HEINRICH BÖLL STIFTUNG
BILDUNG + KULTUR

BAND 8

#public_life

Digitale Intimität, die Privatsphäre und das Netz

#PUBLIC_LIFE

HEINRICH BÖLL STIFTUNG
SCHRIFTENREIHE ZU BILDUNG UND KULTUR
BAND 8

#public_life

Digitale Intimität, die Privatsphäre und das Netz

Hrsg. von der Heinrich-Böll-Stiftung

#public_life
Digitale Intimität, die Privatsphäre und das Netz
Herausgegeben von der Heinrich-Böll-Stiftung 2011
Band 8 der Reihe Bildung und Kultur

Redaktion: Simon Edwin Dittrich
Gestaltung: graphic syndicat, Michael Pickardt (nach Entwürfen von blotto Design)
Coverabbildung: Axel Raidt
Druck: agit-druck

ISBN 978-3-86928-052-3

Heinrich-Böll-Stiftung, Schumannstraße 8, 10117 Berlin
T +49 30 28534-0 **F** +49 30 28534-109 **E** info@boell.de **W** www.boell.de

INHALT

VORWORT

Die Grenze zwischen der Sphäre des Privaten und der des Öffentlichen hat für liberal-demokratische Gesellschaften konstitutive Bedeutung: Wo alles öffentlich ist, gibt es keine Freiheit – es fehlt der Raum, wo wir als Individuen allein oder als Gruppe im Leben und Sterben nur uns selbst gehören, eigenwillig sein dürfen und uns nicht rechtfertigen müssen. Und wo alles privat ist, gibt es keine politische Freiheit, wo wir als Citoyens einer heterogenen Gesellschaft verhandeln, was über den Nahbereich hinaus alle angeht und auf direktem oder repräsentativem Wege von allen mit Mehrheit beschlossen werden muss. Wie weit das Private das Öffentliche begrenzen sollte und umgekehrt, das war seit Beginn der bürgerlichen Gesellschaft strittig und fand historisch höchst unterschiedliche Antworten, in denen zwei große Traditionen zum Ausdruck kommen. Auf der einen Seite betont die liberal-individualistische Tradition den Vorrang der individuellen Freiheit der Person als Schutzanspruch der Freien und Gleichen gegen ungerechtfertigte Herrschaft und Kontrolle. Die liberal-individualistische Tradition sucht die Grenzen des Staates und des Öffentlichen zu bestimmen. Ihr steht auf der anderen Seite eine hegelianisch-kommunitäre Tradition gegenüber, die die Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person betont. Das Recht auf Privatheit ist hier eher das Ergebnis des im Streit der Standpunkte erarbeiteten politischen Urteils, wo die Wahrnehmung der individuellen Freiheit als nicht mehr gesellschaftsdienlich und solidaritätstauglich beurteilt wird, wo also die Grenzen des Privaten erreicht sind und im öffentlichen Interesse ein Recht auf Auskunft, Offenlegung und Intervention in die Sphäre des Privaten gerechtfertigt werden kann.

Klassische Felder, in denen der Streit über die Grenzen des Privaten und des Öffentlichen ausgetragen wird, sind die Beziehungen der Geschlechter, sind Elternrechte, aber auch Rechte wie die informationelle Selbstbestimmung. So werden Grenzen des Privaten in Paarbeziehungen und Familien heute dort gezogen, wo der Staat eine Art «Privatversagen» diagnostiziert und den Auftrag zur Intervention erhält. Das Recht, sich nicht rechtfertigen zu müssen, wird als Macht der De-Thematisierung ungerechtfertigter Herrschaftsbeziehungen zwischen den Geschlechtern kritisiert, es werden Anreize gesetzt, um Väter zur Kindererziehung zu bringen, und es werden Sachleistungen geboten, um das Erziehungsverhalten von Eltern zu beeinflussen, denen man eine dem öffentlichen Interesse dienliche Kompetenz nicht zutraut. Ähnlich verhält es sich mit dem Anspruch auf informationelle Privatheit, die das Bundesverfassungsgericht im Urteil über die Volkszählung von 1983 als individuelles Freiheitsrecht gegen behördliche Ausforschung gestärkt und mit dem Hinweis auf die Kommunikati-

onsbedürftigkeit der Person zugleich begrenzt hat. Die informationelle Freiheit kann und soll nur in kommunikativer Gemeinschaft mit anderen wahrgenommen werden, sagt das Verfassungsgericht in hegelianisch-kommunitärer Tradition. Diese Freiheit der informationellen Selbstbestimmung ist nicht nur ein Schutzrecht gegen den Staat, sondern ebenso eine gesellschaftliche Institution, so wie die Meinungsfreiheit, die Versammlungsfreiheit, die Religionsfreiheit oder die Freiheit der Erziehung der Eltern.[1] Diese Freiheitsrechte werden nicht nur in Gesellschaft mit anderen ausgeübt, sie enthalten auch den Auftrag an den Gesetzgeber wie an die Individuen, dass die Meinungsäußerung, die kommunikative Selbstbestimmung oder der eigensinnige Erziehungsstil im Interesse der Entfaltung einer Gesellschaft der Freien und Gleichen – eben im öffentlichen Interesse – erfolgen sollen.

Das ist ein starker Anspruch, der sich von einem ängstlichen Liberalismus, der sich gänzlich auf Rechtsstaat und individuelle Freiheit zurückzieht, deutlich unterscheidet. Die liberal-individualistische Tradition muss (in den Grenzen der Verfassung und der allgemeinen Sittlichkeit) jedwede Form der Meinungsäußerung oder der Preisgabe von Informationen im Netz als für sich gerechtfertigten Ausdruck individueller Präferenzen akzeptieren. Die hegelianisch-kommunitäre Tradition muss das nicht. Sie unterscheidet zwischen Beiträgen, die wertvoll sind, weil sie in Streit, Überzeugung und Überredung zur Entfaltung einer Gesellschaft der Freien und Gleichen beitragen, und solchen, die unbedeutend sind, weil sie dies nicht tun, wie auch solchen, die schädlich sind und die öffentliche Intervention rechtfertigen.

Wo es um versagende Familien geht, mag dieser starke Anspruch akzeptabel sein. Aber ist er es auch, wenn es um das Nutzerverhalten im Internet geht? Zwar spielt bei den jüngeren wie den älteren Internetnutzern die Sorge um den Datenschutz als Teil des Schutzes der Privatsphäre noch eine große Rolle.[2] Doch davon abgesehen geht der Trend heute zum Öffentlichen. Post-Privacy scheint angesagt, und in den meisten Debattenbeiträgen wird dies mehr oder weniger bewusst durch Rückgriff auf Argumente der liberal-individualistischen Tradition begründet. Technische Möglichkeiten in Verbindung mit individuellen Präferenzen der Nutzer werden als ein unwiderstehlicher gesellschaftlicher Trend gedeutet, dem gegenüber die Gesellschaft die Bringschuld habe, sich mit ihm zu befassen und sich ihm anzupassen. Die liberal-individualistische Argumentation befürwortet diesen Trend und unterstützt ihn, indem sie sich neben Datenschutz für gleichen Zugang und Zensurfreiheit einsetzt – unbestritten wichtige Ziele. Aber kann der Trend zum Öffentlichen in der Gestalt der digitalen Öffentlichkeit auch als Fortschritt der Entfaltung einer Gesellschaft der Freien und Gleichen gedeutet werden? Hierzu einige wenige Beobachtungen und Wertungen:

---

1 Siehe hierzu Ulrich K. Preuss: «Der Freiheitsbegriff des Grundgesetzes». *Freiheit. Hoffnung, Anspruch, Herausforderung.* Reihe Demokratie, Bd. 17. Hg. Heinrich-Böll-Stiftung. Berlin 2009, S. 9-15.

2 Vgl. Andreas Busch: «Kein Ende der Privatheit». WZB-Mitteilungen, Heft 120, 6/2008, S. 26-29.

Rückzug ins Öffentliche

Was ist davon zu halten, dass immer mehr Menschen ihr Konsumverhalten, ihre sexuellen Vorlieben, das Innere und Äußere ihrer Wohnung und ihre Meinung zu politischen Fragen im Internet auf Websites und Blogs veröffentlichen? Und was davon, dass Menschen, die ihr Haus nicht auf Google-Street veröffentlicht sehen wollen, von anonymen Aktivisten denunziert und bloßgestellt werden? Was hier öffentlich genannt wird, ist das veröffentlichte Private. Die Verflüssigung der Grenzen zwischen dem Privaten und dem Öffentlichen, seit den 68er-Jahren eine Forderung zur Durchsetzung einer Gesellschaft der Freien und Gleichen, ist ein «Rückzug ins Öffentliche» und hat, wie es in der Ankündigung einer Performance der Berliner Sophiensaele heißt, «die Welt in eine überdimensionale Häkeldecke verwandelt». Wie das Private die Öffentlichkeit durchdringt, hat Richard Sennett bereits in seinem Buch *Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität* (dt. 1986, engl. 1977) beschrieben. Er zeichnet darin den Weg zur intimen Gesellschaft nach, in der das Private immer stärker das Öffentliche überlagert. Sennett beschreibt nicht nur, er kritisiert auch vom Standpunkt einer Idee des Öffentlichen als Raum des Politischen, den es durch Wiederbesinnung auf die Rollenförmigkeit und Aspekthaftigkeit des öffentlichen Auftritts zu stärken gelte.

Wie kommt es zu diesem Trend der Veröffentlichung des Privaten? Sennett und andere Kritiker sehen darin das Resultat der Individualisierung, die gleichbedeutend ist mit dem Verlust der Einbettung der Person in eine politisch bewusste Klasse, an der die Individuen Orientierung finden angesichts der Fülle tagtäglich zu treffender Wahlentscheidungen. Die orientierende Kraft der Klasse scheint heute, da auch Presse und Fernsehen ihre an die Knappheit der Kanäle gebundene Zentralstellung als orientierende Leitmedien verlieren, ersetzt zu werden durch die in sozialen Netzwerken gewonnenen «Freunde», denen die Aufgabe zugedacht wird, das Gelingen des einsamen eigenen Lebens intersubjektiv zu bezeugen – oder auch in Gestalt anonym verbreiteter Gerüchte zu beschädigen.

Politische Öffentlichkeit

Soziale Netzwerke formen Öffentlichkeiten. Doch was leisten sie für die politische Öffentlichkeit, wie tragen sie zur Verhandlung der Dinge bei, die alle angehen und mit Mehrheit beschlossen werden sollen? Großartiges, das steht außer Frage, wo es um den Widerstand gegen staatliche Zensur, Geheimpolitik, Intransparenz und Unterdrückung geht. Das haben die Revolutionen im Maghreb und in Ägypten eindrucksvoll gezeigt, gleichviel ob sie nun als Internetrevolutionen oder als vom Internet unterstützte Revolutionen zu bewerten sind. Das soziale Netz ist stark, wenn es um Polarisierung geht. Gegen den Feind, den Diktator oder den Gegner, den Parteigänger der Anderen, vermag es in noch nie gesehener Weise zu mobilisieren. Was den konstruktiven Part angeht, den Austausch von Informationen und Meinungen im Prozess der Deliberation, die zu einem gerechten

gemeinwohlverträglichen Ergebnis gelangen soll, ist Skepsis und Kritik angezeigt. Denn soziale Netzwerke, Blogs, Twitter etc. folgen einer Logik der Schwarmintelligenz: sie koordinieren und führen dezentral verstreutes Wissen zusammen und machen es als kollektive Intelligenz nutzbar. Das Problem ist jedoch, so Cass Sunstein in «Republic 2.0» (2007), dass in diesem kollektiven Wissen das gemeinsame Wissen allzu oft die Oberhand gewinnt über das heterogene Wissen der anderen, das abgedrängt oder erst gar nicht zur Kenntnis genommen wird. Sunsteins These ist, dass der politische Diskurs in den sozialen Netzwerken nicht wesentlich über die Freiheit der Wahl von Konsumenten hinauskommt. Über 90 Prozent der von ihm untersuchten 1400 Blogs würden nur auf gleichgerichtete im Netz zugängliche Informationen verweisen und auf diese Weise sich selbst verstärkende Echoräume einer fragmentierten Öffentlichkeit schaffen. Die politische Öffentlichkeit der Gesellschaft der Freien und Gleichen hingegen geht von einer heterogenen Bevölkerung einander fremder Individuen aus, denen es nicht genügt, als Konsumenten Präferenzen zu haben, sondern die sich als Citoyens der Zumutung stellen, in der nicht-gewählten und ungeplanten Begegnung mit den Argumenten und Erfahrungen anderer Citoyens Präferenzen zu erarbeiten und zu geteilten Mehrheiten zu kommen. Wie muss eine digitale Öffentlichkeit organisiert werden, die solchen Ansprüchen genügen können soll? Kann sie, soll sie eine öffentliche Institution der Selbstentfaltung der Freien und Gleichen sein – durch selbstorganisierte Nutzungsformen unterschieden von der endlosen Konsumwelt privater Wahlentscheidungen?

Die Beiträge der vorliegenden Aufsatzsammlung loten vor dem Hintergrund der digitalen Drift die Grenzverschiebungen zwischen Privatheit und Öffentlichkeit neu aus. Den Widerspruch zwischen Positionen, die an Privatheit, Datenschutz und Kontrollanspruch festhalten, und radikalen Positionen der Post-Privacy scheuen sie dabei nicht. Und mit Recht. Denn sie bewegen sich selbst im Feld der öffentlichen Debatte, die vielfältig ist und widersprüchlich und die uns dann zu guten und besseren Ergebnissen führt, wenn wir uns auch den Zumutungen der Andersdenkenden aussetzen und lernbegierig bleiben.

Berlin, im März 2011

Dr. Andreas Poltermann
Leiter der Abteilung Politische Bildung Inland
Heinrich-Böll-Stiftung

JAN ENGELMANN

Bühnenarbeit im Public Life. Eine Einleitung

Das Web 2.0 verändert unsere Vorstellungen von dem, was als Privatsache oder öffentliche Angelegenheit zu gelten hat, auf dramatische Weise. Die gute Nachricht lautet: Diese Verunsicherung hat es hat es auch ohne die technischen Medien immer schon gegeben. Die schlechte Nachricht ist: Wir müssen den Wandel zur digitalen Öffentlichkeit aktiv mitgestalten, ansonsten droht uns eine Tragödie.

Fast jeder kennt diese Situation: der Großraumwagen eines ICE, irgendwo in Deutschland. Die meisten Passagiere sind vertieft in ihre Zeitungslektüre, eine rüstige Rentnertruppe kloppt Skat, auf dem Gang schreit ein Kind. Und nebenan versucht ein Schnurrbartträger aus dem mittleren Management verzweifelt, seinen Vortrag bei einer Klausurtagung zu retten. Ein Fräulein Soundso wird in nervösem Tonfall dazu angehalten, doch endlich die verdammte Powerpoint-Präsentation auf das Smartphone zu senden. Und da das nicht klappt, auch nach dem vierten, fünften Mal nicht, steigert sich das Lamento des öffentlichen Business-Darstellers so langsam ins Kinskihafte. Man wird Zeuge eines grandiosen Scheiterns, bedauert heimlich die arme Sekretärin, die nun die Folgen einer mangelhaften Sitzungsvorbereitung ausbaden muss. Dass ihr verärgerter Chef und sein anstrengendes Always-Online-Getue nun den halben ICE Gutenberg beschäftigen, weiß sie nicht. Der Rest des Wagons fixiert peinlich berührt die neue Ausgabe des Mobil-Magazins oder stülpt irgendwann entnervt die Kopfhörer über: eine Kapitulation vor dem Terror der Intimität, das sattsam bekannte Fremdschämen in einer tagtäglichen Situation der akustischen Belästigung.

Man muss sicher kein Kulturwissenschaftler sein, um zu bemerken, dass der Mobilfunk eine völlig neue Qualität des Sozialen mit sich gebracht hat. Einstmals nicht-öffentliche Gesprächssituationen drängen auf die große Bühne, baden im heimlichen Applaus oder werden, mit der Faust in der Tasche, von der Kritik vernichtet. Liebesschwüre vollziehen sich nicht mehr unter zwei, sondern unter Dutzenden. Teppichmuster-Absprachen nicht als Szenen einer Ehe, sondern als kollektives Voting. Heimliche Absprachen zur nächsten Fraktionsabstimmung nicht im Flüsterton, sondern als Ansage mit offenem Visier. Der digitalen «Informationsgesellschaft» (Sie erinnern sich?) sind zunehmend jene Orte abhanden gekommen, die überhaupt noch als Refugien und Fluchtorte der Abgeschirmtheit

gelten können. Stattdessen finden die meisten sozialen Vollzüge in einer performativen Leistungsschau der Allbetroffenheit statt, als nicht enden wollendes, vernetztes Parlando, CC to all. Willkommen im «public life».

Man muss vielleicht Kulturhistoriker sein, um zu wissen, dass vieles von dem, was wir heute für unangemessen oder zudringlich halten, in früheren Zeiten völlig normal war. Mittelalterliche Märkte waren exzessive Kontaktzonen, sowohl akustisch, taktil wie olfaktorisch. Der absolutistische Herrscher empfing seine Gäste auf dem Klo, wenn es ihm danach beliebte. Mit dem bürgerlichen Zeitalter entstanden neue Einhegungsversuche und Distanzgebote, die – so will es die lange vorherrschende Interpretation – einen «Prozess der Zivilisation» (Norbert Elias) einleiteten. Die meisten Tabuisierungen betrafen den Körper, seine Unversehrtheit und Integrität. In jeder Gesellschaftsform, und war sie noch so klein, wurden Vereinbarungen dafür notwendig, was im privaten Verfügungsraum möglich und im öffentlichen Repräsentationsraum zulässig war. Wie historisch kontingent solche Verabredungen sind, zeigt der interkulturelle Vergleich: Während etwa in Schweden das jeweilige Jahreseinkommen jedes Bürgers offengelegt wird, bewegt sich in Deutschland der ausgehandelte Lohn (mit Leistungszulagen) ungefähr auf der Ebene eines Staatsgeheimnisses. Die Wandelbarkeit unseres Bildes von «Privatsachen» und «öffentlichen Angelegenheiten» wird spätestens dann offenbar, wenn man kulturelle Praktiken von heute auf die Usancen der Vergangenheit bezieht: So hätte etwa die hoch entwickelte Briefkultur im 19. Jahrhundert die einfache Replizierbarkeit in der elektronischen Kommunikation als anstößig empfunden, weil dem singulären, empfindsamen Dialog zwischen zwei Personen eine hohe Wertschätzung zukam.

Die aussterbende Kunst der Sphärentrennung

Mit der Mediatisierung der sozialen Kommunikation im 20. Jahrhundert kam die Vorstellung von klaren Sphärentrennungen zunehmend unter Druck. Das Radio und später das Fernsehgerät wurden zu Mittlern zwischen der sozialen Umwelt und dem heimischen Wohnzimmer, waren als Push-Medien von Information aber noch nicht auf ein Hin und Her der Übertragungswege, die Schaffung eines Kommunikationsnetzes angelegt. Allein das Telefon, jener «unwiderstehliche Eindringling» (Marshall McLuhan) in die zwischenmenschliche Kommunikation, war von Grund auf darauf entworfen, in seiner Rückkanalfähigkeit neben sozialen Beziehungen auch imaginäre Selbstverhältnisse zu ermöglichen. Es tat dies aufgrund seiner paradoxen Leistung, Nähe via Distanz, Einheit in Zweiheit herzustellen. Dass das Internet dieses Potenzial nun in Richtung eines Many-to-Many radikalisiert hat, gehört zu den interessantesten Entwicklungen der Mediengeschichte.

Heute kann von einer umfassenden medialen Durchdringung des öffentlichen Raums gesprochen werden: GPS-fähige Handys verraten den Aufenthaltsort des besten Freundes, abgesetzte Tweets via Twitter empfehlen einen Witz, einen Zeitungsartikel oder eine Revolution. Schon arbeiten Unternehmen an der

Kombination aus Geolocation-Tools und Formen der biometrischen Bilderkennung, die ganz neue Möglichkeiten bieten werden, Schutzräume zu durchdringen und Distanzgrenzen zu überwinden. Die eingeübte soziale Mechanik des Innen und Außen, die Trennung zwischen *private* und *public* geht vor dem Hintergrund einer «Emergenz digitaler Öffentlichkeiten» (Stefan Münker) längst nicht mehr auf.

Wie **Simon Edwin Dittrich**, der diesen Band redaktionell betreute, in seinem Beitrag ausführt, ist McLuhans Metapher des «Globalen Dorfes» im Zeitalter des Web 2.0 zu denken als ein Leben im permanenten Zwischen(t)raum: Zeitlicher und räumlicher Restriktionen enthoben, können wir heute mit beliebig vielen Menschen interagieren, mal mit der Vertrautheit, wie wir sie aus dörflichen Gemeinschaften kennen, mal mit der frei gewählten Anonymität und Distanz, wie sie eher Großstädten zu eigen ist. Die soziale Performance des eigenen «Ich», die seit jeher auf bestimmte Kostümierungen und Rollenrepertoires zurückgreifen musste, kann sich nun zusätzlich auf die Vielheit digitaler Repräsentationsformen stützen, auf Avatare in computergenerierten Umwelten, Geschlechtercamouflagen in Chat-Foren, unterschiedliche Entäußerungsformen in beruflich und privat genutzten sozialen Netzwerken. Doch für diesen «privat-öffentlichen» Zwischenraum werden auch neue Verabredungen notwendig, um die Distanzzonen und Reservate der Intimität neu zu vermessen. Für ein Verständnis des «public life» des 21. Jahrhunderts muss es darum gehen, das seit Aristoteles (und seiner besten Interpretin Hannah Arendt) dichotomisch gedachte Verhältnis von «oikos» und «polis» in eine neue, sorgsam austarierte Balance zu bringen. Wie können wir die beiden Sphären (theoretisch, alltagspraktisch, regulativ) neu aufeinander beziehen?

Die amerikanische Rechtsphilosophin **Helen Nissenbaum** hat, ausgehend von dieser Fragestellung, mit *Privacy in Context* ein weithin beachtetes Werk vorgelegt. Für den vorliegenden Band fasst sie die wesentlichen Thesen daraus zusammen. Statt Privatsphäre normativ als restriktives Kontrollrecht zu begründen, wirbt sie für eine situationsgerechte Analyse der Unversehrtheit des Kontexts, den die jeweiligen Arten der Information, der Gegenstand, Sender und Empfänger in einem Bezugsystem bilden. An ihrem Beispiel des Gesundheitswesens wird deutlich, wie wichtig die Rollendefinitionen der beteiligten Akteure (Ärzte, Pfleger, Patienten, Angehörige, Arbeitgeber, Versicherungsgesellschaften etc.) sind und dass diese nicht ohne Wirkung auf die angelegte Norm informationeller Privatheit sein können. Grundsätzlich, so Nissenbaum, verfügen wir zumeist über intuitive Erkenntnisse, die uns darüber urteilen lassen, «ob bestimmte Informationsflüsse moralische Legitimität genießen oder nicht». Mit ihrem Beharren auf den sozialen Kontext vollzieht Nissenbaum damit im Wesentlichen jene theoriepolitische Entwicklung nach, die bereits Michael Walzer in *Spheres of Justice* unternahm: eine Theorie der Sphärentrennung, die auf dem Prinzip einer «immanenten» Interpretation sozialer Güter und an sie geknüpfter Verteilungsregeln fußt.

Da es in den USA kein so ausgeprägtes Datenschutzrecht wie in Deutschland gibt und dem Leitbild der informationellen Selbstbestimmung kein verfassungsrechtlicher Rang zukommt, denkt der Privacy-Forscher **M. Ryan Calo** in seinem Beitrag über eine handhabbare Definition von Privatsphärenverletzungen nach. Sicherheitslücken entstünden immer dort, wo erstens eine unerwünschte Wahrnehmung von Beobachtung stattfinde und zweitens die Kontrolle über persönliche Informationen verloren ginge.

Wir werden intim, aber alle zusammen

Vor rund zehn Jahren, als die Heinrich-Böll-Stiftung in einer Tagung mit dem Titel «Save Privacy. Grenzverschiebungen im digitalen Zeitalter» den Einfluss der Neuen Medien auf den Datenschutz untersuchte, gab es zwei wesentliche Referenzpunkte der Diskussion: den Terrorangriff vom 11. September 2001 und das erfolgreiche Reality-TV-Format «Big Brother». Während der Sturz der Twin Towers innerhalb der letzten Dekade als eine Art Dammbruch für immer neue staatliche Überwachungstechnologien (wie z.B. Videoüberwachungsanlagen im öffentlichen Raum, Online-Durchsuchung, Vorratsdatenspeicherung) gewirkt hat, mag im Rückblick die Verve, mit welcher der voyeuristische Kitzel eines TV-Containers im Panoptikum-Stil zeitdiagnostisch behandelt wurde, ein wenig verwundern.

Denn von heute aus, und damit wären wir wieder bei der Historizität sozialer Vereinbarungen, war «Big Brother» ein Kindergeburtstag – verglichen mit dem, was als «mediale Kultur der Indiskretion» (Wolfgang Sofsky) längst Einzug gehalten hat. Millionen User posten selbst gedrehte Filmchen auf sozialen Netzwerken, bekringeln sich in digitalen Freundeskreisen über die Missgeschicke anderer oder brechen bei eher randständigen Themen heftigste Edit-Wars in der Wikipedia vom Zaun. Warum sie dies tun, ist nicht immer ganz klar. Was sie damit bewirken, hingegen schon. Die Doktor-Spiele eines Ministers, die mutmaßliche Persönlichkeitsspaltung eines Verlagserben, der Silberblick einer Beutelratte: all diese Ereignisse kurzer, mittlerer und längerer Reichweite hätten uns ohne die konsequente Umgehung der Trennung zwischen öffentlich und privat nie oder zumindest nicht mit dieser Wucht erreicht. Und wer sagt, dass das – zumindest im Falle des Nagetiers – auch besser so gewesen wäre, unterschätzt immer noch den tiefgreifenden Kulturwandel, der sich mit der Wandlung des Internets von einer Art Mega-Kanal zu einer Mehrwege-Plattform im globalen Maßstab ergeben hat. Die aufziehende digitale Öffentlichkeit des 21. Jahrhundert kennt die strikte Trennung zwischen Bühnen- und Zuschauerraum nicht mehr. Das Script zum «public life» spätmoderner Prägung wird kollektiv geschrieben, jetzt, in diesem Moment und überall.

Die Ekstase von Kommunikationen im Social Web hat mindestens zwei Sorten von Kritikern auf den Plan gerufen: die kulturkritischen und die demokratietheoretischen Bedenkenträger. Zu ersteren gehört der Soziologe Richard Sennett, der die digitale Kommunikationskultur mit drastischen Worten beschreibt:

«Manchmal, wenn ich mich durch diese Weblogs klicke, wo Menschen alle Aspekte ihres intimen Lebens online veröffentlichen, kommt es mir vor, als würden sie Müll in einen Abfalleimer, in dem Fall in ihren Computer, tippen. (…) Es ist ein unermessliches Ödland an Geständnissen und Offenbarungen, das diese Blogs ausfüllen.» Sennett unterlegt seine pessimistische Klage mit dem Hinweis, dass die an und für sich positiven Möglichkeiten zur «Selbstveröffentlichung» im Ergebnis leider nur einer «Gesellschaft der Intimität» zuarbeiteten.

An dieser vermeintlichen Verkümmerung des öffentlichen Diskurses setzt auch die zweite Kritiklinie an, für die beispielhaft etwa der amerikanische Verfassungsrechtler Cass R. Sunstein steht. Er nennt weniger den Vorrang des Privaten, sondern vielmehr den Vorrang des Ähnlichen als Hauptgefahr für eine vitale Demokratie. Das Social Web mit seiner Logik der Verlinkung und Rekursivität führe im Ergebnis zu geschlossenen «Informationskokons» und lasse uns im Grunde immer nur das auffinden, was die eigene Haltung bestätige. Diese diskurskritischen Einwände stehen pars pro toto für die immer noch sehr ambivalente Bewertung der aktuellen Netzkultur: Welche langfristigen Effekte hat sie auf unsere Vorstellungen von demokratischer Vielfalt, individueller Meinungsbildung und Vorstellungen eines konstruktiven Konfliktaustrags?

Ralf Bendrath und **Stefanie Sifft** untersuchen in ihrem Beitrag die Auswirkungen von Internetöffentlichkeiten auf etablierte Demokratien. Dabei sehen sie drei Lesarten des Internets durch einen kruden Technodeterminismus miteinander vereint: die euphorische Interpretation, die im Netz eine große Demokratisierungs-Maschine sieht; die skeptische Interpretation, wonach sich im Netz nur die Machtverhältnisse der «realen» Welt gespiegelt wiederfänden; sowie die pessimistische Variante, die vor allem die digitale Spaltung sowie die neue Hegemonie von amateurhaften Subkulturen betont. Gemessen am Ideal deliberativer Demokratie sei das Web 2.0 vorerst lediglich eine «Ermöglichungsstruktur», die hoch spezialisierte Teilöffentlichkeiten herausbilde und die Elitenbildung vorantreibe.

Der grüne Netzpolitiker **Malte Spitz** blickt auf den demokratischen Aufbruch im arabischen Raum. In der Artikulation der Freiheitsansprüche durch eine breite Massenbewegung erkennt er eine neue Qualität des Protests, zu dessen Globalisierung kommerzielle Netz-Angebote und Internet-Service-Provider ihren Teil beigetragen hätten. Hier wurde digitale Nähe gleichsam zu einem entscheidenden Faktor bei der Entfernung von autoritären Regimen. Grundvoraussetzung für eine demokratische und freiheitliche Öffentlichkeit sei, so Spitz, aber das Prinzip der Netzneutralität, also der ungehinderte, diskriminierungsfreie Datendurchfluss. Im Streit um die Aufrechterhaltung dieses politischen und technischen Prinzips gegen Unternehmensinteressen werde sich die Zukunft des Internets als globalem Öffentlichkeitsraum entscheiden.

Gefällt mir! Die (Neben-)Wirkungen der User-Freiheit

Der amerikanische Journalist **Clive Thompson** erklärt anhand von eigenen Erfahrungen und wissenschaftlichen Recherchen die wachsende Faszination von Web-Diensten wie Facebook oder Twitter. Das Gefühl einer virtuellen Kopräsenz steigere sich im Zeitverlauf zu einer umfassenden Ambient-Awareness, bei der das Leben der Anderen in den eigenen Alltag einbezogen werde. In der Tat lässt sich schon seit geraumer Zeit beobachten, dass das technikgestützte Management schwacher Bindungen zu ganz erstaunlichen Ergebnissen bei der Lösung von Alltagsproblemen führt. So kann die Empfehlungskultur des Netzes nicht nur die Wohnungs- oder Jobsuche enorm erleichtern, sondern virale Kettenreaktionen wie Spendensammlungen oder Musikerkarrieren befördern. Privatsphäre ist unter den Voraussetzungen einer «digitalen Intimität» keine geschlossene Blackbox mehr, sondern eher eine offene Schnittstelle zu anderen Online-Identitäten mit dahinter liegenden Biografien.

Da der digitale Alltag nicht nur wesentlich beschleunigter, sondern auch ökonomisch unsicherer geworden ist, verschärfen sich die Voraussetzungen, unter denen Subjekte sich öffentlich darstellen müssen, um ihre «employability» zu sichern. Im Zeitalter der permanenten Jobsuche wird die eigene Biografie zur herausfordernden Tätigkeit, um nicht zu sagen: Arbeit. Die sozialen Netzwerke entsprechen in besonderer Weise dem allgemeinen Bedürfnis, die eigene Persönlichkeit zu «performen» und in den Leistungsvergleich mit anderen zu stellen. Portale wie Facebook, Xing oder StudiVZ sind Foren der Selbstpräsentation, die strategische «Netzidentitäten» und komplexe Inszenierungspraktiken erfordern. Ein Workshop der *Berliner Gazette* mit Jugendlichen hat unlängst deren Verhältnis zur neuen Lebenskunst einer solchen «veröffentlichten Privatheit» untersucht. Wie Seminarleiter **Krystian Woznicki** im Gespräch mit **David Pachali** erläutert, behalten die «digital natives» entgegen dem gängigen Vorurteil ein hohes Bewusstsein für ihre Privatsphäre, indem sie Freundschaften auf Facebook sehr genau auswählen und Informationen nur gezielt weitergeben. Andererseits fehle ihnen fast vollständig das Wissen darüber, welche Verwertungsmöglichkeiten sie den Unternehmen mit ihren freiwillig preisgegeben Daten an die Hand geben.

Angesichts der ubiquitären Verfügbarkeit persönlicher Informationen in den Social Media verweist **Daniel J. Solove**, einer der wichtigsten Stichwortgeber in der US-amerikanischen Privacy-Debatte, auf die Notwendigkeit eines Reputationsmanagements. Das «digitale Gepäck ihrer Vergangenheit» beschäftigt heute schon Abermillionen zeigefreudiger Schüler und hat völlig neue Geschäftsfelder, etwa die gezielte Spurentilgung durch darauf spezialisierte Unternehmen, eröffnet.

Danah Boyd, die derzeit vielleicht einflussreichste Forscherin zur Soziologie der Social Networks, sieht angesichts der Aufregung um das Facebook-Feature News Feed vor einigen Jahren eine neue Grundregel: «Nur weil etwas öffentlich verfügbar ist, heißt das nicht, dass es auch veröffentlicht werden soll. Wenn man etwas Öffentliches noch öffentlicher macht, dann ist das eine Verletzung

der Privatsphäre.» Gerade Jugendliche hätten zwar ein gutes Unrechtsbewusstsein, was z.B. elterliche Schnüffelei in ihren Online-Aktivitäten angeht, seien sich aber oftmals nur ungenügend darüber im klaren, wie nachhaltig Imageverluste und Cyber-Mobbing auf ihre eigene Biografie zurückwirken können. Auch fragt Boyd nach der besonderen Situation gesellschaftlicher Minderheiten: Möchten und müssen Migranten ihre Biografie in authentischer Weise ausstellen oder würde das ihre Zugangschancen mindern? In welchem Umfang sollte ich meine sexuelle Orientierung preisgeben, wenn ich in bestimmten homophoben beruflichen Umfeldern arbeite?

Für die Literaturwissenschaftlerin und feministische Bloggerin **Francesca Schmidt** werden die Grenzen zwischen öffentlich und privat den Geschlechterstereotypen entsprechend im Internet reproduziert. So gebe es beispielsweise eine Genderdifferenz bei der Wahrnehmung von Möglichkeiten, Entscheidungsprozesse oder Diskussionen zu beeinflussen. Als Grund für die vielfach anzutreffende Zurückhaltung von Frauen vermutet Schmidt die zunehmend Präsenz von «Trollen», also jenen meist männlichen Forenbesuchern, die in aggressiver Weise Kommentar-Threads chaotisieren. Blogs und andere Informations-Angebote im Netz stünden, so Schmidt, deshalb immer «im Zwiespalt zwischen den eingeforderten demokratischen Prinzipien von Rede- und Meinungsfreiheit und dem Bedürfnis eines sicheren, aber dennoch zugänglichen Raums für Interessierte».

Datenschutz als Frage nach der Macht(un)gleichheit

Markus Beckedahl, der mit netzpolitik.org eines der meist gelesenen Blogs in Deutschland betreibt, denkt im Gespräch mit **John F. Nebel** über die Vor- und Nachteile von Anonymität bzw. Pseudonymität im Netz nach. Die immer häufiger erhobene Forderung nach Klarnamen kollidiere mit der demokratischen Notwendigkeit freier, ungehinderter Kommunikation – etwa die Kritik an Missständen in einem Unternehmen durch einen Arbeitnehmer («Whistleblowing») oder der vertrauensvolle Austausch über Krankheiten in Selbsthilfeforen. Auch werde die Klarnamenpflicht bei Facebook insbesondere in autoritären Regimen zum Problem, wo der Staatsapparat über die Ermittlung von Passwörtern wichtige Rückschlüsse über oppositionelle Gruppen erhalten kann. Auf technischer Ebene müssten deshalb «Privacy Enhancing Tools» (PETs) gefördert werden, also datenschutzfreundliche Grundeinstellungen in den Social Networks, die standardmäßig die wahre Identität des Users verbergen.

Den Einsatz dieser PETs unterziehen die beiden Datenschutzexperten **George Danezis** und **Seda Gürses** einer kritischen Revision. Bestimmte Anonymisierungswerkzeuge krankten mittlerweile unter den verfeinerten Methoden des Data Mining, das durch die Verknüpfung unterschiedlicher Quellen schließlich doch die Re-Identifizierung von Usern ermöglicht. Auch Identitätsmanagementsysteme, die wie z.B. Microsoft Passport (als proprietäres System) oder Liberty Alliance (als offener Standard) die Verwaltung von Benutzerdaten und sichere Transaktionen im Netz erlauben, böten als vertrauensbasierte Systeme

eine eher schwache Form von Datenschutz. Im Sinne der Nutzer seien demgegenüber PETs, die z.B. bei einem Anbieterwechsel eine leichte Portabilität von persönlichen Daten ermöglichen und technisch eindeutig spezifiziert sind.

«Die Frage des Datenschutzes ist eine nach den Macht(un)gleichheiten in der Informationsgesellschaft», schreibt **Jan Schallaböck** und richtet damit den Blick auf die politische Ebene der Technikfolgenabschätzung. So habe das Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung im März 2010 gezeigt, dass die Einhaltung strenger IT-Sicherheitsvorgaben in den Detailregelungen nur sehr schwer umzusetzen sein dürfte. Für eine bessere Ausbalancierung der staatlichen Sicherheits- und freiheitlichen Nutzerinteressen liegt seiner Meinung nach der Goldene Weg im breiten Einsatz quelloffener Software, die eine Kontrolle der dahinter liegenden Verarbeitungsprozesse ermögliche.

Freiwillige Selbstkontrolle? Oder besser Kontrollverlust?

Der Blogger **Michael Seemann** verweist auf die algorithmischen Bilderfassungs- und Auswertungsverfahren, die ein völlig neues Niveau der Datenverknüpfung ermöglichten. Die freiwillige Zuarbeit der User für die Anreicherung der Datenbestände von Google, Facebook et al. wertet er – wie viele konservative Netzskeptiker – als einen Kontrollverlust. Im Gegensatz zu ihnen zieht er daraus aber einen völlig anderen Schluss, nämlich die Notwendigkeit eines radikalen Umdenkens bei der Funktionslogik von Öffentlichkeit. So sei die Anfrage («query») an einen Datensatz, also die Filtersouveränität der Empfängerseite, heute wesentlich schwerer zu gewichten als das Push-Interesse jener Sender, welche die bürgerliche und massenmediale Öffentlichkeit über zweihundert Jahre bestimmt haben. Im Grunde zielt Seemann damit auch auf eine Art Beweislastumkehr bei der Informationsethik: Datenschutz-Maßnahmen hätten sich in dieser Optik immer als Schrankenbestimmungen einer grundsätzlich schrankenlosen Gemeinschaft der Suchenden zu rechtfertigen. Eine völlig neue Ökologie des Wissens unter dem Banner von Post-Privacy entstünde.

Auch die grünen Netzpolitiker **Konstantin von Notz** und **Nils Leopold** konstatieren das enorme Anwachsen von Bewegungs-, Kommunikations- und Verhaltensprofilen, die das Web 2.0 mit seinen Beteiligungsangeboten und User Generated Content erlaubt. Im Unterschied zu einigen Vertretern der Post-Privacy-Denkschule (wie etwa Jeff Jarvis) ziehen sie daraus jedoch nicht den Schluss, eine vollständige Transparenz von Handlungen im digitalen Raum anzustreben, um gewissermaßen «Waffengleichheit» für alle herzustellen. Stattdessen betonen sie die Bedeutung unterschiedlicher Hierarchieebenen und Verarbeitungsverhältnisse beim Datenaustausch und leiten daraus ein Erfordernis kontextuell begründeter Schutzvorkehrungen ab.

Context matters: Vielleicht sollten sich die Bühnenarbeiter im «public life» einfach an diese Losung halten. Denn eines dürfte zum gegenwärtigen Stand der Debatte zumindest schon unstrittig sein: Finden wir keine kluge Ausbalancie-

rung unserer freiheitlichen und kommunitären Interessen bei der Gestaltung der digitalen Öffentlichkeit, dann droht uns am Ende jener fröhliche Nihilismus, den Funny van Dannen in seinem kleinen Indie-Hit «ICE» verewigte: «Das alles regelt schon der Markt, na klar, das renkt sich alles ein / Und außerdem, es müssen ja nicht alle glücklich sein.»

CLIVE THOMPSON

Die Schöne Neue Welt der digitalen Intimität

«Wen interessiert es schon, was ich den ganzen Tag so treibe?» Anscheinend ziemlich viele. Selbst Mark Zuckerbergs Hund hat neuerdings Freunde auf Facebook. Die Kommunikation über Awareness-Tools wie Twitter könnte unsere sozialen Bindungen nachhaltig beeinflussen. Ein analytischer Blick auf das Gegenwartsphänomen des Umgebungsbewusstseins.

Am 5. September 2006 veränderte Mark Zuckerberg die Funktionsweise von Facebook und löste damit einen Aufstand aus. Nachdem der 24-jährige Vorstandsvorsitzende von Facebook die Seite zwei Jahre zuvor in seinem Wohnheimszimmer in Harvard gegründet hatte, wuchs sie binnen kurzer Zeit auf neun Millionen User. Zuckerberg wusste jedoch, dass Facebook ein großes Problem hatte: Es verlangte von seinen Nutzern viel aktives Surfen.

«Es war sehr primitiv», erzählte mir Zuckerberg, als ich ihn vergangenen Monat danach fragte. Und deshalb entschied er sich, die Seite zu modernisieren. Die Studenten sollten nicht länger ihre Zeit damit verbringen, ziellos umherzuirren, um jede einzelne Seite ihrer Freunde nach neuen Informationen abzusuchen. Stattdessen sollten sie sich einfach bei Facebook einloggen und den News Feed vorfinden, eine Art Liveticker über ihren Freundeskreis.

Als die Studenten an jenem Morgen im September den News Feed sahen, reagierten die meisten zunächst panisch. Facebook hatte sein letztes bisschen Privatsphäre verloren. Den Studenten kam es so vor, als wären sie mit allen, die sie kennen, auf einer riesigen, öffentlichen Party, wo jeder jeden permanent belauschen konnte.

Von den Protesten überrascht, fällte Zuckerberg direkt zwei Entscheidungen. Zuerst fügte er ein Privatsphäre-Feature hinzu, das die User selbst entscheiden ließ, welche Informationen sie über sich teilen wollten. Die zweite Entscheidung war es jedoch, den News Feed ansonsten nicht zu verändern. Er ging davon aus, dass die Nutzer ihren Schock überwinden und den News Feed mögen würden, wenn sie ihn erst einmal ausprobiert hatten.

Er behielt Recht. Innerhalb weniger Tage kehrte sich der Trend um. Die Studenten begannen Zuckerberg E-Mails zu schicken, in denen sie ihm mitteilten, dass sie über den News Feed Dinge erfahren hatten, die sie durch zielloses Surfen auf Facebook nie entdeckt hätten.

In einem Gespräch sagte mir Zuckerberg, dass der News Feed von zentraler Bedeutung für den Erfolg von Facebook sei. «Facebook hat schon immer versucht an Grenzen zu gehen», sagte er. «Wenn man die Leute dazu bringen will, sich mit bisher unbekannten Dingen vertraut zu machen, muss man ihnen eben manchmal etwas abverlangen. Meistens bedeutet das lediglich, dass die sozialen Normen den Vorsprung der technischen Entwicklung aufholen und sich daran anpassen müssen.»

Im Wesentlichen ging es den Facebook-Usern darum, dass sie die minutiösen Updates darüber, was ihre Freunde gerade taten, unnötig fanden. Aber als sie diese Art von Allwissenheit zum ersten Mal erlebten, waren sie sofort fasziniert, sogar süchtig. Wieso war das so?

Amerikanische Sozialwissenschaftler nennen diese Art von permanentem Onlinekontakt «Ambient Awareness», Umgebungsbewusstsein. Dieser Zustand, so die Wissenschaftler, ist in etwa so, als sei man einer Person nicht nur physisch nah, sondern auch gleichzeitig in der Lage, seine Stimmung mittels kleiner Hinweise – Körpersprache, Seufzer, beiläufige Kommentare – aus dem Augenwinkel heraus wahrzunehmen.

Wen interessiert denn das? Ein Selbstversuch

Den meisten Menschen kommt es jedoch absurd vor, jedes Detail ihrer Aktivitäten minutiös festzuhalten. Warum sollte man seinen Freunden alle Einzelheiten seines Tagesablaufs aufzwingen? Und andersherum gefragt, wie viele Belanglosigkeiten aus dem Leben anderer kann man selbst ertragen? Die Ausbreitung von «Ambient Intimacy», elektronisch hergestellter Nähe, kann dabei schnell wie ein moderner Narzissmus erscheinen, der ein bisher unbekanntes Ausmaß erreicht. Es ist die bedeutendste Ausdrucksweise einer Generation Jugendlicher, die mit Promikult aufwachsen und die glauben, dass jede ihrer Äußerungen faszinierend ist und mit der Welt geteilt werden sollte. Seitdem es online gegangen ist, ist vor allem Twitter das Ziel fast schon erbarmungslosen Spotts. «Wen interessiert es denn wirklich, was ich den ganzen Tag so treibe?» fragte sich der *Boston Globe*-Kolumnist Alex Beam in einem Essay über Twitter. «Es interessiert ja nicht mal mich selbst.»

Und tatsächlich, die meisten meiner Interviewpartner, eifrige Nutzer jener Programme und Geräte, die diese Art von Kontakt herstellen, gaben zu, dass sie zuerst nicht verstanden haben, wieso man sowas überhaupt tun sollte. Ben Haley fand das zunächst auch albern, aber nachdem ein paar seiner Freunde entschieden hatten, es einmal auszuprobieren, brachten sie ihn ebenfalls dazu, sich zu registrieren.

Nachdem sich Haley jeden Tag auf Twitter einloggte, erschienen sofort die ein- bis zweizeiligen Updates seiner Freunde auf der Startseite. Er überprüfte sein Benutzerkonto mehrere Male am Tag, manchmal sogar mehrmals in der Stunde. Die Updates waren in der Tat ziemlich banal. Einer seiner Freunde postete, dass ihm schlecht sei; ein anderer, was ihm gerade in den Sinn kam, z.B.: «Ich kann es

wirklich nicht leiden, wenn sich Leute im Bus die Nägel schneiden.» Wieder eine andere Freundin twitterte immer dann, wenn sie sich ein Sandwich machte – sie machte sich jeden Tag ein Sandwich. Jeder sogenannte Tweet war so kurz, dass er so gut wie bedeutungslos war.

Aber im Laufe der Zeit änderte sich etwas. Haley bemerkte, dass er den Lebensrhythmus seiner Freunde langsam auf eine ganz neue Art und Weise wahrnahm. Als eine Freundin von einem ansteckenden Fieber erwischt wurde, konnte er an ihren Twitter-Updates sehen, wann es ihr schlechter ging und wann genau sie über den Berg war. Er bekam es mit, wenn Freunde auf dem Weg in einen harten Arbeitstag waren oder wenn sie riesigen Erfolg hatten. Sogar die tägliche Liste von Sandwiches wurde merkwürdigerweise irgendwie faszinierend – eine Art rhythmisches Klicken, welches mitten am Tag aufpoppte und an das er sich gewöhnte.

Das ist das Paradoxe an Umgebungsbewusstsein. Jedes kleine Update – jedes einzelne Bisschen sozialer Information – ist für sich genommen unwichtig, sogar äußerst banal. Aber zusammengenommen verschmelzen all diese kleinen Schnipsel mit der Zeit überraschenderweise zu einem komplexen Porträt unserer Freunde und Familienmitglieder, wie tausende Punkte in einem pointilistischen Gemälde. So etwas war vorher noch nie möglich gewesen, denn in der echten Welt würde uns kein Freund anrufen, um uns zu beschreiben, wie er sein Sandwich isst. Die allgegenwärtigen Informationen werden zu «einer Art außersinnlicher Wahrnehmung», wie Haley es mir beschrieb, eine unsichtbare Ebene, die über unserem Alltag schwebt.

«Es ist so, als könnte ich jedermanns Gedanken aus der Entfernung lesen», fuhr Haley fort. «Ich liebe es. Es fühlt sich an, als würde ich etwas Unverbrauchtes über meine Freunde erfahren. Es ist, als hätte ich ein Head-up-Display für sie.» Es kann auch zu mehr Kontakten im echten Leben führen, z.B. wenn einer von Haleys Freunden eine Band in einer Bar sehen möchte, über seinen Plan twittert und diejenigen, die es lesen, sich dazu entschließen, auch vorbeizukommen – eine Art spontaner Stammtisch. Und wenn sie dann real zusammentreffen, fühlt es sich komischerweise so an, als wären sie nie voneinander getrennt gewesen. Sie müssen sich nicht fragen «Na, wie war dein Tag?», denn sie wissen es ja schon. Stattdessen fangen sich gleich an, über etwas zu diskutieren, was ein anderer Freund am selben Nachmittag getwittert hat, so als würden sie eine Unterhaltung in der Mitte beginnen.

Facebook und Twitter haben die ganze Sache vielleicht beschleunigt, aber die Idee, Kommunikationsmittel als eine Art «Kopräsenz» zu nutzen, gibt es schon eine Weile. Der japanische Soziologe Mizuko Ito war der erste, der dieses Phänomen in Zusammenhang mit Mobiltelefonen bemerkte: z.B. bei Paaren, die in verschiedenen Städten lebten und sich die ganze Nacht SMS schickten – kleine Updates wie «Ich gönne mir gerade ein Glas Wein» oder «Ich gucke auf dem Sofa Fernsehen». Sie taten dies u.a. deshalb, weil es nicht sehr bequem (oder bezahlbar) war, stundenlang mit dem Handy zu telefonieren. Dabei entdeckten

sie aber auch, dass das kleine SMS-Ping-Pong sich sogar noch intimer anfühlte als ein Anruf.

«Es ist ein Anhäufungsphänomen», erklärte mir Marc Davis, wissenschaftlicher Leiter bei Yahoo und früherer Professor für Informatik an der University of California in Berkeley. «Keine Nachricht ist die allerwichtigste Nachricht. Es ist ungefähr so, als würden Sie mit jemandem zusammensitzen, zu ihm hinübersehen und von ihm angelächelt werden. Sie sitzen hier, lesen Ihre Zeitung, machen etwas nebenbei und lassen die anderen Menschen irgendwie wissen, dass Sie sich ihrer Anwesenheit bewusst sind.» Das ist allerdings auch der Grund, wieso dieses Phänomen so schwer zu verstehen ist, wenn man es vorher noch nie erlebt hat. Sich einfach nur die Twitter- oder Facebook-Seite eines Fremden anzusehen, ist deshalb uninteressant, weil das, was man dort lesen kann, wie sinnloses Geschwafel aussieht. Verfolgt man es aber einen ganzen Tag, dann kommt es einem wie eine Kurzgeschichte vor; nach einem Monat sogar wie ein Roman.

Man könnte die wachsende Popularität dieser Art des Online-Kontakts auch als eine Reaktion auf soziale Isolation betrachten, wie es z.B. Robert Putnam in seinem Buch *Bowling Alone* tut, indem er die moderne amerikanische Unverbundenheit untersucht. Die mobilen Arbeitskräfte müssen mehr und mehr reisen und immer öfter ihre Familie und Freunde zurücklassen. Eine wachsende Schar an Selbstständigen verbringt ihre Tage oft in Einsamkeit. Die Nähe zur Umgebung wird so zu einer Möglichkeit, sich «weniger allein zu fühlen», wie mir mehrere Facebook- und Twitter-Nutzer erzählten.

Die Stärke schwacher Bindungen

Dieses online hergestellte Ambient Awareness führt aber unweigerlich auch zu einer eigentümlichen Frage: Was sind das für Beziehungen? Was bedeutet es, hunderte Facebook-»Freunde» zu haben? Und was sind das überhaupt für Freunde?

Der Anthropologe Robin Dunbar behauptete 1998, dass jeder ein vorprogrammiertes Limit an Menschen hat, die er zur selben Zeit persönlich kennen kann. Dunbar bemerkte außerdem, dass sowohl Menschen wie auch Affen Partnerbindungen entwickeln können, wenn sie eine Art Pflege betreiben. Während Affen dazu das Fell anderer Affen zupfen und glattstreichen, pflegen Menschen ihre Beziehungen durch Konversation. Dabei stellte Dunbar die Theorie auf, dass Affen- und Menschenhirne lediglich eine begrenzte Anzahl an Pflegebeziehungen eingehen können: Solange wir nicht genügend Zeit damit verbringen, unsere sozialen Beziehungen zu pflegen – durch Plaudern, Tratschen oder, im Fall von Affen, Entlausen – , haben wir auch nicht das Gefühl, jemanden so gut zu «kennen», dass wir ihn als Freund bezeichnen würden. Dunbar bemerkte, dass eine Gruppe Affen höchstens 55 Mitglieder hat. Da menschliche Gehirne größer sind, vermutete Dunbar, dass die Zahl unserer größtmöglichen sozialen Kontakte proportional höher sein müsse, also durchschnittlich ca. 150. Und tatsächlich

haben psychologische Studien bestätigt, dass das Wachstum menschlicher Gruppierungen bei ca. 150 Personen nachlässt: Man nennt dies die «Dunbar-Zahl». Verbessern diejenigen, die Facebook und Twitter nutzen, ihre Dunbar-Zahl, weil sie so leicht den Überblick über eine viel größere Anzahl an Menschen behalten können?

Als ich einige Nutzer interviewte, die besonders intensiv soziale Kontakte über das Netz pflegen – Menschen, die Hunderten oder Tausenden anderer auf Twitter folgten –, wurde mir klar, dass die Sache etwas komplexer war, als diese Frage vermuten ließe. Viele der Befragten betonten, dass der Kreis ihrer wirklichen Vertrauten, ihrer Freunde und Familie, nicht gewachsen sei. Permanenter Online-Kontakt hat diese Bande zwar in einem enormen Maße verstärkt, aber ihre Zahl hatte sich nicht erhöht. Tiefgründige Beziehungen werden immer noch in persönlichen Gesprächen aufgebaut und der Tag hat schließlich nur 24 Stunden.

Bei den «weak ties» ist ihre Geselligkeit jedoch wahrhaftig explodiert. Eine solche «schwache Bindung» hat man z.B. zu flüchtigen Bekannten und Menschen, die man weniger gut kennt. Das kann jemand sein, den man mal auf einer Konferenz getroffen hat, jemand aus der Schule, mit dem man sich auf Facebook «befreundet» hat, oder jemand von der letzten Weihnachtsfeier. Im Leben vor dem Internet hätte man solche Bekanntschaften schnell wieder vergessen. Wenn jetzt jedoch persönliche Notizen dieser weitentfernten Menschen in unserem Feed auftauchen, werden wir im Wesentlichen an deren Existenz erinnert. Ich habe diesen Effekt selbst auch schon bemerkt. In den letzten paar Monaten haben sich Dutzende meiner alten Kollegen, mit denen ich vor 10 Jahren in Toronto zusammengearbeitet habe, mit mir auf Facebook «befreundet». Ich lese jetzt täglich ihre zusammenhangslosen Bemerkungen und Updates und stecke mit ihnen mitten in verrückten und witzigen Unterhaltungen. Meine Dunbar-Zahl ist deshalb insgesamt 301: Facebook (254) + Twitter (47) – doppelt so viel wie ohne Technologie. Und trotzdem sind nur 20 davon Familienmitglieder oder Menschen, die ich als enge Freunde bezeichnen würde. Was übrig bleibt, sind schwache Bindungen – aufrechterhalten durch Technologie.

Das schnelle Wachstum dieser «weak ties» kann aber auch etwas Gutes haben. Soziologen haben herausgefunden, dass schwache Bindungen stark dazu beitragen, unsere Problemlösungsfähigkeiten zu verbessern. Wenn man zum Beispiel einen neuen Job sucht und seine Freunde um Rat bittet, werden sie keine große Hilfe sein; sie sind uns zu ähnlich und haben deswegen wahrscheinlich keine wirklich neuen Hinweise. Zufällige Bekanntschaften sind hier erfolgversprechender, denn sie bewegen sich auf einem weiteren Feld und sind uns trotzdem nah genug, um helfen zu wollen. Viele eifrige Twitter-Nutzer – diejenigen, die stündlich originelle Posts abfeuern und dadurch letztlich tausende faszinierte Follower bekommen – nutzen genau diese Dynamik mit aller Macht aus, in der Hoffnung, möglichst jedes Problem mithilfe ihrer vielen Online-Follower lösen zu können.

Es ist aber auch möglich, dass dieser Überfluss an schwachen Bindungen zu einem Problem werden kann. Wenn man täglich Hunderte von Updates darüber liest, mit wem andere Leute gerade zusammen sind und ob sie dabei glücklich sind, dann könnte dies, so befürchten einige Kritiker, unsere Emotionen überfordern und zu wenig Raum für echte und intime Beziehungen lassen. Psychologen haben schon vor langer Zeit herausgefunden, dass Menschen in der Lage sind, «parasoziale» Beziehungen mit fiktionalen Charakteren, z.B. aus dem Fernsehen, aus Büchern oder Boulevardzeitschriften, einzugehen. Parasoziale Beziehungen können einen Teil der emotionalen Kapazitäten unserer Dunbar-Zahl verbrauchen und dabei Menschen aus dem echten Leben verdrängen.

Drum prüfe, wer digital sich bindet

Caterina Fake weist auf eine wesentlich subtilere Gefahr hin: Die bloße Leichtigkeit, mit der sie die Updates ihrer Freunde online verfolgt, macht sie manchmal zu faul, sich die Zeit zu nehmen, die Menschen persönlich zu treffen. «Irgendwann habe ich festgestellt, dass ich das einjährige Kind eines Freundes nur über Fotos auf Flickr aufwachsen gesehen habe», sagte sie. «Dann hab ich mir gedacht, dass ich sie auch mal persönlich kennenlernen sollte. Aber es war komisch; ich hatte auch das Gefühl, dass Flickr dieses Kennenlernbedürfnis bereits gestillt hatte und es deshalb nicht so dringend war. Aber dann dachte ich, ‹Das kann doch nicht alles sein! Ich sollte persönlich vorbeischauen!›» Sie hat ungefähr 400 Leute, denen sie online folgt, vermutet jedoch, dass es sich bei vielen dieser Beziehungen um schwache Bindungen handelt. «Diese Technologien erlauben einem, dass man auf einer viel breiteren Ebene freundlich sein kann. Dabei hat man allerdings immer weniger Aufmerksamkeit für immer mehr Leute.»

Wie es sich wohl anfühlt, zu niemandem jemals den Kontakt zu verlieren? An einem Vormittag letzten Sommer hörte ich zufällig in meinem Stammcafé, wie sich eine junge Frau bei einem Freund über ein Beziehungsdrama beklagte, das ihr gerade auf Facebook passiert war. Ihr Name war Andrea Ahan und sie war die 27-jährige Inhaberin des Restaurants. Sie hatte sich vor kurzem von ihrem Freund getrennt, hatte ihn jedoch nicht auf Facebook «als Freund entfernt», da ihr das zu extrem vorkam. Er kam aber schnell mit einer anderen jungen Frau zusammen, und die beiden begannen öffentliche Unterhaltungen auf der Seite von Ahans Ex-Freund zu führen. Eines Tages stellte sie mit Erschrecken fest, dass seine neue Freundin Sätze zitierte, die Ahan ihrem damaligen Freund in privaten E-Mails geschickt hatte; sie vermutete, dass er die alten E-Mails seiner neuen Freundin gezeigt hatte. Es ist diese Art von seltsam unterschwelligem Psychospiel, das auf Facebook möglich wird und Ahan verrückt machte.

«Manchmal denke ich, dass das alles doch verrückt ist. Jeder sollte sich um sich selbst kümmern und sich nicht in die Belanglosigkeiten und den Tratsch anderer einmischen», sagte sie.

Trotzdem weiß Ahan, dass sie nicht einfach vor ihrem Online-Leben flüchten kann. Die Leute, die sie online kennt, werden nicht aufhören, über sie zu reden

oder unvorteilhafte Fotos zu posten. Sie muss auf Facebook bleiben, um zu beobachten, was über sie gesagt wird. Diese Beschwerde habe ich oft gehört, vor allem von Leuten in den Zwanzigern, die gerade das College besuchten, als Facebook online ging, und die das Erwachsensein nie ohne diese Art des Online-Kontaktes erlebt haben. Für sie ist die Teilnahme nicht optional. Wenn man nicht mitmacht, dann werden andere Leute einfach definieren, wer man ist. Und deshalb teilen wir permanent unsere Fotos, unsere Gedanken, unsere Beziehungen und was wir tun – genau in diesem Moment! –, wenn auch nur, um sicherzustellen, dass unser virtuelles Ich korrekt ist oder wenigstens so, wie wir es der Welt präsentieren wollen.

Das ist auch letztendlich der Effekt dieses neuen Bewusstseins: Es bringt die Dynamik eines Kleinstadtlebens zurück, wo jeder über die Angelegenheiten der anderen Bescheid weiß. Vor allem Studenten sind diejenigen, die diese Erfahrung am schmerzlichsten machen. Weil mehr als 90 Prozent ihrer Bekannten Facebook nutzen, ist es für sie besonders schwierig, sich herauszuhalten. Die Soziologin Zeynep Tufekci hat untersucht, wie Nutzer im College-Alter auf diese Welt der permanenten gegenseitigen Wahrnehmung reagieren:

«Es ist, als würde man in einem Dorf leben, wo lügen wirklich schwierig ist, da jeder bereits die Wahrheit kennt. Die heutige Generation ist immer im Kontakt miteinander. Sie verlieren nie die Verbindung zu ihren Freunden. Deshalb gehen wir zurück an einen historisch gesehen normaleren Ort. Wenn man sich die Geschichte der Menschheit ansieht, dann ist die Idee, dass man sich durch das Leben treiben lässt und dabei von einer Beziehung zur nächsten geht, sehr neu.»

Psychologen und Soziologen haben Jahre damit verbracht zu erforschen, wie die Menschheit sich wohl anpassen würde angesichts der Anonymität der Großstädte und den schmerzhaften Umbrüchen für die mobilen Arbeitsimmigranten – eine Welt voll von einsamen Menschen, die von ihren sozialen Kontakten losgerissen wurden. Jetzt haben wir genau das entgegengesetzte Problem. Tatsächlich kehren die modernen Technologien und Computerprogramme, sogenannte Awareness-Tools, die diese Art von Wahrnehmung herstellen, den eigentlichen Vorbehalt gegen das Internet um. Als das Internet in den Neunzigern Einzug in unser Leben hielt**,** feierten wir es als einen Ort, an dem man sich neuerfinden – jemand anderer werden – konnte.

«Wenn überhaupt, dann schränkt man seine Identität jetzt ein», erzählte mir Tufekci. «Man kann mit seiner Identität nicht herumspielen, wenn man ständig von einem Publikum überwacht wird. Ich hatte mal eine Studentin, die gepostet hat, dass sie sich gerade etwas von Pearl Jam herunterlädt. Daraufhin schrieb jemand an ihre Pinnwand: ‹Ja, genau, haha – ich kenn dich, und auf so was stehst du nicht›.» Tufekci lacht: «Kennen Sie diesen alten Cartoon? ‹Im Internet weiß niemand, dass du ein Hund bist?› Im Internet heutzutage weiß aber jeder, dass du ein Hund bist! Wenn man niemandem verraten will, dass man ein Hund ist, sollte man sich lieber von einer Tastatur fernhalten.»

Digitale (Selbst-)Erkenntnis

Lisa Reichelt, eine Beraterin aus London, die regelmäßig über Awareness-Tools schreibt**,** formulierte es mir gegenüber so: «Können Sie sich ein Facebook für Kinder im Kindergarten vorstellen, mit dem sie bis zum Ende ihres Lebens niemals den Kontakt zu den anderen Kindern verlieren? Wie wird sich das wohl auf das Leben der Kinder auswirken?» Heutzutage entwickeln junge Menschen bereits ein Gefühl für ihre Privatsphäre, das sowohl von Aufmerksamkeit als auch Nachlässigkeit geprägt ist. Sie kümmern sich so sorgfältig wie möglich um ihre Online-Persönlichkeit in dem Wissen, dass jeder zusieht – aber sie haben auch gelernt, die Grenzen dessen, was sie kontrollieren können, gelassen zu sehen und zu akzeptieren.

Es ist leicht nachzuvollziehen, dass einige Aspekte dieser Awareness-Tools beunruhigend wirken können, vor allem wenn sie anscheinend unsere Privatsphäre bedrohen. Aber es gibt auch ein anderes – total anderes – Ergebnis dieser permanenten Updates: eine Kultur von Menschen, die viel mehr über sich selbst wissen. Viele der eifrigen Twitterer, Flickrer und Facebook-Nutzer, mit denen ich gesprochen habe, beschrieben mir einen unerwarteten Nebeneffekt ihrer permanenten Selbstdarstellung. Wenn man bewusst mehrmals am Tag innehält und seine eigenen Gefühle und Handlungen wahrnimmt, kann dies mit der Zeit eine philosophische Qualität annehmen. Es ist ähnlich dem griechischem Ausspruch «Erkenne dich selbst!» oder dem psychotherapeutischen Konzept der Achtsamkeit. (Und tatsächlich, die Frage, die ewiglich im Kopf der Facebook-Website schwebt – «Was machst du gerade?» – kann existentiell aufgeladen erscheinen. Was machst du?) Die Selbstreflexion kann durch die Anwesenheit eines Publikums sogar noch verstärkt werden, indem man, wie meine Interviewpartner angemerkt haben, nicht nur versucht, seine Aktivitäten so präzise wie möglich zu beschreiben, sondern sie für andere auch interessant darstellen will: das Status-Update als Literaturform.

Laura Fitton, Social Media-Beraterin, behauptet, dass ihre ständigen Status-Updates sie zu einer «zufriedeneren, ruhigeren Person» machen. Wenn sie z.B. postet, dass sie einen furchtbaren Vormittag auf der Arbeit hat, dann ist sie dazu gezwungen, noch einmal sachlich darüber nachzudenken. «Man betrachtet sich plötzlich von außen», fügte sie hinzu. In einer Zeit des Umgebungsbewusstseins sind diejenigen, die uns am deutlichsten sehen, vielleicht wir selbst.

Zuerst erschienen am 7. September 2008 in der *New York Times*.

Aus dem Englischen übersetzt von Katja Ullrich.

DANAH BOYD

Living in a publicity world: Privatsphäre und Öffentlichkeit in Sozialen Netzwerken

Justins Haarschnitt, Britneys Sorgerecht: Öffentliche Personen sind die eigentlichen Treiber von Microblogging-Diensten. Über Twitter kann selbst Jordaniens Königin Rania mit den Menschen auf eine so direkte Art kommunizieren, wie es ihr bisher unmöglich war. Spricht sie mit jedem? Sicher nicht. Aber ihre Fangemeinde fühlt sich hier echter an als die, mit der sie auf der Straße konfrontiert ist. Die neue digitale Öffentlichkeit ist eine Herausforderung für unser alltägliches Handeln, unsere Normen und Werte.

Dear Eric Schmidt, privacy is not dead. KTXBY

Indem sie immer wieder argumentieren, die Privatsphäre sei tot, rechtfertigen Technologen, dass sie Daten, die öffentlich verfügbar sind, noch öffentlicher machen können. Es gibt jedoch einen großen Unterschied zwischen der eigentlichen Veröffentlichung von Daten und dem, was bereits öffentlich verfügbar ist.

Wenn Menschen Informationen verfügbar machen, dann machen sie sich dabei selbst auch verwundbar. In sozialen Situationen geht uns das immer so. Wir machen uns deshalb verletzbar, weil wir denken, dass wir auch davon profitieren können. Auf diese Art schließen wir Freundschaften. Wir machen uns aber auch gegenüber Technologien verwundbar, weil wir denken, dass wir davon profitieren können. Genauso wie wir darauf vertrauen, dass Menschen den Kontext verstehen, in welchem wir Informationen mit ihnen teilen, vertrauen wir auch Maschinen. Wenn jedoch unsere Freunde oder Technologien das soziale Umfeld ignorieren, in dem wir etwas veröffentlichen, dann fühlt sich das wie eine krasse Verletzung der Privatsphäre an.

Ich habe eine junge Frau interviewt, die gewagte Fotos von sich auf MySpace gepostet hatte. Als ich sie nach dem Grund dafür gefragte habe, antwortete sie, sie hoffe, von einer Modelagentur entdeckt zu werden. Dabei verwies sie auf andere Prominente (z.B. Tila Tequila), die durch ihre Online-Aktivitäten berühmt geworden waren. Ihr war klar, dass die Bilder ihr Ärger mit Erwachsenen einbringen könnten. Es war ihr jedoch egal, was die Zulassungsbüros von bestimmten Colleges zu sagen hatten. Realistisch gesehen war der Wechsel auf ein College für sie sowieso keine Option. Ihrer Meinung nach könne sie nur «groß

rauskommen», wenn sie berühmt werde. Und deswegen tat sie einiges, was die meisten Eltern aus Ober- und Mittelschicht auf die Barrikaden bringt.

Dabei sollte man im Hinterkopf behalten, dass die meisten Menschen bestimmte Dinge nicht deshalb öffentlich zugänglich machen, weil sie gesehen werden sollen. Das wird z.B. deutlich, wenn man sich die Aussage der 17-jährigen Bly Lauritano-Warner ansieht: «Meine Mutter rechtfertigt sich immer mit der Ausrede, dass das Internet doch ‹öffentlich› ist. Es ist ja nicht so, dass ich irgendetwas tue, weswegen ich mich schämen müsste, aber Mädchen brauchen nun mal ihre Privatsphäre. Ich schreibe ein Online-Tagebuch, um mit meinen Freunden zu kommunizieren – und nicht, damit meine Mutter sich über den neusten Tratsch in meinem Leben informieren kann.»

In einer Öffentlichkeit außerhalb des Internets ist es leicht, seine Privatsphäre zu genießen. Online kann das jedoch ziemlich schwierig und frustrierend sein. Vor allem Teenager beschweren sich, dass einige Autoritätspersonen denken, sie hätten das Recht hinzusehen, nur weil die Möglichkeit dazu besteht. Wenn man dieser Logik folgt, dann dürfte jeder das Tagebuch eines anderen lesen, nur weil er Zugang dazu hat. Und jeder, der die Möglichkeit hat, eine Unterhaltung zu belauschen, hätte dann auch das Recht, genau zuzuhören. Nur weil etwas möglich ist, heißt das nicht, dass es auch sozial angemessen ist. Hierbei kann nämlich schnell Vertrauen verspielt werden. Und nur allzu oft untergraben Eltern die Beziehung zu ihren Kindern, weil sie denken, dass sie ein Recht darauf hätten, in deren Angelegenheiten herumzuschnüffeln.

Nur weil etwas öffentlich verfügbar ist, heißt das nicht, dass es auch veröffentlicht werden soll. Wenn man etwas Öffentliches noch öffentlicher macht, dann ist das eine Verletzung der Privatsphäre.

Denken Sie doch einfach an das News-Feed-Fiasko, das sich vor ein paar Jahren auf Facebook ereignet hat. Facebook hat hier Inhalte gebündelt und diese noch sichtbarer gemacht, obwohl man eigentlich auch schon vorher darauf zugreifen konnte. Im Wesentlichen hat Facebook hier also quasi-öffentlichen Inhalt noch öffentlicher gemacht. Viele Nutzer sind ausgeflippt. Wieso? Es gibt z.B. einen großen Unterschied, ob ich gerade eine Beziehung eingegangen bin, die ich als «kompliziert» beschreibe und man das von meinem Profil erfahren kann, oder ob man es in einer Flut von Updates aus dem News-Feed erfährt. Im Grunde genommen hat Facebook öffentlich zugängliche Informationen veröffentlicht und sie dadurch noch zugänglicher gemacht. IT-Unternehmen tun dies immer wieder. Können sich die Nutzer daran anpassen? Ja, und das tun sie auch. Dabei ändert sich jedoch ihr Verhalten, und sie sind immer wieder mit Schwierigkeiten konfrontiert, die sie so nicht erwartet hatten.

Oft geht es hierbei nicht darum, ob etwas öffentlich oder privat ist, sondern *wie* öffentlich oder privat es ist. Die Menschen sind nicht daran gewöhnt, dass sie jedes Mal, wenn sie das Haus verlassen, von einer Horde Paparazzi verfolgt werden. Wenn wir jedoch argumentieren, dass es okay ist, etwas öffentlich zu machen, das ja sowieso in der Öffentlichkeit stattfindet, dann sagen wir im Grunde genommen auch, dass wir das Recht haben, Paparazzi auf jeden zu

hetzen. Wir machen folglich aus jedem Menschen eine Person des öffentlichen Lebens.

Um eins klarzustellen: Auch wenn viele Teenager gern Promis wären, wissen doch nur wenige um den Preis, den man zahlt, wenn man derart in der Öffentlichkeit steht. Klar, sie haben mit angesehen, wie Prominente, z.B. Britney Spears oder Lindsey Lohan, sich vor den Augen der Öffentlichkeit zugrunde gerichtet haben. Aber meistens sind sie sich nicht darüber im Klaren, welche Rolle Paparazzi bei diesen öffentlichen Nervenzusammenbrüchen gespielt haben.

Eine Welt, in der alles öffentlich ist

Behalten wir mal die Prominenten im Hinterkopf und reden ausführlicher über Öffentlichkeit. Es besteht kaum ein Zweifel, dass das Internet neue Möglichkeiten der Veröffentlichung befördert, indem es dem Durchschnittsmenschen erlaubt, sich eine Zuhörerschaft aufzubauen und offen zu reden. Gleichzeitig bietet es aber auch denjenigen, die bereits wissen, wie sie sich ein Publikum aufbauen, neue Hilfsmittel, diese Öffentlichkeit noch weiter auszubauen. Teilweise ist das der Grund, weshalb Twitter so ein faszinierendes Phänomen ist. Twitter hat sich zu einer Plattform für Promis, B-Promis, Möchtegern-Promis und all ihren Fans entwickelt.

Viele Leute denken, dass Tweets und Status-Updates dasselbe seien. Das sind sie aber nicht, und der Unterschied liegt darin, dass die einen öffentlicher sind als die anderen. Anfangs haben viele Leute Twitter dazu genutzt, um mit ihren Freunden zu kommunizieren. Heute geht es vor allem darum, dass diejenigen, die ein Publikum suchen, mit denen, die ihnen folgen, oder zu ihrer Bekanntheit beitragen möchten, zusammenkommen. Bei Facebook andererseits geht es immer noch vordergründig um die Kommunikation mit einer Gruppe von Ausgewählten, die im Großen und Ganzen unsere Freunde sind. Auch wenn Facebook offensichtlich versucht, dies zu ändern, nutzt der Großteil der User diese beiden Services aber auf sehr unterschiedliche Art und Weise.

Echten Prominenten erlaubt Twitter, genauso wie MySpace, eine intimere Form von Öffentlichkeit. Auf Le Web erklärte Königin Rania von Jordanien, dass sie ohne unzählige Bodyguards gar nicht mehr in die Öffentlichkeit gehen kann; ihre Bewegungsfreiheit ist durch ihre Rolle extrem eingeschränkt. Über Twitter kann die Königin jedoch nun mit den Menschen auf eine so direkte Art kommunizieren, wie es ihr bisher unmöglich war. Spricht sie mit jedem? Sicher nicht. Aber ihre Fangemeinde fühlt sich hier echter an als die, mit der sie auf der Straße konfrontiert ist.

Twitter ist aber nicht nur etwas für Promis und ihre Fans. Es ist deshalb so faszinierend, weil man auf so verschiedene Arten mitmachen kann. Das macht es aber gleichzeitig auch so chaotisch. Bedenken wir kurz, welche Rolle die «Trending Topics» spielen. Bei den Trending Topics wird unsere Aufmerksamkeit am auffälligsten ausgeschöpft. Aber hier werden nicht nur die Beiträge der Nutzer zusammengefasst, sondern auch Spielchen gespielt: Einige Leute wollen

in den Trending Topics Trends kreieren und diese aufrechterhalten. Es gibt zwei Arten von Trending Topics – exogene und endogene. Auf gut Deutsch: solche, die von externen Faktoren gestartet werden, und solche, die sich auf der Seite selbst entwickeln. Exogene Trends beschäftigen sich normalerweise mit Dingen aus den Nachrichten: Michael Jackson oder Haiti. Endogene Trends sind meist Gedankenfetzen, z.B. #LetsBeReal oder #MeWithoutYouIsLike. Beide entstehen von innen heraus. Das «Trending Topic» Wahlen im Iran hat vielleicht aufgrund äußerer Umstände begonnen, wurde aber intern schnell als #IranElection verewigt.

Mich fasziniert an den Trending Topics, dass man durch sie die Seite ganz anders kennenlernt. Man lernt etwas über Menschen, die normalerweise nicht von der digitalen Elite oder den Nachrichten wahrgenommen werden. Laut «What the Trend» war Justin Bieber an 18 der letzten 30 Tage (im Februar/März 2010) in den Top 10. Auch wenn die Mehrheit der Teenager und Mittzwanziger vielleicht nicht auf Twitter ist, so sind die meisten von Justins 1,3 Millionen Followern doch ziemlich jung.

Es sind aber nicht nur die Teenager und Mittzwanziger, die sich durch die Trending Topics ein Gehör auf Twitter verschaffen. Wenn man vielen dieser Gedankenfetzen folgt, die in den Trending Topics vorkommen, wird man schnell feststellen, dass dort viele Schwarze laut und deutlich sagen, was sie denken. Wie mir ein afroamerikanischer User von Twitter erklärte, hat dieses Herumalbern auf Twitter sehr viel mit einer Weiterentwicklung der «Yo Mamma»-Kultur zu tun. Es ist ein Ort, an dem man Dampf ablassen kann, und zwar mit einer Art Humor, der manchmal eben auch vulgär ist. @LilDuvals komödiantisches #witmyrefundcheck macht sich über schwarze Stereotype lustig und ist ein Beispiel für diese Art von Humor.

Ich betone deshalb die Rolle der Schwarzen auf Twitter, weil sie bei manchen ziemliche Verärgerung hervorgerufen hat. Ich bin immer wieder entsetzt, wenn ich mit Rassismus und Klassendünkel in den Sozialen Medien konfrontiert werde, und schon allein die Tatsache, dass diese Phänomene dort vorkommen, sollte uns allen eine Warnung sein. Letzten Sommer, in der Nacht der BET-Awards, waren alle Trending Topics Ikonen der afroamerikanischen Community. Und wie haben nicht-schwarze User darauf reagiert? Einige nicht so nett: «Wow!! Zu viele Neger in den Trending Topics, wenn ihr mich fragt. Vielleicht hat sich diese ganze Twitter-Sache für mich erledigt.» «Hat jemand die Trending Topics gesehen? Ich glaube nicht, dass das hier eine gute Gegend ist. Schließt eure Autos ab, Leute.» «Warum sind diese ganzen Schwarzen in den Trending Topics? Neyo? Beyoncé? Tyra? Jamie Foxx? Ist schon wieder Black History Month? LOL» «So viele Schwarze!»

Sie benutzten das N-Wort und ließen sich darüber aus, wie Twitter zum Ghetto geworden sei. Indem manche User das taten, haben sie den Gedanken verstärkt, dass nicht jeder ein gern gesehener Teil der Öffentlichkeit im Netz ist.

Wessen Stimme zählt?

Wenn man über Öffentlichkeit nachdenkt, muss man sich auch Gedanken darüber machen, wer das Recht und Privileg dazu hat, ein Teil des öffentlichen Lebens zu sein. Wer spricht gern in der Öffentlichkeit? Welche Risiken gehen Leute ein, wenn sie sich öffentlich zu Wort melden?

Viele von uns profitieren davon, wenn sie sich durch Soziale Medien öffentlich zu Wort zu melden. Ich gehöre definitiv auch dazu. Ich führe gerade ein sehr privilegiertes Leben. Dadurch nimmt man aber auch schnell Dinge als gegeben hin. Als privilegierte Person glaube ich, dass ich Autoritäten in Frage stellen kann und dass ich das Recht besitze, gehört und gesehen zu werden. Ich denke, dass meine Meinung wichtig ist und ich meine Lebensgeschichte erzählen kann. Ich gehe selbstverständlich davon aus, dass ich in die Öffentlichkeit gehen kann, ohne dabei Angst haben zu müssen, meinen Job, meinen Partner oder meine Rechte zu verlieren. Ich kann «public by default», also grundsätzlich öffentlich sein, ohne dabei zu große Konsequenzen erwarten zu müssen. Genauso kann ich es überleben, wenn ein Technologie-Konzern Informationen über mich preisgibt, die ich nicht veröffentlichen möchte. Ich kann also sorgenfrei die Öffentlichkeit suchen.

Aber stellen Sie sich nun einmal vor, Sie wären ein Immigrant, dessen Familie vor 30 Jahren hier illegal eingewandert ist, als Sie gerade sechs Monate alt waren. Sie sprechen nicht die Muttersprache ihrer Vorfahren und waren noch nie in dem Land, in dem Sie geboren wurden. Sie sind vor Angst, ausgewiesen zu werden, wie gelähmt. Würden Sie sich dann dabei wohlfühlen, Ihre Lebensgeschichte in der Öffentlichkeit zu erzählen?

Oder stellen Sie sich vor, dass Sie gerade eine Beziehung beendet haben, in der Sie missbraucht wurden. Sie haben zwei Jobs, um zusammen mit den Kindern über die Runden zu kommen. Sie sind völlig erledigt und haben dabei immer die Angst im Nacken, dass Ihr Ex herausfindet, wo Sie sich aufhalten, um Ihnen und/oder den Kindern Schaden zuzufügen. Wie öffentlich will man dann noch sein?

Diese zwei Charakterskizzen sind keinesfalls frei erfunden. Sie basieren auf Menschen, die ich getroffen habe und die einfach nur versuchen, ihr Leben zu leben. Da draußen gibt es viele Leute, die sich große Sorgen darüber machen, wie diese neuen Technologien ihr Leben verändern. Es ist nicht so schwer, besonders ausgegrenzte Menschengruppen auszumachen und sich vorzustellen, was das für sie bedeutet. Eine Vielzahl von Menschen, die einer sexuellen Minderheit angehören, wurde aus dem Militär geworfen, weil man bestimmte Informationen über sie online gefunden hat. Wie ist das aber mit den Leuten, die wir normalerweise nicht als ausgegrenzt bezeichnen würden?

Denken Sie z.B. an die Lehrerin Ihrer Kinder. Wie öffentlich darf sie im Internet sein? Darf sie, je nach Ihrer eigenen Überzeugung, religiös oder atheistisch sein. Ist es okay, wenn sie auf einer Online-Dating-Website angemeldet ist? Darf sie Bilder ins Netz stellen, auf denen sie mit ihren Freunden Alkohol trinkt?

Darf sie als Geliebte oder Freundin in der Öffentlichkeit wahrgenommen werden, wo sie doch sonst immer nur «die Lehrerin» ist? Offline kann sie ganz einfach in ihre Rolle als «Lehrerin» wechseln, wenn man ihr auf der Straße begegnet. Wie schafft sie diesen Rollenwechsel aber online?

Sicher, jeder *sollte* das Recht haben, sich in der Öffentlichkeit wohlfühlen zu können. Das entspricht aber leider nicht der Realität. Die meisten Menschen versuchen einfach nur, irgendwie zurechtzukommen. Wir können es nicht erwarten, dass ausgegrenzte Personengruppen sich immer wieder das Recht erkämpfen müssen, gehört zu werden. Wir sollten es nicht akzeptieren, dass Personen aufgrund der Rollen, die sie spielen, ausgegrenzt werden. Diese «public by default»-Umgebung, bei der alles immer öffentlich ist und auf die wir so stolz sind, wirkt nicht immer demokratisierend; für viele ist sie genau das Gegenteil. Nur weil die Technologie es uns erlaubt, in der Öffentlichkeit zu sprechen, heißt das nicht, dass das jeder auch gern tut oder, nebenbei bemerkt, dass dies auch wahrgenommen wird. Vergessen Sie nicht: Die Technologien zur Schaffung von Öffentlichkeit können uns nicht per se die Aufmerksamkeit anderer garantieren.

Sehen und gesehen werden

Natürlich geht man manchmal auch deshalb online, weil man nach Aufmerksamkeit sucht und sich mit den neuen Verknüpfungsmöglichkeiten von Privatsphäre und Öffentlichkeit auseinandersetzen will. Im Internet werden Privatsphäre und Öffentlichkeit immer wieder neu miteinander vermischt. Ständig entdecken wir neue Hilfsmittel, die eine Weiterentwicklung von alten Tools sind. Oder, wie TV-Moderator Jon Stewart sagte: «Das Internet ist wie mexikanisches Essen – jede Website besteht aus denselben Zutaten, sie werden nur jedes Mal anders kombiniert.»

Kommen wir zu einer Website, die im vergangenen Jahr sowohl Neugier als auch Panik hervorgerufen hat. ChatRoulette war eine seltsame Kombination aus Privatsphäre und Öffentlichkeit. Auf der einen Seite saßen die Teilnehmer in Räumen, die sie normalerweise als privat bezeichnen würden, z.B. im Schlafzimmer oder am Arbeitsplatz. Indem es ChatRoulette aber ermöglichte, willkürliche Verbindungen zu Fremden aufzubauen, wurde es zu einem öffentlichen, vernetzten Raum. Die meisten Benutzer waren sich sicher, dass es nicht möglich war, sie physisch oder digital zu lokalisieren, es sei denn, sie gaben die Informationen selber frei. Dadurch wurde eine Art von Anonymität geschaffen, ein Gefühl der Unverbundenheit, die ChatRoulette sicher erscheinen ließ. Natürlich hat niemand kommen sehen, dass jemand bereits angefangen hatte, IP-Adressen zu erfassen und Fotos mit geographischen Standorten in Verbindung zu bringen. Man handelt hier also nicht so anonym, wie man denkt, es sei denn, man weiß, wie man das Computerprogramm Tor bedient.

Obwohl ChatRoulette nur ein Hype von kurzer Dauer war, kann man daran leicht erkennen, wie Öffentlichkeit und Privatsphäre auch zukünftig auf immer neue Arten miteinander vermischt werden dürften. Wir werden dabei sein, wenn

immer neue Hilfsmittel entwickelt werden, die die Grenze zwischen Privatsphäre und Öffentlichkeit weiter auflösen: Tools, die die Vorteile von Privatsphäre in Frage stellen und die uns neue Argumente liefern, weshalb wir uns in der Öffentlichkeit bewegen sollen. Weder die Privatsphäre noch die Öffentlichkeit ist tot, aber die technischen Möglichkeiten werden beide in Zukunft immer mehr miteinander vermischen.

Es gibt leider kein Patentrezept dafür, wie man die Beziehung zwischen Privatsphäre und Öffentlichkeit verstehen muss. Es gibt keine mathematische Gleichung und keinen einfachen Algorithmus, den man anwenden könnte. Privatsphäre und Öffentlichkeit sind lebende Organismen, ein komplexes Gemisch, das enorm wichtig für die Menschheit ist. Es handelt sich dabei im Grunde um Prozesse, die auf Bedürfnissen, Wünschen und Zielen basieren, die in ganz bestimmten Zusammenhängen eingebettet sind und von den technischen Möglichkeiten immer wieder neu erfunden werden. Egal, wie sehr man versucht, sich zu den Themen Privatsphäre und Öffentlichkeit zu positionieren, man sollte sich darüber im Klaren sein, dass es dafür keine endgültige Lösung gibt. Was man heute will, wird morgen schon wieder etwas anderes sein und das, was Sie selbst möchten, ist vermutlich etwas anderes als das, was Ihre Nachbarn wollen. Dieses Dilemma macht die technologischen Veränderungen so unglaublich chaotisch.

Wenn es um Öffentlichkeit geht, wird es viel einfacher sein, ein neues System zu erfinden, als das, was gerade genutzt wird, weiterzuentwickeln. Wenn man etwas eindeutig öffentlich macht, werden die User einen Umweg finden, um es dann schließlich so nutzen zu können, wie es für sie am sinnvollsten ist. Wenn man den Usern ein Gefühl von Privatsphäre und Intimität gibt, sie dann aber in der Öffentlichkeit bloßstellt, kann es nicht nur einen selbst, sondern auch die User ziemlich teuer zu stehen kommen. Man kann seinen guten Ruf verlieren und, es sei daran erinnert, auch das Leben anderer gefährden.

Teenager-Angst, Eltern und digitale Pubertät

Vielen Erwachsenen fällt es schwer, jungen Menschen dabei zu helfen, sich in dieser neuen Welt der Privatsphäre und Öffentlichkeit zurechtzufinden. Wahrscheinlich auch deshalb, weil Erwachsene genauso verwirrt sind. Das Schlimmste, was man als Elternteil dabei wohl tun kann, ist einen Satz mit «Zu meiner Zeit…» zu beginnen. Was damals war, spielt keine Rolle. Es ist aber sehr wohl wichtig, dass Eltern genauso versuchen, diese ständig wandelbare Umgebung zu verstehen. Anstatt den Teenagern zu sagen, was sie zu tun haben und wieso sie nichts über sich online stellen sollten, sollten Eltern sich lieber Gedanken darüber machen, wie wertvoll es sein kann, offen über etwas zu diskutieren. Eltern können einiges von den Teenagern lernen, schließlich mussten sie früher auch erst einmal aus dem öffentlichen Leben schlau werden. Der Unterschied besteht heute jedoch darin, dass Teenager nun in einer völlig neuen

Umgebung mit dieser Frage konfrontiert werden. Eltern sollten ihr eigenes Wissen als Grundlage nehmen und lernen, den Teenagern aktiv zuzuhören.

Der Schlüssel zum Erfolg liegt darin, sich selbst die wesentlichen Fragen zu stellen: Was wollen Sie erreichen? Was denken Sie, mit wem Sie gerade kommunizieren? Wie würden Sie sich dabei fühlen, wenn jemand anderer zusehen würde? Wie wäre es, wenn das, was Sie gerade gesagt haben, falsch verstanden würde? Diese Themen sollte man bei den Kindern schon früh ansprechen, um ihnen bei ihrer Entwicklung zu helfen. Aber ein Patentrezept gibt es hierfür leider nicht.

Es ist eine aufregende Zeit der Öffentlichkeit, in der man einen besseren Zugang zu Daten hat als jemals zuvor und in der man die Möglichkeit hat, Leute wahrzunehmen, die früher unsichtbar waren. Aber nur weil man die Möglichkeit hat, diese Leute wahrzunehmen, heißt das noch lange nicht, dass diese auch wahrgenommen werden wollen. Und nur weil man denkt, dass man diese Informationen deuten kann, heißt das nicht, dass diese Interpretationen auch zutreffen. Wir entwickeln uns zu einer Gesellschaft, die von Daten getrieben ist, und in mancherlei Hinsicht ist das eine gute Sache. Weiß Gott, ich wäre glücklich, wenn in der Politik mehr Wert auf Daten gelegt würde. Man muss sich aber auch darüber im Klaren sein, dass allein der Zugang zu Informationen weder bedeutet, dass diese Informationen ein korrektes Gesamtbild abgeben, noch dass die Menschen darüber erfreut sind, dass diese Informationen verfügbar sind.

Nur weil viele Menschen in der Öffentlichkeit agieren, muss dies nicht heißen, dass sie keinen Wert auf Privatsphäre legen. Das Forschungszentrum PEW hat herausgefunden, dass 85% der Erwachsenen selbst bestimmen wollen, wer Zugang zu ihren persönlichen Informationen hat. Obwohl man Daten immer auf verschiedene Weisen deuten kann, ist die einfache Annahme gefährlich, dass Menschen, die ihre persönlichen Informationen teilen oder Daten öffentlich zugänglich machen, keinen Wert auf Privatsphäre legen. Wenn man dies tut, dann missachtet man das Umfeld, in dem sich die Menschen bewegen, und welche Erwartungen sie an dieses haben.

Nur weil man sich Privatsphäre wünscht, heißt das nicht, dass man etwas verheimlichen will. Es geht darum, die Kontrolle darüber zu behalten. Oft geht es bei Privatsphäre nicht darum, etwas zu verbergen, sondern darum, einen Raum zu schaffen, den man nicht nach außen öffnen kann. Wenn man bedenkt, dass es bei Privatsphäre darum geht, die Kontrolle zu bewahren, dann kann man auch verstehen, wieso man zu dem Schluss kommt, dass Privatsphäre nicht tot ist. Es gibt gute Gründe, sich in der Öffentlichkeit zu bewegen; die hat es immer gegeben. Aber nur weil man sich in der Öffentlichkeit bewegen will, heißt das nicht, dass man komplett die Kontrolle verlieren möchte.

Dieser Text ist ein Ausschnitt aus dem Vortrag «Making Sense of Privacy and Publicity», den Danah Boyd am 13. März 2010 auf der Konferenz SXSW gehalten hat. Die vollständige englischsprachige Fassung des Texts kann man unter http://www.danah.org/papers/talks/2010/SXSW2010.html abrufen.

Aus dem Englischen übersetzt von Katja Ullrich.

«Aber ich inszeniere mich doch gar nicht bei Facebook, ich bin, wie ich bin.»

Ein Interview von David Pachali mit Krystian Woznicki

Die Digitalisierung der Gesellschaft ist ein Prozess, der nicht zuletzt die Darstellung, Inszenierung und Vermarktung der eigenen Biografie auf eine neue Grundlage stellt. Während das private Selbst zur verwertbaren Ressource avanciert, werden Künstler als ökonomische Role-Models gehandelt. Berliner Schüler und Studenten haben vor diesem Hintergrund bei dem Seminarprojekt «Lebenskünstler» unterschiedliche Experimente durchgeführt.

David Pachali: Im Februar 2011 war im Kunstraum Kreuzberg/Bethanien die Ausstellung «Lebenskünstler» zu sehen. Worum ging's?
Krystian Woznicki: Die Ausstellung zeigte die Ergebnisse eines mehrmonatigen Seminars, das ich gemeinsam mit meiner Kollegin Sarah Curth durchgeführt habe: Was im semi-privaten Bereich des Klassenraums erarbeitet wurde, wurde in der Ausstellung öffentlich gemacht.

Was passiert bei dem Schritt vom Privaten an die Öffentlichkeit?
Der Untertitel der Ausstellung lautet: Zwischen Facebook und Job-Interview. Wir haben bei dem Seminar die klassische Trennung zwischen einem privaten Selbst und einem öffentlichen Selbst in Frage gestellt. Die Auseinandersetzung beginnt bereits dort, wo wir die Teilnehmer/innen des Projekts damit konfrontierten, dass im Seminarraum ständig alles in Text und Bild dokumentiert wird. Wir machen das für die interne Kommunikation, aber auch, weil wir es letztlich der Öffentlichkeit zugänglich machen wollen. Dahinter steht eine Überzeugung: Im Klassenraum wird nicht mehr Wissen «one-way» von A nach B transferiert, sondern es entsteht in einer dialogischen Situation ein ganz neues Wissen. In diesem Sinne begreifen wir die Seminar-Situation als erweiterte Redaktionssitzung. Wenn sich die Redaktion derart öffnet, sollte das auch für den Klassenraum gelten. So können kollaborativ Inhalte für die Zeitung entstehen.

Bei den Teilnehmern des Seminarprojekts «Lebenskünstler» handelte es sich um Schülerinnen und Schüler sowie Studierende von 16 bis 25 Jahren. Wie haben sie auf diesen zwischen Dokumentation und Produktion changierenden Ansatz reagiert?

Alle haben Handys, doch die müssen während des Unterrichts ausgeschaltet sein, Laptops gehören an den höheren Bildungseinrichtungen zum Lernmaterial. Dennoch hat unsere Einführung der Medien in den Klassenraum zu einer gewissen Aufregung geführt. Es gab sehr unterschiedliche Reaktionen: «Ich will auf keinen Fall fotografiert werden». So wie es auch Leute gab, die sagten: «Ich will auf keinen Fall Fotos machen.» Dann wiederum: «Kann ich mich vorher noch ein wenig zurecht machen?» «Kommen wir damit in die Zeitung?» «Bekommen wir dafür Geld?» Wir haben versucht, die Aufregung produktiv zu machen. Einerseits für einen Bewusstwerdungsprozess im Hinblick auf die sich in der gesamten Gesellschaft auflösenden Grenzen zwischen Privatheit und Öffentlichkeit. Andererseits für einen kreativen Prozess, bei dem die alltäglichen Erfahrungen der Schüler und Studierenden als Basis für Experimente genommen wurden. Sounds, Videos, Fotos und Texte sind im Zuge dessen entstanden.

Gab es im Hinblick auf diese unterschiedlichen öffentlichen Sphären unterschiedliche Ansprüche?

Das meiste passte zwar ganz gut in eine Ausstellung, aber eben noch viel besser ins Netz, am besten vermutlich in ein soziales Netzwerk wie Facebook – in diesen merkwürdigen Zwischenraum der permanenten Selbstdarstellung, in dem Privates und Berufliches, Redundantes und Kunst schwer voneinander zu unterscheiden sind. Und doch, so scheint mir, gab es gegenüber der Veröffentlichung im Netz größere Vorbehalte: Würden die im Netz veröffentlichten Inhalte bis in das eigene Facebook-Profil durchsickern? Diese Aussicht schien einigen Beteiligten echte Sorgen zu bereiten.

Ein Schwerpunkt des Seminars lag ganz explizit auf der Selbstdarstellung bei Facebook und Co.

Ja, wir haben versucht, ein Licht darauf zu werfen, wie Inszenierungsprozesse dort ablaufen und mussten bei einigen erst durch eine teils recht dicke Wand der Unbedarftheit, frei nach dem Motto: «Aber ich inszeniere mich doch gar nicht bei Facebook, ich bin, wie ich bin.»

Man hört ja in den Medien oft die Erzählungen vom Personaler auf Facebook und von Jugendlichen, die alles preisgeben. Später kommt dann das böse Erwachen. Stimmt das eigentlich?

Ich denke, man muss differenzieren. Einerseits gibt es durchaus ein Bewusstsein für die eigene Privatsphäre, im Sinne von: «Mit wem teile ich meine Informationen?» «Mit wem freunde ich mich an?» Da werden keinesfalls alle möglichen Leute eingeschlossen, sondern sondiert und sortiert. Das hat uns kaum überrascht, denn offline handeln die meisten nicht anders. Andererseits gibt

es aber eben wenig Bewusstsein dafür, dass diese Privatsphäre immer stärker in Auflösung begriffen ist. Es gibt etwa kaum ein Bewusstsein für die Tatsache, dass Facebook zwar kostenlos ist, man aber mit seinen Daten bezahlt. Aber auch kaum ein Bewusstsein für die Tatsache, dass das «Gefällt-mir»-Prinzip zu einer Theatralisierung des privaten Selbst führt.

Ihr hattet bei dem Seminar mit unterschiedlichen Generationen zu tun: Schüler/innen der 10. und 12. Klasse sowie Erstsemester/innen. Die Unterschiede des sozialen Milieus kommen hinzu: in Neukölln eine Hauptschule – in Charlottenburg eine private Hochschule. Wie unterschiedlich nutzen die Schüler/innen und Student/innen Facebook?
Es gibt auf den ersten Blick mehr Gemeinsamkeiten als Unterschiede: Die Schüler/innen und Student/innen sind ja «digital natives». Wir haben das Projekt also mit dem Bewusstsein konzipiert, dass das Internet und soziale Netzwerke ganz selbstverständlich dazugehören. Gleichzeitig all das aber eben nicht ansatzweise in den Bildungseinrichtungen reflektiert wird – ich meine, im Lehrplan. Entsprechend sahen wir unsere Aufgabe darin, ihnen Denkanstöße zu geben, um sich kreativ und kritisch mit ihrer Position in der digitalen Gesellschaft auseinanderzusetzen. Dabei ist uns vor allem aufgefallen, dass Facebook als Raum der Selbstverwirklichung, sprich: Kultivierung von identitätsstiftenden Distinktionsmerkmalen, vor allem für die Jugendlichen aus den niedrigsten sozialen Sphären besonders wichtig ist – so, als ob sie andernorts nicht so viele Möglichkeiten zur Entfaltung hätten.

In den Sitzungen waren auch Künstlerinnen und Künstler zu Gast. Wie gestaltete sich die Zusammenarbeit?
Für die *Berliner Gazette* gehört das zur Tradition. Wir haben schon immer mit Künstlerinnen und Künstlern zusammengearbeitet. Wir haben bei diesem Seminarprojekt allerdings auch versucht, die Frage «Was bedeutet es, von der Kunst zu lernen?» auf neue Weise zu stellen. In der kulturellen Bildung geht es ja üblicherweise darum, die individuelle Wahrnehmung zu schulen und Kulturtechniken zu lernen. Die Lebensumstände des Künstlers bleiben jedoch außen vor. Unser Projekt schließt diese Lücke – beziehungsweise macht sie erst erkennbar. Die flexiblen Lebensentwürfe von Künstlerinnen und Künstlern sollten als Reibungsfläche dienen. Für eine Generation von Lernenden, die ihre Schul- und Studienzeit vielleicht als die erste und letzte «Festanstellung» in ihrem Leben erfahren, schien uns das besonders dringlich.

Vom Lebenskünstler bzw. Flaneur des Jahres 1839 sagt Walter Benjamin sinngemäß, er habe eine Schildkröte spazieren geführt und einen Gegenentwurf zur herrschenden (Zeit-)Ökonomie inszeniert. Selbstinszenierung und -vermarktung nach dem Vorbild von Künstlern ist aber heute eher eine ökonomische Forderung geworden – eine Anrufung, der man kaum entkommt. Wo bleibt die Kunst? Und wo bleibt das Leben?

Es ist doch so: Lange Zeit hatten Künstler eine soziale Sonderstellung. Sie schienen in einer Art Parallelwelt zu leben, in Abgrenzung zum Bürgertum und anderen sozialen Gruppen. Ohne geregelten Tagesablauf und ohne regelmäßiges Einkommen, statt Beruf eine Berufung, statt feste Identität, viele Masken. Heutzutage ist das Künstler-Dasein allerdings kein Außenseitermodell, sondern Mainstream. Die Anforderungen einer neoliberalen Gesellschaft, man müsse stets flexibel sein, man müsse sich immer wieder neu erfinden, man müsse jenseits der Festanstellung Arbeit finden und sein eigenes Leben zur primären Ressource für das Überleben machen – all diese Anforderungen machen den Künstler zum Vorbild für die gesamte Gesellschaft. Dies hat übrigens auch der Soziologe Zygmunt Baumann kürzlich diagnostiziert. Er sagt, die gesellschaftlichen Veränderungen zwingen viele dazu, ihr Leben als Kunstwerk zu betrachten. Ist das ein Fluch? Oder ein Segen? Die ehrlichste Antwort darauf ist wohl, keine eindeutige Antwort zu geben. Wichtiger ist es, die Bedingungen und Möglichkeiten auszuloten.

Was aber bedeutet dies für unser Verständnis von Privatheit?
Diskutierten wir gestern vornehmlich über die Auflösung der traditionellen Grenzen von Freizeit und Arbeit, reflektieren wir heute, was für Konsequenzen diese Prozesse auf alle Bereiche des Lebens haben. Wenn ich nicht mehr klar zwischen Hobby und Job, Leidenschaft und Pflichterfüllung, Home und Office unterscheiden kann, dann wird im Zuge dessen nicht zuletzt Privatheit neu verhandelt: Sie avanciert zu einer Ressource für die Vermarktung des Selbst. Auch deshalb ist Selbstdarstellung kein unschuldiger Akt, sondern mit den Verschuldungsrisiken des kapitalistischen Systems verbunden. Der Appell ist bekannt: Es gilt die Kapitalien der Privatsphäre schonungslos auszubeuten, um erfolgreich zu sein. Doch wir müssen uns fragen: Wie weit wollen wir damit gehen, den letzten Rückzugsraum als Ressource auszubeuten?

Der Theoretiker Matteo Pasquinelli spricht von einer gesellschaftlichen Verschiebung: Die Werteproduktion bewegt sich von einem «materiellen Raum der Fabrik» zu einer erweiterten «sozialen Fabrik». Und er stellt die Frage: Warum sollten wir nicht für Facebook-Arbeit bezahlt werden?
Diese Frage will darauf hinaus, ob wir Facebook-Arbeit nicht als eine Art Zivildienst ansehen sollten. Doch wie hängen «Dienst an der Gesellschaft» und «Bezahlung» heute zusammen? Es gibt einerseits eine Zunahme von ehrenamtlicher Arbeit, wir werden Zeugen von Phänomenen wie «Generation Praktikum» und erleben, teils am eigenen Körper, Prozesse der Selbstausbeutung. Die Frage «Bekomme ich dafür Geld?» hört man indes immer häufiger dort, wo wir diese Frage nun wirklich nicht erwarten – auch bei unserem Seminarprojekt: «Könnte ich als Schüler für meine Anwesenheit in der Schule nicht Geld bekommen?» Hier sind verschiedene Entfremdungsprozesse im Gange… Es ist ja nicht nur so, dass die digitalen Medien, sondern die Gesellschaft im Zuge ihrer Digitalisierung vor der Herausforderung steht, ein tragfähiges Geschäftsmodell finden

zu müssen. Die Tatsache, dass das Private zur zentralen Hypothek wird, ist ein Symptom unter vielen.

Das vom Berliner Projektfonds für Kulturelle Bildung geförderte Seminarprojekt «Lebenskünstler» wurde von der Berliner Gazette konzipiert und zwischen dem 1.9.2010 und 19.1.2011 an drei Berliner Bildungseinrichtungen realisiert: OSZ Handel 1 (Kreuzberg), Röntgenschule (Neukölln) und SRH Hochschule (Charlottenburg). Die Ergebnisse wurden vom 16. bis 28.2.2011 im Kunstraum Kreuzberg/Bethanien gezeigt und im Internet veröffentlicht: http://lebenskuenstler-projekt.de

DANIEL J. SOLOVE

Bedeuten soziale Netzwerke das Ende der Privatsphäre?

Auf Plattformen wie Facebook geben junge Leute immer mehr persönliche Informationen preis. Diese Offenheit hat gute wie schlechte Seiten. Menschen können ihre Ideen überall hin verbreiten, ohne auf Verleger, Sender oder andere filternde Multiplikatoren angewiesen zu sein. Aber wollen sie auch nach zehn Jahren noch als YouTube-Hype belächelt werden?

Er hat einen Namen, aber die meisten kennen ihn nur als «Star Wars Kid». Millionen von Menschen weltweit kennen ihn, doch unglücklicherweise geht seine Berühmtheit zurück auf einen der peinlichsten Momente in seinem Leben.

Im Jahr 2002, da war er 15, hat sich das Star Wars Kid dabei gefilmt, wie er einen Golfballaufheber schwang als wäre er ein Lichtschwert. Da ihm dabei die fachkundigen Choreografen der *Star Wars*-Filme nicht zur Seite standen, sieht man ihn in dem Video recht unbeholfen herumtapsen.

Das Video wurde von Mitschülern gefunden, Peiniger des Jungen, die es ins Netz stellten, wo es umgehend viele Fans fand und zum Erfolg wurde. In der Blogosphäre wurde der Junge verspottet, man machte sich über ihn lustig als pummeligen Tölpel, als Nerd.

Bald gab es Remixe, Videos des Star Wars Kid, aufgemöbelt mit Spezialeffekten. Einige bearbeiteten das Video so, dass der Golfballaufheber wie ein Lichtschwert leuchtete, andere unterlegten es mit Musik aus *Star Wars*, wieder andere schnitten es mit anderen Filmen zusammen – schließlich gab es Dutzende solcher um Effekte angereicherte Versionen. In einem Videospiel und in den Fernsehserien *Family Guy* und *Southpark* war das Star Wars Kid zu sehen. Es ist eine Sache, wenn jemand von Mitschülern getriezt wird, aber man stelle sich vor, was es bedeutet, wenn einen unzählige Menschen in aller Welt verspotten. Der Jugendliche ging von der Schule ab und musste psychologisch betreut werden. Was dem Star Wars Kid passiert ist, kann jedem passieren, im Handumdrehen. Dass persönliche Informationen gesammelt werden, ist heute schon fast selbstverständlich. Immer mehr Menschen haben Handys mit Kamera, digitale Rekorder, Webcams und andere Aufzeichnungstechnologien, die jederzeit Einzelheiten ihres Lebens aufnehmen.

Zum ersten Mal in der Geschichte kann fast jeder Informationen in alle Welt verbreiten. Es ist nicht mehr nötig, so bekannt zu sein, dass einen die Mainstream-Medien interviewen. Online kann jeder ein weltweites Publikum erreichen.

Durch die Technologie ist es zu einer Kluft zwischen den Generationen gekommen. Auf der einen Seite Schüler und Studenten, deren Leben sich virtuell um soziale Netzwerke und Blogs dreht, auf der anderen Seite ihre Eltern, deren Erinnerungen an Vergangenes aus verblassenden Erinnerungen, vielleicht auch aus Büchern, Fotos und Videos bestehen. Für die Generation von heute ist die Vergangenheit im Internet konserviert, möglicherweise für immer. Es stellt sich die Frage, wie viel Privatsphäre es für Menschen heute, im Zeitalter der allgegenwärtigen Netzwerke, noch gibt beziehungsweise wie viel Privatsphäre Menschen sich noch wünschen.

Generation Google

Die Zahl junger Menschen, die soziale Netzwerke wie Facebook und MySpace nutzen, ist überwältigend. An den meisten Universitäten haben über 90 Prozent der Studierenden eine Seite. Ich nenne die, die heute aufwachsen, «Generation Google». Zahlreiche Bruchstücke ihres Privatlebens werden für immer online sein, auffindbar für kommende Generation durch eine simple Google-Suche.

Diese Offenheit hat gute wie schlechte Seiten. Menschen können ihre Ideen überall hin verbreiten, ohne auf Verleger, Sender oder andere filternde Multiplikatoren angewiesen zu sein. Jedoch birgt dieser Wandel auch erhebliche Gefahren für Privatsphäre und Ansehen. Die *New York Times* wird sich kaum für die neuesten Gerüchte an der Dubuque Senior High School oder der Oregon State University interessieren; Blogger und andere, die online kommunizieren, vielleicht aber schon. Für sie sind Storys und Gerüchte über Freunde, Feinde, Verwandte, Vorgesetzte, Kollegen und andere das Material, aus dem ihre Postings entstehen.

Bevor es das Internet gab, hat sich Klatsch mündlich verbreitet und blieb somit innerhalb enger sozialer Kreise. Durch die durch das Internet entstandenen sozialen Netzwerke können Gemeinwesen in aller Welt wieder das engmaschige Netz ausbilden, das für die vorindustrielle Gesellschaft typisch war und das dazu führte, dass jedes Mitglied eines Stamms, jeder Angehörige einer bäuerlichen Dorfgemeinschaft alles über jeden wusste. Der Unterschied dabei ist nur, dass nun die «Dorfgemeinschaft» die ganze Welt umspannt.

Vermehrt stellen Studierende schlüpfrige Einzelheiten über Kommilitonen online. Die Website JuicyCampus ist ein Forum, in dem Studierende anonym und ohne Überprüfung des Wahrheitsgehaltes schmutzige Geschichten über Sex, Drogen und Suff posten können. Auf einer anderen Website, Don't Date Him Girl, können Frauen über Männer, mit denen sie etwas hatten, lästern – Namen und Fotos inklusive.

Nicht nur von sozialen Netzwerken und Blogs geht eine Gefahr für die Privatsphäre aus. Firmen sammeln allzeit persönliche Informationen über uns. Ihre Kreditkartenfirma weiß, was sie gekauft haben. Kauft man online ein, protokollieren die Anbieter jede Transaktion. Ihr Internetanbieter hat Informati-

onen darüber, was sie online machen. Ihr Kabelfernsehanbieter sammelt Daten darüber, was sie sich ansehen.

Auch die US-Regierung beeinträchtigt die Privatsphäre, indem sie umfangreiche Datenbanken anlegt, die auf verdächtige Verhaltensmuster hin durchsucht werden können. Die National Security Agency überwacht und untersucht Millionen von Telefongesprächen. Andere Behörden überwachen Geldtransaktionen. Tausende Behörden der US-Regierung und der Bundesstaaten verfügen über persönliche Informationen zu Geburten, Heiraten, Berufstätigkeit, Grundeigentum und mehr. Diese Informationen und Daten sind häufig öffentlich zugänglich – und, je mehr sie in elektronischer Form vorliegen, umso leichter sind sie abzurufen.

Die Zukunft des öffentlichen Ansehens

Die weitreichende öffentliche Verfügbarkeit persönlicher Informationen beeinträchtigt unsere Fähigkeit, selbst über das Bild zu bestimmen, das andere von uns haben. Ein guter Ruf spielt in der Gesellschaft eine wichtige Rolle. Um ihn zu schützen ist es wichtig, dass wir unsere Privatsphäre abschirmen können. Abhängig vom Ruf einer Person entscheiden wir, ob wir Freundschaften schließen, uns verabreden, jemanden einstellen, mit Anderen Geschäfte machen.

Manche glauben, der Verfall der Privatsphäre könne dazu führen, dass wir weniger gehemmt und aufrichtiger sind. Wenn jedoch die Verfehlungen aller öffentlich sind, muss das nicht heißen, dass wir einander milder beurteilen. Habe ich persönliche Informationen über Sie, beurteile ich Sie nicht automatisch besser. Es erhöht vielmehr die Wahrscheinlichkeit, dass ich vorschnell ein negatives Urteil fälle. Zudem kann der Verlust der Privatsphäre unsere Freiheit einschränken. Das hohe Maß an Sichtbarkeit in einer transparenten Online-Welt kann dazu führen, dass Fehler, die man einmal gemacht hat, nie dem Vergessen anheimfallen.

Wir wollen die Möglichkeit haben, «von Neuem zu beginnen», uns lebenslang neu zu erfinden. Der US-amerikanische Philosoph John Dewey sagte einmal, eine Person sei nicht «etwas Vollständiges, Perfektes [oder] Abgeschlossenes», sondern «etwas, das sich bewegt, verändert, unstetig ist, etwas Beginnendes und nicht Abgeschlossenes». In der Vergangenheit konnten wir hinter uns lassen, was wir als Jugendliche trieben, wie wir über die Stränge geschlagen haben, und neu beginnen, uns verändern und wachsen. All die Informationen, die online stehen, machen ein solches Vergessen erheblich schwieriger. Heute müssen die Menschen mit dem digitalen Gepäck ihrer Vergangenheit leben.

Diese Offenheit bedeutet, dass Angehörigen der Generation Google wegen Dingen, die sie vor Jahren in ihrer stürmischen Jugend getan haben, eventuell weniger Möglichkeiten offen stehen. Bekannte können private Geheimnisse über sie preisgeben. Sie können das Opfer nicht zutreffender Gerüchte werden. Ob es uns gefällt oder nicht, viele Menschen gewöhnen sich allmählich daran, dass sich immer mehr persönliche Informationen über sie online abrufen lassen.

Was ist zu tun?

Lässt sich eine Zukunft abwenden, in der ein großes Maß an persönlichen Informationen verfügbar ist, ohne dass die Betroffenen darauf Einfluss haben? Einige Technologen und Juristen verneinen dies uneingeschränkt. Sie glauben, das Konzept einer Privatsphäre lasse sich nicht mit einer Welt in Einklang bringen, in der Informationen frei fließen – oder in den oft zitierten Worten von Scott McNealy von Sun Microsystems: «Es gibt heute schon keine Privatsphäre mehr. Findet Euch damit ab.» Auch in zahllosen Büchern und Artikeln wurde das «Ende», der «Tod» oder die «Vernichtung» der Privatsphäre beschworen.

Solche Prophezeiungen sind im besten Fall wenig durchdacht. Es ist immer noch möglich, die eigene Privatsphäre zu schützen, nur müssen wir dazu unser überholtes Verständnis des Konzepts überdenken. Einer Sichtweise zufolge müssen wir, wollen wir unsere Privatsphäre schützen, ganz auf Verschwiegenheit setzen, denn sobald andere Informationen über uns hätten, seien diese dadurch auch öffentlich. Eine solche Sicht der Privatsphäre taugt jedoch nicht für die Online-Welt. Die, die heute aufwachsen, haben ein differenziertes Verständnis von Privatsphäre. Sie wissen, dass persönliche Informationen regelmäßig zahllosen anderen mitgeteilt werden, und ihnen ist auch klar, dass sie, gleich was sie tun, eine Datenspur hinterlassen.

Zu dem feineren Verständnis, das die Generation Google von der Privatsphäre hat, gehört, dass man versucht, ein gewisses Maß an Kontrolle über solche Informationen zu behalten, die öffentlich zugänglich sind. Diese Generation will dabei mitreden, wie und wo Einzelheiten ihres Privatlebens öffentlich werden.

Die Frage, wer die Kontrolle über persönliche Informationen hat, rückte ins Blickfeld, als im Jahr 2006 Facebook eine neue Funktion namens News Feed einführte, die einen automatisch informiert, wenn Facebook-Freunde ihr Profil aktualisieren oder ändern. Die Betreiber von Facebook waren überrascht, dass viele Nutzer empört waren – es gab beinahe 700.000 Beschwerden. Auf den ersten Blick ist die Protestwelle gegen News Feed überraschend. Viele Nutzer, die sich an den Protesten beteiligten, hatten Profile, die komplett öffentlich einsehbar waren. Warum also glaubten sie, ihre Privatsphäre werde verletzt, wenn Facebook Freunde über Profil-Änderungen informiert?

Privatsphäre war für sie nicht gleichbedeutend mit sorgfältig verborgenen Geheimnissen, es war eine Frage der Zugänglichkeit. Sie gingen davon aus, dass die meisten anderen Nutzer ihre Profile nicht so genau anschauen würden, dass ihnen kleine Änderungen oder Updates auffallen würden. Folglich konnten sie Änderungen weitgehend unbemerkt vornehmen. Durch Facebooks News Feed wurden diese Informationen nun aber erheblich sichtbarer. Beim Schutz der Privatsphäre ging es hier also nicht um Geheimhaltung, sondern um Zugänglichkeit.

Im Jahr 2007 kam es erneut zu Protesten, weil Facebook die Privatsphäre verletzt habe. Diesmal ging es um eine Werbeplattform, die aus zwei Komponenten besteht, Social Ads und Beacon. Social Ads schickt jedes Mal, wenn Nutzer

auf Facebook Produkte oder Filme loben, in ihrem Namen, mit ihrem Bild und in ihren Worten Werbung an ihre Facebook-Freunde, in der Hoffnung, dies bilde einen stärkeren Kaufanreiz als konventionelle Werbung. Über Beacon wickelt Facebook den Austausch von Daten mit einer Reihe anderer kommerzieller Websites ab. Kaufte jemand auf Fandango.com eine Kinokarte oder auf einer anderen Website ein, dann wurde diese Information im Facebook-Profil abgelegt.

Facebook startete diese Anwendungen, ohne die User vorher ausreichend informiert zu haben. Manch einer musste plötzlich feststellen, dass er auf den Seiten seiner Freunde Produkte anpries. Für andere war es eine böse Überraschung, dass Einkäufe, die sie auf anderen Websites getätigt hatten, plötzlich Teil ihres öffentlichen Facebook-Profils waren.

Es kam zu einer Welle von Protesten. In einer daraus entstandenen Online-Petition wurde gefordert, Facebook müsse sein Geschäftsgebaren ändern. Rasch hatten Zehntausende unterschrieben, und Facebook nahm eine Reihe von Änderungen vor. Diese Beispiele zeigen, dass es beim Schutz der Privatsphäre nicht immer um die Frage geht, ob man Geheimes für sich behalten kann. Facebook-Nutzer wollten nicht, dass über Social Ads in ihrem Namen Produkte beworben werden. Es ist eine Sache, wenn man schreibt, wie sehr einem ein Film oder eine CD gefällt; es ist eine andere, wenn man als Plakatwand benutzt wird, um anderen Produkte zu verkaufen.

Vom Copyright-System lernen

In Kanada und in den meisten europäischen Staaten sind die Gesetze zum Schutz der Privatsphäre strenger als in den USA, wo es bislang keine umfassende Gesetzgebung dazu gibt. Datenschutzgesetze in anderen Ländern erkennen an, dass man, nur weil man anderen etwas mitgeteilt hat, seines Rechts auf Schutz der Privatsphäre noch lange nicht verlustig geht. In dem Maße, in dem sich Informationen besser und besser erschließen lassen, sollte das Rechtswesen der USA anerkennen, dass es nötig ist, einen gewissen Schutz der Privatsphäre auch im öffentlichen Raum zu garantieren.

Es gibt Bereiche im US-Recht, in denen die Regelung der Informationsverbreitung funktioniert. Das Urheberrecht beispielsweise erkennt das Recht der Öffentlichkeit an, auf Informationen zugreifen zu können und schützt gleichzeitig zahlreiche Werke, von Filmen bis hin zu Software. Um ein Werk urheberrechtlich zu schützen, muss man es nicht abkapseln. Eine urheberrechtlich geschützte Zeitschrift kann man lesen, man kann Privatkopien davon machen, sie anderen leihen. Dennoch kann man damit nicht tun, was man will: Es ist verboten, das gesamte Heft zu kopieren und Raubdrucke zu verkaufen. Im Urheberrecht wird versucht, ein Gleichgewicht zwischen Freiheit und Kontrolle herzustellen – angesichts der anhaltenden Konflikte des digitalen Zeitalters keine leichte Aufgabe.

In Sachen Schutz der Privatsphäre kommt das US-Recht einer Rechtsdoktrin ähnlich dem Urheberrecht am nächsten beim «Appropriation Tort», das

sind Regelungen, die es untersagen, Name oder Abbild einer Person unerlaubt zum eigenen finanziellen Vorteil zu nutzen. Leider hat sich die Auslegung dieser Regelungen so entwickelt, dass es gegen die neuen Bedrohungen der Privatsphäre wenig ausrichten kann. Das Urheberrecht ist in erster Linie ein Eigentumsrecht, das heißt, es schützt das Eigentum an einem Werk, beispielsweise einem Lied oder Gemälde. Um der wachsenden Bedrohung der Privatsphäre gerecht zu werden, sollte der Geltungsbereich des Appropriation Tort ausgeweitet werden. Eine solche Ausweitung könnte eine zu Beginn des 20. Jahrhunderts übliche Auslegung dieses Teils des bürgerlichen Rechts wiederaufleben lassen, der zufolge die Privatsphäre mehr bedeutet als der Schutz des Eigentums. Der Oberste Gerichtshof von Georgia erklärte 1905: «Das Recht einer Person, sich jederzeit dem öffentlichen Blick zu entziehen … ist Teil des Rechts auf persönliche Freiheit.» Aktuell greift diese Regelung nicht in Fällen, in denen der Name oder das Bild einer Person in Nachrichten, in Kunst, Literatur oder auf der Website eines sozialen Netzwerks erscheint. Während der Appropriation Tort davor schützt, dass Name oder Abbild ungewollt zu Werbezwecken verwendet werden, ist eine Verwendung in Nachrichten zulässig. Diese Unterscheidung ist von einiger Bedeutung, denn dadurch lässt sich das Gesetz kaum auf Web-Postings anwenden.

Eine Ausweitung des Appropriation Tort müsste abgewogen werden gegen das Recht, Nachrichten zu recherchieren und die Öffentlichkeit zu informieren. Gelten sollte sie nur für solche Fälle, in denen Fotos oder andere persönliche Informationen in einer Art und Weise genutzt werden, die keinen öffentlichen Belangen dient. Wie diese beiden Güter voneinander abzugrenzen sind, müsste notwendig fortlaufend Gegenstand von Rechtsprechung sein.

Im Zeitalter digital vernetzter Kommunikation muss innerhalb des bürgerlichen Rechts nicht nur der Appropriation Tort überarbeitet werden. Es gibt bereits eine Reihe rechtlicher Werkzeuge zum Schutz der Privatsphäre; allein ihre Definition dessen, was Privatsphäre ist, macht sie wenig wirksam. Bei einer allgemeinen Weiterentwicklung des Rechts müssten Fälle berücksichtigt werden, bei denen, wie im Falle des Star Wars Kid oder bei Facebooks Beacon-Anwendung, private Informationen auf problematische Art und Weise genutzt werden.

Am besten wäre es, wenn derartige Streitfälle außergerichtlich gelöst werden könnten. Elektronische Netzwerke sind heute jedoch derart weitreichend, dass sich Änderungen des bürgerlichen Rechts nicht werden vermeiden lassen. Die Privatsphäre ist heute stark bedroht, und immer mehr Menschen wird klar, wie wichtig ihnen ein Grundrecht auf Schutz der Privatsphäre ist. Um dieses Recht zu schützen, muss die Gesellschaft ein neues, differenzierteres Verständnis von öffentlichem und privatem Leben entwickeln, eines, das anerkennt, dass eine größere Menge an privaten Informationen verfügbar sein wird, das aber gleichzeitig den Menschen eine gewisse Entscheidungsfreiheit darüber gibt, wo diese Informationen erscheinen und wem sie zugänglich sind.

Dieser Artikel erschien zuerst in *Scientific American*, 18. August 2008.

Aus dem Englischen übersetzt von Bernd Herrmann.

FRANCESCA SCHMIDT

Trolljaner im Netz – Wie ist Sexismus, Rassismus und Homophobie beizukommen?

Im Internet weiß keiner, dass du ein Hund bist. Wenn du eine Frau bist und öffentlich feministische Fragen verhandelst, hat das aber mit Sicherheit Folgen. Der viel beschworene digitale Freiheitsraum als Spielplatz für verschiedene Online-Identitäten scheint sich manchmal in einen Ermöglichungsraum für Restriktionen zu verkehren. Ein Erfahrungsbericht über Trolle und Elfen, Kommentare und Netiquette.

Das World Wide Web etablierte sich anfangs als Raum für utopische Visionen. Das Aufbrechen der heteronormativen Matrix und hegemonialen Machtstrukturen schien in greifbarere Nähe gerückt. Doch ein Blick in Diskussions- und Entwicklerforen oder auf Blogcharts[1] u.ä. zeigt, dass dem nicht so ist. Das Internet ist von Männern «erfunden», gestaltet und genutzt worden. Online-Formulare, standardisierte Eingabemasken oder Suchformulare spiegeln eine starre Zweckrationalität wider, in der Verwertbarkeit das oberste Prinzip ist. Vornehmlich Männer beherrschen die breitenwirksamen, vermeintlich öffentlichen Themen des Internets, wie z.B. Politik, Wirtschaft und Technik, während Frauen die anscheinend privaten, weichen Themen (Mode, Stricken, Reisen, Familie usw.) besetzen.[2]

Mit dem Web 2.0 – der zweiten Entwicklungsstufe des Internet, die Empfänger/innen die Möglichkeit gibt, durch kollaborative und interaktive Elemente selbst zu Produzent/innen zu werden – findet eine zunehmende Verschiebung von öffentlichem und privatem Raum statt. Facebook-Gründer Mark Zuckerberg spricht sogar von «Post-Privacy». Jedoch werden Grenzen zwischen öffentlich und privat den Geschlechterstereotypen entsprechend im Internet reproduziert.

Denn was relevanten Öffentlichkeiten zuzurechnen ist, ist immer Ergebnis von Aushandlungsprozessen ressourcenstarker Akteure. Das Gesamtnutzungsbild im Internet zeichnet einen klaren Vorteil für Männer (80% Männer; 68%

1 Blogcharts 01/2011 – von 100 aufgeführten Blogs sind weniger als 5 fünf Frauen.
2 http://www.soz.uni-frankfurt.de/K.G/B1_2008_Hesse.pdf

Frauen)[3], über alle Altersklassen verteilt. Frauen hingegen nutzen vermehrt soziale Medien wie Facebook, die lediglich Teilöffentlichkeiten darstellen und außerdem in einer Linie mit dem tradierten Frauenbild als Trägerin des Sozialen, des Kommunikativen stehen. In der Alterskategorie 18-34 Jahre beträgt der Unterschied lediglich 2% (98% Männer; 96% Frauen). In der jungen Generation ist das Internet Teil des Alltags, beruflich wie privat, jenseits von Geschlecht. Viel entscheidender ist allerdings der Unterschied bei der Wahrnehmung von Möglichkeiten, Entscheidungsprozesse oder Diskussionen zu beeinflussen. Auch hier stehen Frauen den Männern bei denjenigen, die das Netz auch für Diskussionen nutzen, noch immer nach (9% Männer, 4% Frauen). Das Potenzial, Wissen und Erfahrungen von Frauen einzubringen bzw. zu unterstützen, minimiert sich damit, was eben erst in der Wikipedia-Debatte deutlich geworden ist. Der Anteil schreibender Frauen bei Wikipedia beläuft sich gerade einmal auf 10-15%. Als Grund für diesen niedrigen Prozentsatz führt die *taz* den «rauen Umgangston» an, der in den Foren der Wikipedia herrscht.[4] Unberücksichtigt bleibt hierbei jedoch die Frage nach der Qualität des Contents – nicht Masse, sondern auch Klasse sollte Faktor für Erhebungen sein.

Insbesondere queer-feministische Blogs oder Foren, die sich jenseits der hegemonialen Diskurse verorten oder diese «stören» wollen, bilden Teilöffentlichkeiten[5], deren Relevanz und politische Notwendigkeit in Frage gestellt werden. Tatsächlich entwickeln sich vermeintlich private und auf den ersten Blick irrelevante Themen schnell zu gesellschaftskritischen Diskussionen. Zum Beispiel verhandelt das Thema Kinderbetreuung, geführt in einem auf den ersten Anschein unpolitischen Forum für Frauen, strukturelle Versäumnisse der Politik und stellt gesellschaftliche Normen von Mutterschaft in Frage.

Eben jene queer-feministischen Netzwerke und Communities werden im Netz besonders oft konfrontiert mit Sexismus, Homophobie und/oder Rassismus im Netz. Susan Herring bezeichnet solche Communities daher als «verletzbar»: «Such groups can be considered vulnerable populations, in that they tend to be stigmatized and discriminated again by mainstream society.»[6] Die suggerierte Anonymität des Internets verleitet scheinbar Menschen dazu, Meinungen oder Ansichten in Communities einzubringen, die in einer realen Kommunikationssituation unangemessen oder sozial geächtet wären.

Nutzer/innen, die explizit versuchen, die Kommunikation in Netzwerken zu (zer-)stören, werden Trolle genannt. Schon in der nordischen Mythologie

3 http://www.forschungsgruppewahlen.de/Umfragen_und_Publikationen/Internet-Strukturdaten/web_IV_10.pdf 07.02.2011

4 http://www.taz.de/1/netz/netzkultur/artikel/1/wissen-fuer-alle-aber-nur-von-maennern/; http://www.zeit.de/digital/internet/2011-02/internet-frauen-maenner; http://www.spiegel.de/netzwelt/web/0,1518,742951,00.html

5 Siehe die Blogcharts 01/2011, wo dieses Themenspektrum vergeblich gesucht werden kann. http://www.deutscheblogcharts.de/archiv/2011-1.html

6 Susan Herring: *Searching for Safety: Managing a "Troll» on a feminist Discussion Board*. In: *The Information Society.* 18, Nr. 5, Routledge, 2002, S. 371-384.

galten Trolle als Schadensbringer und Bösewichte und stehen somit im klaren Gegensatz zu den heilsbringenden Feen und Elfen[7], was wiederum einer Vergeschlechtlichung insofern entspricht, dass Feen und Elfen als weiblich konnotierte Wesen Wünsche erfüllen und den Zusammenhalt stärken, wohingegen sich mit der Semantisierung des Trolls eine Vermännlichung andeutet. Wenn Troll-Sein implizit eine Vermännlichung ausdrückt, ließe sich argumentieren, dass damit eine Re-Maskulinisierung des Internetraumes erfolgt, wie sich bei unserem Blog www.streit-wert.boellblog.org zeigen lässt, auf dem eine profeministische Debatte bzw. ein Dialog durch Maskulinisten und in diesem Fall Trolle gestört wurde.

Was ist der Streit Wert?

Auf dem Debatten-Blog des Gunda-Werner-Instituts für Feminismus und Geschlechterdemokratie sollen in regelmäßigen Abständen Online-Debatten zu feministischen und geschlechterdemokratischen Themen ermöglicht werden. 2010 wurde das im selben Jahr veröffentliche, grüne Männermanifest «Nicht länger Macho sein müssen», das sich gegen traditionelle Männlichkeitskonzepte sowie hegemoniale Männlichkeit wendet und sich für vielfältige Verständnisse von Männlichkeiten einsetzt (in diesem Sinne profeministisch ist), zum Ausgangspunkt für eine Debatte gewählt.

Alle abgegebenen Kommentare wurden zunächst überprüft und Beiträge, die nicht den Kommentarregeln entsprachen bzw. die Debatte zu unterminieren versuchten, mit einem entsprechendem Hinweis an den/die Kommentator/in, gelöscht. Dieses Vorgehen hat den Ruf nach Zensur innerhalb der Kommentator/innen, dessen bzw. deren Kommentare gesperrt wurden, schnell laut werden lassen, was sie jedoch nicht daran hinderte, weiter zu kommentieren. 15 Blogbeiträge haben sich entweder politisch-pragmatisch oder wissenschaftlich-dekonstruktivistisch-queer mit aktueller Männerpolitik auseinandergesetzt. Insgesamt gibt es 360 freigeschaltete Kommentare (exklusive Pingbacks) und ungefähr 150 sind von der Moderation gelöscht worden. Von Anfang an war klar, dass besonders mit Kommentaren von Seiten sogenannter Männerrechtler/innen zu rechnen ist, da Online-Foren und Blogs wichtige Diskussions- und Vernetzungsmedien der «neuen» Männerrechtler/innen bzw. Maskulinisten sind.[8] Unter Männerrechtler/innen bzw. Maskulinisten ist in diesem Zusammenhang ein Zusammenschluss antifeministisch und zu Teilen misogyn skandalisierender Personen zu verstehen. Eine kleine statistische Erhebung hat gezeigt, dass 46% aller freigeschalteten Kommentare tendenziell antifeministisch waren, während

7 In der Regel spricht man im Internet nur von Trollen, selten von Trullas, die weibliche Form.

8 Thomas Gesterkamp: *Geschlechterkampf von rechts. Wie Männerrechtler und Familienfundamentalisten sich gegen das Feindbild Feminismus radikalisieren*, Bonn 2010, S. 8. Leider fehlen bisher genaue Untersuchungen zur Vernetzung von Männerrechtler/innen im Internet.

nur 39% als tendenziell profeministisch[9] zu bezeichnen sind, der Rest verhält sich nach dieser Kategorisierung eher neutral.

Das scheint den ersten Eindruck zu bestätigen, der entstehen kann, wenn die Kommentare auf dem Blog gelesen werden: Man ist umgeben von Menschen, die eine Revitalisierung von tradierten Rollenbilder proklamieren. Interessant jedoch ist, dass neun von 54 Benutzer/innen 78% aller freigeschalteten Kommentare geschrieben haben. Von diesen neun vertreten fünf eine tendenziell antifeministische, in dieser Hinsicht eher maskulinistische Haltung, drei argumentieren tendenziell profeministisch, eine Person argumentiert eher ausgleichend.

Nach Betrachtung der Zahlen kann man feststellen, dass von den 78% «nur» 42% Männerrechtler/innen zuzuordnen sind. Profeministische Kommentator/innen haben 40% und die nicht zuzuordnenden Personen 18% der Kommentare abgegeben. Diese Zahlen spiegeln zunächst ein ausgewogenes Verhältnis wieder. Tatsächlich wurde der öffentliche Raum, der geschaffen wurde, um Männerpolitiken vielfältig und kritisch zu diskutieren, vornehmlich genutzt, um das Gegenteil zu praktizieren. Mit langen, sich ständig wiederholenden antifeministischen Pseudo-Argumenten, die eine produktive Diskussion unmöglich machten, wurde die Kommentar-Debatte in eine Richtung gelenkt, die der Vielfalt der eigentlichen Debattenbeiträge nicht gerecht wurde. Was positiv hervorzuheben ist und eher selten in feministischen Räumen im Internet vorkommt, ist, dass es nur zwei (Troll-)Kommentare mit sexistischem und rassistischem Inhalt gab. Sie wurden gelöscht.

Wie ist Trollen beizukommen? Einige Gegenstrategien

Grundsätzlich kann jedes Forum, jeder Blog, jede Internetseite, die Nutzer/innen die Möglichkeit der Kommunikation untereinander bietet, von Trollen besucht werden; nicht selten jedoch sind es die «verletzbaren» Netzwerke. Diese stehen/standen in dem Zwiespalt zwischen den eingeforderten demokratischen Prinzipien von Rede- und Meinungsfreiheit und dem Bedürfnis eines sicheren, aber dennoch zugänglichen Raums für Interessierte. Gesperrte Kommentare werden dann sofort mit Zensur gleichgesetzt. Der deutschsprachige Blog www.maedchenmannschaft.net hat mehr als 1.600 dieser nicht freigeschalteten Kommentare zu verzeichnen, die meist sexistischer Natur sind.[10]

Ein anderes probates und mittlerweile oftmals praktiziertes Mittel, Trollen Einhalt zu gebieten, ist die Nutzung der Freischaltfunktion von Kommentaren. Bevor ein Kommentar online geht und somit in die Debatte einfließen kann, muss

9 Es sei darauf hingewiesen, dass es mehr als eine Strömung des Feminismus gibt, so dass die Einteilung zwischen pro- bzw. antifeministisch in diesem Rahmen nur allgemein sein kann.

10 http://maedchenmannschaft.net/sexismus-im-netz-ein-ganz-alltaglicher-kampf/ und http://maedchenmannschaft.net/ihr-durchtriebenen-miesen-fotzen/

er von eine/r Administrator/in gelesen und bewertet werden.[11] Kommentarregeln bzw. die viel beschworene Netiquette sind mittlerweile ebenfalls Standard, stellen jedoch in keiner Form eine technische Hürde für Trolle dar. Eine Strategie ganz anderer Art ist die Monetarisierung der Troll-Kommentare. Dabei wird eine Webseite geschaltet, auf der Troll-Kommentare anonym gepostet werden. Die Einnahmen aus der auf der Seite geschalteten Werbung können dann genutzt werden, um sonst minorisierte Projekte finanziell zu unterstützen. Zwar hilft das nicht zwingend, die Kommunikationskultur zu verbessern[12], doch könnte es Teil einer «größeren», noch zu entwerfenden Strategie sein.

Wie wichtig das Nachdenken über Gegenstrategien ist, hat die letztjährige re:publica10 gezeigt. Hilflos standen dort die Administrator/innen sexistischen Kommentaren im Livechat gegenüber. Bei dem Panel «Das andere Geschlecht – Sexismus im Netz"[13] wurde über Sexismus im Netz gesprochen und im Livechat, der zum Livestream gehörte, Sexismus im Netz praktiziert. Hier zeigte sich, wie schnell eine Online-Diskussion (zer)stört werden kann, und, dass Sexismus im Netz keine Randerscheinung ist. Der viel beschworene Freiheitsraum Internet als Spielplatz für verschiedene Online-Identitäten scheint sich hier zu verkehren in einen Ermöglichungsraum für Restriktionen.

Die Hoffnung, die sich mit der Sichtbarmachung von hinter Namen vermuteten Identitäten verbindet, ethisches Handeln und verantwortlichen Umgang mit Kommunikation und Sprache hervorzubringen, wird durch diejenigen ad absurdum geführt, die überhaupt erst durch die Techniken des Cyberspaces hervorgebracht wurden. So ermöglicht das Internet, eine temporäre Online-Identität anzunehmen, auf deren Konstrukt man sich für einen bestimmten Zeitraum berufen kann. Eben jenen diversen Identitätskonstruktionen bietet das Internet mit seinen Möglichkeiten enormen Vorschub, die sich dann in ganz verschiedenen Communities wiederfinden – was im Sinne einer performativen Ausgestaltung von Gesellschaft nicht zwingend negativ zu bewerten ist. Jedoch setzt sich, wie Peter Weibel es formulierte, konservatives Gedankengut durch.[14] Somit bleibt das Internet ein heteronormativer und in dieser Hinsicht stark konfigurierter Raum. Die Kategorie «sex» bzw. «gender» pendelt z.B., vor allem in Online-Formularen, immer zwischen männlich und weiblich.

Der viel beschworene Begriff der Medienkompetenz wird in Zukunft nicht an Bedeutung verlieren, denn kommunikative, kooperative, transkulturelle und soziale Kompetenzen sind von Nöten, um das Netz von heute in ein Netz

11 Susan Herring verweist darauf, dass Gruppen, die besonders für Trolle und Belästigungen bzw. Bedrohungen «anfällig» sind, von einer strikten, zentralisierten Moderation profitieren.

12 Diese Idee wurde auf dem letztjährigen genderCamp2010 diskutiert: http://gendercamp.posterous.com/trolle-monetarisieren und hier bereits praktiziert: http://dooce.com/hate/

13 http://www.piratenweib.de/republica-sexisticum ; http://antjeschrupp.com/2010/04/15/zwei-drei-gedanken-zum-panel-sexismus-im-netz/; http://re-publica.de/10/blog/2010/04/19/trolle-im-livestream-chat/

14 http://www.taz.de/1/leben/taz-medienkongress-2011/artikel/1/die-buerger-wollen-das-monopol-brechen/ (11.02.1011)

von morgen zu führen – ein Netz, in dem eine Diskussions- und Wissenskultur Einzug hält, die das Individuum und die Gemeinschaft schätzt und frei von Geschlechterstereotypen, Homophobie und Rassismus ist. Unterstützen kann dies auch eine partizipative technische Weiterentwicklung des Netzes. Nicht nur Wissen und Content kommen von Vielen, sondern auch die technischen Grundlagen; Open-Source-Projekte gehen hier mit gutem Beispiel voran. Trolle werden sich auch im Internet der Zukunft tummeln. Vielleicht wird ihnen das Leben aber durch die Entschlossenheit der Nutzer/innen, die Bildung neuer (größerer) Öffentlichkeiten für Themen jenseits des Mainstreams und einem daraus folgenden sozialen Druck in Zukunft schwerer gemacht.

HELEN NISSENBAUM

Privatsphäre im Kontext: Technologie, Politik und die Unversehrtheit des Sozialen

Wie sollte ein kategoriales Bezugssystem aussehen, das genutzt werden kann, um sich dem schwer fassbaren Begriff der Privatsphäre anzunähern, ohne der überkommenen Theorie der Sphärentrennung in öffentlich und privat anheimzufallen? Es geht darum, ein flexibles Beschreibungsmodell zu entwickeln, das in der Lage ist, die oft impliziten informationellen Normen zu erfassen, in die soziales Handeln eingebettet ist.

Der entscheidende Punkt, auf den ich im Folgenden eingehen möchte, ist nicht, dass die Zweiteilung in Privates und Öffentliches an sich problematisch ist, sondern dass sie nicht dazu taugt, auf ihr eine normative Vorstellung von Privatsphäre zu gründen. Zwar mag uns diese Zweiteilung in der Vergangenheit nützliche Näherungswerte dafür gegeben haben, wie weit das Recht auf Schutz der Privatsphäre reichen soll, ihre Begrenzungen sind jedoch in dem Maße offensichtlich geworden, in dem digitale Informationstechnologien grundlegend die Bedingungen gewandelt haben, unter denen wir – Einzelne, Körperschaften und auch die Regierung – Zugriff auf uns und auf Informationen über uns haben – und das sowohl in Bereichen, die für gewöhnlich als öffentlich oder auch als privat galten.

Das Bezugssystem der Unversehrtheit des Kontexts

Die Hauptthese meines Beitrags: Das Recht auf Schutz der Privatsphäre ist weder ein Recht auf Geheimhaltung noch ein Recht auf Kontrolle, sondern ein Recht darauf, dass der Fluss persönlicher Informationen *situationsgerecht,* das heißt *angemessen* ist. Aus dem Konzept der Unversehrtheit des Kontexts ergibt sich eine schlüssige Vorstellung von Angemessenheit. Die Privatsphäre kann dennoch weiterhin als ein wichtiges Menschenrecht, als ein Wert, den es lohnt, gesetzlich und anderweitig zu schützen, ausbedungen werden, jedoch nur im Sinne eines Rechts auf die Unversehrtheit des Kontexts. Wie weit *diese* reicht, ist je nach Kontext unterschiedlich.

Die grundlegenden Bestandteile einer Unversehrtheit des Kontexts sind der soziale Rahmen und die informationellen Normen, die innerhalb eines jeweiligen Rahmens gelten. Die Normen, die den Fluss persönlicher Informationen im jeweiligen Rahmen festschreiben, sind wesentlicher Teil der fraglichen Informationsarten. Die jeweiligen Rollen des Gegenstands, des Senders (der der Gegenstand sein kann) und des Empfängers dieser Information sowie die Grundsätze, die für die Übertragung der Information von Sender zu Empfänger gelten, bilden einen Teil davon. Wird gegen diese Normen verstoßen, nehmen wir das als Übertretung wahr. Das Problem bei vielen umstrittenen sozio-technischen Systemen besteht darin, dass sie gegen etablierte informationelle Normen verstoßen und dadurch die Unversehrtheit des Kontexts gefährden.

Verfechter des Schutzes der Privatsphäre werden nicht zu Unrecht diejenigen des kaum verhohlenen Opportunismus bezichtigen, die vorgeben, die Privatsphäre wahren zu wollen, gleichzeitig aber darauf bestehen, dies müsse abgewogen werden gegen die Notwendigkeit, persönliche Informationen aus Gründen der Effizienz oder des Rechts und der Sicherheit zu sammeln und weiterzugeben. Gleichermaßen könnten sie auch diejenigen, die die Unversehrtheit des Kontexts für einen angemessenen Informationsfluss (und eben nicht dessen Eindämmung) beschwören, des Opportunismus bezichtigen. Das jedoch wäre ein Fehler. Die Privatsphäre, verstanden als Unversehrtheit des Kontexts, ist ein komplexes, labiles Netz von Beschränkungen für den Fluss persönlicher Informationen, das ein Gleichgewicht zwischen verschiedenen Bereichen des gesellschaftlichen und politischen Lebens herstellt. Systeme und Verfahren, die dieses Netz von Beschränkungen grundlegend stören, sind nicht nur eine Gefahr für unseren immer noch wenig beachteten Neuankömmling unter den Werten und Rechten, sie können auch das Gefüge des gesellschaftlichen und politischen Lebens bedrohen.

Einige Kritiker weisen darauf hin, dass die Normen für den Schutz der Privatsphäre im Vergleich unterschiedlicher sozialer Gruppen – und selbst innerhalb von diesen – sehr stark voneinander abweichen, und ziehen daraus den Schluss, dass es sich dabei nicht um einen universellen menschlichen Wert, sondern um eine kulturell sehr relative Empfänglichkeit handelt. Das Bezugssystem der Unversehrtheit des Kontexts setzt gleichfalls hier an, kommt aber zu ganz anderen Schlussfolgerungen. In der Tat unterscheiden sich die Erwartungen der Menschen daran, wie sehr sie den Fluss privater Informationen selbstbestimmt kontrollieren können, sehr. Diese Erwartungen jedoch sind konsequent abhängig von den Eigenschaften der ihnen zugrunde liegenden gesellschaftlichen Situation.

Vom Leben in Kontexten

Im Laufe unserer Leben handeln wir (in beiden Wortsinnen) nicht als bloße Individuen in einer gesellschaftlich nicht ausdifferenzierten Welt, wir handeln als Individuen in jeweils bestimmten Funktionen und Rollen, die sich in dem

Maße wandeln, in dem wir uns durch eine Vielfalt unterschiedlichster gesellschaftlicher Kontexte bewegen. Mit diesen Kontexten meine ich strukturierte gesellschaftliche Umgebungen, deren Eigenschaften sich im Laufe der Zeit (manchmal über sehr lange Zeit) entwickeln, und die von einer großen Menge von Eventualitäten wie Absichten, Orten, Kulturen, historischen Zufällen und so weiter abhängig sind.

Die Idee eines gesellschaftlichen Kontexts ist nicht meine Erfindung. Ich greife zurück auf eine in der Praxis oft bestätigte, unmittelbare Erkenntnis, die die Sozialwissenschaften und die Philosophie konsequent weiterentwickelt haben, nämlich dass Menschen sich zueinander nicht einfach wie Mensch zu Mensch verhalten, sondern dass sie in Rollen handeln, die durch gesellschaftliche Felder herausgebildet werden. In institutionellen Kontexten wie der Ehe oder der Elternschaft gehen die wechselseitigen Erwartungen der Beteiligten auf Regeln zurück, die sich die Einzelnen nicht einfach ausgedacht haben. Michael Walzer postuliert, dass es unterschiedliche gesellschaftliche Bereiche gibt – Politik, Arbeit, Markt, Familie, Staat, Schule und so weiter – die sich durch unterschiedliche gesellschaftliche Aufgaben auszeichnen, deren genaue Bedeutungen den jeweiligen Bereichen nach einem festen Set von Regeln zugeordnet wird.

Selbst innerhalb einer konkreten Gesellschaft kann die Art, in der wesentliche Merkmale in unterschiedlichen Kontexten zum Ausdruck kommen, stark variieren. Ein Aspekt dieser Variabilität ist, wie genau die jeweiligen Merkmale ausdefiniert sind. Bestimmte Kontexte sind bis ins Detail ausdefiniert, beispielsweise Wahllokale, Gerichtssäle sowie stark rituell geprägte Anlässe wie Gottesdienste. In solchen Kontexten ist das Handeln, sind die Gebräuche umfassend festgelegt, und sie werden bis ins Detail von zahlreichen Normen geregelt. Bei demokratischen Wahlen sind in einem Wahllokal die Rollen fest verteilt, und was man in einem solchen Kontext tut oder sagt, wird durch Gesetze, Vorschriften und manchmal auch örtliche Bräuche bestimmt. Im Unterschied dazu unterliegen Kontexte wie geschäftliche Besprechungen oder Wochenmärkte oft nur wenig oder nur zum Teil einem Regelwerk.

Kontexte unterscheiden sich weiter dadurch, wie stark sie institutionalisiert und allgemein oder offiziell anerkannt werden. Gesetze stellen eine wichtige Methode dar, einen Kontext zu kontrollieren und gegebenenfalls Sanktionen zu verhängen. Andere Methoden, mit denen bestimmte Zusammenhänge oder Teilkontexte institutionalisiert werden, sind beispielsweise die Satzung eines Berufsverbands, eines Vereins oder einer Religionsgemeinschaft. Solche Methoden können auch zusammenwirken. Gesetze können einen Rahmen für bestimmte Kontexte schaffen, beispielsweise für Unternehmen oder Berufszweige, der dann von den Regelwerken, die für bestimmte Unternehmen oder Berufszweige gelten, weiter ausgeführt werden, indem sie etwa festlegen, welche Ämter, Ziele, Verfahren und Verhaltensnormen es gibt. Solche ausdrücklich und offiziell festgelegten Normen können sich mit weiteren vermischen, die nur stillschweigend oder nur zum Teil in bestimmten Kontexten greifen. Ich gehe davon aus, dass viele Meinungsverschiedenheiten über Art und Reichweite des Schutzes

der Privatsphäre ihre Ursache in dieser Variabilität von Normen in unterschiedlichen Kontexten haben. Das eine Lager ist nur gewillt, das anzuerkennen (Rollen, Tätigkeiten, Normen, Werte), was offiziell in Gesetzen zum Schutz der Privatsphäre festgelegt ist. Andere hingegen halten auch solche Einschränkungen für legitim, die aus anderen Quellen herrühren, seien es Gepflogenheiten, Kunst, Literatur und selbst Benimmregeln.

Kontexte können sich überschneiden und widerstreiten. Hin und wieder kommt es vor, dass die in einem Kontext gültigen Normen gegen die Normen eines anderen, diesen überschneidenden Kontext verstoßen. In solchen Fällen stehen wir vor einer schweren Wahl: Ein Onkel kann dazu geneigt sein, seiner Nichte einen Job zu geben – aus Zuneigung und weil er zur Familie halten will. Andererseits kann es Gründe dafür geben, einen anderen Bewerber vorzuziehen, jemanden mit größerer Berufserfahrung. Ein Arzt sollte einen Patienten eindringlich davor warnen, dass seine Ernährung sehr ungesund ist, kann aber als Freund davon absehen, da in diesem Kontext ein solcher Rat bevormundend und wie ein Eingriff in die Privatsphäre wirkt.

Obgleich, wenn man die Einzelheiten in bestimmten Kontexten sorgfältig gegeneinander abwägt, eine Handlungsweise einer anderen vorzuziehen ist, gibt es keine allgemeingültige Lösung für Widersprüche dieser Art, und manche können einfach unlösbar sein. Prallen unterschiedliche Kontexte aufeinander, so dass es zu Konflikten kommt, so steht dies doch nicht im Widerspruch dazu, dass unser gesellschaftliches Leben durch unterschiedliche Kontexte strukturiert ist, denn, wie Isaiah Berlin gezeigt hat, bedeuten auch Wertekonflikte nicht, dass der Pluralismus der Werte hinfällig ist. Zwar lassen sich manche Konflikte, mit denen wir es zu tun haben, klären oder sogar lösen, wenn wir uns vernünftiger Strategien bedienen (es gibt derer zu viele, als dass sie hier aufgeführt werden könnten), andere jedoch sind dafür zu tief in unserer Welt verwurzelt. Der Theorie wird man dies nicht ankreiden dürfen – solche Herausforderungen sind ein Teil des Lebens.

Mit Normen

Normen können unterschiedlich ausgelegt werden. Das Konzept einer Norm ist unterfüttert von Sinngehalten, die wir intuitiv erfassen, die von Gepflogenheiten herrühren und aus unserem gelebten Leben. Ich strebe eine Interpretation an, die einer natürlichen so nah wie möglich kommt und die durch die Erkenntnisse einer kleinen Auswahl einschlägiger Studien weiter präzisiert wird.

Wenn ich sage, eine Handlung oder Gepflogenheit werde von Normen bestimmt, meine ich damit nicht nur, dass die Menschen sich im Allgemeinen daran halten, sondern dass sie dies tun, weil sie daran glauben. Desweiteren übernehme ich die Anatomie der Normen, die Raz im Gefolge von Georg Henrik von Wright entwickelt hat und in der vier Schlüsselelemente für Normen aufgeführt werden:

1. ein Element mit Vorschriftcharakter;
2. ein Subjekt, für das die Norm gilt;
3. eine normative Handlung, d.h. eine in der Norm festgelegt Art zu handeln;
4. eine Bedingung für ihre Anwendung, d.h. die Umstände unter denen vom Gegenstand der Norm erwartet wird, dass er normativ handelt.

Die Normen, die unser Leben bestimmen, sind weitgehend in Systeme eingebettet. Spielregeln, Gesetze, die Statuten eines Verbands oder Vereins, die Prinzipien eines beruflichen Ehrenkodex sowie kontextbezogene Normen sind allesamt Beispiele für normative Systeme. Um die Elemente zu finden, die den Zwangscharakter eines normativen Systems ausmachen, muss man sie vor dem Hintergrund des Gesamtsystems betrachten, denn für sich genommen mögen sie beliebig oder gar fragwürdig erscheinen. Bestimmte Verkehrsregeln beispielsweise ergeben nur in einem Gesamtkontext Sinn: Vorschriften wie «bei Rot anhalten» oder «rechts fahren» sind für sich genommen beliebig, spielen jedoch eine wesentliche Rolle im Hinblick auf «bei Grün fahren» und ganz allgemein im Rahmen eines komplexen sozio-technischen Systems, das aus Straßen, Fahrzeugen und Fahrenden besteht.

Die Struktur kontextbezogener informationeller Normen

Kontextbezogene informationelle Normen werden von vier wesentlichen Kennwerten bestimmt: Kontext, Handelnde, Merkmale und Grundsätze der Übermittlung. In der Regel definieren sie, um welche Information es im jeweiligen Kontext geht, für wen sie bestimmt sind, wer die Information ausgibt und empfängt sowie die Grundsätze, nach denen die Information übertragen wird. Anders ausgedrückt, informationelle Normen steuern gemäß bestimmter Grundsätze der Übertragung den Fluss bestimmter Arten von Information über einen Informationsgegenstand von einem Handelnden (der oder die eine bestimmte Funktion oder Rolle spielen) zu einem oder mehreren anderen Handelnden (der oder die eine bestimmte Funktion oder Rolle spielen).

Kontexte sind eine Voraussetzung der Anwendung, beziehungsweise die Umstände sind es, in denen eine Handlungsweise für einen Gegenstand festgelegt wird. Die sich wechselseitig bedingende Beziehung zwischen informationellen Normen und Kontexten wird mit dem Begriff «kontexbezogene Informationsnormen» beschrieben (in der Folge meist abgekürzt als «informationelle Normen»).

Der Gegensatz öffentlich/privat kann verstanden werden als krude Version eines unversehrten Kontexts, in der nur zwei Kontexte mit ihren jeweils eigenen informationellen Normen postuliert werden: Schutz der Privatsphäre im privaten Bereich – alles erlaubt im öffentlichen Bereich. Das System der Unversehrtheit des Kontexts hingegen postuliert eine Vielzahl gesellschaftlicher Kontexte, von denen ein jeder sein eigenes Set von Regeln für den Fluss von Informationen hat.

Akteure

Informationelle Normen kennen drei Platzhalter für Handelnde: die Sender von Informationen, die Empfänger von Informationen und den Gegenstand der Information. Sender und Empfänger können sowohl Einzelne, mehrere als auch Kollektive wie Organisationen, Komitees etc. sein. (Andere Begriffe, darunter Parteien und Akteure, werden im Folgenden für diejenigen benutzt werden, die Information kommunizieren, übertragen, weitergeben oder senden.) Als Gegenstand ziehe ich hier nur Individuen in Betracht, obgleich in vielen Fällen der Gegenstand und der Sender einer Information ein und dieselbe Person sind. Führt man eine informationelle Norm im Einzelnen aus, ist es von entscheidender Bedeutung, die kontextbezogenen Rollen aller drei Akteure so weit wie möglich zu bestimmen, d.h. die Funktionen in denen sie jeweils handeln. Im Gesundheitswesen gibt es beispielsweise zahlreiche informationelle Normen, die es untersagen, Informationen weiterzuleiten, wenn die Gegenstände und Sender Patienten, die Empfänger Ärzte sind. Andere Normen gelten, sind die Empfänger Arzthelfer, Buchhalter, Krankenpfleger etc. Im Gesundheitswesen gibt es informationelle Normen auch für Fälle, in denen Informationen über Patienten von Ärzten an andere Empfänger, z.B. an andere Ärzte, Versicherungsgesellschaften, Ehepartner, fließen.

Durch die Vorgabe, dass die Rollen der Handelnden klar definiert sein müssen, ist das Bezugssystem von der Unversehrtheit des Kontexts ein aussagekräftigeres Medium dafür, Variablen hervorzuheben, die für den Schutz der Privatsphäre von Bedeutung sind. Die Rollen der Handelnden sind eine der entscheidenden Variablen, die Einfluss darauf haben, ob Menschen mit ihren vielschichtigen Befindlichkeiten glauben, ihre Privatsphäre sei verletzt worden oder nicht. Andere Versuche, Grundsätze für den Schutz der Privatsphäre zu formulieren, schlagen fehl, da die Rolle der Handelnden im Hinblick auf die Regeln und die schwierige Gesamtsituation ignoriert oder zu wenig berücksichtigt wird. Die Folge ist, dass wir über unvollständig beschriebene Situationen Entscheidungen treffen sollen, denn selten, wenn überhaupt je, ist der Fluss von Informationen in einer Art und Weise verboten oder gefordert, die unabhängig davon ist, welche Funktionen die Sender, Gegenstände und Empfänger jeweils spielen. Strukturiert man informationelle Normen dadurch, dass man für die Handelnden Platzhalter setzt, dann bestätigt das Bezugssystem von der Unversehrtheit des Kontexts intuitive Erkenntnisse, die besagen, dass die Funktionen der Handelnden entscheidend dafür sind, ob bestimmte Informationsflüsse moralische Legitimität genießen oder nicht. Das trifft sogar in Fällen zu, in denen es auf den ersten Blick nicht so aussieht – beispielsweise dann, wenn jemand sagt, gewisse Informationen seien geheim, damit aber für gewöhnlich meint, sie seien geheim in Hinblick auf bestimmte Handelnde oder im Hinblick auf eine bestimmte Methode der Weiterverbreitung – und eben nicht an für sich geheim.

Wenn wir uns daran stören, dass bestimmte Informationen über uns weitergeleitet wurden, dann stört uns für gewöhnlich nicht die Weiterleitung an

sich, sondern wir sind verärgert, weil etwas auf die falsche Art weiterverbreitet wurde oder an die falschen Empfänger gelangte. Meist sind solche Bedingungen implizit und müssen nicht bis ins Detail ausgeführt werden. In Streitfällen kann es aber dazu kommen, dass verkürzte Aussagen darüber, was Menschen wollen, zu wörtlich genommen und zur Quelle für weitverbreitete Missverständnisse werden.

Wie wichtig die Handelnden im Hinblick darauf sind, ob gewissen Verfahren oder Vorgehensweisen unsere Privatsphäre beeinträchtigen, geht häufig indirekt aus unserem Verhalten hervor, ohne dass dies explizit in eine Theorie gefasst würde. So wie die Kontexte zeigen, dass statt einer bloßen Zweiteilung eine Vielfalt von Bereichen existiert, wird auch durch die Vorstellung, Menschen handelten in Funktionen, aus zwei Akteuren eine Vielzahl von Handlungsweisen. Neben vielen anderen Möglichkeiten, ist es dann wichtig zu wissen, ob die Akteure amtlich oder privat handeln – und in welcher Funktion.

Attribute und Arten von Informationen

Im Bezugssystem der Unversehrtheit des Kontexts sind *Merkmale* oder *Arten* oder das *Wesen* von Informationen entscheidend für informationelle Normen. Im Gesundheitswesen beispielsweise ist der Informationsfluss je nach Rollen und Art der Information unterschiedlich eingeschränkt, das heißt es gelten andere Regeln, je nachdem ob es um den Gesundheitszustand, die Kleidung, die Adresse, die Telefonnummer oder die Bankverbindung eines Patienten geht. Es mag vielleicht drastisch erscheinen, eine Analyse im Sinn der Unversehrtheit des Kontexts auf die Zweiteilung privat/öffentlich anzuwenden, aber dies ist unbedingt erforderlich. Zwar unterscheidet der herkömmliche Ansatz gleichfalls zwischen Arten von Informationen, er kennt jedoch nur zwei Arten; eine Analyse hingegen, die von der Unversehrtheit des Kontexts ausgeht, kennt, zumindest theoretisch, eine unbegrenzte Anzahl von Möglichkeiten.

Informationelle Normen machen bestimmte Merkmale in bestimmten Kontexten passen oder unpassend. Zum Beispiel besagt eine Norm, dass es im Gesundheitswesen in Ordnung ist, wenn ein Arzt einen Patienten nach dessen körperlichem Zustand befragt. Täte ein Arbeitgeber dasselbe am Arbeitsplatz, wäre dies jedoch höchst unangebracht.

Ob etwas angebracht ist oder nicht, ist weder eindimensional noch dual. Beispielsweise verhält es sich nicht einfach so, dass man Privatangelegenheiten mit Freunden beredet und Unpersönliches mit, sagen wir, Kollegen. In vielen Gesellschaften gilt es als unangebracht, sich mit engen Freunden über Gehalt und finanzielle Lage auszutauschen, jedoch als angebracht, darüber mit dem Arbeitgeber und dem Bankberater zu sprechen. Die Umstände, die darüber entscheiden, ob etwas angemessen ist oder nicht, sind ebenfalls vielfältig. Denken wir nur daran, dass Freunde in der Regel wissen, welcher Religion man angehört, während solche Informationen in einem Bewerbungsgespräch oder am Arbeitsplatz nichts zu suchen haben.

Diejenigen, die von mir eine exakte Definition von Informationsarten oder Merkmalen erwarten, muss ich enttäuschen. Ich stütze mich durchgehend auf aus unmittelbarer Erkenntnis gewonnene Einsichten, denn ich gehe davon aus, dass dies zur Erklärung der Unversehrtheit des Kontexts ebenso funktioniert wie für zahlreiche andere Gepflogenheiten und Richtlinien in der Gesellschaft. In der Regel kann man davon ausgehen, dass sich Merkmalsmuster gemeinsam mit ihren Kontexten entwickelt haben und sich entsprechend kaum abschließend und fix darstellen lassen.

Übertragungsgrundsätze

Ein Übertragungsgrundsatz ist eine Einschränkung des Informationsflusses (seiner Verteilung, Verbreitung, Übertragung) von einer Partei zu einer anderen innerhalb eines konkreten Kontexts. Die Werte der Übertragungsgrundsätze bei informationellen Normen formulieren Bedingungen oder Zustände, unter denen solche Übertragungen stattfinden dürfen oder auch nicht. Das Konzept des Übertragungsgrundsatzes ist vermutlich das kennzeichnende Merkmal des Bezugssystems der Unversehrtheit des Kontexts. Obwohl diese Vorstellung augenfällig ist, wird sie dennoch häufig übersehen.

Wie Übertragungsgrundsätze funktionieren, lässt sich wohl am besten anhand von Beispielen zeigen. Eines der hervorstechendsten Merkmale ist die Vertraulichkeit, d.h. die Partei, die Informationen empfängt, darf diese nicht an andere weiterleiten. Andere Kennzeichen sind die Wechselseitigkeit, d.h. der Grundsatz, dass Informationen in beide Richtungen fließen sollen; der Anspruch, der regelt, ob jemand bestimmte Informationen verdient hat; die Berechtigung (ähnlich dem Anspruch), die darüber entscheidet, ob jemand berechtigt ist, etwas zu wissen; der Zwang, der dafür sorgt, dass eine Partei (häufig der Informationsgegenstand) dazu gezwungen oder verpflichtet ist, anderen Personen Informationen zugänglich zu machen; und die Notwendigkeit, die bestimmt, dass eine Partei Informationen einer bestimmten Art benötigt.

Ein Übertragungsgrundsatz könnte sein, dass Informationen freiwillig mitgeteilt werden oder dass dies einvernehmlich geschehen muss. Weitere Möglichkeiten sind, dass dies nur mit Wissen des Gegenstands geschehen darf («Benachrichtigung») oder nur mit Erlaubnis («Zustimmung») oder dass beides der Fall sein muss. Übertragungsgrundsätze können es zulassen, dass Informationen auf einem freien Markt kommerziell genutzt, d.h. gekauft, verkauft, gehandelt oder vermietet werden dürfen. Die Liste ließe sich wahrscheinlich endlos fortsetzen, speziell dann, wenn wir Details und vielfältige Abwandlungen berücksichtigen.

Übertragungsgrundsätze sind nur einer der Werte, die Teil einer informationellen Norm sind. In jedem konkreten Kontext verändern sie sich in Abhängigkeit von anderen Werten für Akteure und Merkmale. Man kann sich das Ganze als Jonglage vorstellen – wie Bälle bewegen sich synchron der Kontext, die Gegenstände, die Sender, Empfänger, Informationsarten und Übertragungsgrundsätze.

Vergleichen wir die Übertragungsgrundsätze, die für das Gesundheitswesen gelten, mit denen für Freundschaft. Wie bei der Freundschaft, könnte man annehmen, geht es absolut vertraulich zu, wenn wir dem Arzt Informationen über einstige und aktuelle Krankheiten zukommen lassen. Im Unterschied zur Freundschaft jedoch steht hier die Vertraulichkeit des Gegenstands an erster Stelle. Es hängt mit der Rolle des Arztes zusammen, dass der Informationsfluss beschränkt bleibt, denn er benötigt vollständige Informationen vom Patienten, um diesen richtig behandeln zu können. Trotz solcher komplexen Regeln, gibt es dennoch offene Fragen und strittige Bereiche. Was für ein Übertragungsgrundsatz gilt beispielsweise für den Fluss von Informationen an Pharmafirmen? Haben Menschen ein Anrecht darauf zu erfahren, ob ihr Sexualpartner HIV-positiv ist oder nicht?

Es lohnt sich, nun noch einmal zu dem anhaltenden, unauflöslichen Streit, mit dem wir uns weiter oben beschäftigt haben, zurückzukehren: der Frage nämlich, ob der Schutz der Privatsphäre ein Recht auf Kontrolle ist oder ein Recht, den Zugang, den andere zu Informationen haben, einzuschränken oder zu begrenzen. Das Bezugssystem der Unversehrtheit des Kontexts zeigt uns, warum wir uns nicht zwischen diesen beiden Positionen entscheiden müssen. Stattdessen gibt sie beiden ihren Ort, denn ob Kontrolle angemessen ist oder nicht, hängt vom Kontext ab, den Arten von Information, dem Gegenstand, dem Sender und Empfänger.

Unversehrtheit des Kontexts als Entscheidungsgrundlage

Anlass für diesen Text ist die Herausforderung, die sozio-technische Systeme und Praktiken mit sich bringen, durch die sich der Informationsfluss in Gesellschaften radikal verändert hat und der sich damit auf Institutionen, Machtverhältnisse, Beziehungen etc. auswirkt. Vorstellungen von Privatsphäre, die bis vor Kurzem taugten, sind, denke ich, heute nicht in der Lage, sich diesen Veränderungen anzupassen, und sie werden dem Hin und Her der Ängste, die diese Systeme und Praktiken hervorrufen, kaum gerecht. Diesen grundlegenden Veränderungen will ich gerecht werden, indem ich, anstelle des Konzepts vom Schutz der Privatsphäre, das der Unversehrtheit des Kontexts postuliere, mit dem sich das Wesen der neuen Zustände systematisch erfassen lässt. Wichtig ist mir dabei die Frage, wann und wie einige dieser Veränderungen legitim Angst, Protest und Widerstand hervorrufen.

Indem ich die Unversehrtheit des Kontexts auf diese Fragen anwende, versuche ich dieses Konzept als Entscheidungsmechanismus dafür zu nutzen, ob und wann ein Verstoß stattgefunden hat. Die Unversehrtheit des Kontexts hilft in dieser Funktion dabei, nicht nur vorherzusagen, wann eine gewisse Handlung oder Vorgehensweise mit einiger Wahrscheinlichkeit zu Protest, Entrüstung oder Widerstand führen wird, sie kann auch die Ursachen für diese Reaktionen finden.

Wie lässt sich mit dem Bezugssystem der Unversehrtheit des Kontexts eine Bewertung einer problematischen neuen Vorgehensweise durchführen, die sich durch den Einsatz eines neuen technischen Geräts oder Systems ergibt? Die Frage, die man sich in solchen Fällen stellen muss, ist: Verstößt die fragliche Vorgehensweise gegen kontextbezogene informationelle Normen? Um diese Frage beantworten zu können, muss man überkommene Gepflogenheiten mit der neuen Verfahrensweise vergleichen. Auch wenn selbstverständlich eine neue Verfahrensweise den Ist-Zustand auf vielerlei Arten verändern kann, lenkt das Bezugssystem der Unversehrtheit des Kontexts unsere Bewertung doch auf die entscheidenden Faktoren des Kontexts: auf die Akteure, Merkmale und Übertragungsgrundsätze.

Um herauszufinden, welche Normen die Oberhand haben, muss der geltende gesellschaftliche Kontext eruiert werden. In einigen Fällen ist das sehr leicht, beispielsweise im Bildungsbereich in einer Grundschule. In anderen Fällen wird dies mehr Arbeit machen, und es kann vorkommen, dass die zu untersuchende Vorgehensweise in einem vermischten oder konfliktträchtigen Bereich stattfindet oder in Bereichen, für die keine umfassenden Normen existieren. Derartige schwierige Fälle müssen nicht undurchsichtig und rätselhaft bleiben. Sollte man seiner Chefin sagen, dass ihr Mann ein Verhältnis hat? Sollten Eltern die Blogeinträge ihrer Kinder lesen?

Man muss untersuchen, ob eine neue Verfahrensweise etwas daran ändert, wer Informationen empfängt (Empfänger), um wen es in den Informationen geht (Gegenstand) und wer die Information übermittelt (Sender). Viel zu wenig wird berücksichtigt, dass es durch neue Informationssysteme häufig dazu kommt, dass sich die Gruppe der Empfänger vergrößert.

Man muss untersuchen, ob die Veränderungen die Art der Informationen ändert, die vom Sender an den Empfänger übertragen werden. Mit Magnetkarten lässt sich beispielsweise nicht nur der Zugang zu vielen Universitätsgebäuden und Studentenwohnheimen kontrollieren, die Karten protokollieren und übermitteln auch wer wann kommt und geht.

Durch neue Verfahrensweisen können sich die Grundsätze, die für die Übermittlung von Informationen zwischen Parteien gelten, ändern. Aktuell können Autofahrer im Nordosten der USA entscheiden, ob sie an Mautstellen bar oder mit dem EZ-Pass bezahlen – und damit darüber, ob Informationen über sie bei Offiziellen landen. Sollten die Barzahlerstellen abgeschafft werden, veränderte sich das System zu einem, in dem Fahrer gezwungen wären, ihre Informationen zu übermitteln.

Wenn neue Verfahrensweisen zu Änderungen bei Akteuren, Merkmalen oder Übertragungsgrundsätzen führen, sollten die Warnlampen angehen, denn hier wird gegen etablierte informationelle Normen verstoßen und dem Anschein nach auch gegen die Unversehrtheit des Kontexts.

Ich habe das Bezugssystem der Unversehrtheit des Kontexts hier als Modell ins Spiel gebracht, um Reaktionen auf Änderungen der Informationspraxis, speziell bei der Informationstechnologie, vorherzusagen und zu verstehen. Die

Unversehrtheit des Kontexts kann eine Messlatte für die Privatsphäre sein, sie kann uns dabei helfen, die allgemeine Gefühlslage einzuschätzen und diese mit der Einschätzung abzugleichen, die Privatsphäre sei verletzt worden.

Aus dem Englischen übersetzt von Bernd Herrmann.

M. RYAN CALO

Die Privatsphärenverletzung neu denken

Zur Entwicklung einer Richtlinie

Durch die Verletzung der Privatsphäre kann auf verschiedene Arten und Weisen Schaden entstehen. Das juristische Konzept der Privacy in den USA greift aber zu kurz, um dem Schutzbedürfnis Einzelner gerecht zu werden. Ein konzeptioneller Entwurf zur Schadensbewertung der Privatsphärenverletzung.

Das Sammeln, Verarbeiten und Verteilen von Daten ist weder notwendig noch hinreichend, um die Privatsphäre eines Individuums zu verletzen. Es ist deshalb nicht *notwendig*, weil eine interne oder «subjektive» Verletzung der Privatsphäre schon allein dort auftreten kann, wo sich ein Individuum unter Beobachtung fühlt, wie es allzu oft der Fall ist. Allein der Gedanke, dass man beobachtet wird, dient als Ausgangspunkt für Jeremy Benthams berüchtigtes architektonisches Design. Studien haben gezeigt, dass die Anwesenheit einer ganz offensichtlich nicht echten Kamera oder Person dazu führen kann, dass sich das Verhalten oder die Einstellung eines Menschen ändert, selbst wenn diese Person sich darüber im Klaren ist, dass gerade eigentlich gar keine Daten gesammelt werden. In einer Studie konnte gezeigt werden, dass Menschen, die nach eigenem Ermessen den Preis ihres Kaffees zahlen konnten, mehr Geld zahlten, nachdem die Forscher Augen auf das Geldbehältnis geklebt hatten. In einer anderen Studie berichteten einige Befragte, dass sie sich unwohl dabei fühlten, bestimmte Dinge in der Drogerie zu kaufen, weil dort eine Kamera-Attrappe installiert war.[1]

Es ist deshalb *nicht hinreichend*, weil sich nicht jede Art der Nutzung von personenbezogenen Daten negativ für diese Person auswirkt. Es wäre ein wenig kurzsichtig von uns, wenn wir jedes dieser Vorkommnisse schädlich nennen würden, obwohl sie der betroffenen Person nur nutzen. Wenn z.B. ein Sanitäter

1 Dieses und andere Argumente habe ich an anderer Stelle noch einmal genauer beschrieben. Zum Beispiel diskutiere ich die Verletzung der Privatsphäre ohne das Sammeln von Daten ausführlich in M. Ryan Calo: *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship,* 114 Penn St. L. Rev. 809 (2010).

in der Geldbörse eines Bewusstlosen nach seinem Ausweis sucht, würden wir uns schwertun zu behaupten, dass dies eine Verletzung der Privatsphäre sei.[2]

Wieso die USA eine neue Sichtweise auf die Verletzung der Privatsphäre benötigen

Ich bin der Meinung, dass sich Innovation und Privatsphäre gegenseitig stützen. Die Privatsphäre unterstützt die Kreativität auf einer individuellen und, wie viele Leute behaupten, sozialen Ebene. Der Wunsch nach Privatsphäre treibt auch Innovationen voran, z.B. als in den 1950er-Jahren die «Hush-A-Phone»-Telefonerweiterung in den USA anderem Telefonzubehör den Weg ebnete. Solange jedoch zwischen Online-Innovationen und dem persönlichen Recht auf Privatsphäre Spannungen bestehen, sollte die mögliche Verletzung von Privatsphäre die Richtschnur für einen Ausgleich dieses Konflikts sein. Damit meine ich, grob gesagt, dass wir zum Schutze der Privatsphäre die Entwicklung bestimmter Innovationen nur dann verhindern sollten, wenn gezeigt werden kann, dass diese tatsächlich Menschen schaden könnten.[3]

Diese Strategie war jedoch bis heute nicht durchführbar. Amerikanische Gerichte und Behörden, z.B. die Federal Trade Commission, haben in der Vergangenheit die Verletzung der Privatsphäre sehr eng definiert. Eine Verletzung der Privatsphäre liegt demnach nur dann vor, wenn sie mit wirtschaftlichem Schaden einhergeht. Dieses Konzept der Verletzung von Privatsphäre fungiert demnach als eine Art Hürde, die einem Zuspruch von Schadensersatz im Wege steht. Wissenschaftler haben jedoch weitaus offenere Definitionen für eine Privatsphärenverletzung vorgeschlagen. Demnach liegt diese z.B. dann vor, wenn zukünftige Risiken für die Privatsphäre absehbar sind oder ein Ungleichgewicht zugunsten institutioneller Macht vorliegt. Auch wenn diese Auslegungen wichtig und korrekt sind, können sie nicht unbedingt als Grundlage zur Durchsetzung von politischen Entscheidungen dienen.[4]

Anstatt den Fokus auf die Verletzung der Privatsphäre zu legen, haben wir uns in den letzten Jahrzehnten vor allem darauf konzentriert, die Nutzer aufmerk-

2 Für eine detaillierte Besprechung meiner Ansichten zum Thema Privatsphärenverletzung siehe M. Ryan Calo: *The Boundaries of Privacy Harm,* 86 Indiana L.J. (2011).

3 Der Telefonanbieter AT&T hat früher seinen Kunden (also allen) verboten, ihre eigenen Telefone mit dem Netzwerk zu verbinden; sie mussten sich ein Telefon von AT&T mieten. Ein Unternehmen hat daraufhin ein Gerät entwickelt, das man mit dem AT&T-Telefon verbinden konnte. AT&T forderte sein Recht ein, dieses Zusatzgerät zu verbieten und die Federal Communications Commission billigte es. Im bahnbrechenden Telekommunikationsprozess *Hush-A-Phone gegen die Vereinigten Staaten* hat das Bundesberufungsgericht in Washington dieses Urteil zurückgenommen und damit festgelegt, dass es rechtens ist, Zusatzgeräte von unbeteiligten Unternehmen an die Telefone anzuschließen. Dieser Präzedenzfall ebnete den Weg für die Entstehung eines komplett neuen Industriezweigs für Telefonzubehör.

4 Diese Einblicke verdanke ich Paul Ohm, der 2010 in einem Workshop für die Privacy Law Scholars Konferenz (Washington, D.C.) ausführlich über dieses Thema gesprochen hat.

samer zu machen und ihnen Wahlmöglichkeiten anzubieten. Im Internet ist alles möglich; die Unternehmen müssen es nur offenlegen. Das «Notice and choice»-Regime, ein System, in dem man Benachrichtigungen erhält und bestimmte Einstellungen frei wählen kann, hat jedoch vor allem deshalb entsetzlich versagt, weil das Hauptinstrument zur Benachrichtigung, die Datenschutzerklärung, viel zu lang und vage formuliert ist, um effektiv sein zu können. Die Konsumenten sind sich weder über die Dinge im Klaren, denen sie «zugestimmt» haben, noch über die wenigen Wahlmöglichkeiten, die ihnen zustehen.[5]

Diejenigen Amerikaner, denen Datenschutz wichtig ist, sind berechtigterweise verärgert über das Ergebnis. Wir erlauben eine Korrektur erst dann, wenn wirtschaftlicher Schaden entsteht. Wir erlauben es, verlangen ja direkt danach, dass Unternehmen eine Datenschutzerklärung verfassen, die sowieso niemand liest, geschweige denn ändern möchte. Und in der Zwischenzeit werden immer mehr Daten gesammelt, verarbeitet und verteilt. Genauso wenig bieten Datenschutz-Verteidiger, zumindest größtenteils, eine verständliche und durchführbare Strategie an, die die Wirklichkeit des E-Commerce mit dem wichtigen Recht auf individuellen Datenschutz vereinen könnte. Wirtschaft und Interessenvertretung fahren wie Schiffe im Nebel aneinander vorbei – manchmal kollidieren sie dabei auch.

Nehmen Sie z.B. die Debatte, die sich um den «Do Not Track»-Mechanismus («DNT») beim Predictive Behavioral Targeting entwickelt hat. In diesem Verfahren wird das Surfverhalten von Usern in Kombination mit ihren soziodemographischen Daten erfasst, um dann auf ihre Produktinteressen schließen zu können. In der Industrie sind einige der Meinung, dass eine rücksichtslose Anwendung von DNT grundsätzliche Funktionen des Internets, wie z.B. Webseitenanalyse und das Aufdecken von Betrug, unmöglich machen könnte. Ohne dafür einen Grund zu haben, nehmen andere an, dass sich so viele Menschen gegen diese Art von Nachverfolgung entscheiden werden, dass Online-Werbung nicht mehr lukrativ genug sein wird, um kostenlose Angebote im Netz finanzieren zu können. Nachdem sie Unmengen an politischem Kapital in die DNT-Gesetzgebung investiert haben, befürchten Datenschutz-Verteidiger – sie sollten es zumindest befürchten –, dass viele Nutzer sich nicht darum kümmern oder es vergessen werden, ihre Zustimmung zu verweigern. Und so werden sich die Nutzer weiterhin in demselben wirren Datenschutz-Dschungel bewegen, wie sie es schon seit Jahren tun. (Nur um es klarzustellen: Ich unterstütze «Do

5 Für eine detaillierte Diskussion zum Versagen von Benachrichtigungen und Wahlmöglichkeiten im Kontext von Datenschutz siehe Fred Cate: «The Failure of Fair Information Practice Principles», in *Consumer Protection in the Age of Information Economy* 361 (2006), ed. Jane Wynn.

Not Track» («DNT») schon allein deshalb, weil es uns dazu zwingt, eine wichtige Diskussion zum Thema Online-Datenschutz zu führen.)[6]

Ich würde sagen, dass wir Kunden am besten schützen und die Bedingungen für Innovationen wahren können, wenn wir uns darauf konzentrieren, Verletzungen der Privatsphäre zu vermeiden und zu entschädigen. Damit meine ich nicht die Verletzung der Privatsphäre, wie sie oft von den Gerichten definiert wird. Das ist zu eng. Und auch nicht die Verletzung der Privatsphäre, wie viele Wissenschaftler sie sich vorstellen. Das ist nicht konkret genug, um es anzuwenden oder als Richtlinie umzusetzen.

Wie ich mir das Konzept der Privatsphärenverletzung vorstelle

Ich schlage vor, dass wir eine Handlung, einen Prozess oder ein Phänomen erst dann als eine Verletzung der Privatsphäre kategorisieren, wenn diese zwei Bedingungen erfüllt sind:

Erstens, wenn eine unerwünschte Wahrnehmung von Beobachtung stattfindet. Damit ist das subjektive Unwohlsein gemeint, das man empfindet, wenn man glaubt oder vermutet, beobachtet zu werden. Beispiele für diese subjektiven Verletzungen der Privatsphäre sind z.B., wenn ein Mieter entdeckt, dass er von seinem Vermieter überwacht wird (Hamberger gegen Eastman), wenn ein Arzt einen seiner Freunde zur Geburt eines fremden Babys mitbringt (De May gegen Roberts) und die allgemeine Überwachung durch den Staat.

Zweitens, wenn persönliche Informationen unter Zwang oder vollkommen unerwartet gegen eine Person verwendet werden. Dies ist die objektive negative Konsequenz daraus, wenn man die Kontrolle über die eigenen Informationen verliert. Beispiele für diese objektiven Verletzungen der Privatsphäre sind u.a. Identitätsbetrug oder eine erzwungene Blutentnahme während einer polizeilichen Untersuchung (Schmerber gegen Kalifornien).

… und wieso?

Was würde dieses Konzept umfassen, das es nicht heute schon abdeckt? Ganz schön viel. Mein Konzept würde z.B. Sicherheitslücken abdecken, auch wenn nicht bewiesen werden kann, dass die dadurch gewonnenen Informationen für Identitätsbetrug genutzt werden. Es könnte auch gelten, wenn man bei Rasterfahndungen ohne angemessenes, rechtsstaatliches Verfahren einbezogen wird. Eine subjektive Verletzung der Privatsphäre kann immer dort auftreten, wo – wie es so oft der Fall ist – eine Person lediglich glaubt oder vermutet, dass ihre Daten in den falschen Händen sind. Man könnte diesen Menschen Schadensersatz zusprechen oder verlangen – und vielleicht ist das ein wenig ergiebiger –

6 Einer der DNT-Mechanismen wurde sogar von einem Partnerunternehmen des Centers entwickelt, für welches ich tätig bin (http://donottrack.us). Ein anderes wird von Mozilla, wo ich Mitglied des Privacy Advisory Boards bin, in seinem berühmten Browser Firefox genutzt.

dass sowohl die Kreditwürdigkeit als auch der gute Ruf der geschädigten Person wiederhergestellt werden, wie es z.B. von Unternehmen wie reputation.com angeboten wird.

Es könnte auch in Situationen angewandt werden, in denen eine Person einen höheren Preis, höhere Raten oder andere negative Konsequenzen für etwas erdulden muss, weil einige wenige Informationen gesammelt wurden, von denen die Person nicht wusste, dass sie für diesen Zweck benutzt werden können, z.B. IP-Adresse oder Browser-Art. Es könnte auch bedeuten, dass man auf eine Liste mit hilflos ausgelieferten Nutzern gesetzt wird (z.B. Ältere oder Behinderte) und man deshalb zum Ziel von Werbemails wird. Eine Wiedergutmachung könnte hier bedeuten, dass man Schadensersatz oder eine gerichtliche Verfügung gegen weitere unfaire Wirtschaftspraktiken zugesprochen bekommt.

Meine Definition von Privatsphärenverletzung ist vielleicht nicht die allerbeste. Und es kann auch sein, dass keine Definition von Privatsphärenverletzung alle Probleme abdecken kann, über die wir uns momentan Sorgen machen. Aber wir sollten es ebenso wenig zulassen, dass die Perfektion der Feind des Guten wird. Anstatt davon auszugehen, dass die Lage des Online-Datenschutzes *vollkommen* in Ordnung ist oder das Sammeln und Nutzen *jeglicher* Daten reflexartig verhindert und bekämpft werden sollte, könnten wir uns auf dem Mittelweg treffen: Wir sollten das Konzept der Privatsphärenverletzung erweitern und nur dann eingreifen, wenn sich eine solche Verletzung hinreichend andeutet.

Aus dem Englischen übersetzt von Katja Ullrich.

JAN SCHALLABÖCK

Grundfunktionen des Datenschutzes

Das Urteil des Bundesverfassungsgerichts hat im Grundsatz die Speicherung von Daten auf Vorrat erlaubt. Für Befürworter wie Gegner von neuen IT-Risikotechnologien geht es letztlich um die Frage, wer wen kontrolliert. Dabei ist Fatalismus nicht angesagt. Es bleibt eine politische Entscheidung, ob wir die zukünftige Gesellschaftsordnung transparenter gestalten wollen oder nicht.

Es ist der 2. März 2010, der Tag, an dem die Entscheidung über die bis dato größte Verfassungsbeschwerde terminiert ist. Schätzungsweise rund 20.000 Kläger schauen wie gebannt auf alles, was mit dem Hashtag #VDS über Twitter gepostet wird, gleichzeitig überträgt Phönix live aus dem Gerichtssaal. Der wiederum ist bis auf den letzten Platz gefüllt. Selten hat eine Urteilsverkündung des obersten deutschen Gerichts solch eine Aufmerksamkeit erfahren.

Man kann sich des Eindrucks nicht ganz erwehren: Ein bisschen sieht es aus wie bei Queen Mum, als schließlich der Präsident des Bundesverfassungsgerichts, Hans-Jürgen Papier, vor sein «Volk» tritt. Es hofft, dass er – quasi als guter König – in der Lage ist, die wildgewordene Regierung wieder zur Raison zu bringen.

Zunächst scheint sich diese Hoffnung auch zu erfüllen, denn das Gericht urteilt: «Die §§ 113a und 113b des Telekommunikationsgesetzes […] verstoßen gegen Artikel 10 Absatz 1 des Grundgesetzes und sind nichtig.» Die Vorratsdatenspeicherung ist gekippt.

Aus der dann folgenden Begründung wird jedoch klar: Es gibt kein allgemeines, aus dem Grundgesetz abgeleitetes Prinzip, dass eine Speicherung auf Vorrat in der Form der Vorratsdatenspeicherung untersagt. Wir haben das Volkszählungsurteil wohl falsch verstanden. Das, von dem viele dachten, dass es eine klare und gute Begrenzung des Gesetzgebers sei, ist ihm doch gestattet: Der Staat darf Daten auf Vorrat speichern (lassen). Allerdings darf er das nur unter Einhaltung strenger IT-Sicherheitsvorgaben, und genau das hat der Gesetzgeber nicht hinreichend beachtet.

Damit hat sich das Gericht zweifelsohne auf einen wichtigen Aspekt konzentriert. Die der IT inhärente Unsicherheit, die mit ihr verbundenen (Rest-)Risiken, machen sie insbesondere mit zunehmendem Einsatz in kritischen Bereichen zu einer Risikotechnologie. Das bedeutet, dass vor dem Einsatz Risikoabschät-

zungen durchgeführt werden müssen, die auch zu dem Ergebnis führen können, dass vom Einsatz der Technik abzusehen ist. Vor dem Hintergrund der «besonders hohen Anforderungen», die das Gericht an die IT-Sicherheit bei der Vorratsdatenspeicherung gestellt hat, ist es durchaus zweifelhaft, ob es überhaupt möglich ist, die Vorratsdatenspeicherung technisch so zu gestalten, dass sie verfassungskonform umgesetzt werden kann. Dies kann und soll hier aber nicht im Detail erörtert werden.

Welche Daten sind eigentlich noch personenbezogen?

Die Vorratsdatenspeicherung ist nur ganz knapp gekippt worden. Mit vier gegen vier Stimmen fiel die Entscheidung zugunsten der Nichtigkeit. Knapper geht es nicht. Nur weil die Nichtigkeit die grundgesetzliche Regelfolge der Verfassungswidrigkeit eines Gesetzes darstellt, reichte das Unentschieden aus. Nun lässt die Nachbesetzung des Bundesverfassungsgerichts mit der Berliner Professorin Susanne Baer hoffen. Ihr Beitrag auf dem Netzpolitischen Kongress der Grünen Bundestagsfraktion im November 2010 zeugte von einer angenehm aufgeklärten Unaufgeregtheit in Hinblick auf netzpolitische Fragestellungen. Wie auch insgesamt die Entscheidungen des Bundesverfassungsgerichts oft erschreckende Zeugnisse für die netzpolitische Inkompetenz des Gesetzgebers darstellen.

Susanne Baer stellte am Rande fest, dass die Dichotomie von «privat» und «öffentlich» problematisch sei. «Stating the obvious» mag man dem entgegen rufen. Schließlich zeigt sich doch im Netz tagtäglich, wie schwer die Grenzen zwischen diesen beiden Kategorien zu ziehen sind. Doch die Implikationen – gerade für den Datenschutz – sind immens, obschon sie im Datenschutzrecht schon stärker berücksichtigt werden, als es ihm oft nachgesagt wird. Dennoch, alte Formeln wie die bekannte Forderung, die der deutschen Version der Hackerethik entstammt: «Private Daten schützen – öffentliche Daten nützen!», sind nicht mehr so einfach anzuwenden.

Eine Problematik, die sich leider auch bei «Open Government Data», der systematischen Veröffentlichung von Datenbeständen seitens der Verwaltungen, stellen wird. Denn nicht nur die Abgrenzung zwischen Privatem und Öffentlichem wird feinsinniger; auch die Bestimmung dessen, was eigentlich personenbezogen ist und was nicht, ist oft kaum mehr zu treffen. Der Gesetzgeber hat im Bundesdatenschutzgesetz die Anwendbarkeit der Datenschutzregeln eben nicht nur für solche Daten vorgeschrieben, die offenkundig personenbezogen sind. Richtigerweise hat er das Datenschutzrecht auch auf solche Daten erstreckt, bei denen die bloße Möglichkeit besteht, den Personenbezug herzustellen (Personenbeziehbarkeit). Nur so können die Regelungen auch Fälle abdecken, in denen das Risiko der Zusammenführung besteht. Die Möglichkeiten effektiver Zusammenführung, der Verknüpfbarkeit oder De-Anonymisierung sind aber mit der zunehmenden Semantisierung (gemeint ist hier die Anreicherung mit durch den Computer interpretierbaren Bedeutungen), den durch Moore's law

stetig steigenden Rechenkapazitäten und der immensen Zunahme verfügbaren Datenmaterials ins Unüberschaubare angestiegen.

Längst taugen die überkommenen Verfahren des ehrwürdigen Statistischen Bundesamtes zur Absicherung der Anonymität der Statistiken nicht mehr. Ratlos scheint man dort vor der Aufgabe zu stehen, wie in Zukunft Daten anonymisiert veröffentlicht werden sollen.

Paparazzi-Schutz oder Machtfrage?

Doch was sind denn nun die Kriterien, mit denen wir künftig beurteilen können, ob eine staatliche Maßnahme oder eine private Datensammlung und -verarbeitung problematisch ist? Einen vielbeachteten Ansatz stellt der von Helen Nissenbaum dar, die die Bedeutung der «kontextuellen Integrität» hervorhebt (siehe ihren Beitrag in diesem Band). Stark vereinfacht: Die Verwendung von Daten muss in ihrem Kontext verbleiben. Werden sie aus dem Kontext gerissen, sind sie potenziell gefährlich. Zurückführen kann man diese Überlegung auf Niklas Luhmann, der im Rahmen der Systemtheorie von der Notwendigkeit der funktionalen Differenzierung in einer modernen Gesellschaft sprach. Der Mensch verhält sich in unterschiedlichen Kontexten oder seinen unterschiedlichen Funktionen eben … unterschiedlich. Er bewegt sich in Systemen mit jeweils unterschiedlichen Regeln. Die neuere Forschung zur Datenschutztechnologie hat, diesem Gedanken folgend, Systeme modernen Identitätsmanagements entwickelt. Sie sollen es dem Individuum erleichtern, diese kontextspezifischen «Teilidentitäten» (oder Personae) seiner selbst zu managen (siehe dazu den Beitrag von George Danezis und Seda Gürses in diesem Band). Zu Ende gedacht müssten wir uns also eine Vielzahl von «*Personae* mit beschränkter Haftung» zulegen, wie es eine internationale Unternehmensberatung vorschlägt.

In seiner «Taxonomy of Privacy» entwickelt Daniel J. Solove insgesamt sechzehn Angriffsdimensionen auf die Privatheit, die er grob vier Oberkategorien zuordnet. Er zeigt damit die Vielfalt dessen, was wir unter dem Begriff von Privatheit als schützenswert zusammenfassen. Er leistet aber auch gleichzeitig einen wichtigen Beitrag zu dessen Systematisierung. Nur wenn wir unterscheiden zwischen z.B. dem Problem der «Appropriation», also der Aneignung von Informationen anderer zur eigenen Verwertung, und dem der Exklusion, also der Verweigerung, dem Betroffenen Auskunft über die von ihm gespeicherten Daten zu geben, dann können wir auch die Risiken einzelner Sammlungen und Verarbeitungen bestimmen.

Beiden vorgenannten Ansätzen ist jedoch gemein, dass sie die Privatheit ins Zentrum der Überlegungen und des Schutzes stellen. Das Konzept des «Datenschutzes» in der auch vom Bundesverfassungsgericht vertretenen Form ist – bei aller Kritik am Begriff selbst – ein weitergehendes. Die Kläger gegen die Vorratsdatenspeicherung und gegen ELENA haben längst erkannt, dass wir keine Behörden brauchen, um uns vor Paparazzi-Eingriffen unserer Nachbarn zu

schützen. Das haben sie manchen, die sich in der Debatte um Google Streetview lautstark zu Wort gemeldet haben, voraus.

Die Frage des Datenschutzes ist eine nach den Macht(un)gleichgewichten in der Informationsgesellschaft. In der Diktion des Bundesverfassungsgerichts ist die informationelle Selbstbestimmung «Grundbedingung eines auf demokratische Mitbestimmung ausgerichteten Gemeinwesens». Mehr noch, es geht um die Frage: Wer hat die Macht über die Daten? Wer kann mit ihnen arbeiten, d.h. sie korrellieren, Prognosen treffen, Profile bilden, Einteilungen und Kategorisierungen vornehmen? Eine hochpolitische Angelegenheit.

Systemwechsel hin zur transparenten Computergesellschaft?

Die Brisanz wird deutlich, wenn wir uns den Gedanken des Systemtheoretikers Dirk Baecker zu eigen machen. Baecker sieht uns in einem Übergangsprozess in eine «nächste Gesellschaft», die Computergesellschaft. Diesen Prozess setzt er gleich mit den Umwälzungen, die jeweils die Einführung der Sprache, der Schrift und des Buchdrucks bewirkt haben. Der Gedanke ist verlockend. Der Ansatzpunkt, den Computer (sprich: Rechner) zum gesellschaftsprägenden Paradigma zu erklären («the difference that makes the difference») ist schlüssig. Denn durch ihn wird es möglich, in nahezu unbegrenztem Umfang Daten zu verarbeiten (sprich: zu berechnen). Daraus folgt nach Baecker, dass der Überschusssinn der «nächsten Gesellschaft» der der Kontrolle ist. Ultimativ geht es also auch um die Frage, wer wen kontrolliert.

John Gilmore schien in seiner Eröffnungsrede auf dem 25c3, dem jährlichen Get-together des Chaos Computer Clubs, überraschenderweise David Brins «Transparent Society» etwas Visionäres abgewinnen zu wollen. Diese 1998 veröffentlichte Dystopie geht davon aus, dass der Überwachungsstaat in der «Computergesellschaft» unvermeidlich und dass diesem Sachverhalt mit einer neuen Form der Offenheit und Toleranz zu begegnen sei (ähnlich argumentiert Michael Seemann im vorliegenden Band). So sehr der Ruf nach mehr Offenheit und Toleranz stets unterstützt werden sollte, so wenig ist es meines Erachtens zwingend, dass die «Computergesellschaft» zwangsläufig in die Überwachungsgesellschaft führen (oder sie fortsetzen) muss. Will man die «nächste Gesellschaft» politisch gestalten und nicht jegliches politisches Handeln zugunsten einer fatalistischen Grundhaltung aufgeben, so muss man tatsächlich eine transparentere Gesellschaft fordern. Aber nicht eine völlige Transparenz aller Informationen über die Menschen, sondern eine weitgehende Transparenz über die Prozesse, mit denen diese Informationen verarbeitet werden, ist zu fordern.

Politisch besteht dann die Aufgabe darin, diese Verarbeitungen und Prozesse zu kontrollieren; zu entscheiden, welche Arten der Verarbeitung sinnvoll sind und welche nicht. Dies zu ermöglichen, ohne sich dabei der Gefahr totaler oder gar totalitärer Medienkontrolle auszusetzen, wie es (der leider kürzlich verstorbene) Andreas Pfitzmann für den Einsatz von DRM-Verfahren in diesem Bereich prognostiziert hat, ist die große Herausforderung. Ein Teil der Antwort liegt auf

der Hand: Es ist der Einsatz von quelloffener Software, die es ermöglicht, tief in die Verarbeitungsprozesse hineinzuschauen. Dieses «Recht auf Einsicht» (frei nach Jacques Derrida) gilt es neu gegen etwa den Schutz des Geschäftsgeheimnisses abzuwägen.

Verbot der Vorratsdatenspeicherung ins Grundgesetz?

Es führt kein Weg daran vorbei, das Politische im politischen Raum zu diskutieren und alle größeren neuen Prozesse und Verarbeitungsmöglichkeiten einer politischen Bewertung im Sinne der Frage nach Machtimplikationen zu unterziehen. Bei der Bewertung können klare Grenzziehungen helfen. Ein Verbot von Vorratsdatenspeicherungen zum Beispiel. Man wundert sich allerdings, warum niemand die tatsächlich notwendige Konsequenz aus dem Urteil zur Vorratsdatenspeicherung gezogen hat: Wenn wir glauben, dass Vorratsdatenspeicherungen nicht erlaubt sein sollten, wenn wir glauben, dass Gesetze wie das eingangs erwähnte verfassungswidrig sein sollten, warum schreiben wir das nicht einfach in die Verfassung? Darüber nachzudenken, wie solche klaren Begrenzungen sinnvoll zu konstruieren sind, wäre möglicherweise endlich einmal ein konstruktiver Beitrag zum Thema «Datenschutz ins Grundgesetz».

Es ist der Fluch und die Chance größerer gesellschaftlicher Transitionsprozesse, dass man neue Grundregeln und Grundprinzipien entwickeln muss. Die Entscheidung zur Vorratsdatenspeicherung spricht dafür, dass wir uns noch einmal grundsätzlicher auf die Suche begeben müssen. Dass die Novellierung der Datenschutzrichtlinie schon Antworten geben wird, ist bisher nicht zu erkennen.

Literatur

Susanne Baer: «Braucht das Grundgesetz ein Update? Bürgerrechte für das Internetzeitalter». Rede auf dem Netzpolitischen Kongress der Bundestagsfraktion von Bündnis 90/Die Grünen am 13.11.2010, online unter http://www.gruenes-blog.de/netzpolitik/1346/susanne-baer-braucht-das-grundgesetz-ein-update-burgerrechte-fur-das-internetzeitalter

David Brin: The transparent society,1998. Auszug online unter http://www.wired.com/wired/archive/4.12/fftransparent_pr.html

Dirk Baecker: *Studien zur nächsten Gesellschaft*, Frankfurt 2007.

Chaos Computer Club (Hrsg.): hackerethics, online unter http://www.ccc.de/hackerethics

John Gilmore: «Nothing to hide?». Vortrag auf dem 25. Chaos Communication Congress, in Fragmenten verfügbar unter http://mirror.informatik.uni-mannheim.de/pub/ccc/streamdump/saal1/Tag1-Saal1-Slot10%3a00--Opening-INCOMPLETE.wmv

Helen Nissenbaum: «Privacy as Contextual Integrity», in: *Washington Law Review*, Vol. 79, No. 1, Februar 2004, S.119-158, online unter http://www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf

Daniel J. Solove: «A Taxonomy of Privacy», in: *University of Pennsylvania Law Review*, Vol. 154, No. 3, S. 477ff. Januar 2006; GWU Law School Public Law Research Paper No. 129, online unter http://ssrn.com/abstract=667622

MICHAEL SEEMANN

Vom Kontrollverlust zur Filtersouveränität

Die Allgegenwart von Aufzeichnungsgeräten verbindet die digitale Welt immer enger mit der analogen. Ist man Teil der Welt, wird man Teil des Internets sein. Suchmaschinen-Abfragen, Leaking-Vorgänge und die steigende Verknüpfbarkeit von Daten haben zu einem Grundgefühl der Informationsüberflutung geführt. In der Bibliothek von Babel muss Öffentlichkeit deshalb radikal neu gedacht werden. Ein Plädoyer für Post-Privacy.

Stehe! Stehe! / Denn wir haben / Deiner Gaben / Vollgemessen! – / Ach, ich merk es! Wehe! Wehe! / Hab ich doch das Wort vergessen!
Johann Wolfgang von Goethe, Der Zauberlehrling

Die USA stehen diplomatisch ohne Hosen da, ein «Shitstorm» bricht über Nestlé herein, ein Blogger prangert ein Zitat des Bundespräsidenten an, der schließlich zurücktritt, private Videos von Jugendlichen verbreiten sich im Netz, das Internet verleibt sich das deutsche Straßenpanorama ein, und in Tunesien und Ägypten verabreden die Menschen sich zum spontanen Regimesturz. Die Welt ist in Aufruhr dieser Tage, und irgendwie hat es mit dem Internet zu tun.

Vor einem Jahr habe ich mich entschlossen, Ereignisse wie diese unter dem Begriff «Kontrollverlust» zu untersuchen. Das scheint etwas unsystematisch, und tatsächlich ist es nicht einfach, eine passende Definition für all diese unterschiedlichen Phänomene zu liefern. Ich versuche es dennoch:

Ein Kontrollverlust entsteht, wenn die Komplexität der Interaktion von Informationen die Vorstellungsfähigkeiten eines Subjektes übersteigt.

Das ist an sich nichts völlig Neues, wir kennen das. Meine These ist aber nun, dass das Internet und die digitale Technik diese Kontrollverluste sowohl in ihrer Häufigkeit als auch in der Intensität ihrer Folgen um ein Vielfaches steigert. Dafür gibt es verschiedene Gründe.

Es gibt kein analoges Leben im digitalen

Den ersten internationalen Durchbruch hatte Wikileaks mit dem Video «Collateral Murder». Man wird Zeuge, wie die Besatzung eines US-amerikanischen Apache-Hubschraubers im Irak eine Gruppe von Menschen zusammenschießt. Zwei von ihnen sind Journalisten für Reuters. Der Familenkleinbus, der hält, um die Verletzten zu bergen, wird gleich darauf auch zusammengeschossen.

Was mich hier interessiert, ist diese merkwürdige Konfiguration von «Zeugenschaft». Die Kamera im Helikopter ist zweifellos ein Kontrollinstrument. Das Oberkommando fliegt mit, bekommt alle Schritte des Apache-Teams zu sehen, und das Material kann hinterher ausgewertet werden. Doch der Kontrollapparat wird nun zum Kontrollverlustinstrument.

Kontrollverlustinstrumente können potenziell alle Apparate zum Aufschreiben von Daten sein. Sensoren, Kameras, GPS-Apparaturen etc. Denn die Menge dieser Apparate steigt unerbittlich. CCTV-Kameras überwachen den öffentlichen Raum, Handys mit Kamera und GPS sind allgegenwärtig, Kreditkartenlesegeräte erfassen beinahe alle Transaktionen und durch die Straßen fährt das Google-Street-View-Auto. Alle diese Geräte schicken immer mehr Daten auf immer größere Festplatten, in immer mehr Geräte und immer mehr ins Internet.

Grund eins für den Kontrollverlust: Die Allgegenwart von Aufzeichnungsgeräten verknüpft die digitale Welt immer enger mit der analogen. Ist man Teil der Welt, wird man Teil des Internets sein.

Public by Default

76.911 Dokumente umfassten die Afghanistandokumente, 391.832 die aus dem Irak, und 251.287 diplomatische Depeschen wurden geleakt. Aber die mutmaßliche Quelle, Bradley Manning, musste nicht 234 Aktenschränke mit einer Kolonne Lastwagen abholen lassen, sondern spazierte mit einer gebrannten Lady-Gaga-DVD aus dem Büro. Da war noch etwas Platz drauf.

Im Digitalen gibt es keinen Unterschied zwischen Schicken und Kopieren. Egal, ob wir eine E-Mail schicken oder eine Website aufrufen: Jede Operation im Digitalen ist eine Kopieroperation. Über 90% aller Befehlssätze eines Computerprozessors sind Kopierbefehle; das Internet ist somit eine riesige Kopiermaschine.

Während in einer Welt der Wände und Entfernungen noch ein großer Aufwand betrieben werden musste, um eine Information an einen Empfängerkreis weiterzuverbreiten, der über eine mittlere Ratsversammlung hinausgeht, muss man heute einen ähnlichen Aufwand betreiben, um dieselbe Information nicht sofort weltweit zugänglich zu machen.

Und wenn man eine Information wieder aus dem Netz herausbekommen will, hat man ein Problem. Nach den Versuchen der US-Regierung, Wikileaks zu schaden, indem man Dienstleister dazu brachte, Verträge mit ihnen zu kündigen,

reagierten die Unterstützer von Wikileaks mit bis heute 1.426 Spiegelungen, also kompletten Kopien aller Daten des Wikileaks-Servers auf anderen erreichbaren Rechnern.

Dieser Vorgang bekam im Jahre 2003 den Namen «Streisand-Effekt». Die Schauspielerin und Sängerin Barbra Streisand versuchte damals die Website Pictopia.com gerichtlich dazu zu zwingen, eine Luftaufnahme ihres Hauses zu entfernen. Der Prozess entfachte das Interesse an dem Bild erst richtig und verbreitete es nicht nur tausendfach im Netz, sondern auch die Information, wer dort wohnt.

Grund zwei für den Kontrollverlust: Das Internet hat die Transaktionskosten für Information enorm gesenkt und tut es weiter. «Leaken» ist sozusagen die Standardeinstellung des Netzes.

Echtzeitarchäologie

Nachdem all die vielen Dokumente aus Afghanistan, dem Irak und all die ganzen Depeschen geleakt waren, stand man nun vor einem riesigen Berg an Daten. Nicht mal der Zusammenschluss der Redaktionen von *SPIEGEL*, *Guardian* und *New York Times* hätte ausgereicht, genug wertvolle Informationen aus diesem Heuhaufen zu destillieren, wenn nicht ein weiterer Umstand geholfen hätte: Die generelle Verknüpfbarkeit von Daten.

Der *Guardian* glänzte als Vorbild, als er vor allem die Kriegsdokumente zu angereicherten Landkarten und interaktiven Diagrammen verarbeitete. Indem man Metadaten wie Orts- und Zeitangaben mit weiteren Daten wie einer Landkarte und einem Zeitstrahl verknüpfte, ließen sich selbst unzugänglichste Datenberge erschließen. Das große Bild des Krieges, seine Dramatik, sein Verlauf und sein (Miss-)Erfolg wurden durch die Interaktion des Nutzers mit den Daten erfahrbar.

Andere sind noch viel weiter. Ob die Analyse von Bestandsdaten oder die Zusammenführung heterogener Daten – den Verknüpfbarkeiten sind keine Grenzen gesetzt. Der neueste Trend ist es, biometrische Gesichtserkennung in Software für den Massenmarkt einzubauen. Bei Apples iPhoto und Googles Picasa sind diese bereits Teil des Produktes und bei Facebook schon im Test. Es ist natürlich furchtbar praktisch, wenn das Fotoprogramm meine Freunde automatisch anhand ihres Gesichtes erkennt und richtig einsortiert. Google forscht intensiv an immer besseren Algorithmen zur Gesichtserkennung, und so wird es nicht lange dauern, bis alle diese Bilder von uns, von denen wir bislang nichts wussten, durch eine entsprechende Google-Suche zu Tage gefördert werden oder uns das Google-Android-Handy automatisch auf der Straße erkennt.

Ein anderes Beispiel ist Gaydar. Im Jahr 2007 stellten Studenten vom MIT eine Software vor, mit der man recht zielsicher Homosexuelle bei Facebook ausfindig machen kann. Sie analysiert ausgehend von einer bekennenden Referenzmenge an Homosexuellen das Netz der frei zugänglichen Freundschaftsverknüp-

fungen und kann mit einer Trefferquote von 86% vorhersagen, ob ein einzelner Facebook-Nutzer homosexuell ist. Outing ist eine Frage des automatischen Lesens von Datenverknüpfungen geworden.

Egal ob Bilderfassungs- und Auswertungsverfahren oder Freundschaftsverknüpfung: All diese Beispiele haben eines gemeinsam. Sie basieren darauf, dass mit der digitalen Technik heute in Echtzeit Analysen und Referenzen zwischen Daten generiert werden können, die unsere bisherigen Vorstellungen übertreffen. Der einzelne Datensatz liegt eben nicht mehr tot an seinem Speicherplatz, sondern wird durch immer neue Verknüpfungsmethoden «angereichert» und damit stets lebendiger.

Im professionellen Umfeld nennt man das dann «Data-Mining», «Targeting» oder «Monitoring» – im Privaten hat man andere Namen dafür: «Adressbuchsynchronisation», «Bilderverwaltung» oder schlicht «Google-Suche». Die ordnenden und verknüpfenden Algorithmen, die hier zum Einsatz kommen, erreichen heute schon eine ungeahnte Tiefe und Komplexität. Es ist, als würde man mit ausgefeilten archäologischen Methoden die *Jetztzeit* analysieren.

Grund drei für den Kontrollverlust wäre also: Daten werden übermorgen für Verknüpfungen offener sein als morgen.

Die Bibliothek von Babel

Halten wir hier einen kurzen Augenblick inne und betrachten die drei Gründe für den Kontrollverlust:

1. Die steigende Masse an Daten durch die Allgegenwart von Aufzeichnungssystemen.
2. Die steigende Agilität der Daten durch deren sinkende Transaktionskosten.
3. Die steigende Verknüpfbarbeit von Daten.

Wenn man in Betracht zieht, dass Punkt eins und zwei sich entlang von «Moores Law» exponentiell weiterentwickeln (Verdopplung etwa alle 18 Monate), kommt man unwillkürlich an den Punkt, der immer wieder schwarz an die Wand gemalt wird: die Informationsüberflutung.

Eric Schmidt, Top-Manager bei Google, behauptete unlängst, dass derzeit in 48 Stunden genauso viele Daten produziert werden, wie in der Zeit vom Beginn der Menschheit bis zum Jahre 2003. Ein Weiterdenken dieses Trends führt uns unweigerlich zu dem, was Jorge Luis Borges in seiner Erzählung «Die Bibliothek von Babel» beschrieben hat. Ein Volk lebt dort in einer Welt, die eigentlich eine Bibliothek ist, in der alle logisch-mathematisch möglichen Bücher vorhanden sind. Alle denkbaren und undenkbaren, alle sinnvollen und nicht sinnvollen, alle geschriebenen und noch zu schreibenden Texte. Einfach alles. 1,956 * 10 ^ 1834097 Bücher à 410 Seiten.

Das Unverständnis vieler Leute gegenüber Diensten wie beispielsweise Twitter rührt aus dieser generellen Unvorstellbarkeit: «Da schreiben also Leute, wenn sie aufs Klo gehen!?» Aktiven Twitterern kommt diese Frage unsinnig vor.

Aber warum akzeptieren ausgerechnet jene, die an vorderster Front des Informationsorkans stehen, diese Informationsüberflutung schulterzuckend?

Hier greift der Grund Nummer drei für den Kontrollverlust. Die Verknüpfbarkeit der Daten erlaubt uns immer besser mit den Informationsmengen des Internets umzugehen. Echtzeitalgorithmen zur Durchsuchung von großen Datenmengen schaffen ein neues Verhältnis von Sender und Empfänger und damit eine neue Öffentlichkeit in der Bibliothek von Babel.

Die Query-Öffentlichkeit

Wir müssen uns fragen: Was ist Öffentlichkeit in der Bibliothek von Babel? Wir kennen Öffentlichkeit vom öffentlichen Raum, in den man sich begeben kann, manchmal begeben muss. Wir kennen auch die mediale Öffentlichkeit der Massenmedien, in denen wir mehr oder weniger öffentlich sein können, je nach Auflage oder Quote. In der Bibliothek von Babel muss Öffentlichkeit aber neu gedacht werden. Eine dritte Form von Öffentlichkeit hat sich längst parallel gebildet. Nur war sie mit herkömmlichen Denkungsarten des Medienverständnisses nicht beobachtbar.

- Die Öffentlichkeit der Google-Suche: Egal, ob ein Blog 3 oder 300.000 Leser am Tag hat. Wenn es über mich schreibt, wird derjenige, der nach meinem Namen sucht, den Eintrag finden. Denn die Kombination seiner Suchworte bestimmt diese Öffentlichkeit.
- Die Öffentlichkeit der eigenen Twitter-Timeline. Es lesen nicht viele Menschen, was ich twittere, das ist auch nicht nötig. Es abonnieren sich meinen Twitter-Stream nämlich nur diejenigen, die sich wirklich dafür interessieren, was ich schreibe. Die Öffentlichkeit meiner Twitter-Nachrichten strukturiert sich aus der Konfiguration ihrer Abonnemententscheidungen.
- Die Öffentlichkeit des Data-Minings. Auch das gehört dazu, dass die Daten, die ich preisgebe, nicht nur in der Weise genutzt werden, wie ich es mir im Vorhinein vorstelle. Sondern dass sie angereichert werden mit anderen Daten und dass darauf Anfragen getätigt werden, von denen ich heute keine Vorstellung habe. Die Öffentlichkeit meiner Daten bestimmt sich aus der Geschicklichkeit der verknüpfenden Algorithmen solcher Dienste.

Kurz: Man muss im Internet die Öffentlichkeit von der anderen Seite, der Seite des Empfängers, aus neu denken. «Query» bezeichnet in der Datenbanktechnik eine Anfrage beliebiger Komplexität an einen Datensatz. Die neue Struktur von Öffentlichkeit nenne ich deswegen «Query-Öffentlichkeit».

Die Query-Öffentlichkeit ist die positive Kehrseite des Kontrollverlusts. Sie ist das Stück Autonomie, dass der Empfänger von Informationen hinzugewinnt, welches der Sender der Information durch den Kontrollverlust verloren hat. Es ist die Invertierung des klassischen Öffentlichkeitsbegriffs und erfordert ein nicht gerade triviales Umdenken. Ein Umdenken, das aber durchaus beobachtbar

bereits stattfindet und – so meine These – sich mit dem Fortschreiten des Kontrollverlusts noch ausweiten wird.

Mit diesem Umdenken von Öffentlichkeit kehren sich auch eine ganze Reihe von Wertpräferenzen um und bereiten damit den Weg für eine andere Informationsethik. Wenn sich – erstens – Information aufgrund ihrer billigen Speicherbarkeit nicht mehr für ihre Existenz rechtfertigen muss und wir – zweitens – annehmen, dass die Querys, die man auf einen Datensatz anwenden kann, in ihren Möglichkeiten unendlich sind, gibt es plötzlich keine legitime Instanz mehr, die sich anmaßen könnte zu entscheiden, was wichtige, unwichtige, gute oder schlechte Information ist. Das Zusammenstellen von Querys und Präferieren von Filtern wäre das radikale Recht ausschließlich des Empfängers.

Gleichzeitig befreien diese unvorhersehbaren, weil unendlichen Querys auch den Sender der Information. Sie befreien ihn davon, Erwartungen entsprechen zu müssen. Denn der Andere kann, weil er in unendlichen Quellen mit perfekt konfigurierbaren Werkzeugen hantiert, keinen Anspruch mehr an den Autor stellen – weder einen moralisch-normativen noch einen thematisch-informationellen. Die Freiheit des Anderen, zu lesen oder nicht zu lesen, was er will, ist die Freiheit des Senders, zu sein, wie er will.

«Filtersouveränität», so habe ich diese neue Informationsethik genannt, ist eine radikale Umkehr in unserem Verhältnis zu Daten. Sie führt bereits hier und da zu Reibereien und kleineren Kulturkämpfen, und ich bin mir sicher, dass dieses Prinzip seine Stärke erst noch voll entfalten wird. In der Wikipedia ist beispielsweise ein Kulturkampf entbrannt zwischen Exklusionisten und Inklusionisten, also jenen, die meinen, Inhalte wegen Irrelevanz löschen zu müssen, und anderen, die dagegenhalten. Und während ich noch vor fünf Jahren Mails oder SMS gelöscht habe, sortiere ich sie heute nur noch weg. Die Empörung im Internet gegenüber den Maßnahmen der Öffentlich-Rechtlichen, die aufgrund des Rundfunkänderungsstaatsvertrags ihre Archive im Netz unzugänglich machen müssen, speist sich aus dieser neuen Betrachtungsweise. Auch bei dem Gedanken an das «digitale Radiergummi» fasst sich der filtersouveräne Netzbürger an den Kopf. Die Sympathie für Projekte wie Wikileaks, aber auch die Forderungen der Open-Data-Bewegung, dass der Staat alle seine Daten zur potenziellen Verarbeitung maschinenlesbar zur Verfügung stellen soll, all das kann direkt als Ausdruck eines neuen filtersouveränen Bewusstseins gelesen werden. Von den Forderungen eines liberaleren Urheberrechts ganz zu schweigen.

Und das wäre also der letzte Grund, der vierte und endgültige, für den Kontrollverlust: Der Wertewandel durch die Filtersouveränität wird dafür sorgen, dass der Mensch den Kontrollverlust nicht nur in Kauf nimmt, sondern sogar gegen alle Widrigkeiten verteidigen wird.

KONSTANTIN VON NOTZ UND NILS LEOPOLD

Jede Generation wird sich den Datenschutz neu erstreiten

Der Datenschutz steckt erkennbar in einer Krise. Diese ist nicht zuletzt der hohen Innovationsgeschwindigkeit im Datenverarbeitungssektor geschuldet. Aber das ist noch kein Grund, ihn komplett verloren zu geben. Selbst in den USA werden mittlerweile die Rufe nach einem umfassenderen Recht auf Privatsphäre laut. Hier einige Vorschläge für neue Standards bei der Regulierung.

Die Veränderungen der Informationstechnologie, der damit einhergehende soziale Wandel und die Folgen sind bislang noch weitestgehend unverstanden. Aus vormaligen Informationsempfängern, deren Techniken individueller Suche nach Inhalten im Netz sich laufend verfeinern, sind zugleich auch Sender und datenschutzrechtlich Verantwortliche geworden.

Preisgegeben haben sie ihr Verhalten bereits zuvor in einem überwiegend rezeptiven Internet, in welchem ihre «click streams» durch das sogenannte «tracking» auswertbar waren und sind. Doch diese Möglichkeit der Erstellung von Profilen potenziert sich im Social Web zu weitaus umfangreicheren Bewegungs-, Bekanntschafts-, Kommunikations- und Verhaltensprofilen. Denn die Nutzer veröffentlichen selbst Inhalte, kommunizieren voll beobachtbar mit Dritten und machen dabei Aussagen über sich und ihre Umwelt.

Datenschutzrechtlich weitaus relevanter sind die Geschäftsmodelle der großen Web-Anbieter. Einige Unternehmen beherrschen den Markt derzeit quasimonopolistisch. Sie verfügen über äußerst detailreiche Informationen ihrer Kunden, oft seitenübergreifend. Daneben entwickeln sich Foren und Bewertungsplattformen, deren Gegenstand konkrete Personen (Lehrer, Ärzte, Handwerker usw.) sind und die oftmals Konflikte provozieren.

Daten entziehen sich zunehmend den Verfügungsbereichen Privater, von Unternehmen oder auch von Nationalstaaten. Mit den Geschäftsmodellen des «cloud computing» wird eine Lokalisierung der Datenverarbeitung oft unmöglich und damit die gesetzliche Bindung der Datenverarbeitung erschwert. Schließlich werfen auch Anwendungen des Ubiquitous Computing zahlreiche datenschutzrechtliche Fragen auf.

Dieser rasante Wandel der Angebote des Internets sowie der damit einhergehenden Datenverarbeitungen führt zu Verunsicherungen. Soziologisch betrachtet kann man den diesen Entwicklungen entgegengehaltenen Daten-

schutz als eine Form gesellschaftlicher Problemverarbeitung verstehen. Funktional besehen schafft er Akzeptanz und Vertrauen für einen als überwältigend neu und übermächtig empfundenen Technikwandel.

Datenschutz in .de und .eu

Normativ gesehen handelt es sich beim Datenschutz um ein Grundrecht. Ziel ist die Freiheit, grundsätzlich selbst zu entscheiden, was mit den einen selbst betreffenden Daten und Informationen geschieht. Die Datenschutzdebatte ist bereits seit gut 40 Jahren ein lebendiger Bestandteil staatlicher Handlungsüberlegungen wie auch des Rechts. Weil der Datenschutz europäischer Prägung übergreifend gesetzlich ausgeformt wurde, betrifft er «mitlaufend» praktisch alle Lebensbereiche und sowohl staatliche als auch nicht-staatliche Datenverarbeitungen.

In Europa, besonders in Deutschland finden sich die wohl differenziertesten Aussagen zu Inhalten als auch Grenzen des Datenschutzes. Mitte der 1990er-Jahre machte sich die Europäische Union große Teile des bundesdeutschen Datenschutzprogramms durch Inkorporation in die Europäische Datenschutzrichtlinie 95/46 zu eigen. Die Mitgliedstaaten regeln den Umgang mit personenbezogenen Daten und Informationen übergreifend und systematisch.

No Privacy – Der amerikanische Weg

Die USA mit ihrem deutlich abweichenden Verständnis von Privatheit prägen nach wie vor das uns bekannte Internet. Facebooks Marc Zuckerberg und Googles Eric Schmitt stehen mit ihrer Rede vom Ende der «privacy» in einer schon längeren Tradition von Äußerungen US-amerikanischer Unternehmenschefs, die nur vor dem Hintergrund des US-amerikanischen Privacy-Verständnisses überhaupt verständlich sind.

Einerseits sind die USA eine Spitze der Datenschutzbewegung. Bereits 1969 kam es dort zu einer breiten Bewegung gegen staatliche Volkszählungspläne. Andererseits hat diese frühe Auseinandersetzung unter dem Begriff «privacy» einen ganz anderen Verlauf genommen als in Europa. Eine unmittelbare Anerkennung eines allgemeinen «right to privacy» durch den Supreme Court erfolgte nie. Es blieb bei einer rudimentären Rechtsprechung, die sich nicht auf Privatwirtschaft erstreckt. Dort bleibt es fast ausschließlich beim Deliktsrecht.

Inhaltlich fällt auf, dass die US-Debatte und das Verständnis von «privacy» einerseits nach wie vor stark von Konstrukten wie «Privatheit versus Öffentlichkeit» oder durch die vom «supreme court» geprägte Formel von der «vernünftigen Erwartbarkeit von Privatheit» geprägt wird. Erst in jüngster Zeit finden sich zumindest wissenschaftliche Beiträge (so z.B. von D. Solove, M. Ryan Calo und H. Nissenbaum), welche komplexere Schutzmodelle anbieten, die starke Ähnlichkeiten mit Grundprinzipien des europäischen Datenschutzes aufweisen.

Die Krise des Datenschutzes

Das Regelungsdefizit liegt zum Teil im Regelungsgegenstand selbst begründet. Mit der Datenverarbeitung wird ein innovatives Feld erfasst, das auch den Gesetzgeber unter ständigen Veränderungs- und Nachbesserungsdruck stellt. Er muss seine Instrumente laufend anpassen, um ein Leerlaufen seiner Regelungen zu vermeiden. Das Vollzugsdefizit ist teilweise hausgemacht. Überbürokratische und nicht unabhängige Aufsichtsbehörden in einigen Ländern verhindern eine effektive Aufsicht.

Zum Teil aber liegt die Krise an einer ideologischen Aufladung der Diskussion. Datenschutz hat sich parallel zum Diskurs sogenannter innerer Sicherheit entwickelt und ist mit ihm eng verwoben. Der sogenannte Kampf gegen den Terrorismus, aber auch die Bekämpfung organisierter Kriminalität sowie der Kriminalität im Allgemeinen haben zu einem steten Ausbau der Sicherheitsbehörden sowie ihrer Aufgaben und Befugnisse geführt. Von Grundrechts- wie Bürgerrechtskundigen wurde dies von Beginn an mit großem Unbehagen beobachtet und kritisiert. Hier gibt es verhärtete Fronten zwischen Befürwortern und Gegnern des Datenschutzes.

Im Bereich der nicht staatlichen Datenverarbeitung sieht es anders aus. Obwohl es allgemeine gesetzliche Regeln gibt, rangiert insbesondere die Regulierung der Datenverarbeitung bei Privatunternehmen bis heute deutlich hinter den Anstrengungen bei der staatlichen Datenverarbeitung. Zum Teil liegt dies daran, dass die Grundrechte im Verhältnis zwischen Privaten (und damit auch zwischen Bürgern und Unternehmen) nur mittelbar gelten sollen. Diese juristische Fiktion allgemeiner Ebenbürtigkeit wirkt besonders dann schräg, wenn es Verbrauchern schlicht an Alternativen mangelt und ihnen strukturell deutlich überlegene Vertragspartner in Gestalt großer Unternehmen gegenübertreten und die Nutzungsbedingungen diktieren. Erst die Datenskandale der vergangenen Jahre haben außerdem das erhebliche Vollzugsdefizit bei den Gummiparagraphen des Bundesdatenschutzgesetzes zutage treten lassen. Sie haben damit den Schutzbedarf des Privatbereichs offenbart, ohne dass der Gesetzgeber bis heute diesen Missstand angegangen ist.

Blinde Flecke der Datenschutzkritik

Die Debatte um den Datenschutz nimmt im Internet einen ganz eigenen Verlauf. Einerseits handelt es sich häufig um gelungene, oft autodidaktische Aneignungen und Aufbereitungen einer komplexen Materie, die zuvor allein noch einem begrenzten Fachpublikum überlassen blieben. Die Veröffentlichungsformen des Internets bewirken damit in gewissem Umfang eine Re-Demokratisierung durch die Rückkehr in den allgemeinen politischen Diskurs. Der Nachteil liegt andererseits darin, dass gelegentlich grundlegendes Fachwissen unberücksichtigt bleibt und Debatten in einigen Bereichen auch hinter den wissenschaftlichen Erkenntnisstand zurückfallen.

Die Debatte des Sommers 2010 um Google Street View polarisierte, denn eine Mehrheit der Bundesbürger stand den Bildveröffentlichungen kritisch gegenüber. Google Street View spitzte den Konflikt zwischen einem US-amerikanischen Verständnis von «privacy» und dem europäischen Konzept der «data protection» zu.

Nach der US-Doktrin sind in der Öffentlichkeit anfallende Daten von vornherein nicht schutzwürdig, denn sie sind dort allgemein wahrnehmbar. Ähnlich der in Deutschland bereits überwundenen Sphärentheorie des Privatrechts bleiben Bürger innerhalb der sogenannten öffentlichen Sphäre datenschutzrechtlich deshalb weitgehend ohne Schutz. Ein kategorialer Unterschied durch die systematische Veröffentlichung und weltweite Abrufbarkeit im Internet, verbunden mit der Möglichkeit der Verknüpfung mit weiteren personenbezogenen Daten, wird dabei nicht gesehen. Es gab deshalb von Beginn an starkes Befremden seitens der «netizens» gegenüber den Plänen der Politik, in diesem Bereich zu regulieren. Die Mehrheit der Bevölkerung bestätigte jedoch das bundesdeutsche Datenschutzverständnis und die zuständige Aufsichtsbehörde. Diese handelte eine Widerspruchsmöglichkeit gegen die Veröffentlichung des eigenen Hauses im Internet aus, weil es eindeutig auf die darin lebenden Personen verweisen kann und mit weiteren personenbezogenen Daten verknüpfbar erscheint. Ganz unstreitig war, dass erfasste Gesichter und KFZ-Kennzeichen gepixelt werden müssen.

Wenn es um das Internet geht, erleben wir die Auferstehung der Ethiken. Von Beginn an war da etwa die sogenannte Netiquette, ein Gespenst, über das viel geschrieben wurde, ohne dass man es je in Aktion sah. Der Plural der Ethiken muss heute betont werden, denn da ist einiges vertreten: Das Bundeskanzleramt etwa forderte jüngst eine «Ethikoffensive für das Internet», und ein Blogger fordert die radikale Abkehr von der individuellen Verantwortungsethik, wie sie zu guten Teilen auch dem Grundgesetz zugrunde liegt. Stattdessen sollen die Informationsinteressen des «Anderen» – in Anlehnung an das Konzept eines französischen Philosophen – im Mittelpunkt stehen. Dabei werden, ganz unbeeindruckt von der Komplexität der realen Datenschutzdebatte, unterschiedlichste Verarbeitungsverhältnisse (Staat und Bürger, Bürger und Unternehmen, Arbeitgeber und Beschäftigte) in einen Topf geworfen.

Mit solchen Forderungen einher geht der Verzicht auf die Formulierung von bürgerrechtlichen Normen und die Beschränkung des Datenschutzes auf reduzierte Schutzprogramme, maximal auf rote Linien. Umgekehrt fordern hingegen radikale Netzpessimisten, oftmals deutlich technikfeindlich angetrieben, «klare Internetgesetze», um dem ruchlosen Treiben des «rechtsfreien» Internets gleich auf ganz vielen Ebenen endlich ein Ende zu setzen. Auch hier ist der Datenschutz zumeist Gegner, und es entstehen merkwürdige Allianzen aus Sicherheitspolitikern, Technikfeinden und Gegnern von Meinungsfreiheit.

Einen Anlass zu einer pauschalen Absenkung der Datenschutzstandards mit Blick auf das Internet gibt es aber nicht. Im Gegenteil: In dem Maße, in dem

sich das Internet zum zentralen Kommunikationsraum der Menschen entwickelt, bedarf es auch und gerade aus grundgesetzlicher Perspektive zeitgemäßer Schutzvorkehrungen, um eine weitestgehend autonome Gestaltung der Möglichkeiten der vertraulichen Kommunikation zu gewährleisten.

«Privacy by obscurity» bietet keine rechtlich akzeptable Lösung. Und der allgemeine «free flow of information» ist als Grundsatz nicht ansatzweise konkret genug entfaltet, um den Grundrechten der Einzelnen tatsächlich entgegenzustehen. Dies gilt ebenso für allgemeine Thesen wie «The internet wants to be free», die in ihrer Allgemeinheit bedeutungslos bleiben. Vielmehr stellen sich auch im Kontext des Internets die Fragen eines verfassungsgemäßen Datenschutzes ganz konkret. Es bedarf zahlreicher Unterscheidungen von Datenverarbeitungen im Internet, die ganz unterschiedliche Bewertungen erfahren können. Dies entspricht dem im bundesdeutschen Datenschutzrecht spätestens seit der Volkszählungsentscheidung maßgeblichen Grundsatz des Verwendungskontextes, der letztlich über den konkreten Schutzbedarf entscheidet.

Zum Teil wird der Erfolg des Web 2.0 von Kritikern des Datenschutzes auch als Beweis fehlender Erwartungen der Menschen hinsichtlich ihrer «privacy» herangezogen. Bereits die Nutzung unzureichend datenschutzrechtlich abgesicherter sozialer Netzwerke etwa wird als der Nachweis eines massenhaften Grundrechtsverzichts gewertet. Auch diese Argumentation überzeugt wenig. Nicht nur bei uns, auch in den USA begleitet den Datenschutz in sozialen Netzwerken vielmehr von Beginn an eine kritische Debatte.

Der Schluss, den Menschen fehle es an Interesse hinsichtlich des Schutzes ihrer Daten, scheint insgesamt gewagt angesichts der fehlenden Handlungsoptionen für die User. Die Intransparenz der im Hintergrund ablaufenden Datenverarbeitungen kommt hinzu. Auch Umfragen deuten immer wieder darauf hin, dass sehr wohl eine große Nachfrage besteht, aber die Nutzer eben die derzeitigen Umstände eher duldend hinnehmen, da es an Alternativen mangelt. Und zuletzt darf auch eine entsprechende – unterstellte – massenhafte «Null-Erwartung» den Gesetzgeber nicht aufhalten. Dieser ist vielmehr grundrechtlich gebunden, wesentliche Teile eines die möglichst autonome Nutzung eröffnenden Schutzprogramms zur Anwendung zu bringen, wenn er strukturelle Ungleichheiten zwischen Nutzern und Anbietern für gegeben hält.

Soweit der individuelle Kontrollverlust als unvermeidliche Folge der technischen Entwicklung angesehen wird und daraus das Ende des Datenschutzes folgen soll, so verfehlt diese These in jedem Falle die normative Ebene. Denn aus einem Sein lässt sich kein Sollen ableiten. Und: Der wirkliche Kontrollverlust tritt erst dann ein, wenn der Gesetzgeber seinen Steuerungsanspruch und seine Schutzverantwortung aufgibt. Denn einen Schutz erreicht man, neben Maßnahmen auf Seiten der Grundrechtsträger, besonders durch Bindungen auf der Seite derjenigen, die Daten und Informationen verantwortlich verarbeiten. Vermeintliche Ausweglosigkeiten beruhen häufig auf einem verkürzten Verständnis von Datenschutz, oftmals wird darunter fälschlich auch noch ein eigentumsanaloges Verfügungsrecht über Daten verstanden.

Zum Teil rührt die Kritik am Datenschutz im Kontext des Internets von «netizens», die sich vom Internet immer noch die «ganz andere Zukunft» versprechen. Nicht selten kommt es dabei zu einer Vermengung mit der Debatte um die Postmoderne, um den Abschied vom Subjektbegriff der Aufklärung, von einem als repressiv verstandenen Vernunftbegriff usw. Das Internet verknüpft sich dann mit einer zumeist vage bleibenden Gesellschaftsutopie der vernetzten Gesellschaft, als deren oberstes Ziel die Transparenz aller Daten und Informationen steht. Entsprechende Beiträge wirken oftmals politikfern und realitätsentrückt. Es wirkt zumindest befremdlich, dass sich auch die Gründer der heute dominierenden Unternehmen der Datenwirtschaft in einer durchaus unheiligen Mischung aus kommerziellem Interesse und persönlicher Überzeugung ebenfalls auf diese Utopien berufen. Ihre Unternehmen sind zumeist zentrale Treiber einer Datensammelei, die gerade für die Nutzer bis heute fast völlig intransparent bleibt. Auffällig und totalitär erscheint, wenn Webevangelikale unitarische Erlösungsmodelle anbieten, bei denen sich Spannungsverhältnisse zwischen Einzelnen und der Gesellschaft zum gedachten Ende hin vollständig auflösen sollen. In der optimalen Allokation aller Informationen entwirren sich die Probleme der Welt – mit magischer unsichtbarer Hand – zum Wohle aller? Dieses Heilsversprechen wirkt angesichts einer weiter zunehmenden Komplexität der Lebenswelten wenig überzeugend. Aus bürgerrechtlicher Sicht fehlen die politische Erdung und der Bezug auf die Grund- und Menschenrechte.

Was ist zu tun?

Den eingangs beschriebenen zentralen Herausforderungen des Internets sind die bundesdeutschen Datenschutzgesetze nicht mehr gewachsen. Sie sind nicht internetfähig und gehören deshalb reformiert. Das Schutzprogramm muss so angepasst werden, dass ein hoher Schutzstandard für die Grundrechte auch und gerade im Internet erhalten werden kann. Mit nationalen Alleingängen ist es nicht getan.

Die gerade eröffnete Reformdiskussion zur EG-Datenschutzrichtlinie 95/46 geht in die richtige Richtung. Darüber hinaus bedarf es weiterer internationaler Impulse, um der globalen Dimension gerecht zu werden. Dazu zählen aussagekräftige Datenschutzabkommen der EU mit den USA sowie etwa die Neuverhandlung des Safe-Harbor-Abkommens, das bislang inhaltlich leer läuft, aber auch internationale Abkommen.

Damit ist der nationale Gesetzgeber nicht entlastet. Er muss ebenfalls seine Hausaufgaben machen. Selbstregulierungen genügen nicht, wenn diese als Gelegenheit zur Absenkung von Schutzstandards dienen. Reformvorschläge existieren bereits seit den unvollendet gebliebenen rot-grünen Modernisierungsbemühungen von 2000. Jüngst haben die Datenschutzbeauftragten in einem Eckpunktepapier wichtige Elemente bereits benannt. Dazu zählen eindeutige Regelungen zur Profilbildung, Verbesserungen des Selbstdatenschutzes, der Transparenz sowie der unabhängigen Datenschutzaufsicht. Bei einzelnen

Problemlagen bedarf es konkreter Einzelregelungen, um möglichst konkrete und sachgerechte Interessenausgleiche zu erzielen.

Insgesamt muss sich der Datenschutz noch deutlicher in Richtung eines Mehr-Ebenen-Ansatzes entwickeln, bei dem neben das «klassische» Ordnungsrecht mittelbare Steuerungsanreize wie das Gütesiegel- und Auditierungsmodell, aber auch Privacy by Design als zumindest für bestimmte Branchen verpflichtende Vorgabe treten. Innovative Steuerungsmodelle sind zu entwickeln, um ein hohes Schutzniveau zu erhalten und damit den Bürgern eine weitestgehende Autonomie hinsichtlich der Daten und Informationen zu erhalten, die sie betreffen oder betreffen könnten.

GEORGE DANEZIS UND SEDA GÜRSES

Illusionen der Kontrolle. Ein kritischer Blick auf den technischen Datenschutz

Datenschutz spielt sich oft zwischen den Paradigmen der Vertraulichkeit und Kontrolle ab. Heilsbringer sind Werkzeuge zur Verschlüsselung oder Anonymisierung nicht, deswegen aber ganz auf sie zu verzichten, wäre fatal. Ein informationswissenschaftlicher Werkstattbericht über die Grenzen des Identitätsmanagements.

In den vergangenen 30 Jahren hat der Gedanke, sogenannte «Privacy Enhancing Technologies» (PET)[1] zu entwickeln – das sind Technologien, die auf Bedenken hinsichtlich von Überwachung und Datenschutz reagieren –, in Forschung wie auch in der Praxis viel Zuspruch gefunden. Solche Technologien sind von Bedeutung, nicht nur weil sie technische Ansätze dafür bieten, Informationen zu verbergen, preiszugeben und ihren Fluss zu steuern, sondern auch, weil sie unserem Verständnis davon, was Datenschutz ist oder sein kann, auf die Sprünge helfen.

Auf derartige Technologien wird sehr unterschiedlich reagiert; sie werden sehr unterschiedlich angewendet. Manche halten die PETs für ein Allheilmittel, andere glauben, sie erfüllten den gesellschaftlichen Bedarf an Datenschutz nicht und böten kaum Schutz gegen die immer mehr um sich greifende Überwachung. In diesem Beitrag wollen wir von einem solchen Entweder–Oder Abstand nehmen. Wir regen stattdessen an, sich mit den PETs in einer Art auseinander zu setzen, der zeigt, dass sie grundlegender Bestandsteil der Debatten zu Überwachung und Datenschutz sind – und umgekehrt.

Datenschutz und Vertraulichkeit

Liegen personenbezogene Daten erst einmal in digitaler Form vor, so ist es, technisch gesehen, sehr schwierig, technisch sicherzustellen, dass Einzelne den Fluss ihrer Daten so steuern können, dass Unbefugte keinen Zugriff darauf

1 Privacy Enhancing Technologies bedeutet etwa «den Datenschutz stärkende Technologien».

haben. Eine Denkrichtung in der Datenschutzforschung folgert daraus, Daten könnten nur dann geschützt werden, wenn PETs die Nutzung von informationsverarbeitenden Diensten erlauben, gleichzeitig aber den Umfang der erfassten Informationen so gering wie möglich halten oder die erfassten Informationen anonymisieren. Entsprechende Technologien setzen auf Verschlüsselung, Datenmischung, Dummy Traffic[2] und andere Mechanismen, um Datenschutznormen wie Anonymität, Nichtrückverfolgbarkeit, unbeobachtbares Handeln und Vertraulichkeit von Kommunikation zu wahren. Technologien, die dieser Logik folgen, bezeichnen wir als Technologien, die Datenschutz mit Vertraulichkeit gleichsetzen.

Ein bekannter, aus dieser Schule stammender Ansatz aus dem Bereich der Sicherheitstechnik setzt sich mit den Bedingungen auseinander, die gegeben sein müssen, damit Kommunikation vertraulich ist, das heißt damit, wer mit wem kommuniziert. Gemeinhin werden solche Techniken Anonymisierer genannt; das bekannteste Beispiel ist «Tor»[3]. Ein solches System «entlinkt» die Identität einer Akteurin von den Spuren, die sie in Informationssystemen hinterlässt. «Anonymität» ist dabei dann hergestellt, wenn eine Einzelperson sich innerhalb einer beschränkten Anzahl von Usern, dem so genannten «anonymity set», nicht mehr ausfindig machen lässt.

Ein anderer Ansatz, der Datenschutz als Vertraulichkeit definiert, setzt auf die Integration kryptografischer Elemente, beispielsweise eines Zero-Knowledge-Protokolls[4], zusammen mit einem entsprechenden Informationsdesign des geplanten Systems, um so die Menge der personenbezogenen Daten zu minimieren. Zwar ist es möglich, in solch einem System User zu identifizieren, versucht wird jedoch, von ihnen gewünschte Funktionalitäten anzubieten, ohne dazu gleichzeitig große Mengen personenbezogener Daten an zentraler Stelle abzulegen.

Aus dem Bereich der Analyse von Datenbanken – dem Datenschürfen («data mining») und der Wissensauffindung («knowledge discovery») – kommt ein weiterer Ansatz, der Datenschutz gleich Vertraulichkeit setzt, das Privacy Preserving Data Publishing (PPDP). Ziel von PPDP ist es, die Analyse von Datenbanken, die personenbezogene Informationen enthalten, auf bestimmte Arten zuzulassen und gleichzeitig bestimmte andere Informationen (solche, die die Privatsphäre

2 Dummy Traffic bezeichnet automatisch generierte Scheininformationen, die zusammen mit den eigentlichen Daten übertragen werden, um es schwieriger zu machen, Informationen aus dem Datenverkehr herauszufiltern.

3 Das Tor-Netzwerk überträgt den Datenverkehr verschlüsselt und zufällig über ein Netzwerk von Servern. Für einen Überblick siehe: http://de.wikipedia.org/wiki/Tor_%28Netzwerk%29

4 Das Zero-Knowledge-Protokoll ist ein interaktives Beweissystem, bei dem sich zwei Parteien wechselseitig dadurch authentifizieren, dass sie sich indirekt über ein beiden bekanntes Geheimnis austauschen – ohne dieses jedoch offen zu legen. Für einen Überblick siehe: http://de.wikipedia.org/wiki/Zero_Knowledge

Einzelner verletzen, indem sie diese eindeutig identifizieren) auszuschließen.[5] Dieses Verfahren ist auch bekannt als «Anonymisierung von Datenbanken». Eine Alternative zu PPDP, die in interaktiven Systemen mit sicherer Eingabemaske eingesetzt werden kann, ist die sogenannte «differential privacy». Dabei wird die Frage, wie sich Datenschutz wahren lässt, gleichzeitig aber statistische Informationen erhoben werden können, auf eine solide theoretische Grundlage gestellt – wobei dieses Verfahren zeigt, wie sehr Spuren verwischt werden müssen, um Rückschlüsse auf Einzelne unmöglich zu machen.[6]

Die Grenzen anonymer Kommunikation und der Anonymisierung

Bei anonymer Kommunikation bleibt die Identität von Individuen innerhalb von Informationssystemen vertraulich. Wie öffentlich diese Spuren in der Folge werden, wird dabei jedoch eher nicht berücksichtigt. Die entsprechenden Ansätze gehen folglich davon aus, die Entlinkung der Spuren, die ein Individuum hinterlässt, bedeute einen wünschenswerten und ausreichenden Schutz der Kommunikation dieses Individuums.

Auf den ersten Blick sieht es so aus, als folgten Datenschutzgesetze der Annahme, Anonymität reiche aus, um die Privatsphäre zu schützen, denn per Definition gilt der Datenschutz nur für personenbeziehbare, nicht aber für anonyme Daten – oder anders gesagt, nur für Daten, die sich zuschreiben und einer Person zuordnen lassen. Entsprechend gilt der Datenschutz nicht für Spuren, die anonyme Kommunikation hinterlässt. Wollte man den Datenschutz auf anonyme Kommunikation anwenden, wäre die Voraussetzung dafür paradoxerweise, dass man sich von der Anonymität verabschieden müsste.

Hier stoßen wir auf ein grundlegendes Spannungsverhältnis zwischen den Erfordernissen des Datenschutzes, den Zielen der Anonymisierer und auch den Wünschen der User. Diese Spannung zeigt sich nicht nur im Hinblick auf Anwendungen wie Anonymisierer. Um Datenschutz wirksam wie umfassend umzusetzen, müssen wir zuallererst eine äußerst umfängliche Überwachungs- und Nachverfolgungstechnologie einsetzen.

Die Frage, ob und wie sich Datenschutz auch auf anonyme Spuren anwenden lässt, wird weiter erschwert durch eine grundlegende Verschiebung bei der Forschung zur Anonymisierung von Daten. Anhand von vorhandenen, anonymisierten Datensätzen wurde in mehreren Fällen gezeigt, dass sich diese mit mächtigen Werkzeugen wiederum entanonymisieren lassen.[7] Solche Angriffe lassen ernsthafte Zweifel daran aufkommen, ob es je möglich sein wird, umfangreiche Datensätze, die relationale Daten über User enthalten (beispielsweise Bewertungen von Filmen), jemals auf sichere Art öffentlich zu machen. Selbst für

5 Beispiele hierfür finden sich z.B. bei Sweeney (2002), Kifer and Gehrke (2006), Li und Li (2007) und Rebollo-Monedero etc. (2008).

6 Ein Überblick über die mathematische Komplexität der Methode findet sich hier: http://en.wikipedia.org/wiki/Differential_privacy

7 Siehe Narayanan and Shmatikov (2008)

den Fall, dass dies möglich wäre, bliebe immer noch unklar, in welche Kategorie anonymisierte Daten fallen, ob Datenschutz für sämtliche Daten gilt und ob es für Verfahren wie PPDP oder «differential privacy» irgendeine rechtliche Grundlage gibt. Die Antwort auf diese Fragen wird sich wahrscheinlich auch auf die Frage auswirken, ob anonyme Kommunikation rechtlich geschützt ist.

Hinzu kommt, dass der Schutz, den Systeme zur anonymen Kommunikation bieten, in dem Maße schwindet, in dem sie genutzt werden, das heißt, bei häufiger, anhaltender Nutzung werden die kommunizierenden Parteien sichtbar. Anders ausgedrückt, bietet anonyme Kommunikation bestenfalls einen taktischen Schutz, da sich auf lange Sicht Profile erstellen lassen. Die Ergebnisse der PPDP, die zeigen, dass Anonymität auf Dauer nicht möglich ist, verstärken dieses Problem noch. Je mehr «data mining» betrieben wird je mehr Daten aus unterschiedlichen Quellen miteinander abgeglichen werden können, desto mehr wird sich auch die Wahrscheinlichkeit erhöhen, dass User doch identifiziert oder anonyme Spuren zu konkreten Sendern zurückverfolgt werden können.

In einer vernetzten Welt, in der sich das Augenmerk weniger auf wesenhafte Eigenschaften und mehr auf Verbindungen richtet, müssen die Wirksamkeit anonymer Kommunikation und der Anonymisierung von Datenbanken zum Schutz der Privatsphäre sorgfältig analysiert werden. Zwick und Dholakia beispielsweise behaupten, dass PETs «Kunden» nur in der falschen Sicherheit wiegen, autonom zu handeln.[8] Ontologisch unterscheidet sich das Wesen des Konsumenten nicht von seinem Abbild auf dem elektronischen Marktplatz. Der Konsument wird durch Sprache zu dem gemacht, was er oder sie ist, und die in dieser Sphäre gängige Sprache wird von (Marketing-) Datenbanken bestimmt. Anonymisierer oder anonymisierte Datenbanken können gegen diese Sprache und ihre Spielregeln nichts ausrichten. Solche Überlegungen zeigen, dass Lösungen, die Datenschutz mit Vertraulichkeit gleichsetzen, ihre Versprechungen womöglich nicht einlösen können.

Es wäre jedoch zu kurz gegriffen, auf Anonymisierer und Techniken zur Anonymisierung ganz zu verzichten, nur weil sie Mängel aufweisen. Vielmehr zeigen die hochgradige Zunahme beim Sammeln personenbezogener Daten die Erfordernis, sich an persönlichen Netzwerken zu beteiligen, wie auch die Beliebtheit der Anonymisierer, wie schwierig, aber auch wie wichtig es ist, in einer überwachten Welt die Privatsphäre durch Vertraulichkeit zu schützen. Die mindeste Reaktion auf diese Herausforderungen ist, dass die Forschung neue Lösungen findet, die den Fortschritten beim Datenschürfen gewachsen sind. Wie Philips zeigt, ist Anonymität von großer Bedeutung, um die Grenzen zwischen Privatem und Öffentlichem abzustecken. Allerdings warnt er auch davor, dies mit der Notwendigkeit zu verwechseln, zum Schutz der Privatsphäre diese wahrenden Normen zu benennen und ihre Einhaltung einzufordern.[9]

8 Zwick und Dholakia (2003)
9 Phillips (2004)

Privatsphäre und Selbstbestimmung

Ein weitergehender Begriff von Privatsphäre begreift diese nicht nur als die Geheimhaltung persönlicher Informationen, sondern auch als die Fähigkeit, selbst zu bestimmen, was mit ihnen geschieht. Dieser Begriff, der nicht auf eine strenge Datenarmut abzielt, rührt daher, dass es in vielen Fällen notwendig und vorteilhaft ist, Daten preiszugeben. Eine selbstbestimmte Verfügung über Daten könnte entsprechend dabei helfen, den Missbrauch von so angehäuften Informationen abzuwenden.

Das Bundesverfassungsgericht hat diese Vorstellung in dem Begriff «informationelle Selbstbestimmung» ausgedrückt. Auch eine Reihe internationaler Richtlinien zum Datenschutz, beispielsweise die Datenschutzdirektive der EU, gehen auf diese Vorstellung zurück.

Das Konzept der Selbstbestimmung stützt jene Art von Privatheit, auf die gegenwärtig Systeme zum Identitätsmanagement (IDM) abzielen. Mit solchen Systemen soll es Einzelnen möglich sein, sich sichere Identitäten zu verschaffen, diese Identitäten mit Attributen auszuzeichnen, die Aktivitäten ihrer Identitäten für sie nachvollziehbar zu machen und Identitäten zu löschen.

Die Forschung in diesem Bereich arbeitet daran, Verschlüsselungstechniken und Protokolle zu entwickeln, die anonyme oder pseudonyme Profile möglich machen, und die möglichst zusammen mit den bereits genannten Anonymisierern genutzt werden sollten. Sie sind außerdem angewiesen auf Richtlinien, die, hinsichtlich der preiszugebenden Informationen, den Zugang zu Diensten regeln.[10] Es handelt sich hierbei um ausgereifte Technologien, und einige ihrer technischen Kernbestandteile werden aktuell schon für kommerzielle Vorhaben genutzt.

MS Passport, das erste Identitätsmanagementsystem, das breite Anwendung fand, war gleichzeitig der erste Fehlschlag. Das System wurde von Dritten abgelehnt, da es sie zwang, einen einzigen Identitätsprovider zu nutzen, nämlich Microsoft.[11] Dass dies dem Identitätsprovider die Möglichkeit gab, die Surfgewohnheiten und Interaktionen sämtlicher Nutzer einzusehen, und die sich daraus ergebenden Bedenken, was Überwachung und eine mögliche Verletzung der Privatsphäre anbelangen, haben bei dieser Debatte allerdings nur am Rande eine Rolle gespielt.

Die Industrie reagierte, indem sie die Liberty Alliance gründete, ein Konsortium, das auf offene Standards innerhalb eines föderal organisierten Identitätsmanagements setzt. Wert gelegt wurde dabei darauf, dass unterschiedliche Identitätsprovider (und nicht ein einziger Big Brother) zusammenarbeiten und Attribute eines Individuums (eines Datensubjekts) beschreiben können. Diese Attribute werden dann vom Datensubjekt an Parteien, die diesen Angaben vertrauen, weitergegeben, worauf dem Subjekt von der dritten Partei bestimmte

10 Siehe Beispiele bei Ardagna et al. (2009) und bei Clauß et al. (2005)

11 Siehe http://underthehood.ironworks.com

Privilegien eingeräumt werden. Diese aus drei Parteien bestehende Architektur, bei der das Individuum die Mittelposition einnimmt, ist inzwischen zum führenden Modell für userzentrierte IDM-Systeme geworden.

Allerdings kann das föderale Modell des Identitätsmanagements nicht all die Bedenken ausräumen, die MS Passport hervorgerufen hat. Zwar setzt dieses Modell auf mehrere Identitätsprovider und darauf, dass die User die Kommunikation zwischen ihnen vermitteln, sollte jedoch ein Identitätsprovider mit einer dritten Partei zusammenarbeiten, könnten sämtliche Aktivitäten der User nachvollzogen werden. Das föderale Modell basiert demnach darauf, dass die beiden anderen Parteien klar voneinander getrennt sind, das heißt, dass sie nicht zusammenarbeiten und so die Privatsphäre verletzen. Diese Modelle werden deshalb auch als «vertrauensbasierte Systeme» bezeichnet. Vom technischen Standpunkt aus stellen sie einen eher schwachen Schutz der Privatsphäre dar.

Eine entsprechende Funktionalität kann auch umgesetzt werden, wenn so genannte «selective disclosure credentials» (d.h. ausgewählt offen gelegte Legitimationen) benutzt werden, ohne dass dabei zu befürchten wäre, Identitätsprovider und ihnen vertrauende Parteien würden gemeinsame Sache machen. Verschlüsselungssysteme lassen es zu, dass ein Identitätsprovider einem Datensubjekt eine Legitimation ausstellt, die dieses dann einer vertrauenden Partei gegenüber offenlegen kann, um so nachzuweisen, dass bestimmte Teile der Legitimation authentisch sind. Die Verschlüsselung stellt dabei sicher, dass Ausgabe und Offenlegung der Legitimation nicht miteinander in Beziehung gesetzt werden können. Dadurch ist wirksam sichergestellt, dass der Datenschutz nicht ausgehebelt werden kann, sollten zwei Parteien gemeinsame Sache machen. Erreicht wird so etwas scheinbar Unvereinbares, nämlich dass einerseits eine Rückverfolgung nicht möglich, andererseits eine Fälschung ausgeschlossen ist. Usern ist es so möglich, Pseudonyme zu erstellen und zu nutzen, die keinen Rückschluss auf ihre eigentliche Identität zulassen, und einer vertrauenden Partei nur bestimmte, beglaubigte Eigenschaften zu übermitteln, beispielsweise eine Altersangabe. Systeme, die mit «selective disclosure credentials» arbeiten, sind im großen Stil in Prototypen umgesetzt worden und werden mittlerweile, beispielsweise von Microsoft, auch ausgeliefert.

Unbestreitbar stellen IDMs, die mit «selective disclosure credentials» arbeiten, im Vergleich zu herkömmlichen, vertrauensbasierten Systemen, einen bedeutenden Fortschritt dar. Welchen Begriff aber haben sie von Selbstbestimmung und Datenschutz?

Der falsche Glaube an die Selbstbestimmung

Die vorherrschenden IDM-Systeme – und dazu gehören auch diejenigen, die auf höheren Datenschutz setzen – stellen die User in den Mittelpunkt der Kommunikation, von wo aus sie oder er den Fluss beglaubigter Attribute vom Identitätsprovider zur vertrauenden Partei steuert. Man kann davon ausgehen, dass

so ein größtmöglicher Datenschutz erreicht wird, da theoretisch die User den Informationsfluss vollständig selbst bestimmen können. In vielen Fällen wird so allerdings die Privatsphäre nicht geschützt und stattdessen den Usern der falsche Glaube vermittelt, sie könnten über die Abläufe selbst bestimmen.

MS Passport deutet auf das Problem hin. Einer Bürgerin wird ein Pass ausgestellt, in dem beglaubigt wird, in welchem Verhältnis sie zu dem ausstellenden Staat steht. Bestimmte Eigenschaften werden beglaubigt und mit biometrischen Angaben verbunden. Dieser Pass oder Ausweis geht dann in den Besitz der Bürgerin über, und sie muss ihn an einer Reihe von Kontrollstellen vorlegen. Bei all diesen Abläufen steht das Subjekt im Mittelpunkt – ohne dadurch aber allzu selbstbestimmt handeln zu können. Ganz im Gegenteil kann man diese Abläufe auch so verstehen, dass den Subjekten hier zweifach Unannehmlichkeiten bereitet werden – sie müssen sich nicht nur anmelden und überwachen lassen, sie sind auch für den Identitätsapparat nichts als bloße Träger von Informationen.

Aktuell eingesetzte IDM-Systeme haben keinen so ausgeprägten Zwangscharakter, wodurch bei Usern der falsche Glaube aufkommen mag, sie könnten selbstbestimmt handeln. Über spezielle Nutzeroberflächen können User auswählen, welche Informationen sie preisgeben und wann sie einen Vorgang abbrechen wollen, weil die vertrauende Partei zu umfangreiche Informationen abfragt. Wahlmöglichkeiten auf dieser Ebene wie auch die Möglichkeit, bestimmte Onlinedienste oder -räume nicht zu nutzen, sind nicht das Gleiche wie Selbstbestimmung. Denken wir dies im Vergleich mit Personaldokumenten weiter, entspricht es der Wahlmöglichkeit, sich per Pass oder Ähnlichem auszuweisen – oder auf das Reisen zu verzichten.

In der Praxis diktiert das Machtverhältnis zwischen einer vertrauenden Partei und einem Datensubjekt, in welchem Maß Informationen von der einen oder von der anderen Seite offengelegt werden müssen. Persönlich aushandeln lässt sich dies im Alltag fast nie. Die Privatsphäre wird hierbei, so die gängige, schiefe Sichtweise, zu einer Anstrengung des Einzelnen, hinter der sich der falsche Glaube verbirgt, es gebe einen individuellen Entscheidungsspielraum.

Die Versuchungen des Treuhänders

In Kreisen des E-Governments wird IDM-Systemen trotz ihrer Nachteile der Vorzug gegeben. Das mag an der Macht der Mittler liegen, die in solchen Systemen festgeschrieben ist: Vom Identitätsprovider ausgestellte Merkmale bestimmen sämtliche Abläufe zwischen Subjekten und Diensteanbietern und das, obwohl doch die User den Kommunikationsknoten bilden. Diese Mittlerposition, die der Provider durch die von ihm ausgestellten Merkmale einnimmt, macht Überwachung im großen Stil möglich.

IDM-Systeme, die den Datenschutz hochhalten, arbeiten mit der Offenlegung ausgewählter Legitimationen, was bedeutet, dass die «Ausstellung einer Identität» und die «Nutzung einer Identität» nicht miteinander in Verbindung

gesetzt werden können. Es ist so möglich, selbst Angriffe, die mit unbegrenzter Rechenleistung arbeiten, abzuwehren. Im Gegensatz dazu, und ganz besonders innerhalb der europäischen Forschungslandschaft, wird in der Regel «vertrauenswürdigen Dritten», sollte dies notwendig erscheinen, die Befugnis eingeräumt, Abläufe zu deanonymisieren. Von den Befürwortern wird eine solche Schwächung des Datenschutzes durch Begriffe wie «Rechenschaftspflicht» und «Betrugsabwehr» verschleiert. Für Kritiker handelt es sich dabei um «Treuhandverfahren» oder schlicht um eine «systematische Überwachung».

Mechanismen für die treuhänderische Hinterlegung von Identitäten arbeiten mit weiteren dritten Parteien, die Abläufe nachvollziehen und Identitäten annullieren können. In der wissenschaftlichen Literatur wird gemeinhin davon ausgegangen, dass solche dritten Parteien Teile der Judikative oder Exekutive sind, Organe die rechtsstaatlich handeln. Herkömmlich jedoch hat die Justiz mit Verschlüsselungstechniken nichts zu tun. In der Praxis wird es sich bei diesen dritten Parteien um Geheim- oder Nachrichtendienste handeln, um Einrichtungen also, denen Regierungen im Allgemeinen den Umgang mit Chiffren und Codes übertragen.

Eine Treuhänderschaft kommt dem Prinzip, ausgewählte Legitimationen offenzulegen, in die Quere, und IDM-Systeme ohne eine solche eingebaute Überwachung sind ohne weiteres denkbar. Erforderlich wäre es dazu, sich von einigen der ergebnisoffenen Pläne für IDM-Systeme zu verabschieden, die es unmöglich machen vorherzusagen, ob anstelle einer kompletten treuhänderischen Hinterlegung auch spezifische Mechanismen, Missbräuche zu verhindern, wirksam sind. Für jeweils spezifische Sicherheitsmerkmale könnten dann angemessene und geeignete Maßnahmen gegen Missbrauch entwickelt werden, beispielsweise um Doppelbuchungen zu verhindern, um User sperren zu können, ohne deren Identität aufdecken zu müssen, und um Spam zu blockieren – ein System, mit dem sich User bewerten lassen. Für ergebnisoffene IDM-Systeme ist dergleichen nicht möglich, denn in ihnen kann man, will man jede Art von Missbrauch verfolgen können, den Datenschutz nur komplett außer Kraft setzen.

Die Dreiecksbeziehung beim Identitätsmanagement beenden

Wenn auch die Wunschvorstellung eines Allzweck-IDMs zum Schutz der Privatsphäre auf Wahlfreiheit und Selbstbestimmung setzt, könnte dieses Gefahr laufen, eben diese Werte zu pervertieren und eine gegenteilige Wirkung zu entfalten. Ein Ausweg aus der Gefahr, dass sich ein System, mit dem die Privatsphäre geschützt werden soll, in ein mächtiges, autarkes Überwachungssystem verwandelt, könnte sein, die Zahl der drei beteiligten Parteien auf zwei zu reduzieren. Möglich wäre dies, ließe man die User im Internet weiterhin ihre Identitäten und Eigenschaften selbst authentifizieren. Für bestimmte, wichtige Eigenschaften der Identitäten reicht dies vollkommen aus. Durch das OpenID-System wie auch durch die selbst ausgestellte Authentifizierung ist es beispielsweise möglich, dass

zwei ansonsten anonyme Transaktionen von derselben Person durchgeführt werden können. Die Forschung hat auch gezeigt, dass Crowdsourcing eine gute Möglichkeit ist, Authentifizierungen durchzuführen, beispielsweise indem ein engmaschiges Netzwerk die von einem Einzelnen für sich behauptete Identität bestätigt.[12]

Für das Ziel, User möglichst selbstbestimmt handeln zu lassen, ist es wahrscheinlich am besten, nicht eine Vielzahl von Providern ins Spiel zu bringen, sondern es den Usern selbst zu überlassen, über die Userdaten zu bestimmen. Dadurch wird es günstig und einfach möglich, zwischen einer Vielzahl von Diensten zu wechseln und Daten lokal zu verarbeiten. Datenschutzregeln und viele Datenschutzprogramme, die scheinbar für die User gemacht sind, sind für eine derartige, simple Architektur nur ein schwacher Ersatz. User und von Usern gesteuerte Software sollten jederzeit dazu in der Lage sein, vollständig auf Informationen, die vorgehalten werden, damit sie bestimmte Dienste nutzen können, zugreifen zu können, diese zu bearbeiten, zu kopieren und zu löschen.

Zudem müssen die technischen Grenzen der IDM-Systeme eingestanden werden. Befinden sich Daten erst einmal im Besitz einer dritten Partei, können IDM-Systeme diese nicht mehr schützen. In solchen Fällen beschränkt sich die Selbstbestimmung der User darauf zu entscheiden, welche Organisation ihre Privatsphäre verletzten darf, sei es böswillig oder durch Nachlässigkeit.

Die Vielzahl der Anbieter von Diensten und die flüchtige Art, in der wir mit vielen von ihnen zu tun haben, macht es Usern nahezu unmöglich zu überblicken, wo ihre Daten vorgehalten werden. IDM-Systeme haben hierfür keine Lösung. Da es zudem schwierig ist, vielschichtige Interaktionen zu anonymisieren, ist die in pseudonymen Profilen enthaltene Information heikel.

Zwar können IDM-Systeme dabei helfen, Authentifizierungsvorgänge nachzuvollziehen; die bei Anbietern von Diensten tatsächlich hinterlegten Nutzerdaten werden von ihnen jedoch nicht tangiert. Entsprechend sind IDM-Systeme, geht es darum, strenge Datenschutzregeln umzusetzen, nur ein Teil der Lösung.

Schließlich gehen IDM-Systeme auch nicht darauf ein, wie Menschen ihre im Fluss befindlichen Identitäten aufbauen und mit ihnen spielerisch umgehen, sei es zwischenmenschlich, sei es im Umgang mit Firmen oder Behörden. Der aktuelle, monolithische Ansatz des Identitätsmanagements stößt in dieser Hinsicht prinzipiell an seine Grenzen.

Schlussfolgerungen

Wir haben die jüngere Geschichte der Datenschutzforschung und ihrer Anwendungen nachvollzogen und einen, notwendig verkürzten, Überblick über

12 Yu et al. (2008), Danezis und Mittal (2009), Brainard et al. (2006)

wesentliche Ansätze gegeben, uns mit anonymer Kommunikation beschäftigt, mit datenarmen Prozessen, der Anonymisierung von Datenbanken und mit Systemen zum Identitätsmanagement und ihren Hintergründen. In allen Fällen haben wir festgestellt, dass breit angelegte Konzepte zum Schutz der Privatsphäre, kommt es zur technischen Umsetzung, sehr speziell und einseitig ausgelegt werden. Zwar ist es unvermeidlich, für eine praktische Umsetzung Kriterien enger zu fassen, jedoch haben wir gezeigt, dass das Übergewicht, das bestimmte Konzepte oder Annahmen dabei zum Nachteil anderer bekommen, die Möglichkeiten Einzelner oder auch großer Bevölkerungsgruppen stark beeinträchtigen und die beabsichtigten Zwecke von PETs abschwächen oder gar in ihr Gegenteil verkehren kann.

Im Besonderen haben wir gezeigt, dass bei der anonymen Übermittlung von Informationen Datenschutz verstanden wird als ein *individuelles Bedürfnis*, Spuren zu verwischen, und dass Datenschutz in Datenbanken als ein Prozess dargestellt wird, bei dem individuelle Informationen verborgen, statistische Informationen aber genutzt werden können – wodurch *eine Logik des wirtschaftlichen Nutzens alle anderen Aspekte übertrumpft*. In Systemen zum Identitätsmanagement wird Datenschutz als die technische Möglichkeit verstanden, Authentifizierungen in einer nicht zurück zu verfolgenden Weise erstellen und nutzen zu können, wodurch, im Namen des Datenschutzes, ein umstrittenes und sehr starres Modell von Identität als Form von Überwachung wiederum geltend gemacht wird. Die Folge ist, dass Dienste zur anonymen Kommunikation und zur Anonymisierung nur bestimmte Aspekte des Datenschutzes unterstützen. IDM-Systeme hingegen, die auf den Schutz der Privatsphäre setzen, sind in eine wesentlich vielschichtigere gesellschaftliche Wirklichkeit eingebettet, die die erreichten datenschützerischen Errungenschaften oft wieder in Frage stellt oder, schlimmer noch, sie möglicherweise in ein verborgenes Überwachungssystem verwandelt.

Aus dem Englischen übersetzt von Bernd Herrmann.

Literatur

Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, Mario Verdicchio: Exploiting cryptography for privacy-enhanced access control. *Journal of Computer Security*, 18(1), 2009.

John G. Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, Moti Yung: Fourth-factor authentication: somebody you know. In: Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM Conference on Computer and Communications Security*, S. 168–178. ACM, 2006.

Sebastian Clauß, Dogan Kesdogan, Tobias Kölsch, Lexi Pimenidis, Stefan Schiffner, Sandra Steinbrecher: Privacy enhanced identity management: Design considerations and open problems. In: *ACM CCS2005 Workshop on Digital Identity Management*, 2005.

George Danezis, Prateek Mittal: Sybilinfer: Detecting sybil nodes using social networks. In *NDSS*. The Internet Society, 2009.

Daniel Kifer and Johannes Gehrke: l-diversity: Privacy beyond k-anonymity. In: *IEEE 22nd International Conference on Data Engineering (ICDE'07*, 2006.
Ninghui Li and Tiancheng Li: t-closeness: Privacy beyond k-anonymity and â„“-diversity. In: *IEEE 23rd International Conference on Data Engineering (ICDE'07*, 2007.
Arvind Narayanan and Vitaly Shmatikov: Robust de-anonymization of large sparse datasets. In: *IEEE Symposium on Security and Privacy* DBL (2008), S. 111–125.
David J. Phillips: Privacy policy and PETs. *New Media and Society*, 6(6):691–706, 2004.
David Rebollo-Monedero, Jordi Forné, Josep Domingo-Ferrer: From t-closeness to pram and noise addition via information theory. In: *PSD '08: Proceedings of the UNESCO Chair in data privacy international conference on Privacy in Statistical Databases*, 2008.
Latanya Sweeney: k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5), S. 557–570, 2002.
Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky, Feng Xiao: Sybillimit: A near-optimal social network defense against sybil attacks. In *IEEE Symposium on Security and Privacy* DBL (2008), S. 3–17.
Detlev Zwick, Nikhilesh Dholakia: Whose identity is it anyway? comsumer representation in the age of database marketing. *Journal of MacroMarketing*, 2003.

SIMON EDWIN DITTRICH

Wat will ick uffm Dorf? Über die Entwicklung des öffentlichen Lebens im Global Village

Wir leben einen Traum, den Zwischenraum. Seine Eintrittsbedingungen sind digital: Smartphones sind Wurmlöcher, Tweets zwitschern wie nervöse Antennen, SMS takten das Abendbrot. Identitäten werden flüssig, und Ich ist jeden Tag ein Anderer. Alles halb so wild, wir erfinden uns nur gerade neu.

Marshall McLuhan beschrieb in seinem Buch *The Global Village*, wie die Welt durch die Vernetzungsmöglichkeiten elektronischer Kommunikationsmittel immer weiter zusammenwachse. Dieses Phänomen wird in letzter Zeit weniger diskutiert, sondern eher als gegeben angesehen. Als Berliner Pflanze stellt sich mir aber sofort die Frage: Wat soll ick uffm Dorf? Mit der Arroganz des Hauptstädters könnte ich sagen: nichts. Aber eben jene Menschen, die Flaneure, digitalen Bohemians, von denen man vermuten würde, dass sie zur Avantgarde gehören, leben besonders gerne im digitalen globalen Dorf – in den Zwischen(t)räumen, zwischen Virtualität und physischer Realität, auch als «meatspace» bekannt. Es ist schön Dorf, wenn alle Freunde nur einen Klick weit entfernt sind, aber manchmal eben auch ein bisschen langweilig.

Dem lässt sich natürlich entgegenhalten, dass die Empfehlungen, die meine Lieblingsblogger/Freunde und Follower aussprechen, wesentlich diverser sind als eine kleine Dorfgemeinschaft. Anders als die verbesserungswürdigen Empfehlungsalgorithmen von Amazon führen sie nicht notwendigerweise zu «more of the same». Eine gewisse Oberflächlichkeit ist einigen sozialen Medien aber nicht abzusprechen. Ich halte es da mit Nick Hornby:

It's about what you like, not what you are like

Dessen Romancharakter Rob Gordon in *High Fidelity* sagt, kurz nach einem One-Night-Stand, es gehe nicht darum, wer man ist, sondern was man mag. Sicher, die Vorlieben und Interessen sind ein sehr wesentlicher Bestandteil der Persönlichkeit eines Menschen, aber bei weitem nicht alles. Sie verändern sich unter Umständen, z.B. durch einen Jobwechsel, wesentlich schneller als Charaktermerkmale, die für wirkliche Intimität, für starke Bindungen notwendig sind.

Genau an diesem Punkt zeigen sich meiner Meinung nach auch die Grenzen digitaler Intimität. Die Oberflächlichkeit der Beziehungen, die durch soziale Medien zustande kommen – ich spreche hier zunächst explizit nicht von denen, die durch soziale Medien erhalten werden –, ist für sich genommen kein Problem. Die Vorteile der sogenannten schwachen Bindungen überwiegen sicherlich (siehe hierzu auch den Beitrag von Clive Thompson in diesem Band).

Die Kultur des «sharing», also des Teilens von Inhalten, insbesondere von Vorlieben und persönlichen Aktivitäten, birgt unglaubliche Potenziale, über physische Distanzen hinweg Kontakte zu knüpfen, zu erhalten und darüber Zugang zu Kreisen zu erlangen, die vor wenigen Jahren noch wesentlich stärker voneinander abgegrenzt waren. Die Attraktivität solcher Bindungen ist natürlich hoch, nicht zuletzt aufgrund der Distanz, die diesen Bindungen durch das Medium inhärent ist. Ob es sich um die Mitglieder eines Taubenzüchterforums oder einer World-of-Warcraft-Gilde handelt, ist dabei eher nicht von Belang. Diesen Communities ist eine gewisse Unverbindlichkeit zu eigen, man teilt gewisse Interessen und hat dabei Spaß, genau wie bei der Verführung, die einem One-Night-Stand in der Regel voraus geht. Wirklich langanhaltende Bindungen resultieren daraus aber eher selten. Die Anzahl der Bindungen aber nimmt zu.

Was bedeutet dies nun für unser globales Dorf? Nun, mit dem Maße, in dem sich die sozialen Praxen in die Zwischen(t)räume des Cyberspace begeben, verändert sich eben auch der gesellschaftliche Raum, in dem wir uns täglich bewegen. Der Raum ist hier nicht nur figurativ gemeint, sondern auch dezidiert physisch. Der Zugang zum digitalen Dorf, den Zwischen(t)räumen ist nur durch einschneidende Veränderungen der Menschen hin zum Cyborg möglich.

I will check my phone at dinner and you will be okay with it

Es gibt einen Tedtalk von Amber Case (@caseorganic), in dem sie erklärt, dass wir alle Cyborgs sind, da wir unsere körperlichen Fähigkeiten durch Technologie erhöhen. Es geht ihr dabei in erster Linie nicht um Prothesen, sondern um Kommunikationstechnologie, Mobiltelefone, Computer und dergleichen. Sie bezeichnet Smartphones als «technosoziale Wurmlöcher», da diese einem erlauben, mit anderen Menschen zu interagieren, unter Umgehung von zeitlichen und räumlichen Restriktionen, auch mit Hilfe unserer zweiten Ichs: dem digitalen Ich, das sich in sozialen Netzwerken, Mailboxen und Webseiten befindet. Diese Geräte erlauben es den Menschen, sich von ihrer Umgebung zu entfernen, ohne sich zu bewegen. Diese Beobachtung erscheint als solche zunächst trivial, ist aber von großer Tragweite, wenn man sie auf die Veränderungen in den sozialen Räumen hochrechnet.

Gesellschaftliche Räume, Gesellschaften und ihre Kulturen bestehen zu einem großen Teil aus Normen und Regeln. Im Allgemeinen lässt sich sagen, dass diese Regeln und Normen sich in den Handlungen der Menschen niederschlagen und umgekehrt. Das bedeutet: In dem Maße, in dem sich die Kommunikationstechnologien verändern und deren Nutzung zunimmt, sich also unsere

Kommunikationshandlungen verändern, werden sich die Normen und Regeln unserer (Dorf-)Gesellschaft ebenso verändern.

Ein deutlicher Indikator für eine solche Art der Veränderung ist die Zunahme schriftlicher, asynchroner Kommunikation. Ein Beispiel ist das Schreiben von SMS beim Essen oder auch nur in Gegenwart von anderen Personen. Als ich Kind war, wäre es undenkbar gewesen, vom Abendbrottisch aufzustehen, um ans Telefon zu gehen. Wenn ich heute mit Freunden gemeinsam esse, kommt es öfters vor, dass mehrere von uns in ihr Telefon schauen, Emails checken, SMS schreiben, Twittern oder auf Facebook schreiben. Natürlich hagelt es auch immer wieder Kritik von Menschen, die es als unhöflich empfinden, wenn man ihnen nicht seine volle Aufmerksamkeit widmet. Aber die Vehemenz nimmt ab.

Eine völlig andere Dimension ergibt sich in Veranstaltungen, in denen eine Person zu mehreren spricht und diese wiederum nonverbal elektronisch untereinander kommunizieren. Während einer Veranstaltung zu twittern ist nicht das Gleiche, wie sich in einer Vorlesung zu unterhalten, denn die Vortragende könnte durchaus auf Tweets eingehen. Es bildet sich ein öffentlicher Zwischenraum.

Der Aufenthalt in diesen Zwischenräumen hat Konsequenzen für die Kommunikationshandlungen in stärker physischen sozialen Räumen. Die zunehmende Laptop-Dichte der letzten Jahre und die damit verbundene Abnahme von Gesprächen zwischen Reisenden, die sich in ihrem jeweils eigenen Zwischen(t) raum befinden, ist ein gutes Beispiel dafür. Das kann man als Segen empfinden oder auch nicht. Bemerkenswert ist es allemal.

Mit der Verlagerung in diese Zwischenräume geht auch eine Veränderung des Selbst einher. Natürlich ist die digitale Persona nur eine Performance, aber das gilt auch für den Rest unseres Ichs. Mit dem Kollabieren der Begrenzung des sozialen Raumes auf zeitliche und örtliche Lokalitäten sehen wir uns aber auch mit völlig neuen Problemen der Aufführung konfrontiert. Die Zuschauer sind nicht definiert, auch der Zeitpunkt der Aufführung ist amorph. Ein Beispiel für die (scheinbare) Aufhebung dieser Definitionen und damit der Grenzen zwischen beruflichem und privatem Selbst ist das Bewerbungsgespräch, in welchem die Bewerberin mit unvorteilhaften Partyfotos konfrontiert wird.

Rollenkonflikte wie diese sind wahrlich per se nichts Neues, aber die Intensität, mit der das Private in den öffentlichen Raum eindringt, ist von einer neuen Qualität. Nehmen wir das Beispiel eines streitenden Paares im Bus. Befinden sie sich im selben Bus, ist beiden die Öffentlichkeit ihrer Handlungen bewusst und der Streit wird sich dementsprechend entwickeln. Findet der Streit am Telefon statt, ergibt sich eine andere Situation. Der Partner im Bus befindet sich in einem Zwischenraum, weder vollständig privater noch öffentlicher Natur. Für die anderen Menschen im Bus verändert sich die Situation in Richtung Privates.

Vom Leben auf dem Dorfe

Insgesamt verlagert sich unser Leben immer mehr in Zwischenräume und wird dadurch häufig auch privater. Natürlich muss man einschränkend sagen, dass

der «digital divide» eine große Rolle spielt. Menschen aus den niedrigeren sozio-ökonomischen Schichten verfügen oft nicht über das notwendige Geld und die Kompetenz, um Zugang zu den Zwischenräumen zu erlangen. Auch Senioren sieht man eher selten mit einem Laptop in der U-Bahn sitzen.

Bei den Unterdreißigjährigen nutzen aber weit über 95% das Internet, und die Mobilfunkprovider sind mit einem rasanten Anstieg der mobilen Datennutzung konfrontiert. In vielen Unternehmen ist die private Nutzung des Internets in gewissem Grade gestattet. In den meisten Dienstleistungsberufen ist es aber z.B. undenkbar, nebenbei zu twittern. Ich hoffe jedenfalls, dass die Busfahrer sich da zurückhalten. Aber für einen signifikanten Teil der Bevölkerung sind die (öffentlichen) Zwischenräume ein fester Bestandteil des (Arbeits-)Alltags.

Das hat dazu geführt, dass sich zumindest in Deutschland einiges an politischem Diskurs in das Internet verlagert hat – der Regierungssprecher twittert, wie oft und gerne kolportiert wird. Dies bietet große Potenziale, auch wenn wir, z.B. aufgrund des «digital divide», noch weit davon entfernt sind, diese auszuschöpfen (siehe dazu auch den Beitrag von Ralf Bendrath und Stefanie Sifft in diesem Band). Das Mobilisierungspotenzial, was die digitalen Kommunikationstechnologien bieten, lässt sich demokratisch nutzen, kann aber auch sehr gut als Überwachungsinstrument für staatliche Institutionen dienen.

Momentan scheint mir dieser politische Zwischenraum und das digitale öffentliche Leben noch hauptsächlich von den üblichen Verdächtigen bevölkert zu sein. Von Bildungsbürgern, Aktivisten, Bohemians, Selbstdarstellern, Politikern und Journalisten, aber eben wenig von alleinerziehenden Müttern, die halbtags eine gering qualifizierte Tätigkeit ausüben. Für die Demonstranten auf den Tahrir-Plätzen dieser Welt gilt ähnliches. Es ist eben nicht die sozio-ökonomisch unterste Schicht, die dort die Mehrheit stellt. Die Bewohner des globalen Dorfes sind sich also zumindest sozio-ökonomisch ähnlicher als die Weltbevölkerung insgesamt. Für die nationalstaatlichen Zwischenräume gilt dies noch viel mehr.

Niemals geht man so ganz

Paradoxerweise sind die öffentlichen Zwischenräume eher privat, denn Siezen unter «Freunden» ist genauso unüblich wie Forenblume2000 zu siezen. Die Höflichkeitsformen des traditionellen Schriftverkehrs sind ja auch «viel zu umständlich», um in der Masse an täglicher digitaler Kommunikation eingehalten zu werden. Aber dort, wo wir Intimität zulassen, kann es auch richtig weh tun, so sehr, dass wir weg müssen, einfach mal raus und uns neu erfinden.

Sich Neu-Erfinden ist ein wesentlicher Bestandteil des Menschen. Man kann ganz postmodern von einer «liquid identity» sprechen oder aber den Menschen als eine Selbstverwirklichungsmaschine begreifen, wie dies der Psychologe Carl Rogers tut. Fakt ist, dass sich der Mensch als soziales Tier stark über seine Beziehungen zu anderen definiert. Wenn Selbstkonzept und erlebte Realität, z.B. in einer Partnerschaft, nicht mehr kongruent sind, dann kommt es zu Problemen.

Der Ausweg ist einfach – eines von beiden muss geändert werden. Ein Weg ist das Suchen eines neuen Umfelds, das einen Menschen sehr verändern kann oder einfach nur vorher unterdrückte Veränderungen zulässt.

Mit den Spuren, die wir in den öffentlichen Zwischen(t)räumen zurücklassen, wird es aber schwieriger, ein Umfeld komplett zu verändern. Jedenfalls ist es nicht so «einfach» wie aus Klein-Gummersbach nach Hamburg zu ziehen, denn unsere Online-Profile bleiben unverändert. Der Autor David Weinberger sagt deshalb, ein Zeitalter der Transparenz müsse ein Zeitalter des Vergebens sein. Ich bin mir relativ sicher, dass er Recht hat; ob es dazu kommen wird, bleibt hingegen zweifelhaft. Doch genau wie Teenager lernen müssen, auf dem sozialen Parkett zu bestehen, müssen wir als Gesellschaft insgesamt über neue Regeln und Normen nachdenken und diskutieren.

Wir können uns alle frei entscheiden, ob wir im «meatspace» verbleiben oder in die digitale Nähe schweifen. Man sollte sich aber darüber im Klaren sein, dass sich Persönlichkeiten, die Aufführungen des Ichs, immer im Miteinander entwickeln. Sicher, es gibt Monologe, aber die gegenseitige Typisierung ist die Norm, und in Einpersonenstücken nimmt der Darsteller meist mehrere Rollen ein. Aufgrund der Vielseitigkeit der Bewohner der Zwischen(t)räume, des digitalen globalen Dorfes bin ich zuversichtlich, dass wir uns nicht in der beengten Intimität des kleinbürgerlich dörflichen Milieus wiederfinden werden. Ohne heftige Diskussionen, gesellschaftliches Engagement und den ein oder anderen Generationenkonflikt wird es sicher nicht gehen. Die Frage, wann es okay ist, (k)eine Freundschaftsanfrage zu stellen, oder diese nicht zu beantworten, ist da sicherlich eines der trivialeren Probleme, zeigt aber schon die Vielschichtigkeit sozialer Bindungen und deren Abbildung.

«Warum haben wir eigentlich so viel Angst?»

Ein Gespräch über Pseudonymität zwischen Markus Beckedahl und John F. Nebel

Wollen wir den Menschen die Freiheit nehmen, die sie jetzt durch Anonymität und Pseudonymität haben? Die Auflösung der Pseudonymität bedeutet ganz klar eine Einschränkung der Meinungsfreiheit und einen kulturellen Verlust, meint John F. Nebel. Wir brauchen deshalb Werkzeuge, die unsere Privatsphäre schützen, sagt Markus Beckedahl.

John F. Nebel: Markus, was bedeuten für Dich Anonymität und was Pseudonymität?
Markus Beckedahl: Anomymität bedeutet für mich, dass ich auf die Straße gehen kann, dass ich in einen Laden gehen kann, mit Bargeld bezahlen kann und dass nirgendwo gespeichert wird, wo ich gerade lang gelaufen bin und was ich gekauft habe. Und insofern bedeutet Anonymität für mich Privatsphäre und nicht das Gefühl zu haben, überwacht zu werden. Pseudonymität hingegen bedeutet für mich, dass ich mich mit einem gewissen Schleier bedecke, aber trotzdem identifiziert werden kann. Da gibt es eine Restwahrscheinlichkeit, dass meine Anonymität aufgehoben werden kann.

Bei Pseudonymität kann ich Identitäten aufbauen, wobei ich bei Anonymität hingegen gar nicht in Erscheinung treten will. Bei Pseudonymität gebe ich mir einen Namen und die anderen im Forum wissen: «Ah, da kommt Forenblume1976» – oder wie auch immer ich heiße. Die Leute dort kennen mich gegebenenfalls nur unter diesem Pseudonym. Ich muss also nicht hinzuschreiben, dass ich Monika Schulze heiße, und habe trotzdem eine Identität und soziale Beziehungen.
Ja genau, du kannst dir eine Identität schaffen. Wenn man sich jedoch aktuelle Forschungen von Soziologen anschaut, dann stellt man fest, dass Menschen, die in sozialen Medien aktiv sind, immer mehr von ihrer normalen Persönlichkeit verraten und viel mehr sie selbst sind, als eine bestimmte Rolle oder Identität anzunehmen.

Führt das aber nicht dazu, dass wir zu Identitäten werden, die mit angezogener Handbremse immer schauen, ob sie ihre echte Identität beschmutzen könnten?

Führt das nicht dazu, dass wir zu vorsichtig kommunizieren und bestimmte Aspekte des Lebens virtuell gar nicht mehr ausleben können, wenn man nicht unter Pseudonym unterwegs ist?
Das werden wir noch herausfinden.

Es ist schon mein Eindruck, dass ich ganz anders vorgehe und mich vorsichtiger verhalte, vielleicht mich nicht mehr traue, das zu sagen, was ich sagen will, wenn ich mit meinem echten Namen dastehe.
Das kann man nicht verallgemeinern. Einem großen Teil der Bevölkerung ist das egal. Sie kommunizieren, wie sie wollen. Sie haben vielleicht kein Gespür dafür, was es bedeutet, etwas in einer digitalen Öffentlichkeit zu kommunizieren. Diese Leute merken nicht, dass ihre Kommunikation für immer im Netz steht und vielleicht auf ihre Person zurückfällt. Dasselbe sieht man beim Verhalten in sozialen Netzwerken. Da denkt man auch, man kommuniziert mit seinen Freunden und kriegt gar nicht mit, wie viele Leute darauf theoretisch zugreifen können – und das dann tatsächlich auch machen. Diese unbedarften Nutzer gibt es. Und es gibt diejenigen, die medienkompetent sind und wissen, dass sie mit verschiedenen Rollen spielen können und sie darauf aufpassen müssen, was sie von sich preisgeben.

Es wird ja von verschiedener Seite gefordert, dass Klarnamen die Regel werden. Das macht doch eine freie Kommunikation und einen Informationsaustausch unmöglich. Ein Beispiel: Du arbeitetest bei einem Unternehmen, das schlechte Bedingungen für Arbeitnehmer hat. Bei einem Frageportal stellst du dein konkretes Problem mit deinem Arbeitgeber rein – und am nächsten Tag hast du die Abmahnung auf dem Tisch. Noch sind wir nicht so weit, aber der Weg dorthin wird gerade geebnet.
Theoretisch sind wir heute schon da. Interessant ist auch, wenn von Politikern Klarnamenpflicht für das Internet gefordert wird. Meistens frage ich mich: Was meinen die damit? Fordern sie tatsächlich, dass man im Netz auf den absurdesten Seiten seinen Klarnamen kommunizieren muss? Auch wenn ich der einzige Deutsche unter Südamerikanern auf einer brasilianischen Webseite bin? Oder bedeutet es, dass diese Politiker wollen, dass in politischen Debatten, in die sie selbst involviert sind, mit Klarnamen und offenem Visier kommuniziert werden soll, weil sie es nur so gewöhnt sind? Vermutlich denken sie, es sei vergleichbar mit einer Diskussionsrunde im Wahlkreis, wo man die Person sehen kann, die einen gerade hart angeht.

Aber wo führt diese Debatte hin?
Problematischer wird es, wenn irgendwann ein verbindlicher Ausweis für das Internet durchgesetzt wird. So etwas ist schon Realität in Italien. Wer als Tourist in ein Internetcafé geht, wird das kennenlernen: Man kommt in Italien nicht ins Internet, ohne sich individuell mit seinem Personalausweis zu registrieren.

Das ist doch die Folge von dem, was wir jetzt erleben. Das kann klein anfangen mit der Klarnamen-Kommunikation mit dem Bezirks- oder Finanzamt. Der nächste Schritt ist doch, dass man vor dem Ins-Netz-gehen seinen Personalausweis durch ein Lesegerät ziehen muss. Dann ist Kommunikation weder pseudonym noch anonym möglich. Werden sich dann noch Menschen z.B. in Sexforen über ihre Vorlieben austauschen? So etwas wird doch nicht mehr möglich sein.

Wir müssen gar nicht über Sexforen reden, auch wenn das natürlich eine häufige Nutzungsform ist. Nehmen wir das Beispiel Krankheit. Durch das Internet hat man erstmalig die Möglichkeit, sich anonym und unabhängig von Ort und Zeit mit vielen anderen Leuten auszutauschen. Man muss nicht in die Selbsthilfegruppe oder das Beratungsgespräch im Krankenhaus gehen, was viele verunsichert und eine gewisse physische Barriere darstellt, sondern man kann sich mit vielen Gleichgesinnten und Betroffenen austauschen, was die Genesung oder das Krankheitsbild angeht. Wer möchte über seine AIDS-Krankheit mit offenem Namen im Netz kommunizieren, wenn noch nicht mal der Freundeskreis darüber Bescheid weiß? Wollen wir den Menschen die Freiheit nehmen, die sie jetzt durch Anonymität und Pseudonymität haben, besser mit ihrer Krankheit umzugehen?

Ich möchte das nochmal runterbrechen: Wenn ich ein Blog betreibe und das mit meinem echten Namen mache, kann ich viel leichter Ärger aller Art bekommen. Die Auflösung der Pseudonymität bedeutet ganz klar eine Einschränkung der Meinungsfreiheit.

Das kann man ja sehr schön in den arabischen Ländern sehen. Dort gibt es viele, die unter Realnamen bloggen, aber gerade diese Menschen sind in Gefängnissen gelandet, weil sie mit ihrem Namen zu ihrer Meinung gestanden haben. Viele andere haben bewusst Pseudonyme gewählt, um offener ihre Meinung sagen zu können. Und sie sind weniger oft von den Folterknechten abgeholt worden. Ohne die Pseudonyme in der Vergangenheit hätte es niemals eine so vitale für Demokratie werbende Blogosphäre gegeben, die so eine kritische Masse gebildet hätte. Letztlich hat die Pseudonymität zur Revolution beigetragen.

Du hättest ohne Pseudonymität wahrscheinlich ein paar Trolle weniger auf Netzpolitik, oder?

Das wäre super. Aber andererseits weiß ich gar nicht, ob ich weniger hätte. Vielleicht würde ich sie dann nur das erste Mal richtig sehen.

Das kann natürlich auch sein, dass mit der Zeit auch mit Klarnamen eine hässliche Diskussionskultur entsteht und die Leute wieder zu Trollen werden, wenn sie an den Effekt der Klarnamen gewöhnt sind.

Viele Medienhäuser hoffen jetzt auf Facebook. In den letzten zehn Jahren haben die Nachrichtenseiten von bild.de bis welt.de mit Nutzerkommentaren experimentiert. Das ist in der Regel tierisch in die Hose gegangen und hat viel Geld gekostet. Die Medienunternehmen und Verlage hoffen jetzt, dass die Menschen

zivilisierter miteinander kommunizieren, wenn sie Facebook und seine Klarnamen einbauen. Ich bin davon nicht überzeugt. Vielleicht befinden wir uns in einem Übergangsstadium: Momentan sind die Leute noch vorsichtiger, aber demnächst blenden es vielleicht viele aus, dass sie unter ihrem Realnamen kommunizieren, und werden weiter rumtrollen, beleidigen, Diskussionen zerstören und zurück in ihren Trollstatus fallen…

Lass uns auch mal über die Nachteile von Pseudonymität reden. Zum Beispiel werden kritische Artikel in Blogs von den kritisierten Firmen oder deren PR-Agenturen kommentiert – unter falschem Namen. Es gab das Beispiel Stuttgart 21, wo diese Vorwürfe gegenüber den Tiefbahnhof-Befürwortern erhoben wurden. Hier wurde ab einem gewissen Zeitpunkt der Eindruck erweckt, es gäbe eine Graswurzelbewegung für das Bahnhofsprojekt. Da wird simuliert, dass es eine bestimmte Meinung gäbe, indem ich eine Horde von Pseudonymen und Identitäten für oder gegen etwas anlaufen lasse. Dieses so genannte Astroturfing ist sicherlich ein Problem der Pseudonymität.

Das ist in der Tat ein zweischneidiges Schwert. Zum einen finde ich es gut, wenn ich in Blogs und Foren kommentieren kann, ohne gleich meinen vollen Namen nennen zu müssen, weil ich eben mit meiner Meinung nicht immer bei Google aufgefunden werden möchte. Andererseits sehe ich bei netzpolitik.org, dass ich manche Kommentare nicht wirklich einschätzen kann. Meistens merkt man, dass sie so geschrieben sind, dass die Kommentierenden einer Lobbygruppe angehören könnten oder die Diskussion in eine bestimmte Richtung gelenkt werden soll. Oft gibt es da gute Anhaltspunkte wie die verwendete Sprache und Argumentationsmuster – aber man hat keinen Namen, sondern ein Pseudonym wie zum Beispiel «Sunny». Man weiß also nicht, wer schreibt jetzt da mit welcher Motivation.

Also doch Pseudonymität abschaffen?

Nein, ich finde es besser, dass wir die Möglichkeit zur Pseudonymität haben und jeder selbst entscheiden kann, wie er oder sie auftreten möchte. Das Problem liegt woanders: Warum haben wir eigentlich Angst, so viel über uns zu verraten? Hier kommen wir zum Post-Privacy-Ansatz. Die Befürworter von Post-Privacy (in diesem Band vertreten durch Michael Seemann) argumentieren, dass die Gesellschaft eben einfach respektieren sollte, dass Menschen verschieden sind, dass die Menschen Fehler machen, dass die Menschen Lernprozesse durchlaufen – und dann hätten wir irgendwann eine viel entspanntere Gesellschaft. Ich selbst bin nicht überzeugt davon, dass unsere Gesellschaft diesen Reifungsprozess durchmacht. Man stelle sich nur mal vor, die Bild-Zeitung würde Leuten hinterher recherchieren, was diese mal freimütig vor 20 Jahren ins Netz gestellt haben…

Aber was bestimmt diese Angst, zu viel von sich preiszugeben? Ist es die Angst, dass die Gesellschaft falsch mit meinen Informationen umgeht? Oder dass

jemand die Informationen falsch interpretiert? Oder die Gefahr, dass ich zu einem bestimmten Zeitpunkt schräg drauf war und schräge Kommentare ins Netz schreibe? Oder betrunken bin und sonderbare Sachen mache? Wenn wir immer mit Klarnamen auftreten würden, müssten wir ja unglaublich aufpassen, dem eigenen Selbstbild und dem gesellschaftlichen Bild, das daraus entsteht, keinen Schaden zuzufügen.
Dafür argumentiere ich deswegen auch nicht.

Schon klar. Ich glaube einfach nicht, dass eine Gesellschaft abstrahieren kann zwischen dem Schulabgänger, der auf einem Foto den kiffenden Gangster-Rapper spielt, und dem Bewerber, der sich auf einen Ausbildungsplatz bewirbt. Solange eine Gesellschaft Hierarchien hat und so verfasst ist wie jetzt, wird das nicht funktionieren.
Andererseits haben wir ein großes Problem aus einer anderen Richtung kommend: Was ist, wenn Bildidentifizierung und Gesichtserkennung auf einmal richtig gut funktionieren? Was ist mit den zig Milliarden Bildern, die geschossen und ins Netz gestellt werden? Wenn das wirklich marktreif ist, dann gebe ich ein: Zeig mir John F. Nebel! Und wo ist er noch überall zu sehen? Dann habe ich auf einmal ganz viele Eindrücke einer Person. Ein massiver Verlust von Anonymität.

Das ist noch einmal eine ganz andere Schiene, wo mir vermutlich auch ein Pseudonym nicht weiterhilft. Und das können wir natürlich noch weiterspinnen. Ich nehme aus deinem Blog drei Texte und erkenne maschinell anhand des Stils alle Texte, die du jemals ins Netz gestellt hast. Egal, ob Du unter Pseudonym geschrieben hast. Und egal, wo Du geschrieben hast.
Die Software gibt's auch schon.

Genau, das gibt es schon. Es sieht also nicht gut aus um die Pseudonymität. Das ist sehr schade. Ich finde es verdammt spannend, dass man sich im Netz verstellen und als jemand anderes auftreten kann. Ich habe mal ein Massively Multiplayer Role Game (MMOPRG) gespielt. Ich war erst als Mann angemeldet, dann als Frau – und auf einmal waren die Leute um einen herum, die meisten von ihnen junge Männer, nicht mehr so böse mir gegenüber eingestellt. Fand ich interessant, wie heteronormativ so etwas sein kann, die armen schwachen Frauen müssen ja beschützt werden und so. Das Spiel mit den Rollen und genau solche Erfahrungen gehen doch verloren. Uns steht da doch ein kultureller Verlust bevor, eben nicht mehr mit Identitäten spielen und sich selbst ausprobieren zu können.
Ja, das wird zu einem Verlust führen. Die eine Denkrichtung sagt: Das ist einfach so. Wir müssen technischen Fortschritt akzeptieren. Die andere Denkrichtung sagt: Wir sollten versuchen, die Technik zu kontrollieren und zu gestalten. Ob das noch klappen wird, ist die große Frage. Wird es uns gelingen, Privacy Enhancing Tools zu schaffen, damit die Privatsphäre erhalten bleibt, oder überlassen wir alles dem technischen Fortschritt und nehmen diesen Verlust einfach so hin?

Was sind diese Privacy Enhancing Tools genau?

Das sind Anonymisierungswerkzeuge, Verschlüsselungswerkzeuge und eben auch Einstellungen in den Social Networks, die standardmäßig auf «Alles verbergen» geschaltet sind. So dass du bewusst erst einmal alles freischalten musst – statt umgekehrt. In solche Technologien müssen wir weiter investieren, das muss der Marktstandard werden. Dabei kommt Deutschland eine internationale Vorreiterrolle zu. Und es ist vorstellbar, dass wir, ähnlich wie grüne Produkte, bald datenschutzfreundliche Produkte in alle Welt exportieren.

MALTE SPITZ

Demokratie braucht das Internet, aber mehr als 140 Zeichen

Teilhabe an politischer Öffentlichkeit ist nicht gleichbedeutend mit einem Netzzugang. Aber nur, wenn der ungehinderte Datenfluss politisch garantiert wird, haben Bürger die Chance, ihre Freiheitsrechte wahrzunehmen. Ein Plädoyer gegen Zensur- und Sperrtechnik.

Wir alle erinnern uns an die euphorischen Kommentare, Debatten und demokratischen Versprechen, die mit der gesamtgesellschaftlichen Verbreitung des Internets zum Ende der 1990er aufkamen. Endlich sei das Medium gefunden worden, dass nicht nur informiert, sondern auch demokratische Teilhabe ermöglicht. Hoch lebe die Partizipation!

Anfang 2011 konnte man den Eindruck gewinnen, dass sich diese Versprechen tatsächlich bewahrheiten würden. Zwar nicht direkt bei uns, aber in anderen Regionen unserer Welt, in Tunesien, in Ägypten und anderswo. Die Bedeutung des Internets als zentraler Kommunikationskanal für einen freien und gleichberechtigten Austausch von Informationen, kurzum das demokratische Potenzial des Netzes, konnte so nicht besser vor Augen geführt werden. Hochgerüstete Diktaturen fürchten sich vor Twitter-Nachrichten und YouTube-Videos und begreifen eine Facebook-Fan-Page offenbar als Gefahr für ihr Regime. Dies zeigt, dass das Internet als das Freiheitsmedium unserer Zeit eine zentrale Hilfe für Veränderungen in unserer Welt ist.

Ähnlich wie der Buchdruck historisch betrachtet die wesentliche Grundlage für die Durchschlagskraft der 95 Thesen eines Martin Luthers war, so sind die Möglichkeiten eines freien Internets heute Bestandteil jedes demokratischen Aufbruchs unserer Zeit. Dafür müssen aber bestimmte Aspekte gewährleistet sein: Menschen und Institutionen, die die Freiheit des Internets verteidigen, sowie die Netzneutralität und die Sicherstellung der Teilhabe am Internet.

Freies Internet als Voraussetzung

Der Wegfall des «Gate-Keepers» und die Aufhebung der einmal idealtypischen Trennung von Nachricht und Kommentar durch das Internet, wie sie noch durch die Redaktionen der klassischen Medien gewährleistet werden sollte, wird von einigen in der Debatte als Risiko für eine unbeeinflusste oder wenigstens trans-

parente Meinungsbildung gesehen. Und auch wenn man soweit nicht gehen will – eine Herausforderung ist dieser ungeregelte Zugang zur «Öffentlichkeit» für den demokratischen Diskurs allemal. Die These aber, dass das Internet unserer Demokratie schadet, wird lediglich von einer kleinen und vernachlässigbaren Minderheit vertreten.

Das soll natürlich nicht darüber hinweg täuschen, dass durch das Netz neue Herausforderungen, wie die oben genannten, entstehen. Und natürlich verändert sich nicht nur der demokratische Diskurs; auch die Propagandaapparate der Diktaturen bleiben nicht auf dem Stand des 20. Jahrhunderts stehen. Gezielte Desinformation und subtile Werbung findet genauso wie in den «alten Medien» auch auf den Plattformen des Mitmach-Internets statt. Die meinungsgetriebene Nutzung von Twitter und Co. lässt gerne einmal Tatsachen in einem anderen Lichte erscheinen. Ist dies aber eine ernst zu nehmende Gefahr, oder überwiegen die Vorteile der neuen Öffentlichkeit? Besteht deshalb ein Bedarf zur Kontrolle oder gar Zensur?

Meinungsäußerungen jeglicher Art zu kontrollieren, um die Minderheit der interessensgesteuerten oder schlichtweg unsinnigen Beiträge herauszufiltern, wäre fatal.

Vielmehr muss die freie und vielfältige Meinungsäußerung im Internet als Chance gesehen werden, mehr Informationen und auf diesem Weg auch ein vollständigeres Bild der Wirklichkeit zu erhalten. Damit diese «wahrheitsstiftende» Funktion des Internets aber zum Tragen kommen kann, muss es ein freies Internet geben. Zensierte Webseiteninhalte, gefilterte E-Mails und die Blockade von offenen Internetplattformen verhindern dieses Potenzial einer neuen Öffentlichkeit. Sie sind das weitaus größere Risiko für unsere Demokratie.

Freiheit verteidigen

Um die freiheitlichen Potenziale des Internets zu verteidigen, muss ehrlich und offen mit den Herausforderungen des Internets umgegangen werden. Ein Rahmen der Internet Governance muss etabliert werden, am besten weltweit, aber mindestens europäisch. Die bisherigen multinationalen Institutionen wie ICANN oder ITU verfehlen ihre Rolle, wenn sie Chancen predigen, sich aber nicht trauen, für diese auch ihre Stimme zu erheben. Ähnliches zeigt der Umgang der Vereinten Nationen mit dem Internet Governance Forum (IGF). Als Multi-Stakeholder-Idee entwickelt, spielt gerade wieder eine reine politische Interessenpolitik die führende Rolle bei dessen Weiterentwicklung.

Beim Umgang mit den Herausforderungen der Digitalisierung bedarf es aber vor allem Verhältnismäßigkeit und eines gesunden Menschenverstandes. Rechtsdurchsetzung wird im digitalen Zeitalter nicht einfacher. Mit einer Überwachungsmaschinerie aus Vorratsdatenspeicherung, heimlicher Online-Durchsuchung und Internetsperren darauf zu reagieren, widerspricht aber genau dem Prinzip der Verhältnismäßigkeit und des gesundes Menschenverstandes.

Demokratie mit der überbordenden Gängelung der individuellen Freiheitsrechte verteidigen zu wollen, ist hoch gefährlich. Jede «Demokratie» der Welt macht sich damit zum schlechten «Vorbild» für andere und erzeugt innere Widersprüche.

Anstatt nach Kontrolle und Zensur zu rufen, die im Kern immer antidemokratisch sind, müssen neue Lösungsansätze gefunden werden. Wie kann man Rechtsdurchsetzung ermöglichen, ohne demokratische Prinzipien zu verletzen? Gleichzeitig darf die Antwort nicht vornehmlich die weitere Kommerzialisierung des Internets sein, wo einige wenige sehr viel entscheiden, kontrollieren und letztendlich den freiheitlichen Charme des Internets nehmen. Statt immer weiter zu kriminalisieren, sollte darüber nachgedacht werden, ob nicht auch die rechtlichen Grundsätze in der digitalen Zeit weiterentwickelt werden sollten. Ein aktuelles Beispiel ist das Urheberrecht[1]. Mit den Möglichkeiten des Web 2.0, so schreibt die Internet-Enquetekommission in einem Arbeitspapier, entsteht im Kontext der «semi-privaten Öffentlichkeitsräume eine vielfache Rechtsverletzung». Etablierte Verbände, die eigentlich für Meinungs- und Pressefreiheit kämpfen, sind im Kampf gegen Filesharer schnell diejenigen, denen andere Grundrechte zweitrangig vorkommen. Kollateralschäden, wie die Vorratsdatenspeicherung, sind ihnen dabei scheinbar egal.

Doch die Freiheit des Internets darf nicht nur in wohlfeilen Appellen hochgehalten, sie muss immer wieder vor Ort verteidigt werden. Der Anfang kann auch in Deutschland gemacht werden. Der Aufbau einer riesigen Sperrinfrastruktur (wie in der Debatte um die Sperrung von Missbrauchsdarstellungen von Kindern gefordert), die politische Zensur erleichtern würde, liegt zum Glück aktuell auf Eis. Trotzdem wird die notwendige Technik hierfür weiter vorangetrieben.

Die großen Anbieter für Zensur- und Sperrtechnik stammen hauptsächlich aus westlichen Demokratien und finden auch dort ihren Einsatz im «Kampf gegen» das ein oder andere Übel. Westliche Staaten sind damit Wegbereiter für die massenhafte Zensur durch die Despoten unserer Zeit und ermuntern sie so zum weiteren Hochrüsten ihrer Kontroll- und Zensurtechnik. Ein erster, aber umso wichtigerer Schritt wäre es, die Ausfuhr entsprechender Technik stärker zu kontrollieren und einen Code of Conduct für den Handel mit dieser Technik zu etablieren.

Netzneutralität sichern

Das Prinzip der Netzneutralität, also die diskriminierungsfreie Durchleitung von Datenpaketen unabhängig von dessen Inhalt, ist in Gefahr. Das Grundprinzip des Internets steht unter Beschuss von Unternehmen. Große Internetanbieter, aber auch das ein oder andere Medienunternehmen, würden gerne zunehmend die privilegierte Durchleitung von Daten einführen. Statt Qualität, Sicherheit

1 Vgl. dazu umfassend: *Copy. Right. Now! Plädoyers für ein zukunftstaugliches Urheberrecht.* Reihe Bildung + Kultur, Bd. 4. Hg. von der Heinrich-Böll-Stiftung, Berlin 2010.

und Kreativität diktiert dann das Geld, welche Angebote im Internet nutzbar sind und welche nicht. Bedeutsamer als in kommerziellen Zusammenhängen ist aber die Netzneutralität für unsere Demokratie. Das Grundprinzip der fairen Gleichbehandlung von Datenpaketen ist elementar, um Demokratie sicherzustellen. Denn wenn Inhalte kontrolliert und die Datenpakete in einzelne Klassen aufgeteilt werden, ist der Schritt hin zur vollständigen Vorkontrolle des Internets nur noch sehr klein.

Hier spielen dann unternehmerische Interessen, wie bspw. der bereits genannte Schutz vor Urheberrechtsverletzungen, häufig genauso eine Rolle wie die Überwachungs- und Kontrollphantasien einzelner Staaten. Netzneutralität ist nicht nur ein technisches Prinzip, sondern Grundlage des freien Datenflusses, also Grundvoraussetzung für eine demokratische und freiheitliche Öffentlichkeit.

Sollte jetzt von diesem Prinzip abgerückt werden, wird ein Zurück zur Netzneutralität in einigen Jahren wohl unmöglich. Die Entscheidung, wie sich das Internet in den kommenden Jahren und Jahrzehnten entwickeln wird, ist auf das engste mit der Frage der Netzneutralität verknüpft. Deshalb ist der Einsatz für die Netzneutralität so entscheidend. Die Zeit, in der das Internet als temporäres Phänomen gesehen wurde, ist endgültig vorbei. Es gilt nun, nicht jene Fehler zu wiederholen, die mediengeschichtlich hinreichend bekannt sind. Wenn die demokratische Kontrolle über eine neue Medientechnik aufgegeben wurde und singulären Interessen, sei es von Staaten oder Unternehmen, zum Opfer fiel, war das nicht von Vorteil für den demokratischen Diskurs. Der Kampf für Netzneutralität ist daher der Kampf nicht nur für ein demokratisches Internet, sondern für unsere Demokratie an sich.

Teilhabe am Internet sicherstellen

Es gehört zum Wesen des demokratischen Diskurses, dass alle an ihm teilhaben können. In der Debatte um die demokratische Rolle des Internets wird oftmals unhinterfragt davon ausgegangen, dass ein Zugang besteht oder leicht erhältlich ist. Für die Staaten Europas mag dies der Fall sein, für große Teile Asiens und Afrikas aber noch nicht, der «digital divide» teilt die Nord und die Südhalbkugel. Selbst wenn die Länder der südlichen Hemisphäre das Zeitalter der Breitbandverkabelung überspringen und gleich in das mobile Internetzeitalter einsteigen, so bleiben dort noch technische Beschränkungen. Erst nach und nach werden die Kapazitäten erweitert und die Stabilität der Netze gefestigt. Zudem muss hier ein Wettbewerb der Anbieter erfolgen. Staatliche Monopole erleichtern die Kontrolle und ermöglichen, von zentraler Stelle aus den Zugang zu beschränken und somit auch einzelnen Personen oder Gruppen den Zugang zu erschweren.

Die Unterstützung beim Ausbau des Internets weltweit ist für einen echten, vielstimmigen demokratischen Diskurs deshalb wichtig – mit offenen Strukturen für die Teilhabe aller. Dies beginnt bspw. beim Ausbau der Satellitentechnik, die

schwerer kontrollierbar ist, und kann bei der Verpflichtung zur Offenheit des Internets bei der Förderung des Netzausbaus enden.

Weder Twitter noch Facebook initiieren den politischen Aufbruch

Die Freiheit des Netzes, die Verteidigung desselben, die Wahrung von Netzneutralität und Zugangsgerechtigkeit sind Grundlage dafür, dass die demokratischen Potenziale des Internets nutzbar gemacht oder noch weiter entfaltet werden können.

Was möglich ist, zeigen die Entwicklungen in Nordafrika Anfang des Jahres 2011. Es wäre vermessen, von einer Facebook- oder Twitter-Revolution zu sprechen. Diese privatwirtschaftlichen Angebote haben die Proteste unterstützt und zum besseren und vor allem schnelleren Informationsfluss beigetragen. Seltener erwähnt, aber eventuell sogar bedeutsamer, ist die Verbreitung von Mobiltelefonen in diesem Prozess.

Twitter oder Facebook waren aber nicht Initiatoren des Protests. Sie waren Öltropfen im Feuer der Revolution und haben die revolutionäre Umwälzung in Schwung gehalten.

Diese Leistung ist nicht gering zu schätzen. Mittels der Plattformen wurde den Protestierenden gezeigt, dass der Widerstand ungebrochen ist und sie nicht allein da stehen – beides wichtige Faktoren bei einem demokratischen Aufbruch. Doch es sind nicht einzelne Anbieter, die wichtig für die Demokratie sind, wie der schnelle Wandel in der Internetlandschaft zeigt. Bestimmte Angebote, die vor zehn Jahren noch für demokratische Teilhabe standen, existieren heute nicht mehr und genauso wird man auch in zehn Jahren auf das Jahr 2011 zurückblicken. Es geht vielmehr um die strukturellen Möglichkeiten des Mediums Internet: Kommunikation in Echtzeit, Wechselseitigkeit der Kommunikation, niedrige Eintrittsbarrieren etc. Die Einfachheit und Schnelligkeit des Internets sind Grundpfeiler für Demokratie und Protest.

Das sieht man im Kleinen bei Demonstrationen vor Ort, wo der Informationsfluss über kleine Infoticker-Seiten oder Twitter läuft. Das aktuellste Beispiel hierfür sind die Protestaktionen zu Stuttgart 21, wo das Internet gerade zu Beginn des Protests die Gegenöffentlichkeit zu den etablierten Medien darstellte. Oder bei demokratischen Umbrüchen ganzer Staaten wie in Nordafrika, wo Informationen über das Internet fließen und gleichzeitig der ganzen Welt zugänglich gemacht werden können. Denn trotz aller Zensur und Kontrolle ist das Internet heutzutage in Teilen unserer Welt für Menschen, die in undemokratischen Staaten leben, die einzige Möglichkeit überhaupt, frei zu kommunizieren.

Demokratie benötigt mehr als 140 Zeichen

Das große Wort Demokratie passt locker in eine kleine Twitter-Nachricht von 140 Zeichen. Damit der Begriff aber zur gelebten Wirklichkeit wird, braucht es Menschen. Menschen, die nach den Spielregeln des demokratischen Diskurses

argumentativ ringen und um die beste Lösung für ein Problem streiten. Auch der demokratische Aufbruch in der arabischen Welt zu Beginn des Jahres 2011 hätte keinen Despoten aus seinem Regierungssitz vertrieben, wenn der Wille zum Umsturz sich nicht durch die Blockade von Plätzen jenseits des Internets manifestiert hätte. Dennoch hat die Verbreitung des Internets die demokratische Bewegung unterstützt. Wir müssen als Demokraten daher die Fähigkeit des Internets schützen und seine Freiheit verteidigen. Bits und Bytes sind zwar nicht die hinreichende Bedingung für Demokratie; die aktuellen Entwicklungen zeigen aber, dass sie notwendig sind für gelebte Demokratie im 21. Jahrhundert.

RALF BENDRATH UND STEFANIE SIFFT

Öffentlichkeit 2.0 und Demokratie

Eine Spurensuche

Ist das Internet (k)eine Demokratiemaschine? Ist Technikdeterminismus die Antwort? Welche Art von Demokratie im Netz wollen wir? Fragen, Überlegungen und acht Feststellungen zur Bedeutung des Web 2.0 für Demokratie und Öffentlichkeit.

Nicht erst seit den aktuellen Revolutionen in der arabischen Welt wird über das Internet als Demokratieverstärker diskutiert. Während es in Tunesien, Ägypten und anderswo um das Netz als Instrument zur dezentralen Selbstorganisation der Bevölkerung geht sowie um die Möglichkeit, mit der globalen Öffentlichkeit zu kommunizieren, hat der Fall Wikileaks grundlegende Diskussionen über die Bedeutung der Transparenz für die internationale Politik angestoßen. Der Streit um die Einführung von Adhocracy in der Enquete-Kommission «Internet und digitale Gesellschaft» des Bundestages verweist auf die Möglichkeiten direktdemokratischer Beteiligung, und die «Zensursula»-Kampagne hat die Hoffnungen auf netzgestützte Kampagnen und e-Petitionen verstärkt.

Wird Politik also dank Facebook und Twitter demokratischer? Ist das Internet eine Demokratisierungsmaschine: Man muss Politik nur reinstecken und hinten kommt Demokratie raus? Und was ist dran an dem Credo der Bloggergemeinde, dass Politik durch das Mitmachnetz offener wird für mehr Bürgerbeteiligung und die Anliegen der «kleinen» User und Leute? Wie viel davon ist wirklich dem Internet und seiner neuen Partizipationsarchitektur geschuldet und wie viel klassischen Partizipationsformen wie Demonstrationen oder Petitionen, die es auch schon vor dem Internet gab?

Wir wollen mit diesem Beitrag ein wenig Klarheit in die Debatte bringen.[1] Wir konzentrieren uns dabei auf die Auswirkungen von Internetöffentlichkeiten auf etablierte Demokratien. Die Entwicklungen in der arabischen Welt sind zwar aufregend, aber dort geht es noch darum, überhaupt erst die Voraussetzungen

1 Ein Überblick über die Debatte findet sich auch hier: Ralf Bendrath: «Demokratiemaschine Internet? Das Netz als Projektionsraum politischer Utopien – und was daraus wurde», FIfF-Kommunikation, 24. Jg (2007), Nr. 3., S. 30-33, http://fiff.de/publikationen/fiff-kommunikation/fk-3-2007/fiff-ko-3-2007-bendrath.

für eine demokratische Nutzung des Netzes herzustellen. Das ist eine andere Geschichte. Unser Beitrag konzentriert sich auf die Demokratie-2.0-Debatte, wie sie in Deutschland und anderswo in der westlichen Welt geführt wird. Wir werden vor allem auf die zugrunde liegenden Annahmen und Begrifflichkeiten der Debatte eingehen. Konkrete Beispiele behandeln wir nur kursorisch und setzen voraus, dass sie weitgehend bekannt sind.[2]

Hoffnungen, Skepsis, Ängste – und ein verschwiegener Technikdeterminismus

Mit dem Internet wurden von Anfang an große Hoffnungen auf eine Revitalisierung der Demokratie verbunden. Das Argument der Euphoriker: Früher haben wir über Fernsehen und Zeitungen nur beobachtet, wie andere Politik machen. Heute sind wir aktive Bürger und «citizen journalists», die ihre Anliegen und Meinungen selbst veröffentlichen. «The blog has given the press to us.»[3] Früher war Öffentlichkeit dominiert durch die Mächtigen aus Politik und Wirtschaft, der Rest durfte zuhören. Heute haben wir mit dem Internet einen Raum für die freien und unvermachteten Diskurse der Zivilgesellschaft, in der jeder das Megaphon selbst in die Hand nehmen kann. Euphoriker glauben im Großen und Ganzen also an die Demokratisierungsmaschine, an den großen Transformator Internet, mit der ihr Traum von einer offenen, lebendigen und unvermachteten Demokratie endlich wahr wird.

Durch das Internet, so behaupten dagegen die Skeptiker, verändert sich gar nichts. Statt eigenen Content zu produzieren, käuen Blogger nur wieder, was sie bei Spiegel Online gelesen haben. Sie betreiben Medienkritik und Medienschelte, schwingen sich auf zu den Wächtern der alten Massenmedien und ihrer Online-Ableger – und bleiben doch nur auf sie reduziert. Auch für Politiker und Parteien ist es immer noch wichtiger, in der Tagesschau vorzukommen als bei Spiegel Online. So werden die vermachteten Strukturen der alten massenmedialen Öffentlichkeit nicht aufgebrochen, sondern im Mitmachnetz nur reproduziert. Das Internet ist so gesehen nichts weiter als ein «demokratischer Mythos»[4] und eine große Reproduktionsmaschine.

Die Pessimisten gehen noch einen Schritt weiter. Sie befürchten, dass das Web 2.0 Demokratie regelrecht verschlechtert. Die vermeintliche Demokratisierungs-Maschine entpuppt sich aus ihrer Sicht als Demokratieverhunzungsmaschine. Im Internet trieben sich vor allem Dilettanten herum. Es verkommt dadurch «zu

2 Ausführlicher diskutiert haben wir konkrete Fälle in einem Vortrag auf dem Politcamp09. Die Folien dazu finden sich unter: http://www.netzpolitik.org/wp-upload/bendrath-sifft_politik-2-0-und-demokratie_2009.pdf.

3 Jay Rosen: The People Formerly Known as the Audience, 2006, http://journalism.nyu.edu/pubzone/weblogs/pressthink/2006/06/27/ppl_frmr.html.

4 Robin Meyer-Lucht: Ex-Wahlkämpfer Machnig: Internet bleibt zweitrangig, Tagesschau sticht Spiegel Online, 2009, http://carta.info/9042/matthias-machnig-wahlkampf-internet-obama.

einem Debattierclub von Anonymen, Ahnungslosen und Denunzianten»[5]. Im Übrigen verzerrt das Netz auch den ur-demokratischen Anspruch, dass politisch alle gleich sind. Es übersetzt die digitale Spaltung der Gesellschaft in eine politische und sorgt dafür, dass die ohnehin Privilegierten nur noch mehr Einfluss bekommen, während die anderen vollends abgehängt werden.

Die verschwiegene Prämisse hinter allen drei Positionen ist ein recht kruder Technikdeterminismus. Egal ob man das Internet als Demokratisierungsmaschine preist, als Reproduktionsmaschine abtut oder als Demokratieverhunzungsmaschine verteufelt – in der Regel wird unterstellt, dass das Internet *als Internet* eine spezifische Wirkung hat. Dass man also vorne Politik reinsteckt, und hinten kommt gleichsam automatisch mehr oder weniger Demokratie raus.

Die Debatte kommt genau daher nicht von der Stelle. Alle reden immer nur darüber, welche Möglichkeiten das Internet bietet, aber kaum darüber, wie diese Möglichkeiten tatsächlich genutzt werden. Die Debatte geht auch deshalb nicht voran, weil wir nicht nur nach den Folgen für «die Demokratie» fragen müssen, sondern auch und vor allem danach, welche der verschiedenen Formen und Aspekte von Demokratie mit dem realen Netz verwirklicht werden. Die Unterscheidung zwischen «virtueller» und «realer» Welt hilft genauso wenig weiter. Es geht nicht mehr darum, ob im Internet neue Formen politischer Öffentlichkeit und Partizipation entstehen. Sondern darum, wie das Mitmachnetz im Mix mit den weiterhin bestehenden älteren Medien und Beteiligungsformen genutzt wird.

Welche Art von Demokratie im Netz?

Um etwas mehr Klarheit zu finden, muss man die verschiedenen Verständnisse von «Demokratie» auseinander halten. Vielen der Internet-Euphoriker schwirrt eine deliberative Diskurs-Demokratie à la Jürgen Habermas im Kopf herum, wenn es um Demokratie und Netzöffentlichkeiten geht. Andere, wie viele in der Piratenpartei, propagieren unter dem Stichwort «liquid democracy» auch Formen direkter Volksdemokratie. Es gibt aber auch andere Vorstellungen von Demokratie, die zwar weniger anspruchsvoll sind, aber darum noch lange nicht undemokratisch. Viele glauben in der liberalen Tradition der Demokratietheorie, dass das Internet vor allem mehr Transparenz bringt, aber nicht unbedingt einen herrschaftsfreien Diskurs. Und es könnte ja sein, dass sich mit dem Internet eher solche Formen von Demokratie «light» verwirklichen als die «Halbfett»-Variante von Habermas oder gar die «vollfette» Direktdemokratie. Wir behandeln im Folgenden den liberalen und den deliberativen Ansatz. Direktdemokratische Vorstellungen wie «liquid democracy» lassen wir beiseite, weil sie bis auf wenige Versuche in der Piratenpartei und anderswo noch nicht wirklich genutzt werden.

5 Bernd Graff: Web 0.0, *Süddeutsche Zeitung*, 8.12.2008

Dreh- und Angelpunkt für Demokratie aus liberaler Perspektive ist die Auswahl der politischen Repräsentanten in freien, gleichen, geheimen und regelmäßigen Wahlen. Demokratie ist also die gute, alte repräsentative Demokratie: Bürger/innen wählen, und Politiker/innen treffen für sie die politischen Entscheidungen. Öffentlichkeit spielt dabei eine wichtige Rolle als *Bildschirm* des politischen Geschehens. Über sie können wir das Tun und Treiben der Politiker *beobachten* und so überhaupt herausfinden, wen wir wählen wollen. So «light» ist das liberale Modell aber gar nicht, wie Wikileaks drastisch vorgemacht hat. Politiker müssen sich in der Öffentlichkeit nämlich auch kritischen Nachfragen stellen und sich für ihr Tun und Lassen rechtfertigen. Wenn uns das nicht passt, können wir sie spätestens bei der nächsten Wahl zur Verantwortung ziehen.

Netz-Öffentlichkeiten kommen dem liberalen Modell der Demokratie nahe, wenn sie zwei Kriterien erfüllen:

- Transparenz: Netz-Öffentlichkeit macht das politische Geschehen transparent und versorgt uns mit Informationen darüber.
- Rechenschaft: Netzöffentlichkeit sorgt dafür, dass Politiker nicht einfach vor sich hinwurschteln können, sondern dass sie sich öffentlich rechtfertigen müssen und für ihr Handeln zur Verantwortung gezogen werden.

Deliberative Demokratie ist weniger ein Gegenmodell als eine reichhaltigere Form von Demokratie. Dreh- und Angelpunkt ist die öffentliche Meinungsbildung in einer aktiven Bürgergesellschaft. Das heißt, wir beobachten die Politik nicht nur und stellen ab und an mal eine kritische Nachfrage, sondern erheben uns vom Zuschauer-Sofa und bringen unsere Anliegen aktiv in den öffentlichen Diskurs ein. Öffentlichkeit ist hier eine *Diskursarena*, in der man mitreden kann. Am Ende entscheiden zwar nach wie vor die gewählten Politiker – aber eben auf der Grundlage einer breiten öffentlichen Meinungsbildung, in der die Stärken und Schwächen der unterschiedlichen Positionen deutlich werden oder sich vielleicht sogar eine Mehrheitsmeinung herausschält. Öffentlichkeit ist auch ein Kommunikationsnetzwerk, in dem Themen, Beiträge und Meinungen, die alle betreffen, zirkulieren und von allen diskutiert werden. Dadurch sorgt sie auch für politische und gesellschaftliche Integration, indem nämlich die verschiedenen Teilöffentlichkeiten im Netz und anderswo keine Diskurs-Inseln und «echo chambers» bleiben, sondern sich miteinander vernetzen und austauschen.

Netz-Öffentlichkeit entspricht also dem deliberativen Diskursmodell der Demokratie, wenn sie neben Transparenz und Rechenschaft auch die drei weiteren Kriterien erfüllt:

- Partizipation: Netz-Öffentlichkeit sorgt dafür, dass nicht nur Lobbyisten Gehör finden, sondern auch diejenigen, die keine politische Macht oder schlagkräftige Organisation hinter sich haben.
- Diskursive Meinungsbildung: Netz-Öffentlichkeit hilft, politische Entscheidungen vorzustrukturieren, indem die Diskussionen darüber dialogisch mit guten Argumenten geführt werden.

- Integration: Netz-Öffentlichkeit schafft politische und gesellschaftliche Integration, indem die verschiedenen Teilöffentlichkeiten keine Diskursinseln bleiben, sondern sich miteinander vernetzen und austauschen.

Reality-Check: Was bedeutet das Web 2.0 für Demokratie und Öffentlichkeit?

Wie also steht es um die Demokratie im *realen* Web 2.0? Und wie viel liberale oder deliberative Öffentlichkeit steckt wirklich darin? Wir haben unsere Ergebnisse in acht Punkten zusammengefasst:

1. Das Internet ist weder eine Demokratisierungs- noch eine Demokratieverhunzungsmaschine, sondern eine Ermöglichungsstruktur. Ob es zu mehr oder weniger Demokratie führt, hängt davon ab, wie die Möglichkeiten des Mitmachnetzes tatsächlich genutzt werden.
2. Es gibt nicht «die Demokratie» im Netz, sondern verschiedene Formen und Aspekte von Demokratie. Ob Politik im Netz zu mehr oder weniger Demokratie führt, hängt auch davon ab, was man unter Demokratie versteht.
3. Parteien und Politiker nutzen zwar die Tools des Web 2.0, aber nicht deren Demokratisierungspotenziale. Sie kommunizieren heute recht effektiv via Blogs, Twitter und Facebook, aber sie nutzen diese Plattformen noch kaum als Rückkanal.
4. Auch politische Diskussionen in der Blogosphäre tragen nur begrenzt zu einer Revitalisierung der Demokratie bei. Denn man bleibt in Kleinbloggersdorf meist unter sich. Man steht sozusagen in kleinen Grüppchen herum und redet *unter*einander, aber kaum *mit*einander. So entstehen segmentierte und oft hoch spezialisierte Teilöffentlichkeiten unter Gleichgesinnten, die vom allgemeinen politischen Diskurs meist abgekoppelt bleiben. Sogar das inzwischen leider abgeschaltete Rivva hat vor allem technikaffine Blogs aggregiert, während z.B. die extrem gut informierten EU-Blogger, die eine sehr notwendige Öffentlichkeit für das neue Staatsgebilde Europa herstellen, außen vor blieben.
5. Die «Zensursula»-Debatte hat die Segmentierung und das Unter-sich-Bleiben der Kleinbloggersdorfer erst dadurch aufgeweicht, dass mit der Online-Petition eine klassische Partizipationsform eingesetzt wurde. Auch der Protest gegen die Vorratsdatenspeicherung wurde erst dann breiter wahrgenommen, als wegen der Massenklage in Karlsruhe und der Großdemonstrationen auch die klassischen Massenmedien berichteten. Diese Verbindung von neuen und alten Partizipationsformen könnte generell einen Weg aus der immer noch weitgehenden politischen Bedeutungslosigkeit von Netz-Öffentlichkeiten weisen.
6. Politik im Netz trägt trotz aller Partizipationsmöglichkeiten eher zur politischen Elitenbildung als zur Egalisierung bei. Die digitale Spaltung und die über soziale Schichten unterschiedlich verteilten Medienkompetenzen

übersetzen sich in eine politische Spaltung der Gesellschaft. Auch deshalb ist es wichtig, dass es Politik auch offline gibt.

7. Insgesamt erfüllen sich die Hoffnungen auf das Internet als Demokratisierungsmaschine bislang nur begrenzt. Das reale Netz stärkt zwar die liberale Demokratie im Sinne von Transparenz und öffentlicher Kontrolle der Politik. Die erhoffte Frischzellenkur für die deliberative Demokratie ist bisher aber ausgeblieben.
8. Das alles ist gemessen an der relativ kurzen Zeit, die das Internet als Medium für die Massen existiert, aber schon ganz schön viel. Wer mehr erwartet hat, ist entweder einem simplen Technikdeterminismus aufgesessen oder hat gezielt unrealistische Hoffnungen geschürt. Politische Institutionen verändern sich als Folge von *politischen* Prozessen und Auseinandersetzungen, nicht aufgrund der Einführung einer neuen Technik. Die Technik kann solche Prozesse nur anstoßen. Gewonnen werden sie in der politischen Auseinandersetzung.

DIE AUTORINNEN UND AUTOREN

Markus Beckedahl bloggt seit 2002 auf netzpolitik.org über Politik in der digitalen Gesellschaft. Er ist Mitgründer der Newthinking Communications GmbH, sitzt als Sachverständiger in der Enquete-Kommission „Internet und digitale Gesellschaft" des Deutschen Bundestages und ist Mitglied des Medienrates der Medienanstalt Berlin-Brandenburg sowie persönliches Mitglied der deutschen UNESCO-Kommission.

Ralf Bendrath ist seit 2009 wissenschaftlicher Mitarbeiter des grünen Europaabgeordneten Jan Philipp Albrecht. Vorher hat er in Berlin, Bremen und Delft zu Sicherheitspolitik und Datenschutz im Internet und zu demokratischen Beteiligungsformen beim Weltgipfel Informationsgesellschaft geforscht. Er ist Autor bei netzpolitik.org und engagiert sich u.a. im Arbeitskreis Vorratsdatenspeicherung sowie bei European Digital Rights (EDRi.org). Wenn er Zeit findet, bloggt er auf bendrath.blogspot.com.

M. Ryan Calo ist seit 2008 Direktor des Verbraucherdatenschutzprojekts am Center for Internet & Society der Stanford Law School. Davor war er Teilhaber bei Covington & Burling, wo er Firmen zu Datensicherheit, Datenschutz und Telekommunikation beraten hat. Sein Forschungsinteresse liegt an den Berührungspunkten von Recht und Technologie. Er bloggt auf cyberlaw.stanford.edu/blog/ryan-calo. Twitter: @rcalo

George Danezis forscht für Microsoft Research in Cambridge. Seine Forschungsinteressen liegen in den Bereichen Computersicherheit und Privacy, insbesondere auf den Feldern anonyme Kommunikation, Verkehrsanalyse, statistische Interferenz und P2P-Sicherheit. Von 2005 bis 2007 war George Danezis als Visiting Fellow an der Katholischen Universität Leuven. Er bloggt auf conspicuouschatter.wordpress.com.

Simon Edwin Dittrich studierte nach dem Abbruch seines Informatikstudiums Soziologie und verdiente nebenbei mit dem Internet und Computern Geld. Er beschäftigt sich mit unterschiedlichen Aspekten der Digitalisierung und weigert sich, deren Chancen ungenutzt verstreichen zu lassen. Er lebt und arbeitet in Berlin. Twitter: @SiEdDi

Jan Engelmann ist Kulturreferent und Koordinator des Programms Öffentlichkeit und Demokratie in der Heinrich-Böll-Stiftung. Herausgeber u.a. von „Die

kleinen Unterschiede. Der Cultural-Studies-Reader“ (1999), „Botschaften der Macht. Der Foucault-Reader zu Diskurs und Medien“ (1999) und „Leidenschaft der Vernunft. Die öffentliche Intellektuelle Susan Sontag“ (2010). Er blockt viel Spam am Tag.

Seda Gürses ist seit März 2009 Post-Doc in der Forschungsgruppe COSIC/ESAT für Computersicherheit und Industrielle Kryptographie an der Katholischen Universität Leuven. Sie beschäftigt sich mit Privatsphäre in Sozialen Netzwerken, Requirements Engineering, Privacy Enhancing Technologies und Identitätsmanagement-Systemen. In ihrer Arbeit nutzt sie Theorien aus den Surveillance Studies, um zu verstehen, wie Überwachung unser Verständnis von Privatheit beeinflusst und welche Konzepte für die Konstruktion informationsverarbeitender Systeme nützlich sind.

Nils Leopold ist Mitarbeiter im Büro von MdB Konstantin von Notz (Bündnis 90/Die Grünen). Er war zuletzt als Referatsleiter am Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) sowie als Bundesgeschäftsführer (2003-2004) der Humanistischen Union tätig.

John F. Nebel begann seine journalistische Tätigkeit bei einem mittlerweile eingestellten Stadtmagazin als Nachtlebenkolumnist. Beim Berliner Blog www.metronaut.de schreibt er mit acht weiteren Autorinnen und Autoren über Themen wie Grundrechte, Freiheit, Überwachung, Netzpolitik, Kommunikationsguerilla, Werbung und Public Relations.

Helen Nissenbaum ist Professorin für Media, Culture and Communication und Informatik an der New York University. Sie befasst sich mit sozialen, ethischen und politischen Folgen von Informationstechnologien und digitalen Medien. Sie hat vier Bücher veröffentlicht, eines davon ist *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, das 2010 bei Stanford University Press erschienen ist.

Konstantin von Notz ist innenpolitischer Sprecher und Sprecher für Netzpolitik der Fraktion Bündnis 90/Die Grünen. Er ist zugleich Obmann der Enquete-Kommission „Internet und digitale Gesellschaft“, Mitglied im Innenausschuss sowie stellvertretendes Mitglied im Rechtsausschuss und im Unterausschuss Neue Medien. Außerdem vertritt er die Grünen in der IuK-Kommission des Bundestages. Twitter: @KonstantinNotz

Danah Boyd leitet eine Forschungsgruppe bei Microsoft Research und ist wissenschaftliche Mitarbeiterin am Berkman Center for Internet and Society der Universität Harvard. In ihrer Forschung untersucht Boyd Alltagspraxen in den Social Media, insbesondere unter Jugendlichen. In letzter Zeit hat sie sich verstärkt mit

den Themen Privacy, Öffentlichkeit und Sichtbarkeit beschäftigt. Sie bloggt auf www.zephoria.org/thoughts/. Twitter: @Zephoria

David Pachali verfügt über langjährige Erfahrungen im Bereich Online-Redaktion und -Konzeptentwicklung (Max-Planck-Institut für Wissenschaftsgeschichte, Carta, iRights.info, reset.to) sowie als Dozent. Journalistische Veröffentlichungen zu Kultur und Politik digitaler Medien. Er bloggt auf http://david.pachali.net.

Jan Schallaböck ist Jurist und war Stipendiat der Heinrich-Böll-Stiftung. Seit 2006 Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein (ULD), dort tätig in nationalen und europäischen Forschungsprojekten zur Entwicklung von Datenschutztechnologien. In diesem Rahmen ist er auch zuständig für internationale Standardisierungsaufgaben, unter anderem als stellvertretender Vorsitzender der Arbeitsgruppe zu Identitätsmanagement und Datenschutztechnologien der Internationalen Standardisierungsorganisation, ISO.

Francesca Schmidt studierte Germanistik, germanistische Linguistik sowie Gesellschaft, Geschichte und Politik Südasiens. Während ihres Studiums beschäftigte sie sich vorrangig mit der Gender- und Frauenforschung in der Literatur. Derzeit ist sie Mitarbeiterin im Gunda-Werner-Institut für Feminismus und Geschlechterdemokratie und verantwortet die Koordination der Website. Privat beschäftigt sie sich mit queeren Aushandlungsprozessen im Internet und bloggt auf www.queer-o-mat.de. Twitter: @QueerOmat

Michael Seemann wurde in Wolfsburg geboren und lebt heute in verschiedenen Wordpressblogs und Podcasts im Internet. Er studierte Kulturwissenschaften und arbeitete als Programmierer. Heute schreibt er über sein Lieblingsthema, den Kontrollverlust, Beiträge für verschiedene Medien. Seine Webseiten sind mspr0.de und ctrl-verlust.net. Twitter: @mspro

Stefanie Sifft ist seit 2010 wissenschaftliche Mitarbeiterin des grünen Europaabgeordneten Gerald Häfner. Vorher hat sie in Bremen zur Europäischen Union und zum Wandel der europäischen Öffentlichkeit geforscht und u.a. politische Kommunikation und Politikmanagement gelehrt. Wenn sie Zeit findet, bloggt sie auf european-polis.blogspot.com.

Daniel J. Solove ist Inhaber des John-Marshall-Harlan-Lehrstuhls an der Fakultät für Rechtswissenschaften der George Washington University. Er ist einer der weltweit führenden Experten für Gesetze zum Schutz der Persönlichkeitsrechte und hat zahlreiche Bücher zu diesem Thema veröffentlicht, u.a. *Nothing to Hide: The False Tradeoff Between Privacy and Security* und *The Future of Reputation: Gossip and Rumor in the Information Age*. Er bloggt auf www.concurringopinions.com. Twitter: @DanielSolove

Malte Spitz ist seit 2006 Mitglied im Bundesvorstand von Bündnis 90/Die Grünen, wo er für Bürgerrechte, eine zukunftsfähige Netzpolitik und moderne Medienpolitik kämpft. Er ist Mitglied im Chaos Computer Club und im Netzwerk Neue Medien. Malte Spitz hat Volkswirtschaftslehre in Berlin studiert und studiert aktuell Politikwissenschaften an der FernUni Hagen. Er bloggt auf www.maltespitz.de. Twitter: @maltespitz

Clive Thompson ist Journalist und bloggt auf www.collisiondetection.net. Er schreibt eine Kolumne für Wired und verfasst regelmäßig Beiträge für das *New York Times Magazine*. Hauptsächlich beschäftigt er sich mit dem Einfluss von Technologie auf Kultur und Gesellschaft. Twitter: @pomeranian99

Krystian Woznicki arbeitete 1995 bis 1998 in Tokio als Korrespondent der *Spex* und Kurator zahlreicher Projekte. Seit 1999 in Berlin primär als Kulturtheoretiker und Medienproduzent tätig. Zu seinen kollaborativen Medienprojekten zählen ein digitales Archiv der Globalisierung (2001-2006), Reader im Zeitschriftenformat (2002-2004) und die Berliner Gazette (berlinergazette.de), in deren Rahmen er seit 1999 zahlreiche Symposien sowie Seminare organisiert und drei Anthologien herausgegeben hat: McDeutsch (2007), Vernetzt (2009) und Modell Autodidakt (2010).

Copy.Right.Now!

Eigentumsfragen sind Machtfragen. Nirgends werden diese Fragen lauter und provozierender gestellt als im Internet: Durch die Digitalisierung geistiger Werke und den schnellen Austausch von Daten und Informationen werden starre Verfügungsrechte aufgelöst. Die Utopie einer globalen und freien Wissensgesellschaft scheint durch eine offene Netzkultur möglich. Auf jeden Fall notwendig ist die Entwicklung innovativer, netztauglicher Marktmodelle – wollen nicht ganze Kulturindustrien aus Musik, Journalismus und Literatur den Anschluss an die kommenden Generationen verlieren. Auch die Urheber geistiger Werke stehen vor neuen Herausforderungen: Wird das Urheberrecht zu einem Nutzerrecht? Oder können die neuen Freiheiten auch neue Macht geben?

Seit rund zehn Jahren beschäftigt sich die Heinrich-Böll-Stiftung mit den Themen Wissensgesellschaft, Open Source, den Fragen der Rechte in Zeiten des Internet. Dieser Sammelband vereinigt Beiträge namhafter Autorinnen und Autoren zur aktuellen Debatte um die Zukunft unserer Kultur.

Mit Beiträgen u.a. von Lawrence Lessig, Tim Renner, Jonathan Lethem, Jeanette Hofmann, Robin Meyer-Lucht, Helga Trüpel und Monika Ermert.

Schriften zu Bildung und Kultur, Band 4:
Copy.Right.Now!
Plädoyers für ein zukunftstaugliches Urheberrecht
Herausgegeben von der Heinrich-Böll-Stiftung
In Zusammenarbeit mit iRights.info
Berlin, April 2010, 140 Seiten
ISBN 978-3-86928-031-8

Bestelladresse: Heinrich-Böll-Stiftung, Schumannstr. 8, 10117 Berlin, Tel. 030-285340, Fax: 030-28534109, E-mail: info@boell.de Internet: www.boell.de

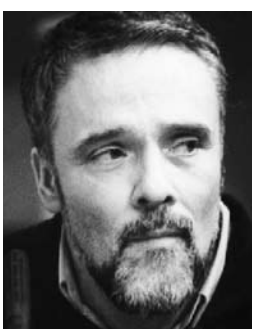
HEINRICH BÖLL STIFTUNG
FREUNDINNEN + FREUNDE

Die Freundinnen und Freunde der Heinrich-Böll-Stiftung unterstützen die Werte und Ziele der Stiftung. Sie fühlen sich der politischen und moralischen Haltung Heinrich Bölls verbunden. Menschenrechte, Kunst und Kultur liegen den Freundinnen und Freunden der Heinrich-Böll-Stiftung am Herzen. Mit ihren Mitgliedsbeiträgen fördern sie unbürokratisch und schnell Menschenrechtsaktivisten, Künstler und Kunstprojekte.

Angebote an die Freundinnen und Freunde:

- exklusive Informationen über die Stiftungsarbeit
- spezielles Veranstaltungsangebot
- politische Begegnungsreisen zu den Auslandsbüros
- Vernetzung im grünen Umfeld
- persönliche Einladungen zu besonderen Veranstaltungen wie der Petra-Kelly-Preisverleihung oder dem Sommerfest des Heinrich-Böll-Hauses in Langenbroich
- Verlinkung unserer Homepage mit ihrer Website

Wir laden Sie ein, Mitglied zu werden und damit Teil unserer grünen Ideenwerkstatt und unseres internationalen Netzwerkes – ob als Privatperson, als Institution oder als Unternehmen. Als Freund oder Freundin tragen Sie dazu bei, Qualität und Selbstständigkeit der Heinrich-Böll-Stiftung langfristig zu sichern.



«Die Heinrich-Böll-Stiftung ist ein Stück autonomer und engagierter politischer Kultur in Deutschland – sie verdient Ihre Unterstützung.»
György Dalos, ungarischer Autor in Berlin

Machen Sie mit!

Heinrich-Böll-Stiftung
Schumannstraße 8, 10117 Berlin
T 030 28534-112 **F** -119 **E** info@boell.de

Informieren Sie sich über unser Programm unter: www.boell.de/freundeskreis

Immer mehr Menschen äußern sich im Internet nicht nur zu politischen Fragen, sondern auch zu ihrem Konsumverhalten oder ihren sexuellen Vorlieben, sie zeigen das Innere und Äußere ihrer Wohnung, lassen uns an den kleinen und großen Dingen ihres Lebens teilhaben. Gleichzeitig wird es durch die entsprechende Software immer leichter, Nutzerprofile zu erstellen, die den Menschen durchleuchten und marktförmig machen. So oder so: Die Grenzen zwischen dem Privaten und dem Öffentlichen verschwimmen, die Sphären durchdringen einander. Bleiben bei diesem Prozess die Persönlichkeitsrechte und das Politische auf der Strecke?

Die Beiträge im vorliegenden Sammelband *#public_life* untersuchen vor dem Hintergrund der digitalen Drift die Bedeutung von Privatheit und Öffentlichkeit heute. Die Gegensätzlichkeit der Positionen, die an Privatsphäre und Kontrollanspruch festhalten oder das Zeitalter von Post-Privacy ausrufen, scheuen sie dabei nicht.

Heinrich-Böll-Stiftung e.V. Schumannstraße 8, 10117 Berlin
Die grüne politische Stiftung **T** 030 285340 **F** 030 28534109 **E** info@boell.de **W** www.boell.de

ISBN 978-3-86928-052-3