisch erscheinen, wenn man bedenkt, dass auch in Europa und in den USA mit

Vorratsdatenspeicherung, ACTA, SOPA usw. die Freiheit im Internet immer stärker gefährdet ist, und dass ein Eintreten für ein freies Internet offenbar nur dann erfolgt, wenn es auch im staatlichen Interesse liegt. Beispielsweise hatte Hillary Clinton im Jahr 2010 in ihren „Remarks on Internet Freedom" angekündigt, dass Amerika für Meinungsfreiheit im Internet eintreten würde, und dann noch im selben Jahr das Wikileaks-Projekt als Angriff auf die nationale Sicherheit bezeichnet. Hinzu kommt auch, dass westliche Firmen jahrelang Überwachungstechnologien unter anderem an nordafrikanische Länder geliefert haben und dies nach wie vor tun[1].

Die Liste an Technologien, die vor Überwachung schützen können, ist lang. „PGP" ist eine alte, aber nach wie vor effektive Methode, um verschlüsselte Nachrichten zu verschicken. „HTTPS Everywhere" sorgt dafür, dass Webseiten wenn möglich nur über nicht abhörbare oder überwachbare SSL-Verbindungen geöffnet werden. „Cryptocat" bietet einen mittels „OTR" („Off the record") verschlüsselten Chat-Kanal und benötigt nichts weiter als einen normalen Webbrowser. „Pond" ist eine Software, mit der Nachrichten ähnlich wie E-Mail, jedoch völlig anonym verschickt werden können. „Briar" versucht möglichst viele verschiedene Medien vom Internet bis zur mit der Post versandten DVD zu einem kohärenten Kommunikationsnetzwerk zu verbinden.

Eine ebenfalls nicht neue aber sich derzeit stark verbreitende Technologie sind die VPNs („Virtual Private Networks"). Ursprünglich vor allem dazu gedacht, um sich von einem beliebigen Internetzugang aus auf sichere Art zu einem internen Firmennetzwerk zu verbinden, werden VPNs auch privat immer beliebter. Es handelt sich hierbei um

---

[1] vgl. Reporters Without Borders, *Enemies of the Internet* report 2013, Five State Enemies of the Internet: Syria, China, Iran, Bahrain and Vietnam. Nachzulesen unter: https://en.rsf.org/special-report-on-internet-11-03-2013,44197.html sowie Report zum Download unter: https://surveillance.rsf.org/en/ (Letzter Aufruf: 31.5.2103)

Dienste, über die man den eigenen Datenstrom über einen sogenannten Tunnel umleiten kann, wodurch die angesurften Internetserver nicht die eigene IP-Adresse „sehen“, sondern nur diejenige des VPN-Providers. Dies führt einerseits zu einer gewissen Anonymisierung, andererseits hat es auch den Effekt, dass man sich zu Internetdiensten verbinden kann, die aufgrund von Zensurmaßnahmen z.B. in einer Firma oder in einem ganzen Land normalerweise nicht erreichbar sind. Für technisch Versierte bieten sich hier „OpenVPN“ oder „Tinc“ zur Installation auf eigenen Servern an, es gibt allerdings auch kommerzielle VPN-Anbieter wie z.B. „VPN4ALL“, oder die Grazer Firma „Hideway“. Einige Unternehmen wie z.B. „Hotspot Shield“ oder „Psiphon“ bieten VPN-Dienste an, die speziell auf Länder mit stark eingeschränkter Internetfreiheit zugeschnitten sind.

Ähnlich wie VPNs, allerdings noch um einiges ausgeklügelter, funktioniert auch das Anonymisierungsnetzwerk „Tor“ („The Onion Router“). Wenn man „Tor“ benutzt, werden Datenverbindungen nicht direkt zu einem Zielserver aufgebaut, sondern mehrfach und nach einer Art kryptografischem Verschachtelungsprinzip zwischen den TeilnehmerInnen des Netz werks hin- und hergeschickt, bevor sie am Zielserver ankommen. Dadurch werden sowohl die Inhalte dieser Verbindungen verborgen, als auch die Information, wer mit wem kommuniziert. Mittels „Tor“ ist es weiters möglich, selbst Inhalte und Dienste in Form von „Hidden Services“ anonym anzubieten. Da die „Tor“-Software für sich alleine genommen nicht einfach zu installieren ist, gibt es darauf aufbauend auch ein vorgefertigtes „Tor Browser Bundle“ sowie die von CD oder USB-Stick startbare „Tails“ Software, welche die Benützung des Anonymisierungsnetzwerks deutlich vereinfacht.

Ein wichtiges Thema im Zusammenhang mit Zensur und Überwachung im Internet ist nicht nur die Entwicklung und Verwendung von Software zur Umgehung, sondern auch die bloße Feststellung, Analyse und Dokumentation von Einflussnahmen. Beispielsweise entwickelt

das „Chokepoint"-Projekt spezielle Software, die Zensur auf globaler Ebene systematisch identifizieren und dokumentieren soll. Andere Projekte wie „Perspectives" oder das „SSL Observatory" der Electronic Frontier Foundation verfolgen ähnliche Ziele und erlauben es jedem, mittels Browser-Plugin beim Aufspüren von Eingriffen in die Internetfreiheit mitzuhelfen. Die EU-Kommission versucht ebenfalls mittels einer Initiative namens „European Capability for Situational Awareness" eine weltweite Karte von Internetzensur zu erstellen.

3. Zentralisierte Dienste

Während die oben angeführten Werkzeuge zur Umgehung von kommerzieller Datensammlung und politischer Überwachung wohl kurzfristig Ziele wie Privatsphäre oder freie Meinungsäußerung unterstützen können, stellen sie wohl kaum eine langfristige Lösung für die Frage der Menschenrechte im Internet dar. Um eine solche Lösung zu finden, wird es abgesehen von der Entwicklung von besseren politischen Rahmenbedingungen auch nötig sein, die fundamentalen Kommunikationsstrukturen im Internet zu überdenken. Es gibt beispielsweise eine steigende Anzahl an Initiativen, die auf dezentrale Kommunikation setzen und von der technischen Architektur her weniger Machtkonzentration als z.B. Google oder Facebook aufweisen. In der Öffentlichkeit wurde hier vor allem „Diaspora" bekannt, es gibt allerdings z.B. im Rahmen der „Federated Social Web" Initiative noch viele weitere ähnliche Projekte. Einige Softwareprojekte wie beispielsweise „Freenet", „TheGlobalSquare", oder „Secushare" arbeiten mit radikal verteilten Kommunikationsstrukturen, die völlig ohne Server auskommen sollen („Peer-to-Peer") und Ähnlichkeiten mit Filesharing-Technologien wie BitTorrent aufweisen. Für solche Ansätze, bei denen der Schutz von Privatsphäre schon beim Entwurf und bei der Entwicklung von Software im Vordergrund steht, ist der Begriff „Privacy-By-Design" gebräuchlich.

4. Schutz der Privatsphäre für alle

Ein Problem mit vielen der erwähnten Tools ist, dass sie oft zu schwierig zu verstehen oder zu bedienen sind. Beispielsweise gibt es „PGP“ seit ca. 20 Jahren, und es ist immer noch ein ausgezeichneter Schutz für viele Bedrohungslagen, dennoch ist es in der breiten Öffentlichkeit kaum bekannt. Dies mag einerseits daran liegen, dass das allgemeine Bewusstsein für den Schutz von Privatsphäre online nach wie noch nicht sehr stark ausgeprägt ist, oder dass Bequemlichkeit einfach einen höheren Stellenwert hat. Es mag aber auch daran liegen, dass die Anwendung mancher Tools nicht benutzerInnenfreundlich genug ist, z.B. weil sie von vornherein von HackerInnen oder AktivistInnen für eigene spezielle Bedürfnisse und ohne Rücksichtnahme auf allgemeine Verwendbarkeit entwickelt werden.

Ein Hardwareprojekt, das es sich zum zentralen Ziel gesetzt hat existierende Technologien einfacher zugänglich zu machen, ist die „FreedomBox“, dabei handelt es sich um ein kleines Gerät, einen sogenannten „Plug Computer“, der als Server in ein bestehendes Heimnetzwerk eingebunden werden kann und dieses automatisch mit einigen Funktionen zum Schutz der Privatsphäre ausstattet. Die FreedomBox kann einige der bereits erwähnten Werkzeuge wie beispielsweise „Adblock Plus“, „Tor“ oder eine VPN-Software benutzbar machen, ohne dass diese erst mühsam auf dem eigenen Laptop, Tablet oder Smartphone installiert und konfiguriert werden müssen. In weiterer Folge soll die FreedomBox auch den dezentralen Austausch von Nachrichten, Fotos und anderen Daten ermöglichen und damit eine Alternative zu Facebook, Twitter, usw. bieten.

In den USA existieren inzwischen außerdem einige Institutionen, die es sich zum Ziel gesetzt haben, Technologien für Menschenrechte im Internet nicht nur zu entwickeln, sondern auch für mehr Menschen zugänglich zu machen. Beispielsweise betreibt die Stanford University das sogenannte „Program on Liberation Technology“, welches eine

beliebte Mailingliste zu dem Thema anbietet, die auch für AnfängerInnen geeignet ist. Das „Open Internet Tools Project“ veranstaltet regelmäßige Konferenzen und informelle Treffen, um an Anti-Zensur-Technologien zu arbeiten und diese verständlich zu machen. Auch die Organisation „Access Now“ arbeitet daran, politische AktivistInnen in vielen Ländern mit Ratschlägen, Trainings und konkreten Technologien zu unterstützen, Handbücher zu veröffentlichen, und neue Entwicklungen zu finanzieren.

Ein weiteres Beispiel für eine Idee, die darauf ausgerichtet ist auch technisch wenig versierten Individuen Technologien zum Schutz der Privatsphäre zugänglich zu machen, sind sogenannte Cryptoparties. Dabei handelt es sich um informelle Treffen, bei denen in lockerer Atmosphäre einfache kryptografische Anwendungen wie zum Beispiel das Verschlüsseln von E-Mails erläutert und geübt werden. Regelmäßige Cryptoparties gibt es inzwischen in vielen Ländern und Städten weltweit, unter anderem im Wiener HackerInnenspace Metalab.

Zusammenfassung

Technische Entwicklungen alleine können die Fragen nach der Menschenrechtslage im Internet nicht beantworten, dennoch spielen sie eine wichtige Rolle, da es ja erst die Art der verwendeten Technik ist, die Zensur und Überwachung überhaupt möglich macht. Man kann die existierende Internet-Infrastruktur natürlich nicht ohne weiteres von Grund auf neu erfinden, aber man kann punktuelle Maßnahmen setzen um sich zu schützen, man kann stark zentralisierte Softwarearchitekturen hinterfragen und Gegenmodelle im Sinne von „Privacy-By-Design“ entwerfen, und man kann Initiativen wie z.B. die FreedomBox und Cryptoparties unterstützen, die dem besseren Schutz von Menschenrechten im Internet dienen.

5.3. Democracy Live? (David Röthler)

Das demokratische Potenzial interaktiver Live-Videosysteme

Keywords: Partizipation, Livestream, politische Kommunikation, Transparenz, Interaktion

1. LIVE-ÜBERTRAGUNGEN AUS PARLAMENTEN 271
2. VON DER INTERAKTION ZUR PARTIZIPATION? 273
3. POLITISCHE KOMMUNIKATION IN LIVE-ONLINE-RÄUMEN 275

1. Live-Übertragungen aus Parlamenten

Transparenz ist eine wichtige Voraussetzung für politische Partizipation[1]. Wenn Bedingungen geschaffen werden sollen, unter denen politische Beteiligung gedeihen kann, müssen Wege gefunden werden, politische Abläufe nachvollziehbar zu machen – zum Beispiel durch den Einsatz interaktiver Live-Videosysteme. Mit diesen Systemen können Diskursräume geöffnet werden oder neue Räume für politische Meinungsbildung und politisches Handeln entstehen.

Politische Entscheidungen werden in den Parlamenten (bzw. allgemeinen Vertretungskörpern) auf lokaler, Landes-, und Bundesebene getroffen. Diese Gremien sind für die Öffentlichkeit grundsätzlich zugänglich. Nun ermöglichen digitale Medien seit einiger Zeit die einfache Übertragung von Ton und Bild aus Gemeinderäten, Landtagen, dem Bundesrat und Nationalrat. Dadurch wird die Zugänglichkeit zu den entsprechenden Sitzungen erweitert und für viele BürgerInnen niederschwelliger, da die Teilnahme ortsunabhängig und

[1] Entsprechend wird auf http://www.data.gov/about, dem Open Data Portal der US-Regierung, Partizipation als Folge von Transparenz betrachtet: „Public participation and collaboration will be key to the success of Data.gov“. (Letzter Aufruf: 3.4.2013)

anonym erfolgen kann. Darüber hinaus wird im Regelfall eine Aufzeichnung der Sitzung im Internet bereitgestellt, die eine zeitversetzte Wiedergabe des Geschehens ermöglicht.

Mittlerweile wird bei Nationalratssitzungen ein Livestream eingerichtet. Ebenso ist ein solcher bei den Sitzungen aller österreichischen Landtage (bis auf das Burgenland) und in einer immer größer werdenden Anzahl von Gemeinden zu finden. Es wird immer schwieriger für die Politik sich diesem Trend zu verschließen, weil von der Allgemeinheit zunehmend Transparenz gefordert wird.

Allerdings gibt es auch rechtliche und politische Bedenken oder gar Widerstände:

In Deutschland scheint die Rechtslage – zumindest auf kommunaler Ebene – die Einrichtung von Livestreams zu behindern. Dort wird ein Gemeinderat nicht als Parlament im staatsrechtlichen Sinne gesehen, sondern vornehmlich als ein Verwaltungsorgan der Kommune. Die Sitzungen müssen zwar öffentlich sein, doch genügt im Regelfall eine „Saalöffentlichkeit". Es gibt eine Entscheidung des Bundesverfassungsgerichts, die Tonaufnahmen eines Journalisten während einer Gemeinderatssitzung verboten hatte, da diese eine schädliche Wirkung auf das Verhalten der Betroffenen hätten, „weil sie jede Nuance aus der Rede, einschließlich der rhetorischen Fehlleistungen, der sprachlichen Unzulänglichkeiten und der Gemütsbewegungen des Redners dauerhaft und ständig reproduzierbar" konservieren.[2] Im Fall der Stadt Konstanz in Baden-Württemberg hatte der Landesdatenschutzbeauftragte entsprechende datenschutzrechtliche Bedenken. Die Persönlichkeitsrechte, nicht allein der GemeinderätInnen,

[2] BVerwGE 85, 283 – Abwehr von Tonaufnahmen in Ratssitzungen, Urteil vom 3. August 1990: http://www.servat.unibe.ch/dfr/vw085283.html (Letzter Aufruf: 3.4.2013)

sondern auch der VerwaltungsmitarbeiterInnen, der ZuschauerInnen und beteiligter Dritter müssten gewahrt werden.[3]

Tatsächlich verändert die Live-Übertragung das Verhalten der Abgeordneten. Sie nutzen die Sitzung verstärkt als öffentliche Bühne für ihre Meinung. Das Bewusstsein, dass die Sitzung live oder als Aufzeichnung gesehen werden kann, hat selbstkontrollierende Wirkung.

Einige Ortsparlamente scheinen – mit dem eher geschlossenen Rahmen – schlicht zufrieden zu sein. So wird die Gemeinde Wiessee in Bayern wie folgt zitiert:

> *„Das Interesse vor Ort an den öffentlichen Sitzungen ist bis auf wenige Ausnahmen relativ gering. Wir denken nicht, dass durch die Übertragung ins Internet in Echtzeit eine recht viel breitere Masse an Interessierten erreicht wird.“*[4]

2. Von der Interaktion zur Partizipation?

Während ein Großteil der Live-Übertragungen dem traditionellen One-to-many-Paradigma folgt und keine Interaktion des Publikums zulässt, wurde beispielsweise bei der Übertragung der Gemeinderatssitzungen der Stadt Salzburg (an denen der Autor dieses Beitrags technisch und konzeptionell beteiligt ist) ein Chat neben dem laufenden Video eingeblendet.[5] In diesem können sich die ZuseherInnen über das Geschehen im Gemeinderat austauschen und die Übertragung mit zusätzlichen Informationen bereichern. Eine in diesem Zusammenhang interessante Variante ist die Beteiligung von MandatsträgerInnen aus dem Gemeinderatssaal am Chat durch die

---

[3] Vgl. Artikel aus der Stuttgarter Zeitung vom 6.6.2012: http://goo.gl/PSVji (Letzter Aufruf: 3.4.2013)

[4] Vgl. Das Bayerische Fernsehen berichtet über Transparenz in den Tal-Gemeinden, Beitrag vom 15.6.2012: http://www.tegernseerstimme.de/gibt-es-etwas-zu-verbergen/34225.html (Letzter Aufruf: 3.4.2013)

[5] Siehe: Salzburger Gemeinderat_14.05.2012, Video: http://www.youtube.com/watch?v=e5OqE6aeCME&feature=share&list=UUVNC2cKWW3YC_OZgEmKIxPA (Letzter Aufruf: 3.4.2013)

Nutzung von Notebooks, Smartphones oder Tablets. Dadurch könnten diese, auch ohne aktuelles Rederecht, einen direkten Kanal nutzen, um mit potentiellen Wählerinnen und Wählern in Kontakt zu treten oder gegebenenfalls ihre Gegenmeinung kundzutun. Wenn man dieses Szenario weiterdenkt, könnte sich die interessante Fragen stellen, wie sich das Gremium und die Diskussionskultur im Gemeinderat oder einem anderen Parlament ändert, wenn viele oder gar alle MandatarInnen sich parallel zur laufenden Debatte über das Medium Chat austauschen. Wenn sich die Sitzungskommunikation solcherart auf den Chat verlagern würde, könnte dies auch gegen die jeweiligen Geschäftsordnungen verstoßen. So stellt beispielsweise §7 der Geschäftsordnung des Gemeinderats der Landeshauptstadt Salzburg[6] fest, dass die Sitzungen des Gemeinderats grundsätzlich öffentlich sind, „die Zuhörer sich aber jeder Äußerung zu enthalten haben". Dies wäre in dem beschriebenen Szenario nicht mehr gewährleistet und würde wohl gegen die Geschäftsordnung verstoßen. Andererseits könnte dadurch eine interessante Form der Partizipation – wahrscheinlich aber nur bei entsprechender Moderation – entstehen. Wenn die Stimmberechtigung bei den gewählten MandatarInnen bliebe, würde dabei das Konzept der indirekten Demokratie beibehalten.

Eine mögliche interessante Folge von Live-Übertragungen ist, dass weitere Wünsche nach Transparenz erfüllt werden. So finden sich seit November 2012 erstmals vorbereitende Dokumente der Salzburger Gemeinderatssitzungen, wie Amtsberichte (Entscheidungsvorschläge,

[6] Siehe: Gemeinderatsbeschluß vom 19. Juli 1966, Amtsblatt Nr. 15/1966 (pdf): http://www.stadt-salzburg.at/pdf/gemeinderatsgeschaeftsordnung_inkl_106__ergaenzung.pdf (Letzter Aufruf: 3.4.2013)

die auf Verwaltungsebene erarbeitet wurden) und die entsprechenden Stellungnahmen im Internet veröffentlicht[7].

Zusammenfassend lässt sich in Bezug auf die Live-Übertragung von Sitzungen der Parlamente festhalten, dass dadurch die Zugänglichkeit und deren Transparenz erhöht wird. Das partizipative Potential wird zurzeit noch nicht ausgeschöpft.

3. Politische Kommunikation in Live-Online-Räumen

Der kanadische Regionalpolitiker Garth Frizzel berichtete im Frühling 2012 in seinem Weblog über die neue Kommunikationsform „Google Hangouts", die er für sich entdeckt hat:

> *„Some time ago, I began regular video-conferences with people. My goal was to talk with people about municipal issues that were affecting them in their cities, whether it was Prince George, or even Victoria, Surrey, Montréal, Winnipeg… wherever. The response was surprising. People liked talking frankly, unfiltered, with no preparation… about issues affecting them. The uptake was great from other elected officials too. […] With no agenda, and no partisan leaning, the discussion has migrated to where random Canadians wanted to take it. It's been an interesting start, and the only observation that's been consistent has been that the open format is one that they LOVED."*[8]

„Google Hangouts"[9] sind Videokonferenzen, die Google mit dem Sozialen Netzwerk Google+ im Sommer 2011 eingeführt hat. Bis zu 10 Personen können an solchen Videokonferenzen teilnehmen und etwa über Whiteboard und gemeinsame Dokumente zusammenarbeiten.

---

[7] Vgl. Amtsberichte zum Altstadtausschuss vom 21.3.2013, Stadt Salzburg: http://goo.gl/9BmfM (Letzter Aufruf: 3.4.2013)

[8] s. http://www.garthfrizzell.com/en-francais-bringing-canadians-together.html (Letzter Aufruf: 3.4.2013)

[9] vgl. https://tools.google.com/dlpage/hangoutplugin (Letzter Aufruf: 3.4.2013)

Eine faszinierende Option sind dabei die „Hangouts on Air“[10]. Diese erlauben die Live-Übertragung der Videokonferenz über Youtube. So kann ein unbegrenzt großes Publikum erreicht werden. Allerdings sind in diesem Fall die Interaktionsmöglichkeiten für die Zusehenden auf die Kommentarfunktion beschränkt. Die Aufzeichnung steht im Anschluss sogleich als Youtube-Video zur Verfügung.

Dieses oder andere Systeme können verwendet werden, um als PolitikerIn mit WählerInnen in Kontakt und Austausch zu treten. Die Grünen in Salzburg haben – begleitet vom Autor dieses Beitrags – im Oktober 2012[11] erste Versuche in diese Richtung unternommen.

Auch Second Life wurde und wird als dreidimensionaler Onlineraum zur Diskussion und Aktion genutzt. So fand beispielsweise 2007 eine Online-Demonstration von Avataren im virtuellen Washington in Second Life gegen den Krieg im Irak[12], sowie eine Podiumsdiskussion zur Bremer Bürgerschaftswahl[13] statt. Auch wenn es nach dem Hype um Second Life vor mehr als fünf Jahren um die Onlinewelt ruhig geworden ist, ist Second Life dennoch aufgrund der Dreidimensionalität für persönliche Interaktion sehr interessant. Die Sprachverbindung ist nicht zuletzt durch Raumklang sehr gut und von hoher Stabilität. Die Personen bzw. Avatare können ihre aktuelle Beziehung zueinander durch den jeweils aktuellen Standort auch den anderen Teilnehmenden klar vermitteln. Wer in einer Gruppe zusammen steht oder sitzt, befindet sich für alle anderen offensichtlich in einem gemeinsamen Gespräch. Dadurch können Online-Treffen auch – wie bei Präsenzveranstaltungen – durch informelle Zusammenkünfte (Pausenge-

---

[10] vgl. http://www.google.com/intl/de_ALL/+/learnmore/hangouts/onair.html (Letzter Aufruf: 3.4.2013)

[11] vgl. https://www.facebook.com/events/123200587832212/?fref=ts (Letzter Aufruf: 3.4.2013)

[12] vgl. http://www.youtube.com/watch?v=qaiGV_Hd0O8 (Letzter Aufruf: 3.4.2013)

[13] vgl. http://www.youtube.com/watch?v=W2bwAhOnq-Y (Letzter Aufruf: 3.4.2013)

spräche) aufgelockert werden. Dieser Umstand verleiht Second Life ein hohes Potential. Allerdings erfordert der Zugang zu Second Life Übung und Erfahrung (vgl. Julian Ausserhofer und Heinz Wittenbrink, Kapitel 4.2 *Web Literacies und Offene Bildung*). Allein die Notwendigkeit der Installation eines Clientprogramms lässt Second Life nicht besonders niederschwellig erscheinen.

Eine Kombination von Präsenz- und Online-Veranstaltung bieten Livestreams, die durch Nutzung der entsprechenden Systeme auch interaktiv gestaltet werden können. Dadurch ist es Online-Teilnehmenden zum Beispiel möglich, sich über Audio und Video zu Wort zu melden.[14] Die Immersivität der Online-Teilnahme an Präsenzveranstaltungen, darunter versteht man das Eintauchen in eine Umgebung mit möglichst vielen Sinneseindrücken, kann durch Audio-/Video-Roboter wie dem Anybot[15] noch erhöht werden. Dieses fernzusteuernde, ähnlich einem Segway funktionierende, auf lediglich zwei Rädern fahrende Gerät, ermöglicht es Teilnehmenden aus aller Welt sich im Raum zu bewegen. Der Preis von $ 9.700,– ist zwar noch relativ hoch, es sind aber bereits günstigere Roboter mit ähnlicher Funktionalität erhältlich. Das Produkt „Double – Wheels for your iPad“ verspricht bei einem im Vergleich günstigen Preis von $ 1.900,–: „Double is the simplest, most elegant way to be somewhere else in the world without flying there.“ Der niedrigere Preis ergibt sich durch die Verwendung des iPads als Hardwarelösung und zur Steuerung.

Abschließend kann festgehalten werden, dass sich synchrone Online-Systeme sehr gut zur Meinungsäußerung, zum Diskurs und für politische Aktionen einsetzen lassen. Als Beispiel kann das EU-Projekt „Europe so Close“ (www.europe-so-close.eu), an dem der Autor

---

[14] Ein Beispiel dafür sind die Village Innovation Talks vom Dezember 2011, s. http://www.dorfwiki.org/wiki.cgi?VillageInnovationTalk (Letzter Aufruf: 3.4.2013) und http://www.flickr.com/photos/davidroethler/6532033821/lightbox/ (Letzter Aufruf: 3.4.2013)

[15] vgl. https://www.anybots.com/ (Letzter Aufruf: 3.4.2013)

dieses Artikels beteiligt ist, genannt werden. In diesem Projekt diskutieren EU-Abgeordnete, ExpertInnen und LobbyistInnen mit interessierten BürgerInnen in Form von Videokonferenzen.

Wichtiger Aspekt bei synchronen Online-Formaten ist die unmittelbare Interaktion trotz beliebiger geographischer Distanz, die diese Kommunikationsform effektiv und attraktiv erscheinen lässt.

Nachteile sind die Zeitgebundenheit sowie der nicht in jedem Fall niederschwellige Zugang zu den jeweiligen Tools. Jedenfalls sind neue Räume für grenzenloses politisches Handeln entstanden. Nicht zuletzt erhöhen die neuen Optionen auch die Chancen der Teilhabe von Menschen mit Betreuungspflichten oder Mobilitätseinschränkungen und gewährleisten so unter Umständen die Einhaltung zentraler Grundrechte.

5.4. Das aktivistische Potenzial von Crowdfunding (Wolfgang Gumpelmaier)

Keywords: Crowdfunding, Zivilgesellschaft

EINLEITUNG 279
1. WAS IST CROWDFUNDING? 280
2. WIE FUNKTIONIERT CROWDFUNDING? 281
3. CROWDFUNDING UND BETEILIGUNG 283
4. VON ENGAGEMENT ALLEINE LÄSST SICH NICHT LEBEN 284

Einleitung

Spätestens seit der „Causa Heini Staudinger“[1] ist der Begriff „Crowdfunding“ und die dahinterstehende Idee auch in Österreich bei der breiten Masse angekommen. Bekannt wurde diese alternative Form der Ideen-Finanzierung unter anderem durch die US-Plattform Kickstarter (www.kickstarter.com), auf der Projekte wie Diaspora (das „Anti-Facebook“) oder die Pebble Smartwatch Erfolge feierten. In Europa war es vor allem der finnische Science-Fiction-Film Iron Sky, der das Thema vorantrieb.

Mittlerweile setzen immer mehr Kreative, Start-Ups und Non-Profit-Organisationen auf diese community-basierte Form der Projektfinanzierung. Auch im Zusammenhang mit politischem und zivilgesellschaftlichem Engagement spielt Crowdfunding eine immer größer werdende Rolle, da die UnterstützerInnen auf diese Weise direkt in ein Projekt miteingebunden werden. Welche Einsatzmöglichkeiten

[1] Als der als Oberösterreicher von seiner Hausbank keinen Kredit mehr bekam, lieh er mit einer Art Crowdfunding Geld von seinen FreundInnen und KundInnen, vgl. http://de.wikipedia.org/wiki/Heinrich_Staudinger (Letzter Aufruf: 15.3.2013)

Crowdfunding bietet und welchen Herausforderungen man dabei möglicherweise gegenübersteht, soll dieser Beitrag erörtern.

1. Was ist Crowdfunding?

Crowdfunding ist eine Form des Crowdsourcings[2], bei der für künstlerische Projekte, Unternehmengründungen und Geschäftsideen, Sozialprojekte, NGO's oder politische Zwecke Geld gesammelt wird. Die Online-Crowd, also die breite Masse der Internet-NutzerInnen, investiert dabei selbst, indem sie ein Projekt finanziell unterstützt und damit dessen Durchführung ermöglicht.

Laut dem Crowdfunding Industry Report 2012[3], der weltweit bisher umfangreichsten Crowdfunding-Studie, existieren vier unterschiedliche Formen von Crowdfunding:

1. equity-based crowdfunding
2. lending-based crowdfunding
3. reward-based crowdfunding
4. donation-based crowdfunding

Die Unterschiede beziehen sich dabei vor allem auf die Art der Gegenleistung, die UnterstützerInnen für ihre finanzielle Beteiligung an einem Projekt erhalten.[4]

Beim equity-basierten Modell (auch „Crowdinvesting" genannt) werden etwa KleinanlegerInnen mit Erfolgsbeteiligungen angelockt, um in ein Start-Up oder eine Geschäftsidee zu investieren. Das lending-basierte Modell wiederum vermittelt Mikrokredite zwischen

---

[2] Traditionell internen gelagerte Teilaufgaben werden beispielsweise über das Internet an freiwillige User ausgelagert, vgl. http://de.wikipedia.org/wiki/Crowdsourcing (Letzter Aufruf: 15.3.2013)

[3] Massolution (2012): Crowdfunding Industry Report – Market Trends, Composition and Crowdfunding Platforms.

[4] Eine entsprechende Infografik (Gumpelmaier, Wolfgang (2013): Die 4 Arten von Crowdfunding.Online) findet online unter: http://www.ikosom.de/2013/04/08/die-vier-arten-von-crowdfunding-infografik/ (Letzter Aufruf: 31.5.2013)

Privatpersonen, wobei sich die Gegenleistung in Form einer Rückzahlung auswirkt. Im Gegensatz dazu werden von den ProjektinhaberInnen beim reward-basierten Modell vor allem ideelle, aber auch materielle Prämien (Dankesnachrichten, DVD's etc.) versprochen, um die Crowd zur Unterstützung zu motivieren. Beim donation-basierten Modell handelt es sich letztlich um die Sammlung von Spenden, wobei abgesehen vom guten Gefühl und einer Spendenquittung zumeist keine anderen Gegenleistungen angeboten werden.

2. Wie funktioniert Crowdfunding?

Üblicherweise präsentieren ProjektinhaberInnen ihre Ideen auf speziellen Web-Plattformen, die sich um eine ansprechende Präsentation, die technische und rechtliche Infrastruktur, den Finanztransfer und das UnterstützerInnen-Management kümmern. Bei erfolgreichen Projekten behalten die Plattformen für die Bereitstellung dieser Infrastruktur eine Provision zwischen 0 und 10 Prozent ein, in manchen Fällen sind hier sogar die Payment-Gebühren (also für Bezahl-Dienste wie PayPal etc.) inkludiert.

Grundsätzlich funktionieren die meisten Crowdfunding-Plattformen nach dem „Alles-oder-Nichts" Prinzip. Das bedeutet, dass die ProjektinhaberInnen das Geld nur erhalten, wenn die angestrebte Zielsumme in der zuvor festgelegten Zeit erreicht wird. Eine Ausnahme von dieser Regel macht etwa die internationale Plattform IndieGoGo oder auch querk aus Österreich. Bei querk können ProjektinhaberInnen sogar entscheiden, ob sie lieber nach dem Alles-oder-Nichts oder dem Mehr-oder-Weniger-Prinzip crowdfunden.

In der folgenden Tabelle findet sich eine Übersicht bestehender Crowdfunding-Plattformen:

EQUITY-BASED (for financial return)	**LENDING-BASED** (for financial return)	**REWARD-BASED** (for non-monetary rewards)	**DONATION-BASED** (for philantropy and sponsorship)
GrowVC (INT) www.growvc.com	Kiva (INT) www.kiva.org	Kickstarter (INT) www.kickstarter.com	GlobalGiving (INT) www.globalgiving.org
Innovatrs (INT) www.innovatrs.com	Zidisha (INT) www.zidisha.org	Indiegogo (INT) www.indiegogo.com	JustGiving (INT) www.justgiving.com
Seedmatch (DE) www.seedmatch.de	Prosper (US) www.prosper.com	Rockethub (INT) www.rockethub.com	FirstGiving (INT) www.firstgiving.com
Crowdcube (UK) www.crowdcube.com	Lending Club (US) www.lendingclub.com	Startnext (DE) www.startnext.de	Betterplace (DE) www.betterplace.org
WeFund (UK) www.wefunder.com	Smava (DE) www.smava.de	Verkami (ESP) www.verkami.com	HelpDirect (DE) www.helpdirect.org
WiSeed (FR) www.wiseed.fr	Zopa (UK) uk.zupa.com	Pozible (AUS) www.pozible.com	Respekt.net (AT) www.respekt.net

Der Vollständigkeit halber soll erwähnt werden, dass sich mithilfe von Plug-Ins oder Widgets wie *IgnitionDeck* (http://ignitiondeck.com) oder *ChipIn* (www.chipin.com) Crowdfunding-Funktionalitäten auch in bestehende Webseiten integrieren lassen bzw. man sich damit eigene Crowdfunding-Webseiten gestalten kann.

Am Beginn jeder Crowdfunding-Kampagne steht eine zumeist längere Vorbereitungsphase, in der vor allem die Projektbeschreibung und ein kurzes Projektvideo erstellt, sowie die Gegenleistungen definiert werden. Das Angebot an Gegenleistungen dient UnterstützerInnen zur Orientierung, in welcher Höhe sie einen finanziellen Beitrag leisten.

Sobald die Crowdfunding-Kampagne startet, geht es vor allem darum, über laufende und transparente Kommunikation auf diese aufmerk-

sam zu machen und umfassend über das Projektvorhaben und die Entwicklungen bei der Umsetzung zu berichten. Üblicherweise geschieht dies durch einen Projektblog und diverse Social Media Kanäle.

3. Crowdfunding und Beteiligung

Über die Frage der Wirkung digitaler Beteiligung per Mausklick wird etwa im Zusammenhang mit Aktionen wie Kony 2012 immer wieder diskutiert. In ihrem Artikel „Slacktivism und Clicktivism – politische Beteiligung mit einem Klick?!"[5] setzen sich Joerg Eisfeld-Reschke und Leonie Geiger vom Institut für Kommunikation in Sozialen Medien mit den unterschiedlichen Beteiligungsformen in der digitalen Gesellschaft auseinander. Darin heißt es:

> *„Wenn politischer Aktivismus nur im Internet stattfindet, dann wird dies mit dem Begriff Clicktivism beschrieben. (...) Wenn dieser Wirkungsgrad über die Grenzen der digitalen in die analoge Welt hinausgeht, nennt man das Slacktivism. Der Begriff Slacktivism setzt sich zusammen aus den englischen Wörtern «slacker» für «Faulenzer» und «activism» für «Aktivismus».*"

In diesem Zusammenhang schwingt immer auch (berechtigte) Kritik mit, denn „um sich als Clicktivist zu engagieren, bedarf es zunächst keiner großen körperlichen oder geistigen Anstrengung."[6]

Beim Crowdfunding wird jedoch aus der virtuellen Unterstützung plötzlich eine reale, nämlich dann, wenn aufgrund der finanziellen Hilfe ganz konkret Projekte umgesetzt werden können. Dieser Meinung ist auch „Data Scientist" und Blogger Christian Prokopp. In seinem Artikel „Crowd Funding Activism: Put Your Money Where Your «Like' Is»[7] beschreibt er es folgendermaßen:

---

[5] s. http://www.ikosom.de/2012/06/21/slacktivism-und-clicktivism-politische-beteiligung-mit-einem-klick/ (Letzter Aufruf: 31.5.2013)

[6] s. ebd.

[7] s. Prokopp, Dr. Christian (2013): Crowd Funding Activism: Put Your Money Where Your 'Like' Is.

> *„In the Internet age many people utilise technology to spread information, make themselves heard, organise demonstrations, or simply click like to show their support for a cause. The latter is sometimes belittled as the equivalent of a couch potato's self-gratifying response to a pressing issue. It gives you a warm feeling but has no impact. (...) Unfortunately, a million likes won't buy them equipment, pay for materials, or feed them when they spend months of their lives to change something which you, I and so many others agree should be changed. Until now, enter crowd funding."*

Dabei geht es nicht immer nur um die reine Finanzierung eines Projektes,

> *„(...) sondern auch um den Aufbau einer Community, der Vernetzung und Kommunikation mit den Fans bzw. dem Publikum oder dem Testen einer Idee. Der Reiz besteht also neben dem finanziellen Aspekt darin, dass man bereits sehr früh mit den späteren „Kunden" in Kontakt tritt und sich Feedback einholt, um sein „Produkt" (etwa einen Film oder eine Idee für ein Startup) zu verbessern. Heutzutage schätzen es immer mehr Menschen, wenn sie in Entstehungsprozesse mit eingebunden werden und aktiv mitgestalten können."*[8]

4. Von Engagement alleine lässt sich nicht leben

Eine Idee hat man schnell, aber für Aktionismus und nachhaltiges Handeln braucht man Geld, auch wenn es „nur" um den Aufbau einfacher Kommunikationsstrukturen geht.

Das bemerkten auch die Beteiligten der zivilgesellschaftlichen Initiative „IG Demokratie" (www.ig-demokratie.at), deren Ziel eine größtmögliche Einbindung der Österreichischen Bevölkerung in einen angestrebten Demokratiereformprozess (Demokratiekonvent) ist – und starteten eine Crowdfunding-Kampagne. Über die Crowd-

---

[7] www.clickittefaq.com/technology/crowd-funding-activism-put-your-money-where-your-like-is/ (Letzter Aufruf: 31.5.2013)

[8] blog.visionbakery.com/2011/11/crowdfunding-muss-man-eingebettet-in-eine-social-media-strategie-sehen/ (Letzter Aufruf: 31.5.2013)

funding-Plattform Respekt.net[9] sammelte die Initiative bisher insgesamt 2.746,– Euro um administrative sowie kommunikative Tätigkeiten finanzieren zu können. Dazu zählt die Erstellung der Webseite www.ig-demokratie.at, die Betreuung diverser Social Media-Kanäle und die Organisation eines Barcamps[10], das im September in Linz stattfindet. Stefan Schartlmüller, einer der Initiatoren von IG Demokratie, beschreibt seine Erfahrungen mit Crowdfunding auf persönliche Nachfrage im März 2013 folgendermaßen:

> *„Crowdfunding hat mehrere Vorteile. Es finden sich nicht nur InvestorInnen, sondern ein breiterer Kreis an Menschen wird auf das Projekt aufmerksam. Für politische Projekte ist es aktuell gar nicht so einfach Mittel zu lukrieren, auch weil dies mehrere Initiativen gleichzeitig versuchen. Ein Grund mehr sich zu vernetzen!"*

Auch wenn Crowdfunding keine einfache Sache ist, so zahlt es sich dennoch aus, wie Schartlmüller resümiert:

> *„Anfangs war es gar nicht so einfach, Aufmerksamkeit zu erzeugen, aber mit vermehrtem öffentlichem Auftritt wurde die Resonanz immer besser. Positiv hat sich auch der Projektendspurt ausgewirkt. Für die Finanzierung der nächsten Schritte werden wir jedenfalls weiter auf Crowdfunding setzen!"*

Dieses Beispiel zeigt sehr gut, welches Potenzial in Crowdfunding gerade für zivilgesellschaftliche und politische Projekte steckt.

Allerdings fehlt es noch an genügend Vorzeigebeispielen, damit auch andere ProjektinitiatorInnen sich ermutigt fühlen, „die Crowd" direkt anzusprechen und um (finanzielle) Hilfe zu bitten. Eine Plattform, die das ändern möchte, ist reset.org. Sie vernetzt engagierte BürgerInnen und deren Ideen zu Themen wie Klimawandel, Frieden oder Neues Wirtschaften mit Menschen, die sich an ebensolchen Projekten beteiligen möchten.

---

[9] http://www.respekt.net/de/projekte-unterstuetzen/details/projekt/436/ (Letzter Aufruf: 31.5.2013)

[10] http://www.barcamp.at/ParCamp_Linz_2013 (Letzter Aufruf: 31.5.2013)

Zusammenfassend lässt sich festhalten, dass die Möglichkeiten von Crowdfunding zwar bereits von einigen zivilgesellschaftlichen AkteurInnen erkannt wurden und zum Teil genutzt werden, wir allerdings im Bereich des politischen Aktivismus zumindest im deutschsprachigen Raum noch ganz am Anfang stehen. Insofern befinden wir uns in einer Experimentierphase, die dazu führen sollte, konkrete Erkenntnisse in weitere Schritte umzusetzen, damit sich Crowdfunding als fixer Bestandteil im Maßnahmen-Mix zivilgesellschaftlicher Initiativen etablieren kann. Ich denke, wir sind auf einem guten Weg dahin.

5.5. Cyberpeace statt Cyberwar – eine Initiative (Sylvia Johnigk)

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

Keywords: Cybercrime, Cyberpeace, Cyberwarfare, Cybersecurity, Digitale Genfer Konvention, Entgrenzung, Ethical Hacking, Kritische Infrastrukturen, Schadsoftware

EINLEITUNG 287
1. MOTIVATION – WARUM CYBERPEACE? 288
2. CYBERWARFARE-REALITÄT? 289
3. BEKANNTE CYBERWARFARE-ATTACKEN 289
4. FORUM INFORMATIKERINNEN 291
5. KRITIK DES FIFF 291
6. WAS TUN? 293
WEITERFÜHRENDE LINKS 295

Einleitung

Vielfach unbemerkt sind wir ZeugInnen eines seit einigen Jahren stattfindenden Wettrüstens im Cyberspace. Immer mehr Staaten bauen militärische Cyberwarfare-Einheiten auf, die aus IT SpezialistInnen bestehen und dem Zweck dienen, IT Systeme abzusichern oder Systeme von „Feinden“ anzugreifen.

Die Aufrüstung mit offensiven Cyberwaffen erhöht aber das Risiko für die Zivilgesellschaft. Im Zuge der Vernetzung und Digitalisierung der Welt steigen die Abhängigkeit und Verletzlichkeit von IT. Im digitalen Raum lösen sich nationale Grenzen, Verantwortlichkeiten und Zuständigkeiten auf. Jede/r kann Gegner oder Feind sein, jede/r kann Partner oder Betroffene/r sein. Konflikte lassen sich dadurch nur noch schwer eingrenzen – und mittels nationaler Strategien lösen.

Daher braucht es Antworten in einer friedenspolitischen Deeskalation. IT Sicherheitsrisiken können durch Dezentralisierung von kritischen Infrastrukturen, Verringerung von Abhängigkeiten und allgemeiner Verfügbarkeit von defensiver Technologie, z.B. durch Transparenz und freie Lizenzen, reduziert werden.

1. Motivation – Warum Cyberpeace?

Jede/r kann Opfer werden, Staat, Unternehmen oder BürgerIn – gezielt, als Zufallstreffer oder als Kollateralschaden. Endgeräte, die im Internet kommunizieren, waren vor zehn Jahren fast ausschließlich PCs und Notebooks. Heute kommunizieren zusätzlich Smartphones, Tablets, SmartTVs und erste Smarthouses.

Die Gesellschaft als Ganzes ist hochgradig abhängig von Elektrizität, Wasserversorgung, Transportunternehmen, etc. Diese Industrieanlagen sind via SCADA (Supervisory Control and Data Acquisition) im Internet mehr oder weniger absichtlich erreichbar und können von überall angesprochen werden. So sind selbst diejenigen betroffen, die nur mittelbar das Internet nutzen.

„Cyberwaffen“ sind frei verfügbar. Angriffswerkzeuge findet man im Internet, zu Hause oder in der Arbeit. Jedes Endgerät, das mit dem Internet verbunden ist, kann erreicht und geschädigt werden. Cyberwaffen sind billiger als konventionelle Waffen. Die Hemmschwelle, solche Waffen einzusetzen ist niedriger, da potentielle Schäden abstrakt sind. Wissen und Handhabung können „leicht“ angeeignet werden.

Die Standardisierung von Hard- und Software erleichtert und effektiviert Angriffe (anfällige Monokulturen). Komponenten in IT-Produkten kommen von verschiedenen Lieferanten und sind kaum kontrollier- oder nachvollziehbar. Mit der Komplexität der Systeme und Anwendungen wächst die Häufigkeit von Schwachstellen, Fehlkonfigurationen und nicht deterministischem Verhalten.

2. Cyberwarfare-Realität?

Es gibt in rund 140 Staaten Initiativen für den Auf- oder Ausbau militärischer Cybereinheiten, die meisten davon mit offensivem Charakter. Cyberwarfare erscheint aus militärischer Sicht verführerisch:

- Keine Gefährdung der eigenen Soldaten,
- Eine Rückverfolgung zum Aggressor ist nicht eindeutig möglich, Herkunft und Identität kann verfälscht bzw. nicht zweifelsfrei geklärt werden
- „Low hanging fruits“: weiche, zivile Ziele schwächen Gegner
- Angriff ist wesentlich einfacher als Verteidigung
- Die Bundeswehr mischt seit 2009 mit und ist seit 2012 nach eigenen Angaben angriffsbereit[1].

In den letzten Jahren wurde immer häufiger der Begriff Cyberwar benutzt, obwohl es sich bislang noch nicht um kriegerische Handlungen im Sinne der Genfer Konventionen gehandelt hat. Vergleichbare Cyberangriffe können aber zukünftig einen Krieg auslösen oder kombiniert mit anderen Waffen in einem Krieg eingesetzt werden. Völkerrechtlich ist Cyberwarfare bisher nur unzureichend geregelt.

Somit lassen sich die zwischenstaatlichen Attacken der letzten Jahre nur schwer einordnen. Noch schwieriger wird es, wenn die Ausmaße der Schäden erheblicher werden und ein Staat den Wechsel zu konventionellen Waffen vollzieht.

3. Bekannte Cyberwarfare-Attacken

- Bei Titan Rain handelte es sich um Angriffsserien auf US-amerikanische Computersysteme u.a. auf Rüstungskonzerne und

[1] Vgl. http://www.bundesheer.at/truppendienst/ausgaben/artikel.php?id=1318 (Letzter Aufruf: 31.5.2013)

auf die NASA. Diese und weitere Hacking-Attacken auf US-Systeme wurden angeblich nach China zurückverfolgt.

- 2007 fand eine DDos (Distributed Denial of Service) Attacke auf die estnischen Regierungswebseiten statt. Vermutlich handelte es sich um eine politisch motivierte Attacke, basierend auf einem Streit über den Umgang mit einem Denkmal russischer Soldaten.
- 2008 gab es in Georgien (Südossetien) verschiedenste Attacken: Webdefacement, Dos Attacken gegen georgische Regierungsseiten und Medien, um während der kriegerischen Auseinandersetzungen die Informationsverbreitung nachhaltig zu unterbinden.
- 2010: *Stuxnet* ist eine Malware zur gezielten Sabotage von Zentrifugen in der Urananreicherungsanlage in Natanz (Iran). Die geschätzten Entwicklungskosten liegen im siebenstelligen Dollarbereich, es wurden mehrere Zeroday Exploits entwickelt und mehrere Personenjahre Entwicklungs- und Testaufwand aufgebracht. Nach einem Bericht der NYT 2012 war Stuxnet Teil einer mehrjährigen amerikanisch-israelischen Cyberattacke (Operation „Olympic games“).
- 2010/2012: *Flame*, eine klassische Spionagesoftware, späht die befallenen Rechner/Nutzer aus und sammelt Daten. Der Trojaner ist lokal auf den Nahen Osten ausgerichtet und besitzt eine raffinierte Löschfunktion, so dass er nach getaner Arbeit nicht mehr auffindbar ist.
- 2011: *Duqu* basiert (wahrscheinlich) auf dem Stuxnet-Code, er hat keine lokalen Präferenzen, eine Angriffs-/Schadkomponente fehlt. Er späht die befallenen Rechner lediglich aus.
- 2012: der Trojaner *Gauss*, späht im staatlichen Auftrag Bankdaten aus, vor allem in Israel und Libanon, basiert auf Flame, wurde mutmaßlich von den USA und Israel entwickelt.

Dies ist nur eine kleine Auswahl bekannt gewordener Angriffe, die in Zukunft allerdings vermutlich zunehmen werden, wenn ein Umdenken ausbleibt.

4. Forum InformatikerInnen

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e.V.) ist ein Zusammenschluss von Menschen, die sich kritisch mit Auswirkungen des Einsatzes der Informatik und Informationstechnik auf die Gesellschaft auseinandersetzen.

Im 1984 gegründeten FIfF engagieren sich Menschen für eine Technikentwicklung, die die Menschenwürde achtet und die dazu beiträgt, Demokratie, Grundrechte und Frieden zu schützen und weiterzuentwickeln. Sie treten im Rahmen ihrer Berufsethik für ein friedliches Miteinander aller Menschen ein und wollen damit freundschaftliche Beziehungen aller Staaten untereinander fördern.

Die Mitglieder wirken in vielen technischen und nichttechnischen Bereichen der Gesellschaft. Zu ihren Aufgaben zählen Öffentlichkeitsarbeit, Beratung und das Erarbeiten fachlicher Studien. Das FIfF gibt vierteljährlich die Zeitschrift FIfF-Kommunikation heraus und arbeitet mit anderen Bürgerrechtsorganisationen zusammen.

5. Kritik des FIfF

- Durch Cyberwarfare wurde eine neue und gefährliche Rüstungsspirale in Gang gesetzt. Wer Cyberwaffen entwickelt und damit angreift, legitimiert den Einsatz auf der Gegenseite!
- Bei Gegnern, die technisch nicht mithalten, wird die Tendenz zum asymmetrischen Krieg verstärkt. Der Hightech Einsatz provoziert eine Gegenwehr durch Attentate und Guerilla Krieg.
- Die militärischen Sicherheitsinteressen bedrohen auch die Freiheit des Internets und der Gesellschaft. Entwicklung von Sicherheits- und Überwachungstechnologie wird staatlich forciert,

Sicherheitsgesetze und Überwachung werden verschärft, anonyme und freie Kommunikation eingeschränkt und die Erforschung und Offenlegung von Sicherheitsschwachstellen behindert.

- Wir leben in einer entgrenzten Welt. Einzelne Unternehmen arbeiten global und über nationale Ländergrenzen hinaus dennoch in einem Intranet zusammen. Netzwerke und Systeme von internationalen Konzernen werden durch AdministratorInnen in Schwellenländern betreut. Produkte werden an Zulieferstandorten in mehreren Ländern entwickelt und global eingesetzt. Infrastrukturen (Strom, Gas, Öl) werden über nationale Grenzen hinaus produziert, verteilt und konsumiert. Standards werden international entworfen und umgesetzt.
- Diesen internationalen Herausforderungen für die IT Sicherheit werden häufig rein national ausgerichtete Maßnahmen wie das Nationale Cyberabwehrzentrum[2], der Cybersicherheitsrat[3] oder die Allianz für Cybersicherheit[4] entgegen gesetzt.
- Cyberattacken sind nur möglich, wenn Schwachstellen geheim gehalten werden. Schwachstellen, die nicht bekannt sind, können nicht gefixt werden, und sind somit auch vom Gegner ausnutzbar. Besonders prekär: Hat ein nationales Cyberabwehrzentrum eine Cyberwaffe, die auf Schwachstellen basierend entworfen wurde, muss diese Schwachstelle vor Verbündeten geheim gehalten werden, da zu viele Mitwisser die Wahrscheinlichkeit steigern, dass die Schwachstelle bekannt wird und die Cyberwaffe dadurch unbrauchbar wird. Selbst die eigene Zivilbevölkerung oder heimische Wirtschaft kann nicht über das Risiko informiert werden.

---

[2] vgl. http://de.wikipedia.org/wiki/Cyberabwehrzentrum (Letzter Aufruf: 31.5.2103)

[3] s. http://www.cio.bund.de/DE/Politische-Aufgaben/Cyber-Sicherheitsrat/cyber_sicherheitsrat_node.html (Letzter Aufruf: 31.5.2103)

[4] s. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/OffenerBereich/dokumente.html (Letzter Aufruf: 31.5.2103)

- Die US Cybersecurity-Doktrin wurde im Jahr 2011 veröffentlicht (genauer: nur der defensive Teil davon). Problematisch ist die vage Definition eines Angriffs, der demnach die nationale Sicherheit gefährdet: (D)Dos Attacken, Sabotage von militärischen und zivilen Systemen insbesondere kritischen Infrastrukturen, Manipulation und Diebstahl von Informationen, Wirtschaftsspionage, Diebstahl geistigen Eigentums, Hacktivismus.
- Cybercrime und Cyberwarfare werden zu wenig differenziert, weswegen potentiell jeder Cyberangriff als Bedrohungen der nationalen Sicherheit der USA interpretiert werden kann.
- Da sich die USA aufgrund ihrer Defizite bei der Abwehr vorbehalten, auf Cyberangriffe auch konventionell zu reagieren, kann die Unschärfe in der Angriffsdefinition dazu führen, dass mit niedriger Eintrittsschwelle IT-Sicherheitsprobleme in einen physischen Krieg eskalieren.
- Wir halten es für einen Fehler, Aktionen von Einzeltätern und Scriptkiddies als Kriegsgrund zu bewerten. Kriminell motivierte Cyberangriffe finden massenweise täglich statt, ein Krieg wäre damit der Normalzustand. Ein so weit definierter Cyberangriff dürfte nicht zum Bündnisfall für die NATO werden.

6. Was tun?

Das FIfF formuliert folgende Forderungen, die laufend ergänzt und ausgearbeitet werden sollen[5]:

- Verzicht auf Erstschlag und Offensive im Cyberspace: Staaten sollen öffentlich darauf verzichten, Cyberwaffen präventiv zum Angriff einzusetzen.

[5] Auf der Jahrestagung des FIfF in Fulda, die November 2012 stattfand, wurde ein Workshop durchgeführt. Es hat sich eine kleine Gruppe gebildet, hierzu wurde eine E-Mailliste eingerichtet.

- Rein defensive Sicherheitsstrategie: Staaten sollen sich verpflichten, keine Offensivwaffen für den Cyberwar zu entwickeln oder gar einzusetzen.
- Digitale Genfer Konvention: Für die Zivilbevölkerung lebenswichtige Infrastrukturen wie Strom-, Wasser-, Gesundheitsversorgung, etc. dürfen nicht angegriffen werden. Eine Verletzung dieses Grundsatzes soll als Kriegsverbrechen gelten.
- Anerkennung eines Grundrechts auf zivilen Ungehorsam und Onlineprotestformen im Internet: Derartige Aktionen dürfen nicht kriminalisiert werden, geschweige denn als Kriegsgrund herhalten.
- Wirtschaftliche Interessen, wie ein Verstoß gegen Intellectual Properties, sind kein legitimer Kriegsgrund.
- Konventionelle Waffen dürfen nicht als Antwort auf eine Cyberattacke eingesetzt werden.
- Staatliche Stellen, Unternehmen und BürgerInnen müssen zur Offenlegung von Schwachstellen verpflichtet werden (ableitbar aus dem Grundrecht auf Integrität, das der Staat schützen muss).
- BetreiberInnen kritischer Infrastrukturen müssen verpflichtet werden, sich selbst zu schützen, bzw. IT-Systeme sicher zu gestalten, zu implementieren und zu betreiben, anstatt nach dem Staat oder gar dem Militär zu rufen.
- Kompetente, transparente Prüfungen und Tests müssen Voraussetzung für eine Betriebserlaubnis sein.
- Gefordert wird eine Entnetzung und Dezentralisierung kritischer Infrastrukturen (wie z.B. DE-CIX).
- Abrüstung der politischen Sprache: Klare Trennung von Cyberwar, Cyberterror, Cybercrime, ethical Hacking, politischen Protestformen.
- Demokratische Kontrolle, Gewaltenteilung, Parlamentsvorbehalt für Cybersicherheitsstrategien und deren Umsetzung.

Weiterführende Links

Aljazeera (2011) Sentinal Drohne durch iranischen Cyberangriff sabotiert? http://www.aljazeera.com/news/asia/2011/12/20111241599102532.html (Letzer Aufruf 13.4.2013)

David Singer (2012) New York Times zu Stuxnet: Obama Order Sped Up Wave of Cyberattacks Against http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&hp&pagewanted=all (Letzer Aufruf 13.4.2013)

Die Beauftragte der Bundesregierung für Informationstechnik (2011) Cybersicherheitsrat http://www.cio.bund.de/DE/Politische-Aufgaben/Cyber-Sicherheitsrat/cyber_sicherheitsrat_node.htm (Letzer Aufruf 13.4.2013)

Economist (2010) Iranische Cybereinheiten http://www.economist.com/node/16481504?story_id=16481504&source=features_box1 (Letzer Aufruf 13.4.2013)

Heise.de (2011) Nato Libyen http://www.heise.de/newsticker/meldung/Bericht-US-Regierung-erwog-Cyberwar-gegen-Libyen-1362698.html (Letzer Aufruf 13.4.2013)

Heise.de (2012) Super-Spion Flame trug Microsoft-Signatur http://www.heise.de/newsticker/meldung/Super-Spion-Flame-trug-Microsoft-Signatur-1590335.html (Letzer Aufruf 13.4.2013)

Heise.de (2012) Supertrojaner Flame gibt Geheimnisse preis http://www.heise.de/newsticker/meldung/Spionagetrojaner-Flame-gibt-Geheimnisse-preis-1709709.html (Letzer Aufruf 13.4.2013)

Heise.de (2012) Der kleine Bruder des Spronagetrojaners Flame http://www.heise.de/newsticker/meldung/miniFlame-Der-kleine-Bruder-des-Spionagetrojaners-Flame-1731263.html (Letzer Aufruf 13.4.2013)

Heise.de (2012) Saudui Aramco: Cyber-Krieg im Nahen Osten http://www.heise.de/tp/artikel/37/37594/1.html5 (Letzer Aufruf 13.4.2013)

Johnigk, Nothdurft (2012) FIfF-Ko 1/2012 Cyberwarfare Sylvia Johnigk und Kai Nothdurft

https://program.sigint.ccc.de/system/attachments/10/original/FK-1-2012_Cyberwar_v2-1.pdf?1332865716 (Letzer Aufruf 13.4.2013)

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia (CCDCOE) Centre http://www.ccdcoe.org/ (Letzer Aufruf 13.4.2013)

Sandro Gaycken (2011) re:publica XI April 2011 http://archiv.re-publica.de/2011/12/04/cyberwar-und-seine-folgen-fur-die-informationsgesellschaft/ (Letzer Aufruf 13.4.2013)

Sneier on Security (2008) Equity Issue Dilemma http://www.schneier.com/blog/archives/2008/05/dualuse_technol_1.html (Letzer Aufruf 13.4.2013)

Spiegel Online (2011) China, blaue Armee http://www.spiegel.de/netzwelt/web/blaue-armee-elite-hacker-fuehren-cyberwar-fuer-china-a-765081.html (Letzer Aufruf 13.4.2013)

Spiegel Online (2009) Bundeswehr baut geheime Cyberwar Truppe auf http://www.spiegel.de/netzwelt/tech/spionage-und-hackerabwehr-bundeswehr-baut-geheime-cyberwar-truppe-auf-a-606096.html (Letzer Aufruf 13.4.2013)

Spiegel Online (2011) Aktivitäten aus China http://www.spiegel.de/netzwelt/web/online-spionage-us-geheimdienst-will-chinesische-hacker-identifiziert-haben-a-803396.html (Letzer Aufruf 13.4.2013)

Spiegel Online (2012) Bundeswehr meldet sich bereit zum Cyberwar http://www.spiegel.de/netzwelt/netzpolitik/cyberwar-die-bundeswehr-kann-nun-auch-cyberkrieg-a-836991.html (Letzer Aufruf 13.4.2013)

Spiegel Online (2012) Bomben gegen Cyberkrieger http://www.spiegel.de/netzwelt/netzpolitik/cyberkrieg-bomben-gegen-cyberkrieger-a-861002.html (Letzer Aufruf 13.4.2013)

Spiegel Online (2012) Interview mit Droege IRK: Ist Cyberwar ein Krieg? http://www.spiegel.de/netzwelt/netzpolitik/ist-ein-cyberkrieg-ein-krieg-a-841096.html (Letzer Aufruf 13.4.2013)

Spiegel Online (2012) Der Wurm als Waffe http://www.spiegel.de/netzwelt/netzpolitik/experten-suchen-nach-kriegsrecht-fuer-den-cyberwar-a-836566.html (Letzer Aufruf 13.4.2013)

Sueddeutsche.de (2011) Wie gefährlich ist der Stuxnet-Bruder? http://www.sueddeutsche.de/digital/computervirus-duqu-entdeckt-wie-gefaehrlich-ist-der-stuxnet-bruder-1.1168324 (Letzer Aufruf 13.4.2013)

Sueddeutsche.de (2012) Ein Gegenschlag ist nicht legal http://www.sueddeutsche.de/digital/cyberwar-und-voelkerrecht-ein-gegenschlag-ist-nicht-legal-1.1430089 (Letzer Aufruf 13.4.2013)

Sueddeutsche.de (2012) Der Cyberkrieg kann jeden treffen http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-treffen-1.146684 (Letzer Aufruf 13.4.2013)

Telepolis (2011) Malware Befall Nevada Drohensteuerung http://www.heise.de/tp/blogs/8/150592 (Letzer Aufruf 13.4.2013)

The Jerusalem Post (2011) Israel Cyberdefense Einheit http://www.jpost.com/Defense/Article.aspx?id=221116

US Militärdoktrin des Department of Defense (2010) Strategy for operating in Cyberspace http://www.defense.gov/news/d20110714cyber.pdf (Letzer Aufruf 13.4.2013)

Wikipedia – Großbrittanien: GCHQ http://en.wikipedia.org/wiki/GCHQ (Letzer Aufruf 13.4.2013)

Wikipedia – Nationales Cyberabwehrzentrum der BRD (NCAZ) http://de.wikipedia.org/wiki/Cyberabwehrzentrum (Letzer Aufruf 13.4.2013)

Wikipedia – Israel Gaza Konflikt http://en.wikipedia.org/wiki/Media_and_the_Gaza_War (Letzer Aufruf 13.4.2013)

Wikipedia – United States Cyber Command USCYBERCOM http://en.wikipedia.org/wiki/USCYBERCOM (Letzer Aufruf 13.4.2013)

Wikipedia – Verdacht auf Angriff aus Russland auf Estland http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia (Letzer Aufruf 13.4.2013)

Wikipedia – Cyberattacke auf Georgien http://en.wikipedia.org/wiki/Cyberattacks_during_the_2008_South_Ossetia_war (Letzer Aufruf 13.4.2013)

Wikipedia – Titan Rain http://en.wikipedia.org/wiki/Titan_Rain (Letzer Aufruf 13.4.2013)

Die Autor*I*nnen

Julian Ausserhofer (http://ausserhofer.net) ist wissenschaftlicher Mitarbeiter im Web Literacy Lab des Instituts für „Journalismus und Public Relations (PR)“ der FH JOANNEUM Graz und promoviert am Institut für Publizistik- und Kommunikationswissenschaft der Universität Wien. Seine Forschungsthemen sind Social Media, Open (Government) Data sowie Datenjournalismus. Ausserhofer lebt in Wien und Graz, visualisiert elektronische Musik und twittert als @boomblitz.

Michael Bauer (vibe.at / AK Vorrat / OKFN) ist biomedizinischer Wissenschafter, Hacker und Aktivist. Seine geheime Leidenschaft ist Freiheit im digitalen Zeitalter.

Wolfgang Gumpelmaier (Mag.) ist selbstständiger Digital Media Consultant (http://gumpelmaier.net), Blogger, Autor und Vortragender. Er beschäftigt sich mit Themen wie Social Film Marketing, Crowdsourcing und Online-Kollaboration. Als Team-Mitglied von ikosom.de hat er sich dem Themenbereich Crowdfunding verschrieben und spürt als TrendScout bei TrendOne aktuellen Entwicklungen des digitalen Lebens nach (http://www.trendone.de). 2011 gründete er mit KollegInnen die Plattform www.ununi.tv, die 2013 als „Crowd University for Modern Life“ neu gelauncht wird. (Foto-Credit: Alexander Kühn)

Sylvia Johnigk studierte an der TU-Berlin Informatik mit dem Schwerpunkt Datenschutz und Softwaretechnik. Seit 17 Jahren im Themenbereich IT-Sicherheit und Datenschutz tätig, ist sie seit 2009 selbständig und berät Großunternehmen. Nebenbei engagiert sie sich im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung FIfF e.V. und ist seit 2009 Mitglied des Vorstands.

Matthias C. Kettemann (Mag. Dr., LL.M. [Harvard]) ist Universitätsassistent und Lektor am Institut für Völkerrecht und Internationale Beziehungen der Karl-Franzens-Universität Graz und Co-Chair der http://internetrightsandprinciples.org Internet Rights & Principles Coalition. Letzte Veröffentlichung: *The Future of Individuals in International Law. Lessons from International Internet Law* (Eleven, 2013). E-Mail: matthias.kettemann@gmail.com, Blog: http://internationallawandtheinternet.blogspot.com.

Thomas Kreiml (Mag.) ist Soziologe und Gewerkschafter mit multipler Schwerpunktsetzung. Nach mehrjähriger Tätigkeit in Projekten zur Bildungs- und Arbeitsmarktforschung beschäftigte er sich ab 2008 in der Gewerkschaft der Privatangestellten – Druck, Journalismus, Papier intensiv mit Fragen der Arbeitsorganisation und des (betrieblichen) Datenschutzes. Seit 2011 ist er in der GPA-djp Bildungsabteilung nicht nur für Bildungspolitik zuständig, sondern arbeitet auch an Initiativen und Projekten zu gewerkschaftlicher Bildung, gewerkschaftspolitischen Entwicklungsfeldern und politischer Mitbestimmung.

Andreas Krisch (Mag.) ist geschäftsführender Gesellschafter der mksult GmbH (http://www.mksult.at) und im Bereich der technischen Datenschutzberatung tätig. Er ist Wirtschaftsinformatiker, zertifizierter Datenschutzbeauftragter sowie technischer Experte für das Europäische Datenschutzgütesiegel EuroPriSe. Weiters: Betreiber von http://www.unwatched.org, Präsident von European Digital Rights http://www.edri.org, Obmann von VIBE!AT www.vibe.at, Berater der Europäischen Kommission im Rahmen der Expertengruppen zu RFID und dem Internet der Dinge sowie Gründungs- und Vorstandsmitglied des Arbeitskreis Vorratsdaten Österreich http://akvorrat.at.

Clara Landler (Mag.[a]) arbeitet als wissenschaftliche Mitarbeiterin am Zentrum für E-Governance der Donau-Universität Krems. In diesem Kontext organisierte und betreute sie die Co:llaboratoryAT-Initiative *Menschenrechte und Internet* zum vorliegende Band. Das Beobachten von Inklusions- und Exklusionsmerkmalen, die Teilnahmemöglichkeiten stets umrahmen, sind ihr begleitendes Interesse in allen thematischen Belangen.

Joachim Losehand (M.A., Dr. phil.) ist Kulturhistoriker, lebt und arbeitet in Wien zu digitaler Kultur, Medien-, Immaterialgüterrecht im 21. Jahrhundert, ist koordinierender Leiter des Studienprojekts *Die rechtliche Situation von Online-Rundfunk und Medienarchiven in Österreich und Möglichkeiten ihrer Verbesserung* im Verband Freier Radios Österreich (VFRÖ) sowie Koordinator der Veranstaltungsreihe *ur21* im Verein für Internet-Benutzer Österreichs (VIBE!AT).

Eva Jana Messerschmidt hat in Freiburg im Breisgau Rechtswissenschaften studiert. Im Rahmen des Referendariats arbeitete sie u.a. am Ludwig Boltzmann Institut für Menschenrechte in Wien (BIM) sowie nach dem Zweiten Staatsexamen als externe Mitarbeiterin vom ao. Univ.-Prof. Dr. Hannes Tretter und als juristische Mitarbeiterin in der Rechtsanwaltskanzlei Lansky, Ganzger & Partner in Wien. Zur Zeit promoviert sie zum hier vorgestellten Thema an der Universität Wien.

Christian Möhlen studierte Rechtswissenschaften an der Albert-Ludwigs-Universität Freiburg i.Br. und der Universidad de Barcelona, anschließend Referendariat mit Stationen in Frankfurt, Berlin und Kosovo. Tätigkeit als juristischer Berater für die Weltbank in Washington und für verschiedene Unternehmen aus dem Energiesektor. Seit 2011 rechtswissenschaftliches Doktoratsstudium an der Universität Wien. Dissertationsvorhaben im Bereich Menschenrechte und Internet (Betreuer Prof. Hannes Tretter / Ludwig-Boltzmann-Institut).

Tassilo Pellegrini (Prof. [FH] Dr.) studierte Handelswissenschaften, Kommunikationswissenschaft und Politologie. Seine Forschungsschwerpunkte liegen an der Schnittstelle von Medienökonomie, -technologie und -regulierung unter besonderer Berücksichtigung neuer Wertschöpfungsformen. Er ist Mitgründer der Semantic Web Company in Wien und seit 2009 Professor am Department Medienmanagement der FH St. Pölten.

David Röthler (Mag.) ist studierter Jurist und arbeitet als Berater für Social Media und EU-finanzierte Projekte. Sein besonderes Interesse gilt innovativen Modellen der Partizipation in der Politik, bei der Generierung von Ideen (Crowdsourcing) oder der Finanzierung von Projekten (Crowdfunding). Er ist langjähriger Referent und Lehrbeauftragter bei zahlreichen öffentlichen und privaten Bildungseinrichtungen. Er ist Mitgründer und Geschäftsführer des Beratungsunternehmens PROJEKTkompetenz.eu. Weiters ist er Mitglied von ikosom.de – Institut für Kommunikation in sozialen Medien, Berlin

Markus Sabadello arbeitet mit vorwiegend amerikanischen Startups an verschiedenen Technologien rund um Identität und persönliche Daten im Internet. Er betreibt selbst ein Open-Source Projekt namens Project Danube (https://projectdanube.org), welches sich unter anderem mit der Entwicklung der FreedomBox und anderen alternativen, dezentralen Kommunikationssystemen beschäftigt.

Stephan Schlögl ist wissenschaftlicher Projektmitarbeiter am Institut für Publizistik- und Kommunikationswissenschaft der Universität Wien und bloggt unter politicipation.net.

Judith Schoßböck (Mag.[a]) ist wissenschaftliche Mitarbeiterin am Zentrum für E-Governance der Donau-Universität Krems. Sie ist redaktionell für das Open Access-Journal JeDEM.org verantwortlich und Mitglied der interdisziplinären Internetforschungsgruppe an der Universität Wien. Zu ihren Forschungsschwerpunkten zählen elektronische Beteiligung, Online-Aktivismus und soziale Bewegungen, Informationsfreiheit und digitale Utopien.

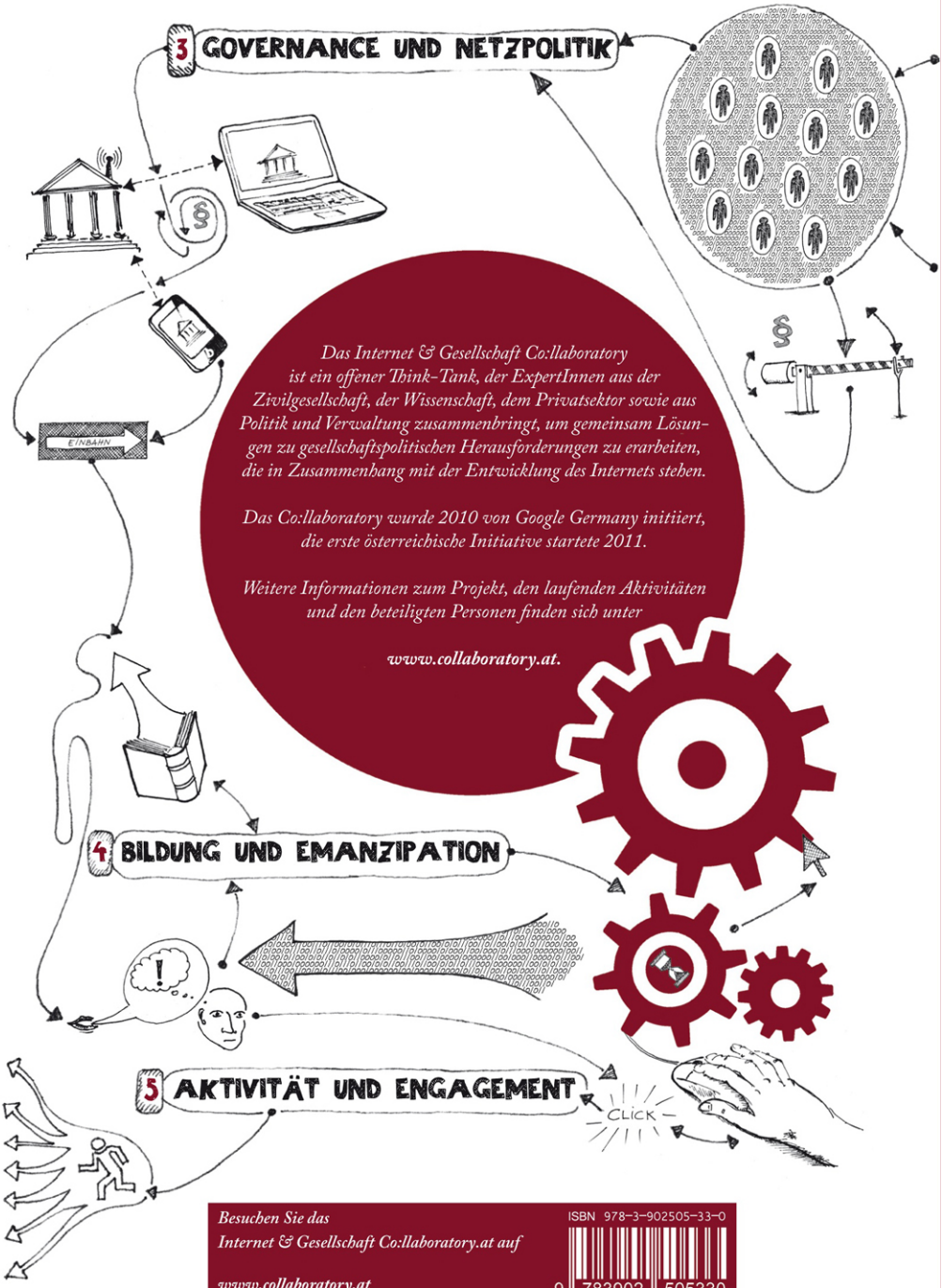
Viktor Szabados (Mag.) war während der ungarischen EU-Ratspräsidentschaft Verbindungsperson des European Youth Forum und Leiter der Arbeitsgruppe *Strukturierter Dialog mit Jugendlichen*. Er wurde als Facilitator und Trainer des Jugendforums der Budapest Conference on Cyberspace und der Europarat-Trainingsreihe von Jugendlichen zur Bekämpfung von Hassreden beauftragt. Weiters: Gründer der Gruppe *Internet gehört allen* in Ungarn, Mitglied der europäischen FYEG Digital Rights Arbeitsgruppe, Mitglied in der Steering Committee der IRP Coalition.

Leonie Maria Tanczer (B.A.) studierte an der Universität Wien und University of Limerick Politikwissenschaft (Forschungsschwerpunkt Gender Studies, Bachelorarbeit zum Post-Gender Diskurs der Piratenpartei Österreich). Seit 2012 im Masterstudium Politische Psychologie (MSc.) an der Queen's University Belfast, setzt sie sich in ihrer Abschlussarbeit mit Geschlechterbildern in der HacktivistInnen-Szene auseinander. Weiters: Mitorganisatorin der FrauenFrühlingsUni 2013, Mitinitiatorin des Netzfeministischen Biers in Wien (#nfbw).

Christof Tschohl (Ing. Dr.) hat seinen wissenschaftlichen Schwerpunkt in der Erforschung der Bedeutung der Grund- und Menschenrechte in der digitalen Informationsgesellschaft. Als Ingenieur der Nachrichtentechnik und promovierter Jurist kombiniert er dabei aktuelle technische Entwicklungen mit verbundenen Fragen der (Grund-) Rechte, insbesondere zur Entwicklung innovativer *Privacy by Design*-Konzepte. Aktuelle Funktionen: Wissenschaftlicher Leiter des Research Institute AG & Co KG, Of-Counsel am Ludwig Boltzmann Institut für Menschenrechte (BIM), Ao. Mitglied der Fachgruppe Grundrechte der österreichischen Richtervereinigung, Lektor an der Donau Universität Krems und an der Universität Wien und Gründungs- und Vorstandsmitglied des „Arbeitskreis Vorratsdatenspeicherung Österreich" (http://AKVorrat.at).

Hans Christian Voigt (Mag.) ist Soziologe aus Wien mit besonderem Interesse für Bedingungen der Dissidenz in sozialen Systemen. 2006 setzt er sein erstes Wiki und später Blog auf und beginnt sich praktisch mit Möglichkeiten betrieblicher Gegenöffentlichkeiten, mit Wissensmanagement in selbstorganisierten Netzwerken und mit Organisationsentwicklung politischer Initiativen zu beschäftigen. Herausgeber von *Soziale Bewegungen und Social Media. Handbuch für den Einsatz von Web 2.0* (Wien 2011).

Heinz Wittenbrink unterrichtet Online-Journalismus und Soziale Medien am Institut für Journalismus und PR der Fachhochschule Joanneum in Graz, wo er seit 2010 das *Web Literacy Lab* leitet. Zuvor arbeitete er nach einem geisteswissenschaftlichen Studium lange in Verlagen und Web-Agenturen. Seine Interessenschwerpunkte sind Schriftlichkeit im Web und Content-Strategie. Wittenbrink hat Bücher zu Markup-Sprachen verfasst; er bloggt (https://wittenbrink.net/lostandfound) und twittert (@heinz).



Das Internet & Gesellschaft Co:llaboratory ist ein offener Think-Tank, der ExpertInnen aus der Zivilgesellschaft, der Wissenschaft, dem Privatsektor sowie aus Politik und Verwaltung zusammenbringt, um gemeinsam Lösungen zu gesellschaftspolitischen Herausforderungen zu erarbeiten, die in Zusammenhang mit der Entwicklung des Internets stehen.

Das Co:llaboratory wurde 2010 von Google Germany initiiert, die erste österreichische Initiative startete 2011.

Weitere Informationen zum Projekt, den laufenden Aktivitäten und den beteiligten Personen finden sich unter

www.collaboratory.at.

Besuchen Sie das Internet & Gesellschaft Co:llaboratory.at auf

www.collaboratory.at

ISBN 978-3-902505-33-0
9 783902 505330