Internet & Gesellschaft
〈Co:llaboratory〉

Eine Publikation des
Internet & Gesellschaft Co:llaboratory.

»Gleichgewicht und Spannung zwischen digitaler Privatheit und Öffentlichkeit«

Phänomene, Szenarien und Denkanstöße

Abschlussbericht
November 2011

1. Auflage

in partnership with:
Google™

Inhaltsverzeichnis

Impressum

Eine Publikation des Internet & Gesellschaft Co:llaboratory

Konzept & Erstellung:
Sebastian Haselbeck · Oliver Klug · Falk Lüke
Max Senges · Katharina Vanzella

Der Bericht wurde verfasst von
Ahmet Emre Açar · Matthias Bärwolff · Ulf Buermeyer
Rafael Capurro · Susanne Dehmel · Hubertus Gersdorf
Philippe Gröschel · Seda Gürses · Stephan Hansen-Oest
Ulrike Höppner · Andreas Jungherr · Christoph Kappes
Ulrich Klotz · Henning Lesch · Falk Lüke · Bernd Lutterbeck
Florian Marienfeld · Matthias Niebuhr · Frank Pallas
Martina Pickhardt · Cornelius Puschmann · Oliver Raabe
Jan Schallaböck · Michael Seemann · Max Senges
Martin Spindler · Sebastian Sooth · Gordon Süß

Projektorganisation 4. Initiative:
Falk Lüke · Gordon Süß

Gestaltungskonzept & Final Artwork:
Jessica Louis · Sabine Grosser, Hamburg
www.jessicalouis.com

Illustrationen:
Cover: Frank Cmuchal · www.smautschi.com
Innenseiten: Anna-Lena Schiller · www.annalenaschiller.com

Produktion:
Produktionsbüro Romey von Malottky GmbH, Hamburg

Wissenschaftliche Grafiken:
Karl-Heinz Steinmüller, Z-Punkt · www.z-punkt.de

Ansprechpartner des Co:llaboratory Lenkungskreis:
Dr. Max Senges · Martin G. Löhe · Dr. Philipp Müller
John H. Weitzmann · Henning Lesch

Email: kontakt@collaboratory.de

Besuchen Sie das Internet & Gesellschaft Co:llaboratory auf
www.collaboratory.de · www.youtube.com/collaboratory

ISBN 978-3-9503139-3-2

Der Lenkungskreis des Co:*llaboratory* über die vierte Initiative

In der jüngsten Initiative untersuchten rund 30 Experten aus Zivilgesellschaft, Wissenschaft und Wirtschaft eine der weitreichendsten, mit dem Internet verbundenen gesellschaftlichen Veränderungen: die von Privatheit und Öffentlichkeit im digitalen Raum.

Diese Transformation wirft eine Fülle schwierigster Fragen auf allen Ebenen der Gesellschaft auf. Der vorliegende Bericht versteht sich daher keinesfalls als abschließende Analyse mit ultimativen Antworten auf alle Fragen, die sich in diesem Kontext stellen. Vielmehr nähert sich der Bericht dem komplexen Thema »Privatheit im digitalen Raum« bewusst mit sehr unterschiedlichen Methoden und Blickwinkeln. Dies beinhaltet gemeinsame Analysen der Autoren des Expertenkreises, Interviews mit hochkarätigen Fachleuten von außen, u. a. mit Bundesinnenminister Hans-Peter Friedrich, ausführliche Erklärungen zu den wesentlichen Begriffen sowie vertiefende Literaturtipps.

Um das Thema in seiner ganzen Breite und Tiefe zu veranschaulichen, erarbeitete die Expertenrunde zum Komplex Privatheit und Öffentlichkeit zunächst eine Landkarte sowie ein Lexikon der Phänomene (Kapitel 1.1 und 1.2). Dies hatte zum einen zum Ziel, die hinter der Veränderung von Privatheit und Öffentlichkeit liegenden technischen Innovationen phänomenologisch zu betrachten. Zum zweiten, um deren gesellschaftliche, wirtschaftliche, psychologische und politische Auswirkungen zu verstehen und zu beschreiben.

In einem zweiten Schritt (Kapitel 1.3) entwickelte das Co:*llaboratory* drei lebensweltliche Szenarien für das Jahr 2035, die hinsichtlich der künftigen Gestaltung bzw. Gestaltbarkeit von Privatheit und Öffentlichkeit jeweils unterschiedliche Entwicklungen zugrunde legen. Die Szenarien dienen also quasi als fiktive »Referenzwelten« für die tatsächliche Entwicklung unserer

Gesellschaft – gesellschaftlich wie technologisch. Sie zeigen auch, dass politische Entscheidungen zu Privatheit und Öffentlichkeit auf fundamental unterschiedliche Gesellschaftsmodelle hinauslaufen. Die Experten haben sich hier ganz bewusst auf die Beschreibung konzentriert, die Bewertung des »Wünschbaren« obliegt anderen.

In einem dritten Arbeitsbereich formulierten die Experten schließlich eine Reihe von »Denkanstößen«, Thesen, die implizit auch Handlungs- oder Erwägungsempfehlungen enthalten (Kapitel 1.4). Auch hier zeigen die Experten jedoch die jeweils sehr unterschiedlichen Perspektiven zu Chancen und Herausforderungen für Privatheit und Öffentlichkeit auf.

In Kapitel 2 des Berichts kommen einige herausragende Experten in Interviews ausführlich zu Wort, neben Bundesinnenminister *Hans-Peter Friedrich* auch die Privacy-Forscherin und Bloggerin *Danah Boyd,* der Social-Media-Pionier und Erfinder des Begriffs »virtual community« *Howard Rheingold,* der Science-Fiction-Autor und Mitbegründer des Cyberpunk *Bruce Sterling* sowie der Medienwissenschaftler *Stefan Münker.* Ihre »Seitenblicke« geben dem Thema Privatheit und Öffentlichkeit eine zusätzliche, auch internationale Perspektive.

In Kapitel 3 werden einige Schlüsselbegriffe wie Anonymität, Pseudonymität, Identität, Öffentlichkeit oder auch Geheimnis ausführlich erläutert. Der Bericht schließt in zwei Exkursen mit praktischen Beispielen wie »Smart Grids«, um die Relevanz des Themas für immer mehr Alltagsfragen zu unterstreichen.

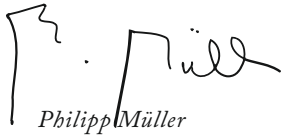
Die vierte Initiative des Co:*llaboratory* hat sich einem anspruchsvollen und kontroversen Thema gewidmet. Dennoch war die Debatte stets von der konstruktiven Suche nach einem gemeinsamen Verständnis und vernünftigen, praktikablen Lösungsansätzen geprägt. Dies erscheint umso bemerkenswerter, da der Expertenkreis durchaus heterogen besetzt war. Das Spektrum reichte dabei von Post-Privacy-Theoretikern bis zur Expertise aus einer Datenschutzbehörde. Im Mittelpunkt der Auseinandersetzung standen unter anderem Fragen nach der Qualität und Funktionalität der Diskurse in der Netzöffentlichkeit sowie nach der Entwicklung der nicht-öffentlichen Nutzung des Internets. Welche Regeln und welche Institutionen benötigt die Gesellschaft, wenn auch künftig öffentlicher Diskurs und private Rückzugsräume gleichermaßen gewährleistet bleiben sollen? Ein weiteres wichtiges Thema der Runde war, wie anonyme und pseudonyme Nutzung von Diensten konzeptioniert werden können und welche Vor- und Nachteile diese jeweils mit sich bringen.

Das Co:*llaboratory* hat sich während der vergangenen eineinhalb Jahre zu einem Expertennetzwerk entwickelt, in das mehr als 150 Netzbürger, Internetforscher und -unternehmer ihre Expertise einfließen lassen. Es versteht sich als Multi-Stakeholder-Plattform für netzaffine Akteure aus Zivilgesellschaft, Wirtschaft, Wissenschaft, Verwaltung und Politik, die im Rahmen des Co:*llaboratory* Beiträge zu Fragestellungen rund um die gesellschaftliche Nutzung des Internets in Deutschland entwickeln. Dabei geht es besonders darum, die Vordenker und »pragmatischen Idealisten« für die Initiativen und Arbeitsgruppen (Ohus) des Co:*llaboratory* zu gewinnen. Es stehen also Motivation und Expertise, nicht Seniorität und Repräsentativität im Vordergrund des Community-Buildings. Mit der dritten und vierten Initiative konnte das Co:*llaboratory* beweisen, dass auch sehr kontroverse Fragestellungen mit dem Multi-Stakeholder-Ansatz konstruktiv und fruchtbar bearbeitet werden können.

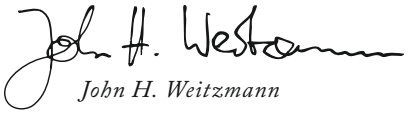
Wir möchten uns an dieser Stelle bei allen Experten der vierten Initiative für ihr ehrenamtliches Engagement und die inspirierende Zusammenarbeit bedanken. Wir hoffen, ab November 2011 mit vielen von Euch auch in der Ohu »Privatheit & Öffentlichkeit« die spannendsten Entwicklungen weiter zu besprechen und neue Wege in die Zukunft zu finden.

Mit freundlichen Grüßen
Der Co:*llaboratory* Lenkungskreis

Max Senges

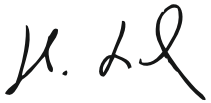


Philipp Müller



John H. Weitzmann

Martin G. Löhe

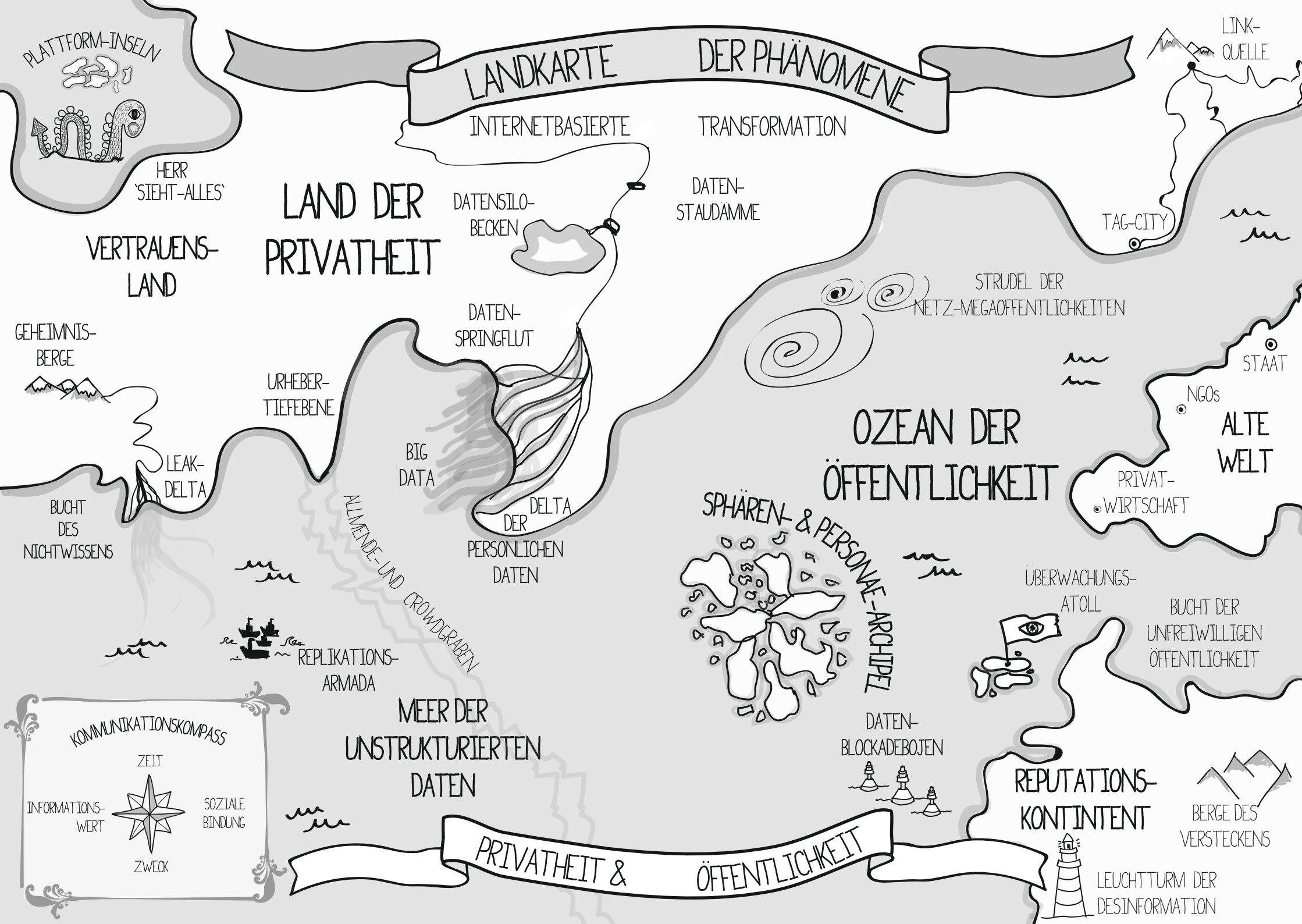


Henning Lesch

1 Privatheit und Öffentlichkeit: Phänomene, Szenarien, Denkanstöße

1.1 Landkarte der Phänomene

In der Landkarte der Phänomene werden exemplarisch einige der Besonderheiten des Wandels von Privatheit und Öffentlichkeit durch die Allgegenwertigkeit des Internets und die zunehmende Digitalisierung grafisch dargestellt.


LANDKARTE DER PHÄNOMENE
PRIVATHEIT & ÖFFENTLICHKEIT
LAND DER PRIVATHEIT
OZEAN DER ÖFFENTLICHKEIT
MEER DER UNSTRUKTURIERTEN DATEN
INTERNETBASIERTE TRANSFORMATION
PLATTFORM-INSELN
HERR 'SIEHT-ALLES'
VERTRAUENS-LAND
DATENSILO-BECKEN
DATEN-STAUDÄMME
LINK-QUELLE
TAG-CITY
STRUDEL DER NETZ-MEGAÖFFENTLICHKEITEN
GEHEIMNIS-BERGE
DATEN-SPRINGFLUT
URHEBER-TIEFEBENE
STAAT
NGOs
ALTE WELT
PRIVAT-WIRTSCHAFT
LEAK-DELTA
BIG DATA
DELTA DER PERSONLICHEN DATEN
BUCHT DES NICHTWISSENS
ALLMENDE-UND CROWDGRABEN
SPHÄREN- & PERSONAE-ARCHIPEL
ÜBERWACHUNGS-ATOLL
BUCHT DER UNFREIWILLIGEN ÖFFENTLICHKEIT
REPLIKATIONS-ARMADA
DATEN-BLOCKADEBOJEN
REPUTATIONS-KONTINTENT
BERGE DES VERSTECKENS
LEUCHTTURM DER DESINFORMATION
KOMMUNIKATIONSKOMPASS
ZEIT
INFORMATIONS-WERT
SOZIALE BINDUNG
ZWECK

1.2 Lexikon der Phänomene

Zu Beginn der Auseinandersetzung mit dem Wandel von Privatheit und Öffentlichkeit durch das Internet wurde deutlich, dass die Experten der vierten Co:*llaboratory* Initiative aufgrund ihrer veschiedenen Forschungs- und Arbeitschwerpunkte ein sehr unterschiedliches Verständniss von den Begrifflichkeiten und den wichtigsten Problemen, Chancen und Phänomenen haben. Um sicherzustellen, dass alle Phänomene dieses Wandels zur Sprache kommen und um einen Großteil der Begriffe zu erläutern wurde das Lexikon der Phänomene erarbeitet.

1.2.1 Grundlagen

Privatheit als informationelle Differenz

Privatheit und Öffentlichkeit sind zwei Begriffe, die wir ohne Zögern verwenden und deren Konzepte uns im Alltag geläufig zu sein scheinen. Was wir zuhause tun, ist privat, und was wir öffentlich tun, tun wir auf der Straße, vereinfacht gesagt. Schon die Griechen unterschieden vom Gehöft (Oikos) die Agora, auf der man sich versammelte und auf der Institutionen angesiedelt waren, die der Allgemeinheit dienten. Bei näherem Hinsehen werfen sich allerdings Fragen zu diesen geläufigen Konzepten auf.

In einer gedanklichen Versuchsanordnung befindet sich eine Person in einem Raum – würden wir hier von Privatheit schon sprechen, obwohl wir nichts über die Welt außerhalb des Raumes wissen? Wäre nämlich der Raum auf einer Insel und gäbe es außerhalb des besagten Raumes keine weitere Person, so hätten wir Robinson auf seiner Insel ganz allein aufgestellt. Hier würden wir zögern, zu sagen, der einsame Robinson sei »privat« auf seiner Insel. Privatheit als Konzept hat also immer mit mehr als einer Person zu tun.

Wenn wir nun in einem zweiten Gedankenexperiment zwei Personen in einem Raum aufstellen und eine dritte außerhalb des Raumes, würden wir wohl noch sagen, die zwei im Raum seien »privat«. Aber wo ist hier die Öffentlichkeit? Ist die Person draußen allein »Öffentlichkeit«, obwohl sie nicht im Raum ist? Es wird also nicht einfacher, je länger man nachdenkt, und es ist so gesehen beim ersten unbelasteten Anlauf nicht so recht klar, was die beiden Begriffe genau bezeichnen: die Situation einer Person, eine jeweilige Situation zwischen Personen, echte Räume oder gedachte Sphären?

Im obigen Versuchsaufbau haben wir die Situation, in der sich unsere Personen befinden, nur als »Raum« beschrieben und nicht erläutert, wie man sich die Situation genau vorzustellen habe. Ist das, was wir oben »Raum« genannt haben, in dem zwei Personen sitzen, wirklich ein Gebäude moderner Bauart, oder ist es ein tief einsehbares Glasgebäude, in das der Dritte hineinsehen kann, oder ist es ein Zelt, durch das Laute dringen, die der Dritte hört? Wenn der Dritte diese Laute hört, ist es Sprache, die er inhaltlich versteht? Und würde Privatheit entstanden sein, wenn der eine die Sprache der anderen nicht verstehen würde – ein Kaspar Hauser mitten in New York? Oder ist die geschilderte Raumsituation vielleicht nur eine abgesteckte Fläche, ein Claim, in dessen Mitte zwei auf je einem Stuhl sitzen und weit entfernt am Horizont der Dritte, der beide weder hören noch richtig sehen kann? Was wäre hier privat und was öffentlich?

Bei näherem Nachdenken leuchtet ein, dass für diese Situationen der Aspekt der Information eine Rolle spielt: Mal *hört* der Dritte, mal *sieht* er – oder eben nicht. Und was er sieht und hört, das kann Bedeutung für ihn haben, mal nur für ihn, mal auch für andere. Die Konzepte von Privatheit und Öffentlichkeit sind also von Information und ihrem Trägermedium nicht zu lösen – und zwar weit bevor der Computer überhaupt erfunden wurde. Und wie wir am Beispiel Kaspar in New York gesehen haben, können sie auch nicht von der Bedeutung von Sprache und anderer Zeichen getrennt werden. *Das Private und das Öffentliche unterscheiden sich hinsichtlich Information. Privatheit ist, wo informationelle Differenz besteht.*

Medien

In dieser Situation unserer archaisch fiktiven Aufstellungen verändern nun Medien alles. Die Schrift, die als Information sichtbar macht, was vorher fast immer körperlich an Menschen gebunden war (menschliche Äußerungen gab es nicht ohne anwesende Menschen), ermöglicht Durchbrechungen des Privaten, weil Zugang zu den Schriftzeichen den Zugang zum Menschen ersetzt. Das Buch macht die Information so reproduzierbar, dass sie an beliebigen Orten zu Dritten gelangen kann. Der Fotoapparat konserviert auf Fotos das Äußere des Augenblicks, die *Erscheinung* der Dinge. Und diese nimmt auch die Fernsehkamera mit Halbfotos pro Sekunde auf, nur dass sie diese visuellen Augenblicke via Sender über Geräte zu Empfänger-Massen multipliziert. Und alle diese Medien tragen Information, die womöglich privat ist, hierhin, dorthin, in die Welt. Sie tragen im Extremfall nach Art des »Big Brother«-Fernsehformates das Intimste sofort in Echtzeit in die ganze Welt, mit oder ohne Zustimmung des Betroffenen und – im Unterschied zum TV-Format – nicht als inszenierte Handlung, sondern als echte.

Kenntnis als unwiderruflicher Kopiervorgang

Schon bei diesen alten Medien kann man die Verletzung des Privaten nicht ungeschehen machen und Schaden schwerlich kompensieren, weil der öffentliche Widerruf genauso wenig hilft wie eine Zahlung in Geld. Information, die den Empfänger erreicht hat, hat sich quasi in ihm fortgesetzt, so dass diese neben dem Substrat besteht, dessen Vernichtung oder Untersagung den Duplikationsprozess nicht mehr revidieren kann. Pointiert: Die Bücherverbrennung kommt zu spät, wenn die Bücher gelesen sind. *Kenntnis ist ein unwiderruflicher Kopiervorgang.*

Technik, Erwartung, soziale Normen

Natürlich sind heute Verletzungshandlungen nicht die Regel, weil wir gelernt haben, mit diesen technischen Innovationen umzugehen. Wir wissen heute, dass wir Plätze mit Menschen fotografieren dürfen, nicht aber das Gesicht des Einzelnen. Man kann sich also vorstellen, dass jede dieser Innovationen den Umgang von Menschen mit Privatheit und Öffentlichkeit verändert hat, dass sie also alte Verhaltensmuster verändert und neue soziale Normen geschaffen hat. Die Vorstellungen von Privatheit und Öffentlichkeit sind *Erwartungshaltungen an unsere Umwelt in Bezug auf informatorische Sachverhalte.* Denn anders als unsere Vorfahren wissen wir nämlich auch, dass wir auf öffentlichen Plätzen damit rechnen müssen, in gehörigem Abstand fotografiert zu werden, als Beiwerk nämlich. Der Fotoapparat hat auf unsere Vorstellung davon, wie weit wir mit Beobachtung rechnen, zurückgewirkt. Und in den heutigen Konzepten wie *Privacy by Design* (vgl. auch den Begriff des *Informationsschutzes)* zeigt sich die gegenläufige Entwicklung, dass Technik und Prozesse über Eigenschaften verfügen, mit denen Erwartungshaltungen erfüllt werden können. Diese Erwartungshaltungen zeigen sich auch bei den heutigen Schlüsselbegriffen *Privacy by Default, Einwilligung, Datenvermeidung, Datensparsamkeit, Datenhoheit, Informationsrecht* und *Transparenz.* Dabei sollte man nicht dem Irrtum unterliegen, dass Technik immer der Erwartungshaltung zuwiderlaufen muss: Schon der Beichtstuhl dient dem Schutz des *Beichtgeheimnisses* und er ist – zusammen mit Regelungen des kanonischen Rechts[1] – eine Entwicklung zu Barockzeiten, um den einfachen Stuhl des Priesters durch Technik und Norm auf ein höheres Schutzniveau zu heben.

Die Gesellschaft hat lange gebraucht, um auf Fragestellungen, die von neuer Technik ausgelöst wurden, Antworten zu finden. Nicht nur die Frage, in welcher Situation man Menschen fotografieren darf, war von Belang. Es ging beispielsweise auch darum, ob man Briefe an Fremde öffnen darf und, wenn ja, welche. Es ging um die Frage nach der Behandlung von Kommunikationsakten wie Ehrverletzungen und Gewaltaufrufen und solchen Akten, die sich

1 http://www.vatican.va/archive/DEU0036/__P3F.HTM – Beichtstuhl, Ort Kirche, Gitter und »Außerhalb des Beichtstuhls dürfen Beichten nur aus gerechtem Grund entgegengenommen werden«.

gegen staatliche Rechtsgüter richten – und diese Diskussionen sind teilweise durch das Internet wieder entflammt. Wir haben das allgemeine Persönlichkeitsrecht weiterentwickelt, das Presserecht geschaffen, Betretungsrechte im Mietrecht geregelt und vieles andere mehr.

Die Geschichte von Privatheit ist eine eigene, lange Geschichte. Was wir jedoch mit dieser Raffung zeigen können: Erstens sind die Strukturen von Privatheit und Öffentlichkeit schon früh in der Menschheitsgeschichte angelegt. Zweitens beruhen sie (mitsamt ihren Problemen) auf der Spannung zwischen Individuum, das sich selbst und die Grenze zwischen sich und Umwelt erfahren will, als etwas Getrenntem auf der einen Seite und seinen dafür notwendigen Kommunikationsbedürfnissen mit anderen Menschen (einzeln oder in Gemeinschaft) auf der anderen Seite. Und sie setzen sich, drittens, in den typischerweise gestiegenen Kommunikationsbedürfnissen der komplexer gewordenen Gesellschaft fort – Arbeitsteilung, Leistungsaustausch, Industrialisierung, Medien, Dienstleistungsgesellschaft und Urbanisierung seien als Schlagwörter genannt, um dieses Bedürfnis zu veranschaulichen. Plakativ: Der autarke Bauer auf seinem *Oikos* im Allgäu kann die Balance für sich meist leichter finden als der Kommunikationsberater in Berlin.

Das Hinzutreten des Computers

Vor rund 40 Jahren kommt der *Computer* in den Alltag und speichert Daten, was der Impuls für *Datenschutz* ist. Geregelt wird – wir müssen ab jetzt den Zeit- und Inhaltsraffer nutzen – zunächst der Kern: Ansprüche auf der Basis einer Vorstellung von *»Herrschaft über Daten«,* die regelmäßig »personenbezogen« sind, in Prozess-Schritten erhoben und verarbeitet werden. Und sich von der Grundidee her in abgetrennten Systemen befinden, die von Staat und Privatunternehmen betrieben werden. Diesem Gedanken wiederum liegen Ideen aus dem späten 19. Jahrhundert zugrunde, vor allem das *»Right to privacy«* von Warren/Brandeis, wonach jedem Individuum das Recht zustehe, selbst zu bestimmen, inwieweit seine »Gedanken, Meinungen und Gefühle«, mithin personenbezogene Informationen, anderen mitgeteilt werden sollten.

Autonomie und Gemeinwohl

Vor fast 30 Jahren wird dann angesichts der umstrittenen Volkszählung das »Recht auf informationelle Selbstbestimmung« vom BVerfG geboren, genauer: aus dem allgemeinen Persönlichkeitsrecht abgeleitet. Dies ist das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Wer nicht wisse, was mit seinen Daten geschehe, werde aus Vorsicht sein Verhalten anpassen, argumentiert das Gericht. Dies erinnert uns an die Vorstellung eines Panoptismus (griech. Panoptes = »das alles Sehende«) nach dem Vorbild eines perfekten Gefängnisses, des *»Panopticons«* von Jeremy Bentham, der im Grunde ein architektonisches Prinzip der Überwachung darstellt, bei dem die Beobachteten in der dystopischen Reinform permanent keine Privatsphäre haben, weil sie ihnen nicht gewährt wird. Dieser Aspekt des »Beobachtet-Fühlens« bringt neben dem bisherigen individual-grundrechtlichen Aspekt den *Gemeinwohl*-Aspekt als neuen Gesichtspunkt ins Spiel. Hier geht es nämlich um eine vorsorgliche Maßnahme, um die *Meinungsfreiheit* und damit das Funktionieren der *Demokratie* zu sichern. Es spielen also in modernen Demokratien zwei Rechtsaspekte bei unserer Fragestellung mit:

- Wie viel Privatheit braucht es, um das Grundrecht nicht zu verletzen? Und:
- Inwieweit kann der Informationsfluss nicht nur gegenüber staatlichen Organen, sondern gegenüber allen gesellschaftlichen Teilen, so gestaltet werden, dass er den demokratischen Meinungsbildungsprozess unterstützt?

Wir sind hier wieder beim Zweck der *Agora* im (Stadt-)Staat der *Polis* angekommen.

Informationssysteme als Vermittler und Verdichter von sozialer Realität

Pointiert gesagt: Die Privatheit des einen darf nicht verletzt werden, für die Meinungsbildung muss aber Wissen über andere irgendwie gewonnen werden

(auch durch eigene Anschauung), damit der politische Prozess funktioniert. Ein Paradoxon, das nur dadurch aufzulösen ist, dass gesellschaftliche *Schutzsphären* entstehen, welche Daten über andere möglichst in wissenschaftlichen Studiensituationen gekapselt, anonymisiert, mehrfach aggregiert und abstrahiert und in gesellschaftlichen Teilsystemen verarbeitet bzw. medial vermittelt an Dritte gelangen lassen, damit sie Meinung werden können, die nicht ohne Grund genau diese Meinung geworden ist und nicht nur aus der kleinen Welt des meinenden, wählenden Bürgers stammen. Am Beispiel erläutert: Wer etwa seine politische Wahlentscheidung auch von Sozialpolitik abhängig machen und Lösungsvorschläge zu sozialen Brandherden bewerten möchte, muss vorher empirisch und konkret gewonnene Erkenntnisse haben, damit seine gesamte Wahlentscheidung nicht auf Vermutungen beruht. Wie geht das heute? Mit *Informationstechnik,* die Daten erhebt und auf irgendeine Art auch zwischen den Beteiligten tauschen lässt. Der demokratische Aspekt gibt also einen Transparenzimpuls in gesellschaftliche Systeme, die sich in technischen Informationssystemen niederschlagen, die wiederum potentielle Gefahrenherde für die im selben Atemzug ausgerufene informationelle Selbstbestimmung sind. Auch hier zeigt sich also die Spannung, dass einerseits Information fließen soll, die andererseits aus der Realität menschlichen Handelns kommt und mitunter gar nicht anders als aus der Realität des Einzelnen abgeleitet werden *kann*.

1.2.2 Allgemeine Phänomene

Während also national die Systeme zur Vernetzung tendieren müssen, um Komplexität zu bewältigen, und weltweit die Globalisierung ihren Lauf nimmt, tritt vor 20 Jahren das Internet in die Welt. (Dass zehn Jahre zuvor, also gleich nach dem Volkszählungsurteil, die ersten Mailboxen in Deutschland entstanden, die Information weit weg, sogar an unbekannte physische Orte und das bis zur Einführung des Zeittaktes für Ortsgespräche sogar mit Flatrate transportierten, ist eine Pointe der Geschichte: Diese Infrastruktur war ja zum Teil bewusst geheim.) Mit dem Internet macht die Entwicklung wieder einen Sprung. Durch weltweite Kommunikation verwirklichen sich große Chancen für eine globale Kommunikation in Echtzeit, durch Kommunikation von Transaktionsdaten werden Wirtschaftsprozesse effizient ermöglicht und so der Wohlstand vermehrt.

Umgekehrt zeichnet sich das Internet durch eine Reihe von Eigenschaften und hierdurch hervorgerufenen Phänomenen aus, welche Konsequenzen für unser Thema »Privatsphäre und Öffentlichkeit« haben.

- ***Ubiquität:*** Beispielsweise sind durch die Allgegenwärtigkeit und Überallverfügbarkeit, die Ubiquität von Information, ihre Schriftlichkeit und die vielfältigen Vervielfältigungs- und Replikationsmechanismen drei starke Phänomene zu beobachten, welche die Trennung von Räumen oder Sphären entweder gefährden oder nur rudimentär abbildbar machen. Das Netz tendiert dazu, informatorische Differenz so auszugleichen, wie es auch die Finanzmärkte handhaben. Wir haben es hier mit einem Phänomen der Globalisierung zu tun: Nach den Waren, den Finanzen, den Umwelteigenschaften beginnt nun die Information global die Verhältnisse zu verändern.

- ***Transaktion:*** Beispielsweise entstehen durch die Vermischung von Kommunikation und Transaktion Chancen und Risiken; dem Social Commerce der Empfehlungskäufe steht gegenüber, dass diese Transaktionen neue Daten generieren, die aus dem Privaten ins Öffentliche strömen können und zum Teil ja sogar sollen; was sonst ist denn der Beitrag eines Nutzers in einem sozialen Netzwerk, er habe soeben einen bestimmten Artikel gekauft? So ist also der Satz aus dem Cluetrain-Manifest, »Märkte sind Gespräche«, nur die halbe Wahrheit. Vollständig lautet der Satz der Zukunft: »Märkte sind Gespräche über Firmen, Produkte, Transaktion und Käufer«, wobei klar wird, dass nicht nur der Käufer unmittelbar über sich selbst erzählt, sondern mittelbar eben auch über die Transaktionen, die er getätigt hat.

- ***Identität:*** Beispielsweise ist Information im Vergleich zum Buch sehr einfach, unbeschränkt und kostengünstig reproduzierbar, so dass sich in Kombination mit weitgehender Fälschbarkeit neue Probleme für den Schutz des Privaten ergeben, weil die Identität des Urhebers einer Information nicht gesichert ist. Ohne Identitätsmanagement kann es »innerhalb des Systems« immer nur abgeleitete Vertrauensstellungen geben, welche aber »von außen« prinzipiell gleichwertig sind.

- ***Simulacrum:*** Beispielsweise repräsentiert das Internet Information der physischen Welt, so dass die Unterscheidung zwischen Original und Kopie, Vorbild und Abbild, Realität und Imagination schwierig geworden ist (Stichwörter *»Simulacrum«* nach Baudrillard, *»Virtualität«, »Hyperrealität«* und Ähnliches): Was unterscheidet »Einkaufen« in der einen Welt von »Einkaufen« in der anderen Welt? Aus der radikalen Sicht eines »Ich« muss es in beiden Fällen physische Bewegung vornehmen, Kommunizieren, bis die Ware kommt. Jenseits solcher sehr theoretischer Überlegungen stellt sich aber immer dann, wenn ein Prozess sein Pendant in der digitalen Welt gefunden hat, immer die Frage nach den *Datenspuren,* dem *Datenschatten.* Schon Lukrez erklärte in *De Rerum Natura* die Sichtbarkeit der Dinge mit ihren feinen Schichten, die sie aussenden, bis sie auf unsere Netzhaut treffen; er versuchte so ohne das Konzept von Göttern zu erklären, dass unsere Wahrnehmung auf Atomen beruht, der unvergänglichen Urmaterie, die sich in ständiger Bewegung im leeren Raum befindet und durch Kollision Natur erschafft. Reicht heute die Digitalisierung bestimmter Vorgangsabschnitte aus, um wie selbstverständlich von ihrer Spurenfreiheit auszugehen, oder müssen wir uns wie in der physischen Welt damit anfreunden, dass manche Vorgänge genauso wenig unbeobachtet sind wie der Einkauf von Biolamm am Stand des Lieblingsbauern auf dem städtischen Biowochenmarkt? Und um wie oft stellt sich diese Frage, wenn unser Handeln auf Kommunikation ausgerichtet ist, also mit der Absicht durchgeführt wird, Information zu erzeugen?

Sphären und Personas

Die Vorstellung, den Menschen umgäben Ringe von *Sphären,* die wie *Zwiebelhäute* übereinandergeschichtet sind, ist zwar vor allem im Recht noch anzutreffen, das die Konzepte der »Intimsphäre« und der »höchstpersönlichen« Sphäre bzw. Handlungen innerhalb der Privatsphäre kennt. Das Sphärenmodell ist aber nicht nur sozialwissenschaftlich veraltet, es wird auch durch das Internet für jedermann sichtbar in Frage gestellt. Wir haben zwar eine personale Identität, bewegen uns aber in verschiedenen sozialen Strukturen mit verschiedenen *Personas.* Wir zeigen in der Familie, unter Freunden, »Surf-Freunden«, im Sportverein und so weiter unterschiedliche Seiten von uns. Eine Information, mit der wir in einem sozialen Umfeld freizügig umgehen, wollen wir in einem anderen nicht preisgeben. Typisch, sagt man, seien fünf Gruppen von bis zu zehn Personen.[2]

Diesem Konzept fehlt es an Praktikabilität. Unterstellt man, dass dasselbe Modell auch auf die Onlinenutzung übertragen werden kann, so muss man konstatieren, dass auch die besten Internetdienste die Personas bis heute nicht annähernd oder auch nur modellhaft umsetzen können, ganz zu schweigen davon, dass die Komplexität und die Bedienbarkeit nach heutigem Ermessen für normale Nutzer nicht beherrschbar wären. Es ginge eben nicht nur darum, die Suchabfragen oder -keywords, den sozialen Graphen, die Interessen, die Käufe, die Kalenderplanungen, die Geolokation und Ähnliches abzubilden. Es müsste darum gehen, auch Finanzdaten und Gesundheitsdaten und ähnliche große Bereiche flexibel abzubilden (vielleicht in einem geschützten Modul). Und all diese Daten auch noch Sphären zuzuordnen, damit jedermann praktikable Personas hat.

Die Schwächen der Personas als Konzept zeigt aber auch das Nachdenken darüber, dass sie nur eine Generalisierung von individuellem und relativem

2 http://www.thinkoutsidein.com/blog/2011/05/small-connected-groups/

Vertrauen ist, das wir in unterschiedlichen Kontexten intuitiv anwenden. Dies soll sogleich gezeigt werden.

Kontext von Kommunikationsakten, Kommunikationsgeschichte als soziale Realität

Ein weiterer Aspekt ist der *Kontext* einer Information. Fehlender, unvollständiger oder gefälschter Kontext ist schon immer ein Thema menschlicher Kommunikation gewesen, weit vor der Erfindung des Computers. Wir kennen dies etwa aus vielfältigen Diskussionen um »aus dem Kontext gerissene« Interviewzitate. Zum Kontext gehört auch, dass der Absender zu erkennen gibt, welche Vertraulichkeitsstufe sein Kommunikationsinhalt haben soll, z. B. durch Flüstern, Zwinkern, Zur-Seite-Nehmen, besondere Zeit- und Ortswahl (»nachts am Grenzstein«) und Ähnliches. Hierzu fehlt es im digitalen Teil der Welt noch an Kultur, weil die Schriftform scheinbar wenig Differenzierung bietet.

Aber Kontext ist nicht nur ein Absenderthema. Schon immer setzte ein Erkenntnis- und Verstehensakt meist ein gewisses Vorverständnis, d. h. ein bestimmtes Wissen, beim Empfänger voraus. Jedes Medium hat idealerweise die Aufgabe, Kontext mit zu tragen und die Dinge nicht »herauszureißen«, aber wie soll es sicherstellen, dass der Empfänger über ausreichende Kontextinformation verfügt? Das ist kein abstraktes Wissenschaftsproblem, sondern eines der größten Probleme des heutigen Internets, nein: eines jeden digitalen Mediums.

Wie wollen wir beispielsweise damit umgehen, wenn einzelne Kommentarbeiträge bei Diskussionen in sozialen Netzwerken zu löschen wären, also z. B. Kommentar Nummer sieben, wenn acht und neun auf ihn Bezug nehmen und so notwendigen Kontext verlieren würden? Hier zeigt sich wie im Prismenglas, dass Gespräche mehrerer Personen aus einer höheren Warte ein »übergeordneter« Kommunikationsakt sind, die entstellt und zerstört werden, wenn man sie reduktionistisch zerlegt und mit den zerlegten Teilen nach Belieben verfahren will. Darf man Nummer sieben löschen, wenn sie den wesentlichen Impuls zur Diskussion beigetragen hat? Es ist auffällig, dass in der Praxis des Internets über diesen Punkt häufig gestritten wird. Ist das Ergebnis nicht »gemeinsam« erarbeitet, wird ein Folgebeitrag nicht entwertet, wenn man ihm den Kontext nimmt? Wir haben derzeit keine Lösung. Dass Information aus der Vergangenheit zerstört wird, dass sie vergessen wird, verschwindet, das kennen wir. Was wir nicht kennen, ist, dass einzelne Kommunikationsakte noch während des gemeinsamen Kommunikationsaktes unwiderruflich im Jetzt gelöscht werden, und dies auch noch durch einseitigen Akt eines Teilnehmers, der sich womöglich aus besten Gründen auf seine Rechte beruft. Nicht anders übrigens, wenn ein Dritter einen Beitrag geschrieben hat, der vom Betroffenen zur Löschung veranlasst wird. Das ist, etwa im Falle von Beleidigung und Volksverhetzung, ein ohne Zweifel richtiger Vorgang, doch taucht hier ein Phänomen auf, was auch unser Thema betrifft. Pointiert gesagt: Das Löschen als *actus contrarius* mag angemessen sein, aber in wessen »Sphäre« ist das von der »Persona« Gesagte, nachdem es weltweit verschriftlicht wurde? Man könnte, ganz gegen die herrschende Meinung, sagen: Was geschehen ist, ist geschehen – ganz so, als seien wir über eine Straße gegangen und wären dabei von einer Kamera aufgenommen worden. Die Strecke noch einmal rückwärts zu gehen, hilft hier nicht. Und so haben wir auch hier einen Konflikt, den das Internet im Vergleich zum Buchdruck verschärft, denn die Information im Internet können wir häufig nicht »verbrennen« und es gibt gute Argumente, dass wir uns vielleicht sogar auf den Gedanken einlassen müssen, eine alte Falschinformation genauso als historische Schlechtleistung stehen zu lassen wie die Gräueltaten in unseren Geschichtsbüchern, die wir ebenfalls nicht löschen. Welche Kommentare der Individuen während der Kommunikation einander Kontext sind, ist eben auch das Ergebnis sozialer Interaktion und somit soziale Realität, die einfach ist, wie sie ist.

Relativität, Vertrauen, Kontextualität, Intuitivität

Wie auch immer man die kulturellen Wurzeln von Privatheit im Detail betrachten mag, sie haben mit *Vertrauen* zu tun: *Wer darf was wissen?* Und

zwar entweder, ganz archaisch, weil wir befürchten müssen, dass uns der andere früher oder später Nachteile zufügt. Aber auch weil wir befürchten müssen, dass eine Information ohne unsere Zustimmung oder unser Wissen *Dritten* zur Kenntnis gereicht wird und uns daraus Nachteile erwachsen könnten. Schließlich, und hier wird das Problem des analogen und digitalen Informationsflusses wieder offenbar, wird durch den letzten Schritt des Austretens aus unserem Kenntnisbereich für uns nicht mehr klar, wen eine Information bereits erreicht hat.

Es ist also *potentiell jedermann ein Wissender,* was uns die Entscheidung darüber, wen wir was wissen lassen, vor allem von dem Vertrauen abhängig machen lässt, dass er erstens uns keine Nachteile zufügt und zweitens diese Information nicht »leakt«. Während man bis vor kurzem noch gesagt hätte: »Vorsicht ist die Mutter der Porzellankiste«, würde man seit kurzem sagen: *»Vorsicht, jeder ist ein Wikileaks.«*

Wegen der Bedeutung der Beziehung zu jedem Einzelnen mutet es also zu simpel an, von »der Privatsphäre« oder »den Personas« als einem Modell, einem statischen Gefüge zu sprechen. Vielmehr scheint es so, als handelte es sich erstens aus Sicht des Subjektes um das Kondensat aus einer Vielzahl einzelner Beziehungen zu anderen Personen (1:n) und zweitens als Denkmodell um die soziale Verdichtung des Verhaltens aller Personen (n:n) in einer Referenzgruppe, einem Land, einem Kulturkreis. Etwas zugespitzt: Wer empirisch messen will, was »das Konzept der Privatsphäre weltweit« ist, braucht Daten über ein repräsentatives Set von sieben Milliarden Menschen und muss folglich n-Fakultät Beziehungen erfassen. Eine Aufgabe für die Soziologie, die keine kleine ist.

Zur personalen Relativität kommt eine weitere Dimension hinzu. Ein Mehr oder Weniger an Vertrauen zwischen Menschen ist kein statischer Zustand, sondern wird vergeben, erworben und kann verloren werden, ist also ein *zeitlich gestreckter Prozess.* Wer kennt nicht die Reue nach einem Vertrauensbruch, die Information überhaupt gegeben zu haben? Hinzu kommt noch mehr Komplexität. Es entsteht Vertrauen durch Kommunikationsakte, insbesondere dadurch, dass eine Information vertraulich gehalten wird, aber auch dadurch, dass zwei sich gegenseitig ins Vertrauen setzen, sich also gegenseitig Geheimnisse anvertrauen.

Auf Dauer ist tieferes Vertrauen aber nicht nur an Kommunikationsakte, sondern auch an *tatsächliches Verhalten* gebunden. Nur durch Nichterzählen über einen gewissen Zeitraum erweist sich, dass es richtig war, sich zu offenbaren. Umgekehrt werden Zweifel wach, wenn sich die Person, der man Vertrauen geschenkt hatte, sich in irgendeiner Weise gegen den Vertrauenden wandte, in extremo bei einem Angriff auf die körperliche Unversehrtheit. Sieht man einmal von einem naiven Urvertrauen ab, so können wir nie wissen, ob es eine Kraft gibt, die stärker ist als wir, den Vertrauensbruch zu erwirken (Beispiel: Erpresser E erpresst von A den Aufenthaltsort von B). Und wir können, da wir von außen auf andere schauen, rational kaum sicher sein, wie weit ihre innere Motivation reicht. Dieser Aspekt des Vertrauens und seiner zeitlichen, prozessualen Komponente ist kaum analysiert, geschweige denn in den heutigen Konzepten integriert, verstanden oder gar technisch implementiert. Dabei wäre es noch die einfachere Übung, unterschiedliche Vertrauensstellungen zwischen Personen abzubilden. Die große Schwierigkeit wird sein, aus äußeren Merkmalen des Kommunikationsverhaltens auf geänderte Vertrauensgrade zu schließen. Es werden, nach allen heutigen Erkenntnissen, immer Menschen sein, die über das Maß an Vertrauenswürdigkeit entscheiden, ob direkt oder indirekt durch die informationstechnische Abbildung des gewährten Maßes, unabhängig von seiner objektiven Gerechtfertigkeit. Und so werden wir es immer mit dem *Phänomen zu tun haben, dass Informationen, die bereits verteilt wurden, nach einer Verminderung der Vertrauenswürdigkeit nicht mehr an die Stelle gehören, an die sie zuvor verteilt wurden.* Dies ist ein weiteres Phänomen, was den Wunsch nach einem *»Roll-Back«* auslöst.

Schließlich gibt es ein weiteres Problem mit dem Modell der Personas. Es berücksichtigt nicht die *Systematik, nach der wir entscheiden,* in welcher

Sphäre wir uns befinden und welche Persona wir anwenden. Auch kann es sein, dass das Modell von Ausnahmen so durchlöchert ist, dass nicht mehr viel von ihm übrig bleibt. Fünf Beispiele aus der Fülle des Lebens: So wird das zusammenwohnende Ehepaar während des Trennungsjahres möglicherweise den Nullpunkt an Vertrauen erreicht haben (»Familie«), während zweitens die Kinder des Ehepaares alle familiären Geschehnisse den Nachbarn erzählen und drittens die Mutter jeden Abend mit einem »Surfing Friend« intime Geheimnisse austauscht. Auch wird die Frage, ob man seinen Wohnungsschlüssel seinem Nachbarn geben sollte, weniger von Sphären und Personas als von individuellem Vertrauen abhängen. Fünftens gibt es unter gutverdienenden Steuerberatern derselben Kanzlei (»Arbeit«) möglicherweise die gleiche Freizügigkeit mit Einkommensinformationen wie sechstens unter Hartz-IV-Empfängern, die sich zum ersten Mal in ihrem Leben vor einem Amt treffen und schon von daher wissen, welche Einnahmen sie haben. Es gibt also keinesfalls allgemeingültige Regeln, sondern eine höchst komplexe »Business Logic«, nach der Menschen mit Information gegenüber anderen Menschen umgehen. Es kann gut sein, dass wir es hier mit nicht formalisierbarem, höchstem Wissen zu tun haben, das wir *Intuition* nennen, weil es das älteste Wissen des Menschen repräsentiert, das noch älter ist, als er selbst: *Wem kann ich vertrauen und wie weit kann ich das – in dieser Sekunde?* Schon der Fisch hatte vermutlich Erkennungsmuster, wie er feindliche Wesen erkannte.

Peer-to-Peer-Öffentlichkeit, handelnde Dritte, Publikation – die Befreiung der Daten aus der Datenbank

Neue Komplexität ist auch entstanden, wenn wir die Struktur der Beteiligtenverhältnisse ansehen. Zwar hat es immer schon Konstellationen mit drei Beteiligten gegeben, etwa wenn A mit C über B spricht oder wenn A ein Foto von B gemacht und dieses C gegeben hat. Unsere heutigen Rechtskonzepte gehen jedoch als Prototyp von einer Beziehung Bürger-Staat oder Bürger-Unternehmen aus, mithin von Zweierbeziehungen. Durch das breite Auftreten von Möglichkeiten, für jedermann im Web zu schreiben (»WriteWeb« als Teil von »Web 2.0.«) sind jedoch einige der Massenphänomene *Dreierbeziehungen,* beispielsweise das Zuordnen von Personennamen und E-Mail-Adresse auf Fotos. Dieses *»Tagging«* ist seit kurzem zum Normalfall geworden, und zwar nicht auf großen sozialen Netzwerken, sondern von Bilderdiensten, Bildbearbeitungsprogrammen und Spezialanwendungen. Auch die Möglichkeit, fremde *Adressdaten* hochzuladen, ist inzwischen auf dem Weg zum Standard. Hinzu kommen Dienste wie *Bewertungsdienste,* beispielsweise Spickmich.de (Lehrer) und docinsider.de (Ärzte), die darauf abzielen, dass Informationen über bestimmte Bürger (in ihrer beruflichen Funktion) publiziert werden. Noch weiter gehen Dienste, wie das inzwischen abgeschaltete rottenneighbour.com, auf denen anonym *Cybermobbing* betrieben werden kann. Zu diesem Zweck des Cybermobbings werden heutzutage viele Web-2.0-Plattformen genutzt, beispielsweise Videoportale, bis der Rechtsverstoß gemeldet wird. Wieder andere wie Jigsaw.com machen es zum Geschäftsmodell, dass Nutzer die verkäuflichen Kontaktdaten Dritter eingeben und hierfür einen Dollar erhalten – *Micro-Datenhandel* in Heimarbeit ist das. Und dazu, durch Dritte den Personen Orte zuzuweisen wie den Fotos bei where-is-this.com, ist es nur ein kleiner Schritt: Check deine Freunde ein und tu was für den ganzen Clan.

Wir beginnen uns damit zu befassen, dass Bürger Daten anderer Bürger erfassen. Dabei haben wir zusätzlich damit zu tun, dass diese Bürger eben keine Fachleute sind und folglich sich der Tragweite ihres Handelns häufig nicht klar sind, wenn dies nicht vorsätzlich wie beim Cybermobbing geschieht. Vom Gefühl, »mein Fotoalbum zu beschriften«, bis zur Vorstellung, auf einem fremden Dienst in der Cloud personenbezogene Daten Dritter abzulegen, ist es mitunter noch ein großer Schritt. *»Privacy Violation by Crowdsourcing«* ist ein neues Phänomen. In diesem Zusammenhang ist auch das »Sprechen über einen Dritten« zu erwähnen, dass es zwar schon in frühen Internetforen gab, mit der Möglichkeit maschineller Analysen werden aber auch hier quasi »harte« Daten generiert: Es ist kein Problem, aus Tweets mit Geburtstagsgrüßen das Geburtsdatum beinahe aller Twitterer zu ermitteln. Weitere Fragen tun sich auf: Darf der Staat auf derart gewonnene Daten zugreifen oder besteht gegebenenfalls ein Verwertungsverbot? Lässt es sich dauerhaft wertungsmäßig unterscheiden, dass jedermann Fotos von

Demonstrationen machen und diese im Internet veröffentlichen darf, wohingegen die Polizei an spezifische Voraussetzungen gebunden ist?

Schauen wir uns die IT-Systeme an, welche die Daten halten, sieht es nicht anders aus. Während der *Datenaustausch zwischen Privatunternehmen* mit Großrechnern der 70er unwahrscheinlich war, tauschen heute Unternehmen alle möglichen Daten in standardisierten Formaten. Dass überhaupt Unternehmen Daten in großem Umfang publizieren, ist ein Phänomen der Vernetzung. Wo man früher noch Daten mühsam standardisierte (von den ersten Ansätzen der EDI in den 60ern bis zum weltweiten UN/ISO-Standard EDIFACT), Datenträger tauschte und dann per DFÜ bewegte, erledigen heute APIs mit Webservices den Austausch standardisiert und in Echtzeit. Von der Öffentlichkeit kaum wahrgenommen sieht man dies im B2B-Bereich sehr gut, in dem beispielsweise das »Procurement« Unternehmen verbindet. Aus den alten *Solitären* sind also *vernetzte Solitäre geworden, ein Netz.* Heute haben wir die nächste Stufe erreicht: Daten werden zwischen Onlinediensten ausgetauscht, nur dass es diesmal hauptsächlich Kommunikation von Endnutzern betrifft. Tweets landen in Suchmaschinen und auf Facebook oder Google+, Bilder des einen Fotodienstes werden in einem anderen angezeigt, Apps lesen Kontaktlisten aus und transferieren selbige so zwischen zwei Systemen. Aggregatoren wie FriendFeed oder rivva sammeln Kommunikation ein und zeigen sie an eigener Stelle an. Spezielle Ereignisdienste wie Pubsubhubbub sorgen dafür, dass andere Dienste über Änderungen informiert werden. Theoretisch sind wir heute so weit, dass jede Information überall sein könnte, was nicht nur Informatiker vor Herausforderungen stellt, sondern auch Endkunden verstört: Ehe man sich versieht, sind Daten in Drittsysteme repliziert. Ganz neue Dienste versuchen die allerorten verteilten digitalen Fotos an einer Stelle zu sammeln (Beispiel everpix.com), lösen aber weder die Ursache vielfach gleicher Inhalte noch unsystematisch verteilter Inhalte, sondern reparieren den Zustand mit einer Umgehungslösung. Die erste Konsequenz: Dem Laien ist nicht mehr klar, welches System eigentlich was wohin kopiert hat, die Vorstellung von getrennten Publikationen schwindet – das Internet ist *eine einzige große Publikation Milliarden verlinkter Seiten,* das *neue Buch der Bücher.* Die zweite Konsequenz: Wer ist hier eigentlich noch der Dienstanbieter erster Ordnung, der die Information als Erster ins Netz speiste, wer ist Anbieter zweiter Ordnung (der sie verbreitete) und wer hat technisch und rechtlich die Kontrolle über den Replikationsvorgang? Es wird schwieriger, dem Autor seine (Text-)Symbole zuzurechnen, und es wird auch schwieriger, die Institution zu identifizieren, der man vertrauen kann.

Institutionen, Gruppen, Un-Strukturen

Auffällig an den Veränderungen im modernen Internet ist auch, dass die festen Strukturen von Institutionen, die wir bisher kennen, um neue Strukturen und höchst amorphe Gebilde ergänzt werden, die neu für uns sind. Wo wir es gewohnt sind, einzelne Personen, privatwirtschaftliche Unternehmen und staatliche Organe sowie bestimmte Sonderfälle wie NGOs zu erkennen, finden wir nun Personenanordnungen, die für uns in der digitalen Welt neu sind und die wir im Recht nicht als eigenständige Phänomene sehen.

Wenn Nutzer beispielsweise auf einem Fotodienst Fotos markieren, sprechen wir gern von ihnen als der »*Crowd*«. In manchen Konstellationen, wenn ein gemeinsam nutzbares Gut entsteht, wird neuerdings auch auf den Begriff der *Allmende* zurückgegriffen. Dieses Phänomen der Crowd ist neu in der digitalen Welt und es kann über Macht verfügen. Vielleicht muss man es in der Dichotomie zwischen Privatheit und Öffentlichkeit zu Letzterer zählen. Aber kann sie nicht zugleich auch ein neues soziales Gefüge sein, das eigene Informationen hat, die innerhalb der Crowd bleiben sollen?

Und: Wer ist hier im klassischen Sinne der Autor des Inhalts, wer ist das Subjekt, dem wir vertrauen können? Offensichtlich verbindet die Personen nur ein abstraktes Ziel, dass man ihre Fotos mit bestimmten Schlüsselwörtern wiederfinden möge. Aber ein gemeinsames Zusammenwirken dieser Art ist neu in der digitalen Welt, obwohl wir bei genauem Hinsehen Ähnliches von den Wegzeichen der Wanderer kennen, die in Einzelarbeit und ohne Kenntnis voneinander an einem gemeinsamen Zweck arbeiten. Anders etwa bei

einem Wiki, das der Entdeckung von Plagiaten dient: Hier verfolgen die Beteiligten einen klaren gemeinsamen Zweck, der ein Anfang und wohl auch ein Ende hat, und gehen arbeitsteilig vor. Entsprechendes gilt, wenn Nutzer gemeinsam an Landkarten arbeiten. Anders wieder, wenn sich ein sogenannter »Twitter-Shitstorm« ad hoc bildet, sich binnen Stunden explosiv entwickelt, um sich sodann wieder niederzulegen. Hier gab es vielleicht keinen gemeinsamen Zweck und hier ist vielleicht nicht einmal ein Ende auszumachen – wann sind »Gespräche der Gesellschaft« (z. B. über Staatsverschuldung) zu Ende? Ergebnis: *Wir finden Anordnungen von kommunizierenden Menschen vor, deren Dauer sehr unterschiedlich sein kann, deren Zweck mehr oder weniger bestimmt ist, von Menschen, die mehr oder weniger voneinander wissen und deren soziale Bindung unterschiedlich stark sein kann.* Auf der einen Seite bestehen beispielsweise langfristige Aktivitäten mit einem bestimmten klaren und gemeinsamen Zweck und enger sozialer Bindung der Beteiligten, man nehme nur das gemeinsame Hochladen von Bildern einer Feier und das Taggen dieser Bilder. Auf der anderen Seite finden wir Aktivitäten, die entweder kurz sind oder die gar kein definiertes Ende haben, die keinen definierten Zweck haben und bei denen die Beteiligten keinerlei Bindung eingehen und womöglich auch gar keine Kenntnis voneinander haben. Was wir im öffentlichen Raum noch als »Ansammlungen« oder »Versammlungen« kennen, zeigt sich in der digitalen Welt als amorphes »Etwas«, als dynamische »Un-Struktur«. Hinsichtlich dieser Beobachtungen ist unser Konzept von Sphären und Personas wohl noch nicht leistungsfähig genug. Und das, obwohl es dank Technik schon lange Lebenssituationen gibt, in denen Menschen soziale Strukturen wie in einer wissenschaftlichen Laborsituation herausbilden – beispielsweise 1.000 Personen, die als 1er-, 2er-, 6er-Gruppen an Bord eines Überseedampfers gehen und nach sechs Wochen mit veränderten Gruppenstrukturen das Schiff verlassen, um danach in einem »Melting Pot« wiederum Veränderung zu erfahren.

Im Extremfall wissen die Beteiligten nicht einmal, dass Daten gesammelt und bestimmten Zwecken zugeführt werden, beispielsweise bei Stauwarnern, die Bewegungsdaten übermitteln. Dieser Effekt wird sich mit dem *Internet of Things* verstärken, wenn noch mehr Dinge miteinander kommunizieren und erst recht niemand mehr weiß, warum und worüber und welche Schlüsse sie dabei ziehen. So wurde heute schon bekannt, dass sogenannte »Smart Meter« über den Stromverbrauch sogar das abgerufene Fernsehprogramm erkennen lassen, wenn die Messung sehr genau ist.[3]

Mega-Öffentlichkeit, Query-Öffentlichkeit, Unsichtbarkeit

Die Öffentlichkeit, die durch das Internet entsteht, hat nie gekannte Ausmaße. Jede Webseite, die nicht explizit einem geschlossenen Benutzerkreis zugeordnet wurde, kann von Milliarden Menschen eingesehen werden. Zusätzlich überwindet sie unsere gelernten Erfahrungen von Distanz und Nähe: Wir können in Sekunden zwischen New York, Rio und Dänemark hin und her klicken. Und schließlich überwindet das Web auch zeitliche Vorstellungen, denn grundsätzlich muss man sich die Daten unbegrenzt haltbar vorstellen. Diese drei Phänomene kennzeichnen *»Mega-Öffentlichkeit«*, die uns noch fremd ist. Dabei ist paradox, dass auch die Öffentlichkeit unseres Hauses unbegrenzt ist: Es kann ja jeder US-Bürger, jeder Brasilianer und jeder Däne an ihm vorbeispazieren und uns ins Fenster schauen.

Bezüglich unseres Hauses sind wir aber doch recht sicher, dass außer ein paar Nachbarn und Menschen, die nicht weit von uns wohnen, niemand vorbeischauen wird. Dieses Urvertrauen fehlt uns im Digitalen, obwohl die Verhältnisse dort nicht anders sind: Es kommt ja nur auf unsere Website, wer sie angesteuert hat (in der Regel über eine Suche, »Query/*Anfrage-Öffentlichkeit«).* Anders formuliert: Wie weit die Öffentlichkeit tatsächlich reicht, entscheidet der Empfänger.

Im Unterschied zur alten Welt jedoch wird er, der Empfänger, normalerweise nicht gesehen, während er selbst sieht und beobachtet. Die *Unsichtbarkeit des Sehenden* ist also ein weiteres Phänomen.

3 http://www.heise.de/newsticker/meldung/Smart-Meter-verraten-Fernsehprogramm-1346166.html

1.2.3 Spezielle Phänomene

Große Kommunikationsdienste / Plattformen

Das Internet hat schon seit Anbeginn die Möglichkeit geboten, auf Basis definierter Protokolle und Formate (E-Mail, FTP, WWW …) eigenständige Serverapplikationen aufzusetzen, um anderen die Möglichkeit zur Kommunikation zu bieten. Die drei Datenstrukturen Kommunikationsdaten, Personendaten und Verhaltensdaten finden sich schon in den alten Foren (Bulletin Boards), in denen Nutzer kommunizierten. Dabei mussten sie sich häufig anmelden, was Nutzerdatenspeicherung zur Folge hatte, zudem wurden über Logfiles einfache Zugriffsprotokolle erstellt.

Mit Auftreten der großen Web-2.0-Dienste, vor allem großer sozialer Netzwerke, kam es jedoch zu einer quantitativen Veränderung, die man als qualitativen Sprung ansehen muss: Wo jeder zweite Bürger der Onlinepopulation, zumeist unter Klarnamen, in einem einzigen großen Dienst mit anderen kommuniziert, entstehen zusätzlich zu den eigentlichen Kommunikationsinhalten aussagekräftige Interessensprofile und Muster der sozialen Interaktion und der Interaktion mit allen Systemteilen, die tiefe Analysen seines Verhaltens zulassen.

Umgekehrt prüfen die Anbieter der Dienste mit hohem Aufwand Beiträge von Nutzern auf verschiedene Rechtsverletzungen und Verletzungen von Nutzungsbestimmungen, und sie schalten Profile frei, erteilen Hinweise oder »Verwarnungen« und deaktivieren Nutzerprofile. Dies erfolgt, um eigener Haftung zu entgehen und den Nutzen des Dienstes zu erhöhen. In kommunikativer Hinsicht nehmen diese Anbieter aber auch eine Sonderstellung in der Kommunikation ein und sind vielleicht als Letztinstanz in einem freiwilligen und somit privat-vorstaatlichen Mechanismus einer mehrstufigen Selbstkontrolle anzusehen. Man könnte sie also statt als potentielle Täter von Verletzungen der Privatheit ebenso als ordnendes und schlichtendes Element begreifen oder installieren.

Diese Anbieter können auch als Treuhänder von Daten anzusehen sein, denen die Daten von Nutzern anvertraut werden. Es gelten jedoch drei Besonderheiten: Zum einen haben Anbieter zusätzlich generell vollen Zugriff auf Verhaltensdaten. Das Paradoxon ist daher, dass der Nutzer, indem er vertrauensvoll handelt, gerade hierdurch erst ein wesentliches Risiko schafft. Zum anderen haben die Anbieter für die Zukunft der Nutzung die Herrschaft über die Mechanismen der Plattform und können so faktisch (Änderung von Privatsphäre-Einstellungen, neues Funktionsmodul) oder rechtlich (Nutzungsbestimmungen) starken Einfluss auf die künftige Handhabung von Privatheit und Öffentlichkeit nehmen. Schließlich gibt es Schnittstellen- und Plattformkonzepte, bei denen die Anbieter Dritten eine gewisse Vertrauensstellung gewähren. Eine App, die auf Daten eines sozialen Netzwerks mit Zustimmung des Nutzers zugreift, holt sich zwar dessen Zustimmung, auf korrekte Funktion kann der Nutzer aber nur vertrauen, weil die App bis zu einem gewissen Punkt durch den (Plattform-) Anbieter zertifiziert ist.

Es fällt auf, dass die Anbieter hinsichtlich des Gefährdungspotentials sehr ähnlich wie E-Mail-Hoster zu beurteilen sind. Wir haben uns nur bei Letzteren daran gewöhnt, dass unsere E-Mails über Server Dritter versandt werden (und das auch noch zumeist im Klartext), genauso wie wir uns längst daran gewöhnt haben, Transaktionsdaten an Banken und Kommunikations- oder Bewegungsdaten an Telekommunikationsunternehmen zu liefern. Die Besonderheit ist aber, dass die Anbieter der neuen digitalen Dienste erstens neuartige und noch nicht verstandene Funktionen entwickeln (Beispiel: Geokoordinaten über WLAN) und zweitens neue soziale Praktiken prägen (Beispiel: Check-ins, Foodspotting …) – und dies auch noch in einem atemberaubenden Tempo, denn soziale Netzwerke stießen erst 2007 auf Masseninteresse. Es kann daher nicht verwundern, dass es durch das Handeln der großen Internetdiensteanbieter zu gesellschaftlichen Friktionen kommt.

Aus subjektiver Sicht der meisten Nutzer ist allerdings zweifelhaft, ob es wirklich ein Konzept von »Plattform« im Sinne eines abgegrenzten Bereiches

gibt. Zwar ist die Software eine geschlossene, abgegrenzte, doch ist für eine einzige Person völlig unklar, was außer der von ihr selbst bestimmten Daten öffentlich ist und was privat. Aufgrund komplexer Privatsphäre-Einstellungen wird ein greifbares Bild von »Räumen« nämlich verhindert. Ebenso ist aufgrund von Datentransfers zwischen Plattformen manchmal nicht klar, welche Daten zu welcher Plattform »gehören«. *Es gibt also kein genaues Bild von Systemgrenzen, »Plattformen fransen aus«, was uns den Umgang erschwert.* Wo das Ziel der Plattform ist, mit granularen Einstellungen maximalen individuell-situativen Schutz zu erreichen, verhindert genau dieses aber ein klares Bild der Situation, weil man nicht »Herr Alles-Sieht« ist.

Verschränkung von Kommunikation und Transaktion

In der heutigen Internetwelt sind Transaktionswebsites (insbesondere E-Commerce) von Kommunikationsdiensten getrennt und nur mit Links verknüpft (z. B. ein Facebook-Link auf einen Shopartikel). Zu den Sharing-Funktionen, die diese Links erzeugen, sind aber in jüngerer Zeit kaum merklich andere Daten hinzugekommen: Shares werden gezählt (»Anzahl Tweets«), im E-Commerce-Umfeld tauchen über Social Plug-ins Kontaktlisten auf. Aufgrund der Kundenwünsche, die gern nach Empfehlung kaufen, und der Wünsche der Anbieter, die gern mehr verkaufen, werden sich diese beiden Welten in den nächsten Jahren stark verschränken. Wir wissen noch nicht, welche Formen dies genau annehmen wird. Es ist jedoch naheliegend (Phänomen blippy.com, iTunes-Käufe auf Ping), dass Käufer bestimmter Schichten und Produkte eine weitere Datenspur der Transaktionsdaten im Web hinterlassen werden. Dies bedeutet, dass ein bisher eher als privat empfundener Bereich nun teilweise öffentlich wird. Eventuell werden wirtschaftliche Anreize die Nutzung beschleunigen (»3 % auf Ihren Kauf, wenn Sie ihn Ihren Freunden erzählen«). Bei Spezialanbietern in sensiblen Bereichen, aber auch bei Vollsortimentern kann es zu unerwünschter Veröffentlichung kommen, sei es technisch bedingt oder durch Fehlverhalten der Nutzer.

Daten als Tauschgut

Seit Einführung werbefinanzierter Internetangebote hat sich die Sicht geprägt, der Nutzer eines Dienstes bringe seine Daten gegen eine Leistung des Diensteanbieters ein. Dies gilt nicht nur, soweit die Auslieferung von Werbung in irgendeiner Weise maßgeschneidert ist, sondern auch wenn andere Verwertungsformen (z. B. Direktansprachemöglichkeit durch Headhunter) bestehen oder der Anbieter selbst wiederum Nutzerdaten handelt. Hier ist zum Teil ein komplexes ökonomisches Verwertungssystem entstanden, das auf diesem Grundmechanismus basiert.

Außer den naheliegenden Perspektiven des klassischen Datenschutzes sind hierzu weitere Aspekte zu sehen, die unsere Gesellschaft künftig beschäftigen könnten. Erstens könnte es Menschen geben, die aus finanziellen Gründen faktisch gezwungen sind, ihre Daten zur Verwertung anzubieten. Der wohl geringe wirtschaftliche Wert von einigen Euros ist nach der gegenwärtigen Schutzsystematik kein Grund, das Problem zu geringschätzen, denn maßgebliche Konsequenz ist die Preisgabe eines Freiheitsrechtes. Zweitens könnte dieser Tauschaspekt den Umgang mit Daten im digitalen Zeitalter generell ändern. Drittens entstehen neue Geschäftsmodelle, z. B. treten Dritte als Treuhänder von Daten auf oder Anbieter veröffentlichen Kaufdaten und entgelten dies dem Käufer. Viertens könnte ein echtes »do ut des« die Tätigkeit der Diensteanbieter selbst ändern – sei es, dass sie den Nutzer als Kunden begreifen, sei es, dass sie sich, um Kunden zu gewinnen, auch in dieser Hinsicht in Wettbewerb geben, beispielsweise dadurch, dass sie den Nutzern mehr Rechte in den Nutzungsbedingungen zuweisen.

De-Publizierung

Die Aussage »Das Internet vergisst nichts« mag als pädagogisch intendierter Rat richtig sein, fachlich ist sie in ihrer Unbedingtheit falsch. Ganze Dienste werden vom Netz genommen, weil die Unternehmen insolvent sind. Ein Beispiel wäre die Community X. Einzelne Onlineprodukte rechnen sich nicht und werden eingestellt. Verlagspublikationen werden eingestellt. Bei technischen

Relaunches werden Kommentare nicht übernommen. Nutzerkommentare von E-Commerce-Shops verschwinden, weil jährlich 30 % des Artikelstammes aus dem Sortiment genommen werden. Öffentlich-rechtliche Anstalten sind zur Depublikation verpflichtet. Unternehmen nehmen alte Websites vom Netz, weil sie einen Relaunch machen. Vorstände begrenzen Archivdauern der Websites auf gesetzliche Fristen, so dass ältere Pressemitteilungen verschwinden. Wer findet heute noch die Geschichten der sogenannten »New Economy«?

Die Konsequenz dieser Erkenntnis ist, dass im digitalen Medium (genauso wie bisher auch) bestimmte Teile von Kommunikation verschwinden können, welche mit Privatheit zu tun haben. Zu denken ist an die oben genannte De-Kontextualisierung, zu denken ist aber auch daran, dass explizite Klarstellungen oder gezielte Störinformationen verschwinden. Wenn also – wie im »echten Leben« auch – es dem Betroffenen gelang, seinen Aufenthaltsort vorzutäuschen, weil er hierzu Grund hatte, könnte es sein, dass genau diese Handlung durch De-Publikation verschwindet und somit die Ur-Darstellung allein steht.

Unfreiwillige Öffentlichkeit / Intentionalität

Wer kennt sie nicht, die vielen Geschichten versehentlich öffentlich geposteter Veranstaltungseinladungen oder die für privat bestimmten Statusmeldungen von Politikern. Hinzu kommt die Kategorie unverstandener Privatsphäre-Einstellungen sowie allgemein unverständliches Zusammenwirken verschiedener Software-Module (Geolokation auf OS-Ebene, auf Browser-Ebene, auf Dienste-Ebene).

Zu den nicht intendierten Privatsphäre-Verletzungen gehören ebenso Daten, die ein anderer bereitstellt, beispielsweise Kontaktdaten bzw. Adressbücher, die Daten Dritter enthalten, von denen der Hochladende aber glaubt, sie seien »mein Adressbuch«, und die Rechtsverletzung gar nicht wahrnimmt.

Ein drittes Phänomen stellen Daten dar, bei denen sich der Veröffentlichende nicht darüber im Klaren ist, dass diese Daten im Zusammenhang mit anderen Daten bestimmte Schlüsse zulassen. Beispielsweise könnte man aus einer Abfolge von Einkäufen und einem abendlichen Tweet schließen, dass der Akteur ein Candle-Light-Dinner mit einer Blondine hatte und was man hierbei aß.

Ein viertes Phänomen liegt vor, wenn maschinelle Verfahren unser Verhalten analysieren und dabei Wahrscheinlichkeiten zutage fördern, die uns gar nicht bekannt waren. Beispielsweise lässt sich die Eigenschaft eines Mannes, dass er homosexuell ist, mit einer hohen Wahrscheinlichkeit aus seinem sozialen Graphen schließen, wenn unter seinen Freunden einige als homosexuell bekannt sind (MIT 2007). Auch die Trinkgewohnheiten lassen sich beispielsweise erfassen, wenn jemand häufig schreibt, was er gerade trinkt, welche alkoholischen Getränke er gerade gekauft hat, wenn er Bilder postet, unter denen Dritte Schlüsselwörter wie »betrunken« posten.

Ausschluss, Verabseitigung, Anonymisierung, Verschlüsselung, Verstecken

Es gibt eine Reihe von bekannten Verfahren, wie im Internet Privatheit hergestellt wird. Das einfachste Verfahren besteht in der Wahl eines Kommunikationsmittels, das die Kommunikation prinzipiell nur mit definierten Empfängern voraussetzt, beispielsweise E-Mail oder Chat. *Ausschluss* undefinierter Teilnehmer findet aber auch statt bei geschlossenen Benutzergruppen, z. B. in Foren. Zu den IT-technischen Mitteln gehört ebenso, die gesamte Kommunikation in einen abseitigen Bereich zu verlegen, beispielsweise durch Benutzung eines seltenen Ports. Künftig kann auch eine Möglichkeit darin bestehen, sich ein eigenes Netzwerk aufzubauen – Ad-hoc-Mash-ups, neue Wireless-Dienste mit hoher Reichweite und Body-to-Body-Networks[4] können die gesamte Situation verschieben, indem sich viele Menschen für bestimmte Zwecke aus dem Internet ausschließen.

4 http://www.wired.com/epicenter/2010/10/people-could-carry-future-phone-network-nodes/

Während der Inhalt auf den genannten Wegen jedoch leicht ermittelt werden kann, gehen zwei weitere Techniken weiter: *Anonymisierung* verschleiert die Identität der Teilnehmer, *Verschlüsselung* codiert die Kommunikationsinhalte selbst mit einem Schlüssel, der nur berechtigten Personen zur Verfügung stehen soll. Eine weitere Möglichkeit besteht darin, die Information zu *verstecken*. Das geht entweder mit hergebrachten Verfahren wie Geheimschriften und Geheimsprachen, aber auch mit neuen digitalen Mitteln, z. B. indem man die Information mit technischen Mitteln so in andere einbettet, dass sie nicht ohne Weiteres erkannt wird *(Steganographie)*.

Bei der Entwicklung dieser Techniken ist auffällig, dass es fast immer aufdeckende Gegenmittel gibt, vom Abhören unverschlüsselter Mails über den Port-Scanner bis hin zur Steganalyse und Kryptanalyse. Absolute Privatheit, die nicht gebrochen werden kann, gibt es im Internet nicht; selbst ein guter Anonymisierungsdienst kann nur dann nicht abgehört werden, wenn man ihn selbst betreibt. Es ist heute nicht vorhersehbar, wer im Kampf der Methoden und Gegen-Methoden die Oberhand haben wird. Vielleicht werden sogar aufdeckende, die Privatheit brechende Verfahren eines Tages jedermann zur Verfügung stehen.

Blockade, Desinformation, Noise

Neu bei den modernen Kommunikationsmitteln ist, dass man ihr Funktionieren durch Einflussnahme auf die Infrastruktur stören kann. Was man beim Handy schon als Störsender oder »Handy-Blocker« kennt, geht auch bei Funksignalen aus WLANs und anderen Funknetzen, welche diese Internetprotokolle nutzen. In der Zukunft ließe sich so beispielsweise gezielt eine Nutzung an bestimmten Geokoordinaten unterbinden. Dies ist freilich eher ein Instrument digitaler Kriegsführung.

Grundsätzlich ist dies aber auch für den Privatnutzer denkbar, die Kommunikation von Endgeräten anderer auf diese Weise mit einem »*Internet-Blocker*« zu blockieren; in einem Café könnte man mit Störsender oder Internet-Blocker das Twittern nach außen blockieren und auf diese Weise eine Sphäre sichern. Ein ähnliches Phänomen zeigt sich bei einem Patent, wo das Handy aufgrund seiner Standortinformation die Kamera deaktivieren kann; dies könnte Aufnahmen von Musikveranstaltungen und Ähnliches verhindern und so also eine Sphäre Dritter schützen. Technologie spannt hier also einen Schutzschirm auf, der sowohl zum Schutz von Intellectual Property als auch zum »Sphären«-Schutz verwendet werden kann.

Ein weiteres Phänomen ist gezielte *Desinformation*. So ist es ein Leichtes, durch alte Fotos ein falsches Bild zu vermitteln oder durch Software falsche Geokoordinaten zu generieren. In Zukunft sind Automaten und Robots für solche Tätigkeiten gut geeignet, um programmiert bestimmte desinformierende Datenstrukturen zu hinterlassen. Auf diese Weise können falsche und irreführende Daten erzeugt werden – nichts anderes macht ja heute schon derjenige, der bei Registrierungsformularen bewusste Falschangaben macht, um seine Privatsphäre zu schützen.

Sobald Maschinen diese Aufgaben übernehmen, wird es auch möglich sein, ein Informationsrauschen zu erzeugen, das andere Informationen überdeckt. Um ein heute mögliches Verfahren zu nennen: Ein Browser-Plug-in könnte vordefiniert und automatisch so lange verschiedene Webseiten aufrufen, bis die vorgetäuschten Interessen von der Profiling-Engine des Werbevermittlers für die maßgeblichen gehalten werden. Nicht absichtsvoll, sondern zufällig erzeugte Desinformation könnte man als Informationsrauschen oder *Noise* bezeichnen. Zehn vom Nutzer eingegebene Abfragen gehen in 150 von der Maschine erzeugten Abfragen unter, die eine falsche Datenspur legen. So ähnlich arbeitet seit 2005 schon das Browser-Plug-in *TrackMeNot*, das die Interessen-Erkennungsmechanismen von Suchmaschinen irritieren soll, indem es maschinell neue Suchabfragen erstellt. Setzt man das Plug-in jedoch in Deutschland ein, wird eine Pointe deutlich: Aufgrund der falschen Abfragesprache können die Abfragen von der Suchmaschine erkannt und ignoriert werden. Die Tarnkappe funktioniert also nicht. Niemand weiß, ob es eines Tages gelingen kann, jegliche Datenspuren mit Fehlinformation zu

verwischen. Sobald aber die Spuren Muster aufweisen, wird die Verdeckungsabsicht deutlich und der Nutzer ist enttarnt. Es ist ein Katz-und-Maus-Spiel der Algorithmen, Spion und Spion.

Algorithmik

Ein weiteres Phänomen ist die Gewinnung von Daten aus bestehenden Daten mit Hilfe von Logik oder Algorithmen in Verbindung mit anderen Daten. Man könnte hier neben den freiwillig abgegebenen Daten und den observierten Daten auch von abgeleiteten Daten sprechen.

So können etwa Wahrscheinlichkeitswerte zu Bonität, Krankheiten und Kriminalität aus der Gesamtbetrachtung von Personendaten und Statistiken erstellt werden. Dies erfolgt mit Bonitätsdaten schon lange im E-Commerce zum Nutzen der Beteiligten. Ebenso lassen sich gesundheitliche Risiken aus Statistiken der Luftüberwachung ableiten. Über tiefe Textanalyse können beliebige Objekte analysiert werden, z. B. Reisedaten von Personen (vgl. recordedfuture.com) und anderes mehr.

Wir können derzeit nicht absehen, wie leistungsfähig und aussagekräftig die Verfahren der Zukunft sein werden. Neben den vielen Chancen zeigen sich aber auch Risiken. Zum einen werden maschinelle Hinweise gegeben, hinsichtlich welchen Aspektes eine Person genauer zu betrachten ist, so dass die Chance, ein privates Faktum aufzudecken, deutlich steigt. Beispielsweise könnte man religiöse Minderheiten aufgrund ihres Einkaufsverhaltens eventuell gut erkennen. Und wo maschinelle Schlüsse plausibel sind, etwa hinsichtlich der Kriminalitätsrate einer Person, bewirken diese Hinweise tatsächlich ein Verhalten der Umwelt, das dieselben Konsequenzen wie die Aufdeckung eines tatsächlichen Faktums haben. Wer von einem Fraud-Detection-System der Zukunft als »wahrscheinlich ein Dieb« klassifiziert wird, wird die Handschellen sehen, die er als Dieb erhalten hätte. Wir haben es also bei zutreffenden Schlüssen mit einer Aufdeckung des Ungewollten zu tun und bei falschen Schlüssen mit der Wiedergeburt des menschlichen Vorurteilswesens mit maschinellen Mitteln.

Inhalteüberwachung

Relativ jung ist die Inhalteüberwachung, die im digitalen Raum wegen maschineller Verfahren die Inhalte von Kommunikation weitgehend analysieren kann und die somit ein Sonderfall der Algorithmik ist. Schon bei der Untersuchung von Mails werden für werbliche Zwecke Interessensprofile erzeugt; dies ist kein Geheimnisbruch, da die »Einsicht« durch »nichtsehende« Maschinen geschieht und Informationen mit Kenntnis des Absenders in die Sphäre des Betreibers geraten, der diese Maschinen betreibt. Ein ähnliches Problem tritt bei maschineller Erkennung von Spam und Fake-Profilen auf, hier wird vor allem in sozialen Netzwerken die Kommunikation inhaltlich analysiert, was ebenso bei Social Media Monitoring Anwendung findet. Schließlich sind – neben Kriminellen – auch Staaten mit der maschinellen Inhalteanalyse befasst, wobei hierzu auch Schnittstellen bereitgestellt werden. Unter dem hier betrachteten Gesichtspunkt ist evident, dass alle diese Anwendungen eine Softwaregattung vorantreiben, die das Potential hat, sphärenüberschreitenden Informationsfluss auszulösen, der von Absendern und Betreibern nicht gewollt ist, und somit zu schwerwiegenden Konsequenzen führen kann. Beispielsweise ließe sich, um nur den Fall öffentlich verfügbarer Information zu betrachten, anhand gecrawlter Filmrezensionen und mit statistischen Daten über das Ausleihverhalten homosexueller Frauen die Homosexualität einer Autorin mit hoher Wahrscheinlichkeit vermuten.

Automatisierung

Ein neueres Phänomen sind auch Applikationen, die halb- oder vollautomatisch Daten sammeln, welche der herkömmlichen Privatsphäre zuzurechnen sind. Einige dieser Applikationen veröffentlichen diese Daten auch. Beispielsweise publiziert blippy.com Transaktionen, die mit Kreditkarten getätigt wurden (Vorläufer ist Apples Ping), voyuurl.com veröffentlicht URL-Folgen von Browsersessions, GPS-Tracker speichern Geokoordinaten für Dinge aller Art (insbesondere Autos) und Personen, Facebook zeichnet gelesene URLs sowie Bücher, Musik und Filme auf und veröffentlicht diese in der Timeline.

Zusätzlich zu diesen technischen Phänomenen beginnen Menschen, mit *Selftracking* ihre Lebensgewohnheiten und Fähigkeiten zu messen und zu analysieren, wie im Portal quantifiedself.com. Beispielsweise werden Schlafgewohnheiten in Relation zu Lebensgewohnheiten gemessen, Wissenslücken bei Quizzes maschinell erkannt, Launen auf mögliche Ursachen geprüft, Surfverhalten optimiert und Sport sowie Essensgewohnheiten und Körpergewicht analysiert. Hierzu wird zum Teil spezialisierte Hardware (insbesondere *Sensoren)* verwendet, die künftig auch in Kleidung als *Wearable* eingebettet sein kann und für die ferne Zukunft als *Implantat* diskutiert wird. Diese modernen Ideen haben ihr unbestritten sozial adäquates Pendant im Gesundheitswesen *(M-Health),* bei dem Herzfrequenzen, Blutdruck, Position und andere medizinische Werte an Server übermittelt werden, beispielsweise bei Demenzpatienten.[5]

Alle nicht medizinisch motivierten Verfahren sind gesellschaftlich umstritten. Viele Nutzer und Unternehmen erwarten neuartige Erkenntnisse und halten die aktuellen Phänomene für den Vorboten des Datenschattens, der uns künftig in der *Ambient Intelligence* begleiten wird, und halten diese Entwicklung für die logische Fortsetzung der Erfassung öffentlich zugänglicher Bilddaten. Erste Kritiker warnen vor einer Veränderung, die soziale Zwänge auslöst, ohne dass die Folgen absehbar wären.

Anonymität und Pseudonymität, De-Anonymisierung

Anonymität und Pseudonymität gibt es nicht erst seit Erfindung des Internets, doch auch sie bereiten strukturelle Probleme, je genauer man hinsieht. Denn beide Konzepte gibt es nicht isoliert, sondern es kann sie nur in Bezug auf andere Menschen geben: Während es einerseits dem Bergbauern vielleicht in seinem kleinen Umfeld gar nicht möglich ist, anonym aufzutreten, kann dies

5 http://ne-na.de/medica-web-armbanduhr-fuer-demenz-patienten-sensoren-ueberpruefen-vitalfunktionen/001132

für denselben Bergbauern in einer fremden Stadt die Regel sein, da ihn dort niemand erkennt. Beide Konzepte setzen nämlich mindestens eine weitere Person voraus, den Wissenden bzw. Nicht-Wissenden. Dieser kann die Identifikation der Person entweder gar nicht vornehmen (Anonymität) oder er gehört als Wissender zu einem begrenzten Personenkreis, der die Identität dieser Person anhand von Merkmalen erkennen kann, während der Nicht-Wissende die Identität nicht erkennen kann. Dabei ist der Name der Person der naheliegendste Fall möglicher Merkmale: einen *Anonymous* scheinen wir nicht zuordnen zu können, einen *Peter Pan* hingegen schon. Was aber, wenn es nur eine Person gäbe, die sich Anonymous nennt, und zehn, die sich Peter Pan nennen? Wie man sieht, dreht sich auch die Identifizierbarkeit um, weswegen es genau genommen auf die Bedeutung des Namens nicht ankommt. Allein entscheidend ist, ob wir eine eindeutige *Adressierung* einer Person vornehmen können, und dabei kann es statt eines Namens auch ein ganz anderes Merkmal sein, z. B. einmalig eindeutige Kleidung, ein Apfel auf dem Kopf, ein roter Hahnenkamm, die jeweils als Adressierung dienen. Hinzu kommt, dass die Adressierung so weit von Dauer sein muss, dass ein Wiedererkennen möglich ist: Die Rose im Knopfloch hilft beim Blind Date, den Partner zu erkennen, hebt aber dessen Anonymität erst auf, wenn er sie bei einer weiteren Gelegenheit trägt, so dass wir die Person als bekannt erkennen. Adam und Eva wären also auch dann nicht anonym gewesen, wenn sie sich keine Namen gegeben hätten – ein Wiedersehen genügt.

Vielleicht muss man also sagen, dass Anonymität der theoretische Urzustand ist, der so lange aufgehoben ist, wie sich eine Person innerhalb einer sozialen Struktur bewegt und mit anderen interagiert. Wer dann wieder anonym sein will, muss sich dorthin begeben, wo sich sein gewohntes Personenumfeld nicht befindet – und so ist das Weggehen in eine andere Stadt, ein anderes Land oder auf einen anderen Kontinent der typische Fall des bürgerlichen Neuanfanges, der mit Anonymität wieder beginnt.

Im Internet dienen Anonymität und Pseudonymität zunächst dem Schutz der Person. Ihre Identität soll nicht für alle (= öffentlich) erkennbar sein – es

entsteht also Privatheit als ein Für-sich-Sein bzw. Untereinander-Sein. Dabei taucht eine Reihe von Phänomenen auf. Erstens ist dieser Schutz unabhängig vom Zweck der Handlung, kann also auch böser Absicht dienen. Ein Beispiel: Derselbe Lehrer, dessen Pseudonymität ihn eben noch vor seinen Schülern schützte, kann diese eine logische Sekunde später nutzen, um verbotene Bilder von Schülerinnen herunterzuladen. Anonymität und Pseudonymität sind also zwangsläufig ambivalent, je nach Absicht der Person. Zweitens gibt es technische Mittel, die Anonymität aufzuheben, wie Gesichts-, Stimm- und Texterkennung, was im Nachhinein den Schaden stark erhöhen kann, weil der Betroffene sich gerade in der Annahme, geschützt zu sein, sehr klar artikuliert hat. Drittens kann man in der Komplexität des Internets schon einmal »versehentlich die Tarnkappe verlieren«, was zum selben Ergebnis führt. Viertens setzt Kommunikation ein Wiedererkennen von Absendern der Kommunikationsakte voraus, weswegen auch der anonyme Nutzer sich wiedererkennbar zeigen muss und so womöglich einzigartige Merkmale preisgibt, zumal Kommunikation auf ihre Fortsetzung angelegt ist. Und fünftens behaupten viele, mit anonymen Personen sei im Vergleich zu identifizierten Personen nur weniger Vertrauen zwischen den Beteiligten möglich. Gerade hier ist die Anonymität aber zugleich ein Stück »*Privacy in Public*«, in der die Beteiligten sich mehr anvertrauen können, weil sie sicher sein können, dass der Kontakt ohne ihr Zutun nicht das digitale Medium verlässt. Es scheint also die Schutzwirkung der Anonymität zum einen von der Absicht der Beteiligten und zum anderen von der Ein- bzw. Mehrseitigkeit der Beziehungen abzuhängen.

Ein weiterer Aspekt ist, dass ein *Identitätswechsel* aufgrund einiger Phänomene zum Teil schwierig geworden ist. Zwar kann man im Extremfall für einen Neuanfang den Namen wechseln, doch machen öffentliche Fotos und bestimmte Profilinformationen es nötig, auch das Aussehen zu verändern. Von den ersten Fällen, in denen Polizisten ihren Aufgaben nicht mehr nachgehen können, weil sie aufgrund von Internetdaten gut identifizierbar sind, wird berichtet.[6] Auch anhand dieses Beispiels zeigt sich, wie ambivalent die Veränderungen sind, denn was der Erkennung von Tätern dienen kann, kann den Einsatz von Polizisten verhindern.

Mittel- und langfristig ist es fraglich, ob es Anonymität und Identitätswechsel überhaupt geben kann für Personen, die im Internet kommunizieren. Es gibt eine Reihe von Technologien, welche die Aufdeckung bezwecken. Beispielsweise wird in der *Autorenerkennung* (aus der forensischen Linguistik) versucht, Merkmale von Autoren mit Wahrscheinlichkeitswerten zu versehen und Autorenidentität mit Textvergleichen zu erkennen. Neben diesem gern »*sprachlicher Fingerabdruck*« genannten Prinzip gibt es auch den *technischen Fingerabdruck,* beispielsweise ergibt die Kombinatorik aus Browser- und Systemeigenschaften häufig eine eindeutige Identität (siehe panopticlick.com). Auch kann heute anhand sozialer Interaktionsmuster (wer kommuniziert wann mit wem worüber) eine Identität mit Wahrscheinlichkeiten versehen werden. Die *Augmented ID* befasst sich mit der Kombination aus Gesichtserkennung und zeigt dem Gegenüber Personendaten des Betrachteten. Fügt man nun noch die Erkenntnisse zu Algorithmen, Automatismen und *Ambient Intelligence* hinzu, sieht man die Entwicklung: Die Anzahl von Auslösern bzw. Sensoren steigt, die Einspeisung ins Internet nimmt zu, die Analysefähigkeiten von Software nehmen zu. Wer hier noch kommunizieren will, muss im Allgemeinen bleiben und sich in jeder Beziehung verwechselbar verhalten, so dass Kommunikationszwecke infrage gestellt werden. Wie soll ich meine Identität und ein Innen und Außen trennen, wenn ich mich nicht kommunikativ abgrenzen darf?

Big Data

Nach der mooreschen Faustregel verdoppelt sich die Anzahl der Transistoren je Chip in weniger als zwei Jahren. Grob gesagt verdoppelt sich Rechenleistung je Euro jährlich. Hinzu kommt leistungsfähigere Software, z. B. für Virtualisierung und Skalierung. Seit neuestem ist es möglich, 1 Petabyte (= 1.000 Gigabyte) an Daten innerhalb einer halben Stunde zu sortieren; für diesen Rekord wurde die Aufgabe auf einem System von 8.000 Servern verteilt.[7]

6 http://blog.zdf.de/hyperland/2011/09/das-ende-der-anonymitaet-im-netz-auch-fuer-polizisten/

7 http://business.chip.de/news/Google-So-werden-1-Petabyte-an-Daten-sortiert_51591014.html

Was Techniker »Big Data« nennen, also neuerdings mögliche schnelle und günstige Auswertung sehr großer Datenmengen, bietet viele Chancen für die menschliche Gesellschaft. Einige davon sehen wir schon heute: etwa Live-Stauwarnungen auf Landkartendiensten, welche diese Daten aus den Positionsdaten der Fahrzeuge gewinnen, oder Statistiken und Prognosen über aufkommende Krankheiten mit regionalen und zeitlichen Angaben. Andere Dienste sind am Horizont sichtbar wie simultan funktionierende Echtzeit-Übersetzungen, die aus einer Vielzahl von Übersetzungen im Internet gespeist werden. Wieder andere, wie Hochrechnungen und Analysen gesellschaftlicher Trends (Beispiel: Berechnung makroökonomischer Trends) und politische Problemlösungen, können durch Kenntnis von Daten über komplexe Systeme und Strukturen erleichtert werden; die Gesetzgebung kann so empirisch fundiert werden (Stichwort: evidence-based policy). Aus einer gewissen Perspektive können hierunter eines Tages auch Abstimmungsdaten aus Bürgerbeteiligung und Ähnlichem fallen. Wir könnten aus vielen Quellen, insbesondere sozialen Netzwerken, neue empirische Daten erhalten und auswerten, um menschliches Sozialverhalten zu erforschen und so – pathetisch ausgedrückt – die »*Soziologie 2.0*« begründen.

Wir wissen heute noch nicht, wie hoch der Preis für solche Erkenntnisse sein wird. Wie auch sonst bei Datenbeständen bestehen hier Risiken, allen voran Missbrauch, fehlerhafte Anonymisierung und versehentlich oder absichtlich geleakte Veröffentlichung dieser Daten. Dabei könnte es sein, dass durch die Kumulation von Big Data mit anderen Phänomenen Probleme der De-Anonymisierung entstehen. Es ist nämlich nicht ganz klar, wie schädlich beispielsweise eine anonymisierte Liste aller ehemaligen Mieter eines Hauses ist (Wohnung, Zeitraum etc.), wenn das Haus nicht hundert, sondern nur vier Mietparteien hat. Würden nämlich hierzu nun weitere Big-Data-Töpfe zugemischt wie die Bonität und Krankheitsdaten, könnte man aussagekräftige Wahrscheinlichkeitsberechnungen darüber durchführen, wer als Rollstuhlfahrer im Erdgeschoss auszog und wer als »Besserverdiener« im selben Monat das Penthouse anmietete.

In jedem Fall bleibt eine – wenn auch sehr geringe – Wahrscheinlichkeit eines Datenunfalls, der möglicherweise ungekannte Auswirkungen auf die Privatsphäre von Millionen Menschen hat. Schon 1990 hatte der geplante Verkaufsstart von Lotus Marketplace, einer CD mit Datensätzen von 120 Millionen US-Haushalten, erhebliche Proteste ausgelöst. Big Data ist einerseits ein quantitatives Problem, hat aber auch eine qualitative Seite, weil auf neuen Anwendungsfeldern neue Daten genutzt werden, die *Data Value* haben, und weil Verschiebungen sozialer Strukturen denkbar sind, etwa wenn bei einer bestimmten Krankheit jeder erkrankte Bürger namentlich bekannt würde.

Raumüberwachung, Überwacher-Überwachung

Jedermann kennt heute das Thema der Videoüberwachung von Kunden und Mitarbeitern durch Privatunternehmen, aber auch durch Staatsorgane (vor allem an öffentlichen Plätzen), das vielerorts diskutiert wird. In jüngerer Zeit fügt sich hier ein neues Phänomen ein: *Bürger überwachen Bürger.* Auf der einen Seite sind Pennycams für jedermann günstig verfügbar (z. B. bei eBay und hier http://megaspy.net). Zum anderen werden Smartphones mit hochauflösenden Kameras der Regelfall sein, die bereits heute Videos (z. B. via UStream) live streamen können. Schließlich werden wir, getrieben durch die großen Internetanbieter, das Vordringen von Videotelefonie an den Arbeitsplatz und auch ins Heim erleben, so dass häufig Kameras mit Internetanschluss vorzufinden sein werden. Es ist nur noch eine Frage des Zeitpunktes, bis Kameras allerorts direkt ins Internet streamen können und auch von außen ansprechbar sind. Denn auch hier schreitet die Technik fort, WLAN-Technologie mit 16 Gigabit pro Sekunde ist noch in diesem Jahrzehnt zu erwarten.[8] Drahtlose Funknetze mit Reichweiten deutlich über die heutigen WLAN-Standards hinaus sind angekündigt.

8 http://blog.infotech.com/analysts-angle/peering-ahead-multi-gigabit-wireless-will-replace-cables/

Hinzu kommen noch zwei weitere Phänomene. Die oben schon angesprochene GPS-Signal-Ermittlung findet nicht nur bei Handys statt, sondern auch bei Fahrzeugen und bei Dingen, die wir wiederfinden wollen, z. B. Laptops (übrigens inklusive Datenübermittlung und Nutzerfoto vom Dieb). Entsprechende Technologien kommen für die Ortsbestimmung von Personen zum Einsatz, z. B. für Kranke und Kinder. In Kombination mit Gesichtserkennung und Auto-ID-Verfahren im Zusammenhang mit RFID-Chips ist damit der nächste Schritt sichtbar: Zu den Videos und Ortsangaben kommen Personendaten hinzu. Was wie eine zufällig entstehende Dystopie aussieht, wird in Teilbereichen schon erprobt: So gibt es etwa in den Niederlanden einen Pilotversuch, bei Nahverkehrsmitteln die Videoüberwachung um Gesichtserkennung zu ergänzen, damit über Datenbankabfragen Personen mit Hausverbot maschinell erkannt werden können.[9] In den USA wird der erste Gerichtsbeschluss kontrovers diskutiert, wonach ein GPS-Empfänger für polizeiliche Ermittlungen ohne richterlichen Beschluss zur Ortsbestimmung des Verdächtigen eingesetzt werden darf.[10] Unabhängig davon kann es vorkommen, dass Sicherheitsmängel es Dritten ermöglichen, sich der technischen Infrastruktur zu bedienen, beispielsweise Stalker für die Ortsermittlung ihrer Opfer.[11]

Neben diesen faktisch entstehenden oder beabsichtigten Veränderungen entwickeln sich weitere Phänomene: Unter *Policing the Police* wird das Phänomen verstanden, dass Bürger Polizisten überwachen (vgl. OpenWatch.net und den CopRecorder, »inverse Überwachung«). Ebenso entstehen Szenarien im Sinne einer *Bürgerwehr* oder militanten Gruppen, die andere Bürger überwachen (»Türken überwachen Kurden«). Und schließlich bleibt am Ende die Frage, ob nicht durch massenhafte Datensammlung von Bürgern und Unternehmen sich nicht die Diskussionslage um staatliche Überwachung verschiebt: *Outsourcing* staatlicher Überwachung an die Bürger.

Technische Entwicklungen verschieben also die Grenze des Möglichen. Ob es hierbei zu technischen Gegenmitteln kommen wird (siehe oben, z. B. Blockaden und Noise), ist unklar; bei der Videoüberwachung wird es kein sinnvolles Gegenmittel geben, da wir uns nicht ständig vermummen wollen. Es bleibt also eine Frage des Sollens und der Normsetzung, ob und an welcher Stelle des Entstehens diese Risiken eingedämmt werden sollen. Wir gehen derzeit davon aus, dass in zehn Jahren und mehr die faktischen Verhältnisse zu Veränderungen führen werden. Vielleicht müssen sich künftige Generationen sogar daran gewöhnen, dass sie außerhalb der von ihnen kontrollierten Räume ständig beobachtet werden können.

Schluss

Die Ausführungen der ersten Abschnitte haben gezeigt, dass das Internet als der dem Buch und den Massenmedien folgende mediale Umbruch nicht nur die Informationsverarbeitung der Menschheit allgemein verändert, sondern auch Auswirkungen auf Privatheit und Öffentlichkeit haben wird. Denn die Grenze zwischen beidem ist in vielerlei Hinsicht fließend und unscharf, und sie ist eine Grenze, die mit der Durchlässigkeit für Information unmittelbar zu tun hat. Wenn jede Information überall ist, gibt es keine Privatheit mehr. Private Information ist das, was im Innen ist und vom Außen getrennt ist; sie ist informatorische Differenz. Auch die bloße Erscheinung ist Information, sie kann mit Mitteln des Internets ebenso übertragen werden und diese Information wirft daher gleiche Fragen auf.

Das Internet bringt Mechanismen mit sich, welche die informationelle Trennung von Innen und Außen aufheben, z. B. weil Information zwischen gesellschaftlichen und technischen Systemen kopiert werden kann. Man

9 http://www.ret.nl/over-ret/nieuws-en-pers/ret-start-proef-met-gezichtsherkenningscameras.aspx

10 http://www.wired.com/threatlevel/2010/09/public-privacy/

11 http://blogs.law.nyu.edu/privacyresearchgroup/2011/04/stalkers-exploit-cellphone-gps-the-wall-street-journal-august-3-2010/

könnte daher annehmen, dass Internetmechanismen a priori die Grenze der Privatheit in dem Sinne verschieben, dass es mehr Öffentlichkeit und weniger Privatheit gibt. Doch ist diese Prognose völlig offen, solange nicht geklärt ist, ob die neuen Technologien nicht auch »Gegenmittel« hervorbringen, beispielsweise spezielle und geschützte Endgeräte, Blockademechanismen, großflächige private Netze und Ähnliches – so wie Webanalyse-Software zur Entwicklung von Plug-ins geführt hat (Anzeige von Analyse-Software beim Surfen) und wie die Onlinewerbung den Ad-Blocker provozierte.

Besorgniserregend, weil die Autonomie betreffend, sind eine Reihe von Technologien, welche Aussagen erzeugen können, die für den Nutzer nicht vorher erkennbar sind, namentlich Algorithmen zur Identitätsermittlung wie Autorenerkennung, aber auch Analysen von Verhaltensdaten. Kritisch sind auch identitätsaufdeckende Techniken, von der Gesichtserkennung bis zum Erstellen von »Fingerabdrücken« aus aller Art von Informationen. Die Gefahren könnten sich durch die Ausdehnung ins Internet of Things und die Automatismen verstärken.

Ambivalent ist auch die Frage nach Anonymität und Pseudonymität, weil diese zwar eine wünschenswerte Option darstellen, aber mit guter und mit schlechter Absicht eingesetzt werden können – und folglich sind auch die Entwicklungen ambivalent. Ebenso ist die Frage nach Privatheit nicht schlechthin mit einem »100 %« zu beantworten, denn wo Information von Mensch zu Mensch unter Abwesenden nicht unmittelbar übertragen werden kann und mit Hilfsmitteln mittelbar nicht geschehen darf, gibt es kein komplexes soziale Gefüge, gibt es keine moderne Gesellschaft.

Wir werden, weil viele Technologien von der Gesichtserkennung und der Geokoordinatenermittlung bis zur verschriftlichten Alltagskommunikation im Web (»WriteWeb«) mit sozialen Graphen noch sehr jung sind oder sogar wie Big Data und Semantic Web noch am Anfang stehen, die Sachlage ständig beobachten und bewerten müssen und bei der Grenzsetzung flexibel bleiben müssen.

Kurzfristige Überforderung im sozialen Gebrauch neuer Technik, korrekturbedürftige technische Fehlentwicklungen, unangemessene Reaktion der Beteiligten sind ebenso wahrscheinlich wie Über- oder Unterregulierung, weil das Tempo der Entwicklung alle Systeme der Gesellschaft berührt. Doch dieser Umbruch ist aus einer historisch-kulturellen Perspektive nicht der erste – und die hinter den Phänomenen verborgenen Konzepte, Strukturen, Probleme und Lösungen sind so alt, dass es überraschen würde, wenn die Menschheit die Vorteile des Umbruches nicht langfristig zu nutzen und die Nachteile zu beherrschen in der Lage wäre.

1.3 Szenarien: Privatheit und Öffentlichkeit im Jahr 2035

Präambel

Herman Kahn, 1967: A scenario is »a hypothetical sequence of events constructed for the purpose of focusing attention on causal processes and decision points«.

Einleitung

Wie schon bei der vorangegangenen Co*llaboratory*-Initiative zu »Regelungssystemen für informationelle Güter« haben wir auch in dieser vierten Initiative Szenarien für das Jahr 2035 erarbeitet, in denen mögliche Konstellationen »plausibel, logisch und spannend« abgebildet werden. Dabei geht es uns weder um den Entwurf von Utopien noch den Entwurf von Dystopien – ein gerade im hochbrisanten Themenfeld »Privatheit und Öffentlichkeit« nicht immer einfaches Unterfangen.

Weshalb Szenarien?

Szenarien sollen beitragen zur

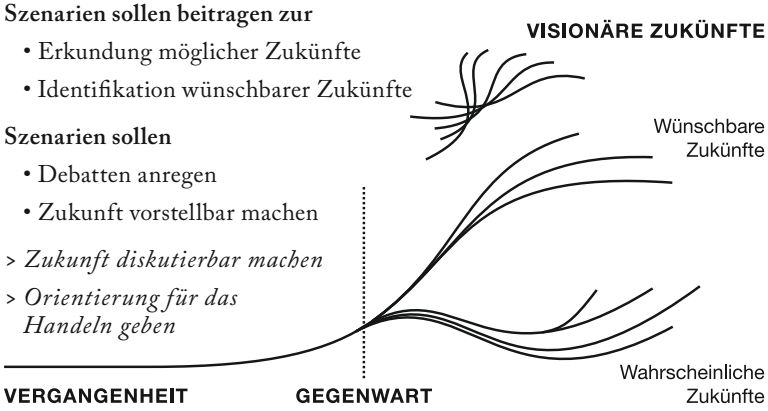
- Erkundung möglicher Zukünfte
- Identifikation wünschbarer Zukünfte

Szenarien sollen

- Debatten anregen
- Zukunft vorstellbar machen

> *Zukunft diskutierbar machen*

> *Orientierung für das Handeln geben*



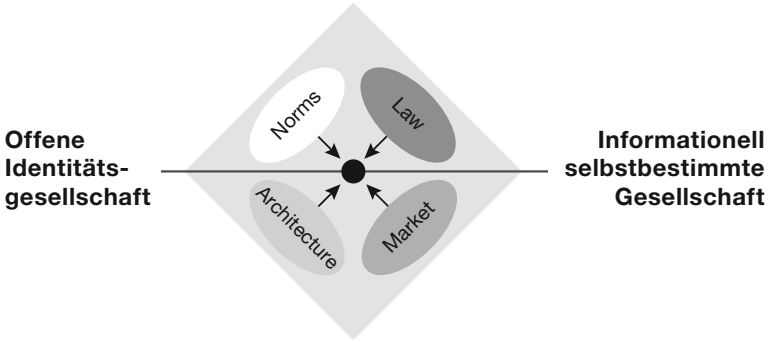
Wann ist ein Szenario »realistisch«?

Dr. Karlheinz Steinmüller
Z_punkt The Foresight Company

Die von den Experten erarbeiteten Szenarien erlauben einen Blick auf mögliche Konstellationen zum zukünftigen Umgang mit Privatheit und Öffentlichkeit. Ausgehend von bereits gegenwärtigen Entwicklungen, der technologischen Weiterentwicklung, der zunehmenden Digitalisierung und den Erwartungen der Experten wird deutlich, dass Privatheit und Öffentlichkeit neuer Regelungen und Einstellungen bedürfen. Hier setzen unsere drei Szenarien an.

In Anlehnung an Helen Nissenbaums Ansatz *»Privacy as a contextual integrity«* haben wir versucht, Rollen und Kontexte für Privatheit und Öffentlichkeit in der Zukunft zu definieren. Die Szenarien werfen einen gedanklichen Blick in ein mögliches 2035. Dies erlaubt uns, die wesentlichen Teilaspekte, die im Kontext von Privatheit und Öffentlichkeit zu diskutieren sind, zu identifizieren, die zu erwartenden Entwicklungen plastisch vorstellbar zu machen und damit die Grundlage für eine ergebnisoffene Diskussion zu schaffen. Gleichzeitig wird damit eine Diskussion über Privatheit und Öffentlichkeit losgelöst von tagesaktuellen und gegenwärtig diskutierten Fragestellungen ermöglicht. Als Grundannahme sind wir davon ausgegangen, dass der Zugang zum Internet ubiquitär und drahtlos sein wird und jedermann jederzeit und zu praktisch vernachlässigbaren Kosten auf Internetdienste zugreifen kann *(»always on«)*. Als weitere Prämisse liegt den Szenarien zugrunde, dass technologische Entwicklung, veränderte Nutzungsgewohnheiten und Innovationen es ermöglichen, nahezu jegliche Kommunikation, Verhalten und Tätigkeiten einer Person digital zu erfassen, und dass diese Informationen potentiell nutzbar, weitergabefähig und veröffentlichbar sind.

Unter Berücksichtigung der vorstehend genannten Grundannahmen und Prämissen hat sich bei der Erarbeitung der Szenarien eine erste polare Aufteilung in Privatheit (Verschlossenheit) und Öffentlichkeit (Transparenz) ergeben. Entscheidende Stellschraube der Szenarien ist damit die Kontrollierbarkeit des Informationsflusses, welche fließend von absoluter zu nicht vorhandener skalierbar ist. Bei der Erarbeitung des Szenarios der informationellen Selbstbestimmung hat sich frühzeitig eine weitere Untergliederung



als sinnvoll herausgestellt. Zum einen kann die technische Implementation der Garant der Selbstbestimmung sein (technokratischer Ansatz), zum anderen kann die informationelle Selbstbestimmung im stetigen Diskurs über sie garantiert werden (diskursiv-partizipativer Ansatz). Demgegenüber spielt der technokratische Ansatz in dem Szenario der Öffentlichkeit (Transparenz) eine untergeordnete Rolle, sodass für eine weitere Untergliederung keine Notwendigkeit bestand.

Die Ergebnisse des Wechselspiels zwischen den beteiligten Stakeholdern – Endnutzer, Service-Anbieter, Regulierungsbehörden, soziale Normen – sind indessen nicht abzusehen; ebenso wenig wie die sozialen Normen zu Privatheit und Öffentlichkeit im Internet im Jahre 2035. Hier divergieren die drei von uns entwickelten Szenarien denn auch maßgeblich. Während im Szenario der selbstbestimmten Privatheit die Idee der »Privatsphäre« fortbesteht und diese aktiv von Endnutzern gestaltet und gegenüber Dritten geschützt wird (und zudem soziale Normen dieses Paradigma stützen), sind es im Szenario der fremdbestimmten Privatheit große, staatlich regulierte und weitgehend vertikal integrierte Service-Anbieter, die Aspekte von Privatheit der Endnutzer schützen. Die entsprechenden Aufgaben werden also hier von Endnutzern an zentrale Instanzen delegiert. In dem Szenario der Öffentlichkeit (Transparenz) schließlich ist die Unterscheidung von Privatheit und Öffentlichkeit weitgehend aufgehoben, unterstützt durch soziale Normen sowie Rechtsgrundsätze zu Toleranz und Nichtdiskriminierung.

1.3.1 Freie Daten für freie Bürger (Öffentliche Privatheit)

In diesem Szenario hat die Privatheit jegliche Bedeutung verloren. Alle Informationen über jedermann stehen allen jederzeit zur Verfügung. Während in den 2010er Jahren noch von »Datenskandalen« die Rede war, ließ die Empörung in den 2020ern schnell nach, und die Erkenntnis setzte sich durch, dass die Veröffentlichung persönlicher Informationen kaum negative Folgen hat. Die vorherrschenden Prinzipien sind dementsprechend Integrität, Transparenz und Toleranz: Früher brisante Informationen wie politische Überzeugung, Krankheitsgeschichte, sexuelle Orientierung oder Religion werden toleriert und/oder von anderen Bürgern und Firmen genutzt, häufig zum Vorteil der jeweiligen Merkmalsträger.

Timeline

2012 Start-up verwendet Gesichtserkennungssuchtechnik und bietet Identitätsaggregationssuchen an.

2015 Personensuchmaschinen werden zu Browsern für soziale Strukturen: Wer ist Lebenspartner von wem? Wer ist mit wem wie intensiv in Kontakt?

2016 Das Daten-Desaster: Die US-Immigrationsdatenbanken mit allen biometrischen Informationen und der Mehrzahl der großen Onlinedienste (Identitätsverwalter) wird »gehackt«.

2017 Gesichts- und Objekterkennung auf Fotos wird allgemein verfügbar. Viele Eigenschaften wie Raucher/Nichtraucher, Hobbys etc. werden von Programmen zugeordnet.

2019 Die erste nutzbare und kommerziell erfolgreiche Datenbrille mit Eingabeinterface (iGoggles) kommt auf den Markt.

2020 Die G22-Staaten unterschreiben das Grundrecht auf Breitbandzugang. Unter den Nichtunterzeichnern ist die Schweiz. Sie glaubt damit das Bankgeheimnis vor dem Kontrollverlust zu bewahren.

2021 Nach allerlei verschiedenen Reputationsmaßen führt Facebook den allgemein anerkannten Glaubwürdigkeitsindex ein (Digital Credibility Rank, DCR), der aus verschiedenen sozialen Situationen und Kennzahlen einen eindeutigen Wert generiert.

2022 Objekterkennung und Gesichtserkennung auf Videos.

Geschichte

»Es sind die Bücher, die es beweisen«, denkt sich Horst A., als er an diesem Morgen des 04. Juli 2035 auf der Couch sitzt und sein Regal anstarrt. Niemand, den er kennt, hat noch welche. Nicht dass die Leute weniger lesen, noch nie erreichten Autoren so viele Menschen wie jetzt. Aber warum sollte man mit schweren Bänden ein Regal vollstellen, wenn ganze Bibliotheken nur einen Bruchteil des Speicherplatzes im Telefon belegen? Horst A. aber mag Bücher, er mag ihre ehrwürdige Aura, ihren leicht modrigen Duft. Sie beweisen, dass er nicht mitgekommen ist, in der falschen Zeit lebt. Genau das hat ihm gestern sein Chef gesagt. In dem Segelzeug-Versandhandel war Horst A. einer der letzen drei, die noch ins Büro gekommen sind, um zu arbeiten. Alle anderen erledigten ihre Aufgaben zu Hause, im Park oder wo auch immer. Horst A. wollte nur bei der Arbeit »on« sein. Wenn er sein Notebook ausmachte, war er praktisch nicht mehr zu erreichen und deswegen versuchte es auch niemand. Doch selbst das kleine Büro war seinem Chef jetzt zu teuer geworden und Horst A. war ihm schon lange auf die Nerven gegangen. »Mensch, Sie sind jetzt 40 und haben nicht mal iGoggles«, hat er Horst A. beim Exit-Gespräch angeblafft.

»iGoggles besorgen« steht also ganz oben auf der Liste »Schritte ins neue Leben« von Horst A., die er gerade geschrieben hat. Dass er sein Leben ändern muss, ist klar. Dieser Technikverweigerungstick, das geht einfach nicht mehr, findet Horst A. Geld ist nicht das Problem, sein Vater hat die Reederei damals gut verkauft, doch Bücher sind auch nicht alles. Er muss mehr auf die Menschen zugehen. Ohne Technik kommt man heute nur noch mit Rentnern und Kindern in Kontakt.

Noch am selben Tag kauft Horst A. die Brille. Und ist enttäuscht. Stundenlang fummelt er an ihr rum, doch irgendwie funktioniert nichts richtig. Die meisten können einfach ihre Datenpersönlichkeit importieren, aber Menschen wie Horst A., die so etwas nicht besitzen, müssen die Brille erst intensiv anlernen. Als es so einigermaßen klappt, will Horst A. die iGoggles in der Innenstadt ausprobieren. Die Werbeplakate sprechen ihn jetzt direkt an. »Horst, du siehst so aus, als ob du ein schönes Helles gebrauchen könntest«, steht auf dem Plakat von Mondinger. Aber Weißbier mochte Horst A. noch nie. Vor dem holografischen Schaufenster von H&M sollen ihm eigentlich automatisch die perfekt passenden Jeans gezeigt werden. Stattdessen sieht Horst A. eine Auswahl von weiten Baggypants, auf die er so gar nicht steht.

Genervt vom Umherirren mit der neuen Brille betritt Horst A. eine Bar in einer stillen Straße. Hier war er noch nie. Es ist noch früh am Abend und so sind wenige Gäste da. Am Tresen sitzt ein Mann, der ebenfalls eine Brille trägt und mit leerem Blick ins Nichts starrt. Vielleicht ein Seelenverwandter? Mehr aus Spaß probiert Horst A. noch einmal die iGoggles aus. Sofort erscheint ein unendlicher Datenstrom virtuell vor seinen Augen. Sascha H., der Name steht ganz oben, ist eher sein genaues Gegenteil. Ihre Interessen decken sich nur zu 15 Prozent. Über Sascha H. kann man alles im Netz erfahren, er hat eine sagenhafte CredCount-Rate von 1467. Dagegen kann Horst A. mit seinen 134 nicht ankommen. Schnell findet Horst A. auch den Grund für die miese Laune von Sascha H., die immerhin mit Horst A.'s eigenem Befinden zu 89 Prozent übereinstimmt: Tumor im Kopf, unheilbar, die Ärzte geben ihm noch ein paar Jahre. »Mensch, und ich bin schlecht drauf, der hat einen verdient«, denkt sich Horst A. und ergoogelt das Lieblingsgetränk von Sascha H. »Zwei Margarita bitte«, sagt Horst A. zum Barkeeper und setzt sich neben Sascha H. »Super, das kann ich echt gebrauchen«, sagt dieser und lacht. Die Brille hat funktioniert.

Längst bei der dritten Runde Margarita angekommen, diskutieren die beiden immer noch intensiv. »Ist dir das nicht total unangenehm, dass einer wie ich, der dich noch nie gesehen hat, weiß, wie du nach der ersten Chemo nur am Kotzen warst?«, fragt Horst A. nach einem kräftigen Schluck. Sascha H. schüttelt energisch den Kopf. »Quatsch, wieso denn? Ich lebe dieses offene Leben, da stehe ich voll dahinter. Seit ich alles über meine Krankheit verbreite, habe ich so viel Unterstützung und Ratschläge erhalten, so viele Krebsspezialisten und Psychologen könnte keine Krankenkasse bezahlen.

Und ich konnte so vielen anderen helfen. Offenheit zerstört die Stigmatisierung und vergrößert das Wissen. Was öffentlich ist, gehört der Öffentlichkeit, also allen. Je mehr öffentlich wird, desto mehr besitzen alle. Und wenn es weniger wird, verlieren alle.« »Prost«, sagt Horst A.

Beide lachen immer lauter. Zwei Margarita-Runden später torkeln der Technikverweigerer und der digitale Bohemien Arm in Arm ins Freie. Beinahe wären sie über eine junge Frau gestolpert, die zusammengekauert am Straßenrand sitzt. Sie sieht nicht aus wie die typische Pennerin. Ihre Gesichtszüge sind fein, die Kleidung ist dreckig und löchrig, aber modisch. Eine Datenbrille trägt sie nicht. »Boah, was ist denn mit dir passiert?«, spricht Sascha H. sie an. »Tja, ich komm aus der Schweiz«, sagt die Frau mit einem gequälten Lächeln. »Aber so schlimm ist das doch gar nicht«, sagt Sascha H. »Doch«. »Nee, denn wir geben dir einen aus«, sagt Horst A., überrascht über sich selbst.

Zurück in der Bar werden die Männer schnell wieder nüchtern. Die Lebensgeschichte von Sofia C. ist nicht zum Lachen. In der Schweiz gibt es kaum noch Jobs, die meisten Schweizer gehören wie Sofia C. zum Datenprekariat. Ihre Festplatte ist 15 Jahre alt und die gesamten Informationen über sie darauf ergeben nur 150 Terabyte. So jemanden bedienen selbst Kaufhäuser nicht gern, eine Krankenversicherung gibt es nur für Wucherbeiträge und, na ja, gute Männer machen in der Regel einen großen Bogen um Sofia C.

Bei diesem Punkt errötet Horst A. ein bisschen. Ihr CredCount von nur 23 stört ihn gar nicht so. Sofia C. erzählt weiter. Sie ist nach Deutschland gekommen, um ein neues Leben anzufangen. Sie will sich ein Netzwerk aufbauen, raus aus der Datenfalle. »Aber wie soll das gehen? Ich bekomme ja nicht mal einen Kredit für die iGoggles«, sagt sie. Die Banken, bei denen sie gewesen ist, vergeben prinzipiell keine Kredite an Schweizer. Dafür beauftragen die Häuser CredCount-Anbieter, die mit diskriminierenden Kriterien operieren, um die Kreditwürdigkeit ihrer Kunden einzuschätzen. Horst A. versucht sie zu trösten. »Weißt du, ich bin eigentlich auch Datenprekariat. Ich habe nur das Glück, dass ich geerbt habe.« Seine Stimme wird lauter. »Da muss man doch was machen!« Sascha H. blickt ihn an mit leuchtenden Augen. »Da kann man was machen«, sagt er. »Was denn?«, fragen Horst A. und Sofia C. gleichzeitig. »Passt auf«, sagt Sascha H., »Horst, wenn du wirklich so wütend bist, schreib das doch mal auf. Du hast ja eh nichts zu tun. Pack deine ganze Wut da rein. Und ich sorge dafür, dass das richtig viele lesen.«

Ein Jahr danach muss Horst A. immer noch lachen, wenn er an den Abend denkt, an dem seine zweite Karriere als Kämpfer gegen die Datendiskriminierung begann. »Rassisten im Anzug« hatte er seinen Eintrag betitelt, den Sascha H. auf die +1000-Homepage stellte, das Network der Deutschen mit den höchsten CredCount-Raten. Der Text verbreitete sich rasend schnell. Mehrere berühmte Kunden derjenigen Banken, die Sofia C. keinen Kredit geben wollten, drohten zu wechseln, wenn der Faktor »schweizerisch« nicht umgehend aus dem verwendeten Algorithmus entfernt werden würde. Als auch noch die Politiker Druck machten, gaben die Häuser klein bei.

Befeuert von diesem Erfolg, erstellten Horst A., Sascha H. und Sofia C. ein Ethik-Snipplet, das die Nutzer auf alle Unternehmen, die Schweizer diskriminieren, anwenden konnten und so auf diese Praktiken hingewiesen wurden. Bald hatten sie zwei Millionen Follower. Die meisten Firmen und Banken haben sich davon nicht beeindrucken lassen, aber immerhin: Zehn haben ihre CredCount-Berechnungen so verändert, dass Schweizer nicht automatisch als kreditunwürdig eingestuft werden. Horst A. schaut auf sein Regal. Bücher liest er immer noch gern, aber das Gefühl, in der falschen Zeit zu leben, kennt er nicht mehr. Vor allem seit Sofia C. bei ihm eingezogen ist.

1.3.2 Die vertrauende Gesellschaft (Selbstbestimmte Privatheit)

Über Privatheit und Öffentlichkeit entscheidet in diesem Szenario jeder einzelne Bürger. Das Wissen über technische Funktionsweisen ist weit verbreitet, die Folgen der Digitalisierung sind präsent. Obwohl es technisch einfach wäre, alle anfallenden Daten für vollständige Profile jedes Nutzers zu verbinden, ist die Gewährung von Privatheit selbstverständlich geworden und wird durch technische und rechtliche Rahmenbedingungen gefördert und gewährleistet. Dazu gibt es vielfältige Gestaltungsmöglichkeiten, da viele verschiedene Kommunikationswerkzeuge, -protokolle und anbieter existieren, die Dank ihrer Offenheit individuell erweitert und miteinander kombiniert werden können. Viele, oft offene Systeme kommunizieren miteinander. Technische und rechtliche Möglichkeiten zum Schutz von Daten sind in alle Produkte integriert und können von den Nutzern nach Bedarf an- oder abgeschaltet werden. Das dafür nötige Bewusstsein und technische Verständnis entwickelte sich als Antwort auf die verheerenden Folgen der Datenskandale der 2010er Jahre. Respekt für die Privatsphäre anderer gilt als Grundregel, die allen früh nahegebracht und in aller Regel respektiert wird. Es gibt ein ausgeprägtes Bewusstsein für die Probleme, die sich ergeben können, wenn private Daten missbraucht werden. Aktivisten, Anbieter von Diensten und staatliche Stellen arbeiten immer wieder zusammen, um die Gewährung von Privatsphäre zum Standard zu machen.

Timeline

2014 Diaspora, ein dezentrales soziales Netzwerk, hat mehr Nutzer als Facebook und Google+ zusammen.

2014 Sonderbeauftragter für Internetfreiheit in der Obama-Administration wird eingesetzt; Bundeskanzlerin ernennt Internetfreiheitsminister für Dezentralisierung.

2015 Immer mehr Menschen gehen aus Angst vor Gesichtserkennung nur noch verhüllt und mit Gesichtsmaske auf die Straße.

2016 Das Daten-Desaster: Die US-Immigrationsdatenbanken mit allen biometrischen Informationen und der Mehrzahl der großen Onlinedienste (Identitätsverwalter) werden »gehackt«.

2017 Die Huffington Post gelangt in den Besitz der kompletten Krankenakte von Rupert Murdoch – und veröffentlicht sie nicht. »Jeder hat ein Recht auf Privatsphäre – auch die anderen.« (Arianna Huffington am 14. Juli 2017 zur Washington Post)

2018 Bild schafft Leserreporter ab, richtet die Rubrik »Was wir nicht veröffentlicht haben« ein und startet diese Aktion mit der BildFreiheits-Kiste (Hard- und Software zum selbstbestimmten Umgang mit Informationen): »BILD privatisiert!«

2019 Die FRITZ!Box wird standardmäßig mit Serverfunktionalität zum selbstbestimmten Umgang mit persönlichen Daten geliefert.

2020 Verbot von Überwachungskameras in der Öffentlichkeit und Fingerabdruckscannern.

2021 Howard Jones (16) aus Cedar Rapids, Iowa, verliert einen Prozess gegen seine Eltern, denen er vorwirft, sie hätten ihn von seinen illegalen Aktivitäten abhalten können, wenn sie ihn nach dem Stand der Technik überwacht hätten. Dies löst auch in Deutschland Diskussionen über die Gewährung von Privatsphäre für Jugendliche aus.

2022 In Großbritannien entscheiden künftig Jurys aus Bürgern, Verwaltungsbeamten und Experten über die Freigabe geheimer Regierungsinformationen. Diese Maßnahme wird von der Open Government Initiative ausdrücklich begrüßt.

2024 Technische und soziale Formen der Gewährung von »Schutz der Privatsphären Dritter« werden Bestandteil des Unterrichts in ganz Europa.

2025 Gemeinschaftliche und einfach zu betreibende Anonymisierungsserver am eigenen Anschluss haben sich als gesellschaftlich hoch geachtete Privacy-Unterstützungsmaßnahme weit verbreitet, IPSec ist selbstverständlich für alle kommerziellen Diensteanbieter im Internet.

2030 Alle Daten werden verschlüsselt per Verknüpfungen zwischen den mobilen Endgeräten verteilt; auch der letzte verbliebene zentralisierte Telekommunikations-Provider stellt den Dienst ein.

Geschichte

Carsten L. schmunzelt. George A. redet nun so begeistert von der nachhaltigen Mobilität wie er selbst vor 25 Jahren. Damals, 2010, war er auch 23, so wie George A. jetzt. Carsten L. hatte damals alles auf Elektroautos gesetzt. Heute leitet er eine Kette von Mobilitätscentern, die E-Autos verleihen und verkaufen. Anfangs hielten ihn viele für einen Spinner, heute gilt das eher für die, die noch mit Benzinern unterwegs sind.

Über 90 Prozent fahren nun mit Elektrofahrzeugen. Das Interesse war schon groß, als man gezielt Bewegungsprofile mit aktuellen Verkehrsdaten verbinden konnte, um bei geringem Verbrauch möglichst schnell ans Ziel zu kommen. Durchgesetzt haben sich diese, aber erst nachdem die Anbieter nicht mehr auf die Erstellung von Profilen einzelner Nutzer setzten, sondern ausschließlich die Nutzer selbst dezentrale Profile anlegen konnten und die Anbieter nur noch mit anonymisierten und bereits aggregierten Daten arbeiteten. Wie die Datenaktivisten das damals in der Branche gemeinhin verbreitete »weil es eben geht« zu einem »weil es eben auch sicher geht« erweitert hatten, bewundert Carsten L. auch heute noch. Carsten L. war einer der Ersten, die diese Neuerung anboten – und der Erfolg gab ihm recht. Heute ist es die Standardeinstellung, dass die Profile der Fahrzeuge vom Halter verwaltet werden. Trotzdem beteiligen sich viele an Studien zur Mobilität, indem sie ihre Profile anonymisiert zur Verfügung stellen. Schließlich hilft das, Verkehr und Ressourcennutzung zu optimieren. Auch George A. hat heute Morgen gerade seinen Datensatz auf die Anonymisierungsdatenbank der Max-Planck-Gesellschaft hochgeladen.

Es schmeichelt Carsten L., dass sich ein guter Mann wie George bei ihm als Berater bewirbt. Die öffentlichen Informationen über George A. im Netz bestätigen seinen positiven Eindruck. Die als privat markierten Bereiche seiner Profile sind nur über kleine Hacks zugänglich. So wie bei fast allen Menschen heute.

Nur eine Frage hat Carsten L. an seinen Bewerber noch. Im öffentlichen Bereich des Profils hat er zahlreiche Fotos gefunden, die George A. und seine Freunde bei privaten Feiern und in nicht sehr schmeichelhaften Situationen zeigen. »Ich habe die Fotos von Ihnen und Ihren Freunden online gesehen und bin nicht sicher, ob das wirklich so gedacht ist. Ist das nicht eher privat? Und wissen Ihre Freunde davon?« George A. lächelt. Er antwortet: »Darüber haben wir auch eine Weile diskutiert, aber wir fanden irgendwie, dass das ja auch dazugehört. Es ist natürlich schon privat, aber letztlich dürfen das alle von mir wissen. Meine Freunde sehen das ähnlich. Und natürlich ist nichts als öffentlich markiert, was einen Beteiligten stört. Das wäre ja auch wirklich nicht in Ordnung.«

Carsten L. ist zufrieden. Offensichtlich ist George A. jemand, der sich Gedanken über die Konsequenzen seiner Entscheidungen macht. So einen kann man brauchen. Carsten L. nutzt die Gelegenheit, ihn gleich in die Privacy Policy der Firma einführen: »Gut, dass Sie schon daran gewöhnt sind, solche Absprachen zu treffen, wir machen das hier nämlich ähnlich. Wissen Sie, wir

können hier wirklich feiern … von den Weihnachtsfeiern könnte ich einige Geschichten erzählen. Aber damit alle wirklich entspannt sein können, haben wir vereinbart, dass die Fotos nicht jeder sehen soll, sondern nur die engsten Freunde. Darauf haben wir uns bei unserem Privacy Workshop vor ein paar Jahren geeinigt. Der findet jedes Jahr statt und wir finden jedes Jahr wieder, dass das eine gute Idee ist.« Carsten L. denkt einen Moment nach. »Der Workshop wird übrigens auch für Sie wichtig, in vier Wochen findet er wieder statt. Wir sprechen dabei auch immer über die neuesten technologischen Entwicklungen und Gestaltungsmöglichkeiten im Privacy-Bereich. So bleiben unsere Privacy Guidelines immer aktuell und State of the Art, auch für unsere Kunden. Unser Anspruch ist es, in allen Bereichen innovativ zu sein und eine Vorreiterrolle einzunehmen – nicht nur im Bereich der nachhaltigen Mobilität. Sie wissen ja, dass uns das erfolgreich gemacht hat. Ich freue mich, wenn Sie dabei sind – so Sie den Job wollen.« Er streckt George A. die Hand entgegen. Der lacht – und schlägt ein.

Es ist spät geworden, als Carsten L. seinen neuen Mitarbeiter verabschiedet. Ihn nach seiner Zusage mit allem vertraut zu machen, hat doch etwas gedauert. Carsten L. muss sich beeilen, damit er es noch pünktlich zum Elternabend in der Kindertagesstätte von Helene und Luise, seinen Jüngsten, schafft. Da seine Frau Karla wieder einmal für einen wichtigen Kunden unterwegs ist, muss sein 15-jähriger Sohn Jan auf die beiden kleinen Geschwister aufpassen. Zum ersten Mal verzichtet Carsten L. heute auf die Videoübertragung aus der Wohnung. Schon ein merkwürdiges Gefühl. Aber Jan war sehr überzeugend, als er sagte, dass er erstens ein Recht darauf habe, unbeobachtet zu sein, auch wenn er auf die Kleinen aufpasst. Und zweitens habe er sowieso schon oft bewiesen, dass er in solchen Situationen verantwortungsvoll sei. Das stimmt. Und außerdem: Privatsphäre steht allen zu, auch den eigenen Kindern. Als ein höchstrichterliches Urteil vor einigen Jahren dieses Recht dahingehend präzisierte, dass auch Jugendlichen ab einem gewissen Alter überwachungsfreie Räume zur Verfügung stehen müssten, gab es zwar zunächst eine heftige Debatte. Doch letztlich hat es sich bewährt. Nur wenn er seinem Sohn private Freiräume gewährt und nicht alles über sein Leben weiß, kann Jan auch lernen, mit dieser Freiheit richtig umzugehen. Und, denkt sich Carsten L., sein Jan ist wirklich auch schon ziemlich erwachsen.

»Elternabende sind ermüdend«, denkt er, als er auf einem viel zu kleinen Stuhl in der Kita sitzt, »besonders nach so einem langen Tag.« Doch es gibt Dinge, da will Carsten L. nicht fehlen, wenn sie entschieden werden. Es war in letzter Zeit zu einigen Zwischenfällen gekommen. Kinder hatten sich offenbar gegenseitig so sehr an den Haaren gezogen, dass diese ausgerissen wurden. Und mehrfach waren teure Spielgeräte kaputtgegangen, was das Budget des Kindergartens doch deutlich strapazierte. Die Erzieher traf keine Schuld: Man kann nun einmal nicht immer überall gleichzeitig sein.

Die Leitung des Kindergartens wollte nun mit den Eltern diskutieren, ob die Raumvollüberwachung (RVÜ) wieder aktiviert werden sollte, die installiert, aber auf Elternbeschluss nie aktiviert worden war. Die Erzieher könnten so im Nachhinein genau nachvollziehen, was passiert ist, und entsprechend reagieren. Zudem könnte so eine automatisierte Auswertung der Verhaltensmuster der Kinder erstellt werden, denn die RVÜ kann auch Interaktionen zwischen den Anwesenden messen und daraus Rückschlüsse ziehen – zum Beispiel, welche zwei Kinder sich streiten.

Nun streiten sich erst einmal die Eltern. Die einen möchten Klarheit haben und dafür sorgen, dass diese Zwischenfälle sich nicht wiederholen. Die anderen finden die Raumvollüberwachung eine viel zu weit gehende Maßnahme. »Wir könnten alternativ natürlich auch mehr Erzieher einstellen«, gibt der Leiter des Kindergartens zu bedenken. Und rechnet vor, was dies kosten würde – ein durchaus stattlicher Betrag, den die Eltern zusätzlich entrichten müssten. Carsten L. ist sich unschlüssig. Zusätzliche Erzieher würden auf jeden Fall die Kosten für den Kindergarten deutlich verteuern, aber die Kinder permanent überwachen zu lassen? Das ginge ihm dann doch zu weit.

Die Diskussion will nicht enden, bis der Leiter einen Vorschlag macht: Befristet für vier Wochen würde ein zusätzlicher Erzieher engagiert. Wenn

die Probleme sich dann wiederholt hätten, könnte man neu entscheiden, wie man verfahren möchte. Carsten L. ist damit zufrieden. Auch die anderen Eltern lassen sich auf den Vorschlag ein. Die Zusatzkosten halten sich in akzeptablem Rahmen und Luise und Helene können weiter unbeschwert in den Kindergarten gehen.

Als er endlich zu Hause ankommt, sind die Kleinen schon im Bett. Jan sitzt in seinem Zimmer und liest ein Buch. »Na, alles gut gelaufen?«, fragt der Vater. Jan schaut hoch: »Klar.« »Na dann, danke fürs Aufpassen. Gute Nacht.« Carsten L. geht in die Küche und holt sich ein Bier aus dem Kühlschrank. Der ist immer voll. Ein Sensor erkennt automatisch, was aufgebraucht ist. Dann kommt der Lieferservice und füllt ihn wieder auf. Anfangs haben sich diese Dienstleister über den Verkauf der Datenauswertung finanziert. Heute ist es selbstverständlich, dass das nicht stattfindet. Dafür stellt der Lieferservice der Familie eine wirklich gute Auswertung der Einkäufe bereit, die nicht nur bei der Budgetverwaltung hilft, sondern auch ethische und ökologische Kriterien beim Einkauf berücksichtigen kann. Alles genau so, wie Carsten L. und seine Familie das wollen. »Muss echt keiner wissen, was für einen Joghurt ich esse. Oder welche Soaps ich sehe.« denkt sich Carsten L., lässt sich auf das Sofa fallen und winkt den Videoscreen an. Endlich Entspannung. In Gedanken geht er den Tag noch einmal durch. Morgen wird er seinem neuen Mitarbeiter George A. noch etwas über die Geschichte erzählen, wie er es damals geschafft hat, die Profilautonomie des Autofahrers zu einem guten Verkaufsargument zu machen.

1.3.3 Nichts zu befürchten (Technikbestimmte Privatheit)

Auch in diesem Szenario spielt die Privatheit eine große Rolle. Allerdings liegt die Verantwortung dafür kaum bei den Nutzern, sondern beim Gesetzgeber und den wenigen Kommunikationskonzernen. Möglich gemacht hat dies die Schließung der offenen Geräte und des Internets, wie es bis zum Ende der 2010er Jahre existierte. Die Datenskandale, Viren, Spam und Hackerangriffe trieben die Nutzer schnell zu wenigen großen Firmen, die aus einer Hand fest geschlossene Systeme aus Netzwerk, Programmen, Geräten und Inhalten anboten. Diese konnten den Nutzer einerseits die erwartete Sicherheit und Komfort bieten, andererseits vollautomatisch die individuellen Privatheits-Präferenzen ermitteln und umsetzen. Insbesondere das Verfallsdatum für Daten stellte die Sorglosigkeit des frühen Informationszeitalters wieder her. Die Aufteilung des Internets in nationale Netze ermöglichte eine gesetzliche Regulierung der Anbieter. Dementsprechend entstand auf demokratischem Weg ein feingranulares Regelwerk zu Privatheit und Öffentlichkeit.

Timeline

2012 Android und Symbian werden zu geschlossenen Systemen, nur registrierte Entwickler dürfen Anwendungen bereitstellen, über Aufnahme in den Market entscheiden die Hersteller.

2013 Windows-Anwendungen nur noch über den MS-Market.

2014 Google kauft Verizon, Comcast und HTC.

2014 Erste Managed-Privacy-Dienste: Algorithmen finden automatisch individuelle Privatsphären-Einstellungen für soziale Netzwerke, allerdings kostenpflichtig.

2015 Wegen Spam, Angriffen, Unzuverlässigkeit bei E-Mail und Telefon wickeln die Nutzer fast sämtliche Kommunikation über geschlossene Systeme wie Skype und Facebook ab.

2016 Das Daten-Desaster: Die US-Immigrationsdatenbanken mit allen biometrischen Informationen und der Mehrzahl der großen Onlinedienste (Identitätsverwalter) werden »gehackt«. Außerdem Gmail-Disaster: Alle Nachrichten aller Google-Mail-Konten werden geleakt und sind unwiderruflich öffentlich verfügbar. Zahllose persönliche und professionelle Zerwürfnisse sind die Folge.

2017 Großer Zulauf bei Anbietern mit Managed Privacy (Gated Communities).

2018 Microsoft kauft Telefónica, Telekom und Lenovo.

2025 Geräte ohne vollständige Kontrolle der Nutzer durch Trusted-Computing-Module sind praktisch bedeutungslos, da von keinem Netzanbieter zugelassen.

2027 Isolation der Anbieter gegeneinander, E-Mail praktisch bedeutungslos.

2027 Abtrennung des Internetverkehrs erster westlicher Staaten: USA, Venezuela, Singapur, EU; grenzüberschreitender Datenverkehr wird grundsätzlich blockiert, sobald Inhalte in einem der beiden Länder illegal sein könnten.

2028 Kommission beginnt Arbeit am Datenschutzgesetzbuch (DSchGB): demokratisch ausgehandelte, feingranulare Regelung von Rechten und Pflichten von Nutzern und Anbietern.

2029 Managed Privacy gehört zum Standardangebot, sagt 95 % der Nutzerentscheidungen zur Privatsphäre korrekt voraus.

2029 Benutzung des Netzes in Deutschland nur noch mit staatlich registriertem Kennzeichen, drastischer Rückgang von Urheberrechtsverletzungen, Angriffen, Beleidigungen.

2030 DSchGB tritt in Kraft, insbesondere Löschfristen: Jede Information hat ein Haltbarkeitsdatum, nach dem sie komplett entfernt werden muss.

2031 Isolation der übrigen Nationalstaaten.

ab **2033** Jährliche Novellierung des DSchGB, um technologische Entwicklungen zu berücksichtigen und Innovationen zu ermöglichen.

Geschichte

Julia F. lacht viel an diesem Abend. Sie trifft sich mit ihren besten Freundinnen, genießt die Unbeschwertheit in der Runde. Julia F. hat den ganzen Tag an einer Präsentation für den Folgetag gearbeitet und freut sich, jetzt einfach mal abschalten zu können. Unter dem Tisch liegt das Notebook aus ihrer Firma, an dem sie den ganzen Tag saß.

»Du hast es gut«, hatte die Mutter ihr noch mit auf den Weg gegeben, als Julia F. nach ihrem wöchentlichen Besuch bei den Eltern aus der Tür ging. Manchmal muss Julia F. daran denken, wie viel eingeengter das Leben ihrer Mutter war. In die Stadt gehen, sich mit Leuten treffen, vielleicht auch mal über die Stränge schlagen? Unmöglich. Am nächsten Tag wäre alles im Netz dokumentiert. Fotos und Videos würden erscheinen. Auch die, die nicht gerade vorteilhaft waren. Und wirklich jeder konnte sie sich anschauen, man hatte keinerlei Einfluss darauf. Viele Menschen zogen es deshalb vor, zu Hause zu bleiben. Aber sicher war man da auch nicht wirklich.

Für Julia F. eine überaus bizarre Vorstellung. Zum Glück ist das längst nicht mehr so. Sie kann machen, was sie will. Wie und wo sie das macht, wissen nur die Leute, von denen Julia das möchte – und natürlich Passanten, die sie kennen. Aber auch wenn jemand zu fotografieren anfängt, ist das für sie kein Anlass zur Sorge. Die Freigabe der Bilder ist automatisch mit ihren Wünschen verknüpft. Ohnehin verfallen Inhalte nach kurzer Zeit, wenn Julia F. sie nicht ausdrücklich aufheben will.

Sie bemerkt an ihrem Nebentisch einen Mann, der ihr irgendwie bekannt vorkommt. Sie schaut hinüber, und der Mann steht auf und geht auf sie zu. »Julia, oder?«, fragt er vorsichtig. Als sie Ja sagt, hellt sich sein Gesicht auf. »Wahnsinn, ich bin's, Holger. Wir haben damals doch bei dem alten Meyer in der Universitätsvorlesung immer nebeneinander gesessen.« Julia muss auch lachen. »Holger, na klar! Du hast ja auch schon lange nichts mehr von dir hören lassen.« Die beiden prosten sich zu.

»Wie auch«, sagt Holger D., »wir haben es nie geschafft, unsere Kontaktdaten auszutauschen. Bei wem bist du jetzt?« »Bei Akamoogle«, gibt Julia F. ihm Auskunft. Holger D. guckt für einen Moment etwas enttäuscht: »Tja, dann ist es jetzt wohl zu spät. Ich bin bei Amazebook.« Das kommt leider vor, aber dass man sich entscheiden muss, hat Julia F. schon früh gelernt. In mehr als einem Netzwerk zu sein ist unrealistisch. Das ganze Leben funktioniert doch über die darin abgebildeten Vertrauensketten! Julia F. hat sich das Netzwerk ausgewählt, das ihre Freundinnen und Kollegen benutzen. Holger D. ist zwar ein netter Typ, denkt sich Julia F. Und auf die überaus absurde Idee, sein Amazebook-Konto netzwerkübergreifend mit ihrem zu verknüpfen, ist auch er nicht gekommen. Bevor man einen Account übergreifend gestaltet, muss man der Person schon hundertprozentig vertrauen können. Und der Prozess ist auch nicht einfach. Bevor irgendetwas passieren kann, sind eine eingehende staatliche Sicherheitsprüfung und eine fünfstellige Kaution für den Fall von IT-Sicherheitsproblemen fällig.

»Wir können uns doch Briefe schreiben wie unsere Urgroßeltern.« Holger D. lacht und zaubert einen Stift hervor. Julia F. zögert kurz und schreibt dann ihre Adresse auf.

Ob er schreiben würde? Ob sie zurückschreiben würde? Julia F. ist auf dem Weg nach Hause. Sie kann sich nicht daran erinnern, je einen Brief erhalten oder geschrieben zu haben. Das wäre ja etwas Romantisches. Aber doch eine ziemlich weltfremde Idee. Die Post hat den Briefversand vor Jahren eingestellt. Nun werden nur noch Pakete befördert. Aber man kann einen Brief natürlich auch als Paket schicken.

Julia F. ist nicht mehr ganz so gut gelaunt. Und als sie zu Hause ihre Tasche öffnet, verstärkt sich ihr Missmut noch. Ihr Firmennotebook vermisst sie, offenbar hat sie es in der Kneipe liegen gelassen. Doch immerhin, eine Katastrophe ist es nicht. Die Präsentation und die meisten anderen Daten sind noch da. Einen »Personal Computer«, wie es früher einmal hieß, gibt es nicht mehr. Immer raffiniertere Gadgets haben dessen Konzept vollkommen überflüssig

gemacht – heute benutzt praktisch jeder wie Julia F. einen der »Private Spaces« bei einem der verbliebenen drei internationalen Internetanbieter. Sie muss auch nicht fürchten, dass das Notebook in falsche Hände gelangt. Mit dem physischen Notebook kann niemand anderes etwas anfangen, weil keiner an die Daten herankommen würde.

Als sie am nächsten Morgen in die Firma kommt, empfängt sie David Z., ihr Projektpartner, mit einem wissenden Grinsen. Alle fünf Mitarbeiter und auch ihr Chef sind Mitglieder bei Akamoogle und haben die Fotos, die Julia F. für sie freigegeben hat, angeschaut. Gemeinsam sind sie außerdem mit den anderen vier Partnerfirmen in der Bürogemeinschaft vernetzt. Alle entwickeln Verwaltungssoftware. Die Arbeitsdokumente haben automatisch gesetzte Lese- und Schreibrechte. So können, wenn nötig, alle Mitarbeiter der Partnerfirmen ein Dokument einsehen und bearbeiten.

Der Chef hat Julia F. das neue Notebook schon auf den Schreibtisch gestellt. Julia drückt auf den Knopf und wie erwartet sind alle Daten da. Zwei Stunden später hält sie ihre Präsentation mit David Z. »Safe4Save« soll die Firma endlich in die schwarzen Zahlen bringen. Damit sollen Informationen längerfristig erhalten bleiben, ohne die Sicherheitsstandards aufzuweichen. Drei Versionen hatten sie schon eingereicht, die vierte hat die Genehmigungsabteilung von Akamoogle endlich zugelassen. Jetzt fehlt nur noch das Okay des Gesetzgebers. Das kann dauern. Aber das ist ja auch richtig so, denkt Julia F. Wäre die Genehmigung einfacher zu bekommen, hätte sie gestern wohl nicht so einen schönen Abend haben können. Und mit ihrem Notebook hätte sie auch das Ergebnis wochenlanger Arbeit verloren. Dann schweifen ihre Gedanken zu Holger D. Ob er wohl geschrieben hat?

1.4 Denkanstöße

Die im Folgenden dargestellten Thesen und Einschätzungen waren in unterschiedlicher Intensität Gegenstand der Diskussion im Rahmen des Co:*llaboratory* »Privatheit und Öffentlichkeit«. Sie erheben weder den Anspruch abschließender Gültigkeit, noch sind sie vom Konsens der eingeladenen Experten getragen. Sie zeigen vielmehr eine Vielfalt von Überlegungen, die in der Gruppe vertreten waren, und mögen so auch eine Vielfalt der gesellschaftlichen Debatte widerspiegeln. Wir werten dies als Beleg, dass die Diskussion um die gesellschaftliche Weiterentwicklung des Verhältnisses von Privatheit und Öffentlichkeit noch alles andere als abgeschlossen ist. Auch aus diesem Grunde haben wir uns entschlossen, die Thesen als »Denkanstöße« zu bezeichnen.

Wir hoffen, dass einige der hier formulierten Gedanken dazu dienen, die weitere gesellschaftliche Debatte zu befruchten. In jedem Fall haben die Teilnehmer und eingeladenen Experten die Arbeit an diesem Bericht mit vollem Engagement und mit Gewinn für ihren eigenen Diskurs geführt.

Entwickelt wurden die Thesen in einem iterativen Verfahrensmix aus Brainstorming, Clustering und Konsolidierung. Das erste Brainstorming führte zu vier Themenkomplexen, die in anschließenden Workshops in Gruppen erörtert wurden: Ökonomie, Regulierung, Kompetenz und – vielleicht etwas jenseits des Vorangegangenen stehend – Aggregation. Im Rahmen der Schlussredaktion haben wir uns entschlossen, diese Struktur in Attribute – neudeutsch Tags – zu überführen und um weitere zu ergänzen.

Information als Ressource

Digitale Information ist auch eine Ressource und Grundlage sozialer und wirtschaftlicher Austauschprozesse.

Tags: Ökonomie

Digitale Informationen haben mittlerweile einen erheblichen Anteil an der wirtschaftlichen Wertschöpfung. Man kann sie also als Güter im klassischen ökonomischen Sinn begreifen. Soweit diese Daten personenbezogen oder personenbeziehbar sind und Privatheit als grundlegende Prämisse gesellschaftlich anerkannt wird, lässt sich das traditionelle Paradigma des Datenschutzes auf solche Daten anwenden. Dieses traditionelle Paradigma verankert den Datenschutz im Persönlichkeitsrecht und verknüpft ihn unmittelbar mit der Würde des Einzelnen. Allerdings ist es durchaus plausibel, insbesondere aus der Perspektive ökonomischer Effizienz, dieses Paradigma als zu weitreichend zu erachten und zumindest komplementär alternative Regulierungsansätze zu erwägen.

Die Frage ist also, inwiefern persönliche Daten als prinzipiell schutzwürdig anzusehen sind oder wie dieser Schutz in Abwägung von Persönlichkeitsrechten sowie statischen und dynamischen Effizienzerwägungen geregelt sein sollte. Beide Extreme sind offensichtlich nicht zielführend: ein Laissez-faire-Regime würde den Machtasymmetrien nicht gerecht, eine vollständige Verdrängung privatdisposiver Freiheiten wäre dagegen der Dynamik des Marktes nicht angemessen.

OpenData4Research

Durch die unterschiedliche Verfügbarkeit von Daten über menschliches Verhalten entsteht eine Wissenskluft zwischen öffentlicher und proprietärer Forschung. Alle Akteure sollten sich dafür einsetzen, möglichst viele dieser Daten für öffentliche Forschung bereitzustellen.

Tags: Agreggation

Firmen werden immer mehr zu Eigentümern großer Datensets über menschliches Verhalten, die in ihrem Umfang kein Gegenstück haben. Häufig werden diese Datensets firmenintern zur Marktforschung oder Produktoptimierung analysiert. Der öffentlichen Forschung liegen in der Regel keine vergleichbaren Datensets vor. Potentiell tut sich hier eine datenbedingte Wissens-/Erkenntniskluft zwischen firmengelenkter und öffentlicher Forschung auf. Dies kann nicht im gesellschaftlichen Interesse liegen.

Datenhandel

Die rechtlichen Rahmenbedingungen für eine »Ökonomisierung« des Austausches von Daten – oder, falls der Nutzer im Besitz der Daten ist, über die Erteilung von Zugriffsberechtigungen – für Unternehmen, die diese Daten nutzen wollen, müssen praktikabel und einfach handhabbar sein.

Tags: Ökonomie

Die praktische Umsetzung eines »Tausches« von Daten gegen einen Gegenwert (z. B. Geld oder Services) muss auch für Personen, die diese komplexen Vorgänge nicht überblicken können, einfach verstehbar und in der Darstellung transparent sein.

Im Bereich des Urheberrechts hat das Beispiel der »Creative Commons«-Symbole gezeigt, dass es mit gut verwendeter Symbolik möglich ist, eine Vielzahl von urheberrechtlichen Aspekten bei der Einräumung von Nutzungsrechten einfach zu lösen.

So könnte die Verwendung von einheitlichen, leicht verständlichen Symbolen auf einer Website in gleicher Weise auch typische Datenverarbeitungsvorgänge grafisch darstellen. Typische Datenverwendungen könnten z. B. sein: die Erhebung von Profildaten, die Speicherung von Bewegungsdaten, die Weitergabe von Daten an Dritte, das Tracking von Klickverhalten auf einer Website für Zwecke der Optimierung der Auswahl von Werbebannern etc.

Wenn eine einheitliche Nutzung von bestimmten Symbolen erreicht würde, könnten Unternehmen diese Symbole freiwillig einsetzen, um Wettbewerbsvorteile zu erlangen. Eine gesetzliche Regelung, die die Gestaltung und den Inhalt der Symbole regeln (z. B. durch ein »Gremium«) und den Einsatz der Symbole auf Websites verpflichtend vorsehen würde, würde dem Ansatz der »Datenökonomie« jedoch besser entsprechen. Da die Diensteanbieter in der Regel international agieren, wären auch international geltende Regelungen geboten.

Die Durchsetzung der Symbolnutzung könnte sich darauf beschränken, dass für die Nichtverwendung bzw. das »Lügen« über die tatsächliche Einhaltung Sanktionen vorgesehen wären. Über das Wettbewerbsrecht könnten dann Verstöße durch Mitbewerber geahndet werden. So könnte Chancengleichheit auf dem Markt hergestellt und Datenschutz tatsächlich zu einem echten Wettbewerbsfaktor gemacht werden.

Die Schwierigkeit dieses Modells besteht einerseits darin, dass jemand bestimmen müsste, welche Symbole welche Datenverwendungen darstellen, und andererseits wie die Symbole im Hinblick auf neue Entwicklungen aktualisiert werden könnten. Hier müssten Lösungen diskutiert und entwickelt werden, die Verbindlichkeit für die Beteiligten (Nutzer und Unternehmen) und Flexibilität gewährleisten können.

Mit diesem Modell könnte jedoch ein wesentlicher Teil der »üblichen« Datenerhebungen und -nutzungen abgedeckt werden. Individuelle Nutzungen, die z. B. dann zwischen Unternehmen und Betroffenen ausgehandelt werden könnten, könnten durch ein gesondertes Symbol dargestellt und dann kontextbezogen mit erweiterten, individuellen Vereinbarungen ergänzt werden.

Informationelle Güter

Persönliche Daten wie Eigentum zu behandeln löst nicht die zentralen Herausforderungen, die sich aus ihrer Verarbeitung ergeben. Die Entwicklung eines eigenständigen Rechts der informationellen Güter erscheint sinnvoll.

Tags: Ökonomie, Recht

Bereits jetzt ist der Schutz personenbezogener Daten dem Eigentumsrecht sehr ähnlich konstruiert. Wie beim Eigentum an einer Sache darf ein Datensatz nur genutzt werden, wenn eine Rechtsgrundlage besteht. In aller Regel erfolgt diese auch jetzt schon vertraglich oder vertragsähnlich. Gleichzeitig treten aber die Probleme der technischen Kontrolle, die beim Immaterialgüterschutz, insbesondere dem Urheberrecht, im Netz existieren, in ähnlicher oder sogar verschärfter Form auf.

Mit einem Verständnis von persönlichen Daten als Gut werden Machtungleichgewichte, wie sie aus dem Verbraucherrecht bekannt sind, zu einem drängenden Problem. Die Freiheit des Einzelnen, seine Daten im Austausch gegen Geld, geldwerte Vorteile oder andere Daten preiszugeben (oder eben auch nicht), ist immer dann potentiell gefährdet, wenn die andere Partei über mehr oder bessere Informationen, einzigartige Güter oder dem Vertragspartner unbekannte technische Möglichkeiten der Datenauswertung verfügt. Für einzelne Konsumenten besteht, mit anderen Worten, in bestimmten Situationen nur eingeschränkt die Möglichkeit, eine an ihren eigenen Präferenzen und Interessen ausgerichtete Entscheidung über die Preisgabe von Daten zu treffen. Der Interessenausgleich zwischen wirtschaftlichen, gemeinwohlorientierten und individuellen Bedürfnissen kann über eine Gestaltung des Schutzes persönlicher Daten über die Konstruktion eines »Eigentums an persönlichen Daten« nur unzureichend gewährleistet werden.

Es ist kaum möglich, privaten Daten einen stabilen Wert zuzuweisen. Jeder hat für eine bestimmte Information ein anderes Auswertungsinteresse und unterschiedliche Datenauswertungsprozesse. Der Nutzen einer Information ist ihr nicht inhärent, sondern ergibt sich aus der konkreten Auswertung anhand einer konkreten Frage. Auch aggregierte, strukturierte Datensets vieler Menschen haben innerhalb eines Auswertungskontextes keinen stabilen Wert. Die Daten veralten schnell und inflationieren mit ihrer Ausbreitung. Zwar gibt es einen Markt, in dem Datenmassen größeren Umfangs gehandelt werden, daraus aber auch auf den Wert einer bestimmten Information zu schließen (und damit dem Verbraucher einen Anhaltspunkt zu geben), ist so gut wie unmöglich.

Zweitverwertung

Der Konsument sollte neben der Erstverwertung auch die Zweitverwertung seiner Daten übernehmen. Die Datenökonomie muss durch einen transparenten und fairen Tausch gekennzeichnet werden.

Tags: Ökonomie, Kompetenz

Digitale personenbezogene Informationen sind zunehmend eine ökonomische Ressource und Grundlage wirtschaftlicher Austauschprozesse. Der »Handel« mit personenbezogenen Informationen hat schon heute einen erheblichen Einfluss auf soziale Kontexte. Die ökonomische Verwertung von Daten findet auf zwei Marktplätzen statt.

Auf dem ersten Marktplatz (Erstverwertung) findet zwischen den Datenproduzenten (Datensubjekten) und Unternehmen ein Tauschhandel statt (Beispiel: Bereitstellung von Profildaten gegen Bereitstellung von Serviceangeboten).

Auf dem zweiten Marktplatz (Zweitverwertung) werden die Daten der Produzenten (Datensubjekte) zwischen Unternehmen gehandelt. Erst hohe Datenvolumen (Aggregation der Daten) bilden die Grundlage für Verwertbarkeit.

Allerdings findet der Handel mit Daten bzw. die Vergabe von Nutzungsrechten derzeit weitestgehend intransparent statt. Der Konsument ist lediglich darüber informiert, dass es diese Zweitverwertung seiner Daten gibt. Über das Marktvolumen und den Wert seiner Daten ist er nicht informiert. Intermediäre bestimmen den Wert von Profildaten. Aktuell wird der Wert einer personenbezogenen Information nicht auf einem freien Markt gehandelt, sondern einseitig von Unternehmen bestimmt (Beispiel: Facebook »vergütet« die Vermarktung von Profildaten als Grundlage der Aggregate und Werbezielgruppen mit der Bereitstellung des Zugangs zum Social Network). Der Marktwert von Profildaten findet sich als Resultat von Angebot und Nachfrage zwischen Unternehmen (Zweitverwertung von Profildaten) und nicht zwischen den Datenproduzenten und den Unternehmen.

Der Datenproduzent möchte in Zukunft auch ökonomisch an der Zweitverwertung seiner Daten beteiligt werden. Als autonomer Marktteilnehmer kann er bestimmen, zu welchen Konditionen er seine Daten einer Erst- oder Zweitverwertung zuführt. Digitale personenbezogene Informationen fließen so als wirtschaftliches Tauschobjekt in einen »fairen« Deal. Fairness ist individuell verhandelbar. Beispiel: Bei der Registrierung wird bereits mitgeteilt, was mit den Daten passiert und dass damit das Geld verdient wird. Wenn der »Deal« abgelehnt wird, macht die Gegenseite ein Angebot.

Demgegenüber könnte man auch folgende Auffassung vertreten: Der Konsument hat kein ökonomisches Interesse an Zweitverwertungsprozessen seiner Daten. Er sieht darin keinen Mehrwert, verfügt gegebenenfalls nicht über die erforderliche Medienkompetenz, um das Marktmodell zu verstehen. Ein selbstbestimmtes Handeln mit seinen Daten findet er zu kompliziert und unnötig.

Standardverarbeitungstypen definieren

Sinnvoller Datenschutz ist nur dann möglich, wenn unterschiedliche Regelungen und Vereinbarungen für unterschiedliche Datentypen und Verwendungen möglich sind. Darum bedarf es einer Typisierung.

Tags: Recht

Es gibt persönliche und personenbezogene Daten höchst unterschiedlicher Art, die nicht nur individuell, sondern auch strukturell anderen Methoden der Datenauswertung zugänglich sind. Was für eine Art von Daten in einem Kontext eine sinnvolle Regelung ist, kann in einem anderen kontraproduktiv sein. Eine pauschale Verregelung für alle Formen persönlicher und personenbezogener Daten ist daher weder praktikabel noch bringt sie die gewünschten Ergebnisse.

Das heutige Datenschutzrecht bietet keine adäquaten und verständlichen Antworten auf die Vielzahl verschiedener Aushandlungsprozesse zwischen den Vertragspartnern. Dies zu beheben ist nur durch eine strukturierte rechtliche Würdigung der gängigen Prozesse beispielsweise analog der Aufteilung in Kaufverträge, Mietverträge, Dienstleistungsverträge etc. möglich. Diese Typisierung könnte z. B. für die Datennutzung im Rahmen von Zahlungsabwicklungsvorgängen, Marktforschungsdatenüberlassungen oder Drittparteinutzung verbindliche Kriterien definieren, die ein hohes Maß an Verlässlichkeit für die beteiligten Parteien garantieren.

Verständliche Datenschutzerklärungen

Privacy Policies müssen einfacher und »human readable« werden. Sonst haben sie keinen Effekt.

Tags: Recht, Kompetenz

Da die wenigsten Menschen Zeit und Muße haben, sich Datenschutzbestimmungen durchzulesen, und noch weniger Menschen die technische und rechtliche Expertise haben, sie zu verstehen, selbst wenn sie sie lesen, sollten modularisierte und größtenteils standardisierte Datenhandhabungspraktiken entwickelt und genutzt werden. Dabei wäre es sehr wünschenswert eine Sprache zu nutzen, die auch Nicht-Juristen verstehen. Da dies häufig nicht möglich ist, sollten einfach verständliche Beschreibungen der Praktiken und für häufige Module grafische Symbole genutzt werden. Als Vorbild dafür könnte Creative Commons dienen, auch wenn starker Widerstand jener Unternehmen zu erwarten ist, deren Geschäftsmodell derzeit auf der Sammlung und Auswertung der Nutzerdaten beruht. Durch eine Vereinfachung der Datenschutzrichtlinien würde erstmalig einer Mehrheit der Nutzer die Möglichkeit gegeben werden, tatsächlich zu verstehen, wozu sie ihr Einverständnis erklären, wenn sie einen neuen Account anlegen, online einkaufen oder neue Programme auf ihren Mobiltelefonen oder Computern installieren. Dadurch kann dann ein Vertrauensverhältnis zwischen den Anbietern und Nutzern entstehen, das sich nicht zuletzt für die Anbieter auszahlen wird.

Haftung

Firmen, die mit Nutzerdaten handeln bzw. die bei der Nutzung ihrer Dienste systematisch Nutzerdaten sammeln, müssen im Falle des Verlustes dieser Daten stärker haftbar gemacht werden. Dies könnte entweder durch Bußgelder bei Fahrlässigkeit im Umgang mit den ihnen anvertrauten Daten geschehen oder durch die Einführung eines Anspruchs auf Schmerzensgeld auf Seiten der geschädigten Nutzer.

Tags: Recht, Ökonomie

Zurzeit droht Firmen bei Verlust oder Missbrauch von Nutzerdaten vor allen Dingen ein Rufschaden, aber das auch nur, wenn der Verlust hinreichend Öffentlichkeit erreicht. Gesetzliche normierte Bußgeldtatbestände können nur sehr punktuell angewendet werden. Beide Elemente haben lediglich Abschreckungsfunktion. Der derzeitig normierte gesetzliche Schadensersatzanspruch läuft fast völlig leer, weil ein finanzieller Schaden meist nicht nachweisbar ist. Firmen haben hohe Anreize, Nutzer dazu zu ermutigen, Daten an sie weiterzugeben, allerdings nur wenige Beweggründe, diese Daten angemessen zu schützen.

Statt einer Auflistung sei hier nur noch einmal auf die Datenpanne bei Sony hingewiesen, bei der nach Angaben der Financial Times Deutschland 77 Millionen Nutzer betroffen waren. Obschon in diesem Fall der Rufschaden immens war und möglicherweise zu einem Umdenken führt, wird dies innerhalb der Branche wohl nicht zu einem systematischen Wechsel der Sichtweise kommen, da sich diese Betrachtungen nur schwer in die wirtschaftlichen Risikoberechnungen einbeziehen lassen.

Durch stärkere Haftung der Firmen würde ein Anreiz für bessere Sicherung der Daten geschaffen. Diese Anreizstruktur zu Gunsten eines systematischen Ausbaus der Sicherung könnte einen ganz eigenen Markt von Versicherungen (Data Insurance) entstehen lassen, der gleichzeitig auch die Standardisierung des (sichereren) Umgangs mit Daten vorantreiben würde.

Schutzpflicht

Der Staat muss seine Aufgabe als schützende Instanz neu bestimmen. In der derzeitigen Praxis datenschutzbezogener staatlicher Regulierung ist ein zunehmendes Zurückziehen auf das bloße Sicherstellen der prinzipiellen nutzerseitigen Beeinflussbarkeit zu beobachten. Der Aspekt der staatlichen Schutzpflicht geht jedoch zunehmend verloren.

Tags: Recht

Die Handlungsautonomie von Bürgern, die mangels Wissen oder Kompetenz nicht in der Lage sind, von ihren Beeinflussungsmöglichkeiten tatsächlich angemessen Gebrauch zu machen, wird dadurch letztendlich nicht erhöht, sondern reduziert. Entgegen der Erwartung führt das herrschende Datenschutzkonzept im Internet insofern nicht zu einer größeren Autonomie der Menschen. Im Gegenteil: Die Handlungsautonomie der Menschen wird verringert. Denn mit dem Verweis auf die Datenhoheit des Nutzers folgt im Ergebnis eine Verlagerung des Prognoserisikos von zukünftigen Gesellschafts- und Technikentwicklungen auf den Betroffenen.

Im klassischen System des öffentlich-rechtlichen Datenschutzes waren aufgrund der Förmlichkeit von Verwaltungsverfahren die Akteure, Prozesse und Verarbeitungsschritte beim Umgang mit personenbezogenen Daten noch klar strukturiert und vorhersehbar, mithin auch ordnungsrechtlich sanktioniert und verfahrensrechtlich abgesichert zu fassen. Im nicht öffentlichen Bereich und mit den aufkommenden sozial-digitalen Phänomenen (Web 2.0) wird die Prognose über die möglichen Datenverwendungen und Prozesse für den legislativen Entscheider schwieriger. Die klassische Ex-ante-Beurteilung als Reaktion auf veränderte Realweltbedingungen und die notwendige Anpassung des Regulierungsrahmens scheitert an prognostischen Unsicherheiten im Spannungsfeld von »Innovationsoffenheit« und Verbürgung des grundrechtlichen Schutzes. In der Folge zieht sich der Gesetzgeber aus seinen auch im Verhältnis Bürger/Bürger bestehenden Schutzpflichten

zurück und begibt sich damit auch seiner Einschätzungsprärogative. Statt der eigenen Wertung wird der Typus »Datenhoheit« geprägt, der die Entscheidung über gewünschte und unerwünschte Datenverwendungen dem Betroffenen überträgt. Damit verkehrt sich das Regel-Ausnahme-Verhältnis der klassischen Anschauung (gesetzliche Wertung/Einwilligung). Es muss deshalb vor dem Hintergrund, dass die Gefahren für die informationelle Selbstbestimmung zwischen privaten Akteuren im Internet ja nicht geringer zu bewerten sind, als im Verhältnis des Staates zu seinen Bürgern, die Frage gestellt werden, ob es legitim sein kann, nun regelmäßig dem Betroffenen das Prognoserisiko aufzubürden, wenn schon der Gesetzgeber an der Komplexität der Systeme scheitert. Sinnvoll scheint es insofern, vielmehr der Frage nachzugehen, wie der Gesetzgeber das notwendige Wissen effektiv in seine Entscheidungsprozesse integrieren kann.

Nachträgliche Regelungsmechanismen

Das bislang vorherrschende Paradigma der präventiven Beeinflussung von Systemplanung und -entwicklung muss um neue, nachträglich wirkende Mechanismen angereichert werden.

Tags: Recht

Der derzeitige Regulierungsansatz im Datenschutz folgt im Grundsatz einem Top-down-Modell und schlägt angesichts neuer, der Bottom-up-Methode und dem Prinzip der Emergenz folgender Entwicklungsmodelle fehl. Die bisherige Regulierung im Bereich des Datenschutzes geht im Grundsatz von bewusst und planerisch gestalteten »Systemen« aus, für welche dann normative Regeln gesetzt werden, an denen sich der Planungs- und Gestaltungsprozess auszurichten hat. Neue Entwicklungsparadigmen folgen jedoch oftmals dem Prinzip der »Emergenz«, bei dem nicht mehr »Systeme geplant werden«, sondern im Zuge dynamischer Orchestrierung und Rekombination geradezu plötzlich (im Vergleich zum alten Paradigma) »entstehen«.

Für das bisherige Regulierungsparadigma geht damit schon der Ansatzpunkt für die Regulierung – der Planungsprozess – verloren. Regulierung nach dem bisher etablierten Paradigma schlägt damit für eine zunehmende Anzahl von Fällen schon im Ansatz fehl. Dies wiederum führt zur Notwendigkeit neuer Ansätze für datenschutzbezogene Regulierung, mittels derer sich auch bottom-up gerichtete, emergenzähnliche Phänomene und Sachverhalte beeinflussen lassen. Wegen der fehlenden Vorabbeeinflussbarkeit erscheinen hier prinzipiell lediglich ex post wirkende Regulierungsmechanismen tragfähig und sollten daher in der Zukunft eingehender betrachtet werden. Hierbei sollte gewährleistet sein, dass eventuelle Eingriffe sich auf die geringstmögliche Eingriffstiefe beschränken und nicht etwa auf Basisdienste abzielen, auf Grundlage derer neben unerwünschten auch gesellschaftlich wünschenswerte Ergebnisse entstehen können.

Erlaubnis- statt Verbotsprinzip

Diese These zielt nicht auf einen Abbau des rechtlichen Datenschutzes ab, sondern verweist vielmehr darauf, dass sich das heutige Verbotsprinzip als wenig effektiv und weitgehend aufgeweicht herausstellt. Ein Umbau hin zu einem Erlaubnisprinzip mit klar formulierten Verboten kann in der Rechtspraxis zu mehr Klarheit und für den Betroffenen zu mehr Sicherheit führen.

Tags: Recht

In den vergangenen Jahrzehnten wurden immer wieder neue Erlaubnistatbestände geschaffen, die zum Teil sehr weitgehend sind und zur Subsumtion mannigfacher Tatbestände verwendet werden. In der Laiensphäre führt dies dazu, dass Betroffene kaum mehr zwischen Sachverhalten unterscheiden können, in denen sie eine rechtswirksame Einwilligung zu erteilen haben und solchen, in denen ihre Einwilligung obsolet ist. Die aus dem Verbotsprinzip notwendigerweise große Weite der Erlaubnistatbestände führt dazu, dass sich Betroffene nur selten mit dem tatsächlich stattfindenden Eingriff in ihre Grundrechtssphäre konfrontiert sehen und verarbeitende Stellen sich zugleich ständig auf den Freifahrtschein der Erlaubnis ausruhen können.

Dem könnte ein Modell gegenüberstehen, das die Verarbeitung von personenbezogenen Daten erlaubt, in Sonderfällen aber verbietet. Eingriffe können in Intensivitätsstufen unterschieden werden, aus denen Anforderungen für Transparenz und Einwilligung abgeleitet werden können.

Unverletzlichkeit der Cloud: Das Konzept der Unverletzlichkeit der Wohnung muss auf digitale Devices und Cloud Computing ausgedehnt werden.

Begründung: Auf jedem Smartphone als Zugangspunkt und allen digitalen Kommunikationskanälen, Datenarchiven und Datensammlungen sind immer und überall mehr private und umfassendere Daten als in einer Wohnung sammelbar.

Privacy by Design und Macht

Privacy braucht geschlossene Systeme. Solcherlei geschllossene »Datensilos« können problematische Machtkonzentrationen bei Plattformbetreibern mit sich bringen.

Tags: Ökonomie, Recht

Der Ruf der einzelnen Nutzer einer Plattform, ihre Privatsphärenbedürfnisse untereinander durchzusetzen, setzt die Plattform als Informationskontrolleur voraus. Der Anspruch an Plattformanbieter, doch bitte umfangreiche Kontrollmöglichkeiten für Privatsphäreneinstellungen seiner Nutzer bereitzustellen, versetzt die Anbieter in eine Position, die in etwa derjenigen gleicht, die Thomas Hobbes für den Staat vorhergesehen hat. Weil der Mensch dem Menschen ein »Privatsphäreneindringlingswolf« ist, wendet man sich an den zentralen Privacy-Leviathan-Anbieter, dass er mit seinem Zugangs-(Gewalt-)Monopol die virtuellen Grenzen und Wände der Menschen untereinander durchsetzt. Die Privacy-Optionen versetzen also Anbieter in eine staatsähnliche Position – aber eben im Gegensatz zum Staat nicht durch Gesetze, sondern durch Codes. Alle haben sich umso mehr dem Regime des jeweiligen Anbieters zu unterwerfen, je mehr sie auf dessen Datenschutzstrukturen angewiesen sind.

Es entwickelt sich derzeit eine neue Machtasymmetrie, die niemand richtig im Blick hat, weil wir in Sachen Daten noch zu sehr im Sinne von Besitz und Ort – unserer alten geopolitischen Ordnung – denken, anstatt zu verstehen, dass sich alles zunehmend um Zugang und dessen Regulierung dreht. Es geht im Moment darum, dass sich Konzerne und ihre Plattformen als neue Ordnungsmächte im Digitalen etablieren (als Ablösung für den Staat), und die Datenschützer sind ihre eifrigsten Helfer.

Um Privacy zwischen einzelnen Nutzern einer Plattform herstellen zu können, braucht es eine unhintergehbare Macht, die Strukturen anbietet, um

diese durchzusetzen. (Alternativ sind einzig und allein Verschlüsselungsverfahren denkbar, die sich aber aufgrund ihrer Unhandlichkeit bislang nicht durchsetzen konnten. Außerdem geht es bei Verschlüsselung immer nur um Kanalverschlüsselung und nicht um objektbezogenes Zugriffsmanagement. Objektbezogene Verfahren wie DRM wiederum würden den Umgang mit einem Social Network unendlich verkomplizieren und für Zentralisierung anfällig machen. Siehe DRM-Debatte im Urheberrecht.) Einziger Ausweg ist das zentral gemanagte Datensilo, wie z. B. Facebook oder Google+.

Endnutzer und Intermediäre

Es muss für Endanwender immer die Möglichkeit geben, das Internet so zu nutzen, dass sich sämtliche anwendungsspezifische Funktionen so weit wie technisch möglich in den Endpunkten befinden und damit ihrer direkten Kontrolle unterliegen. Ebenso muss es aber auch möglich bleiben, Anwendungen so zu gestalten, dass Intermediären eine unterstützende Rolle in deren Ausgestaltung zufällt.

Tags: Kompetenz, Recht

Seit mehr als 30 Jahren gibt es eine disziplinenübergreifende Debatte zur grundlegenden Architektur des Internets. Während es als anerkanntes Prinzip gilt, anwendungsspezifische Funktionen in den Endknoten des Internets zu implementieren – TCP mag hier als kanonisches Beispiel für zuverlässigen Ende-zu-Ende-Datentransfer gelten –, ist es ebenso plausibel, in vielen Fällen wichtige Anwendungsfunktionen an zentralere Intermediäre zu delegieren – siehe etwa Routing und DNS. Eine genügend flexible Architektur des Internets muss also prinzipiell beides erlauben: Funktionen in den Enden sowie im Netz und dies in möglichst feingranularer Abstufung. Normative Debatten sollten diese empirische Prämisse als Wert an sich ernst nehmen.

Es ist nur bedingt sinnvoll, die fälligen gesellschaftlichen Debatten zu Privatheit und Öffentlichkeit im Internet primär entlang von Konzepten wie Datenhoheit und ähnlichen zu orientieren; stattdessen erscheint es angezeigt, Flexibilität bei der Gestaltung und Platzierung von Anwendungsfunktionen zu fördern. Konkret: Es sollte für Endanwender immer die Möglichkeit geben, das Internet so zu nutzen, dass sämtliche Funktionen über Best-Effort-IP-Service hinaus in den Endpunkten und damit unter ihrer unmittelbaren Kontrolle liegen. Dies bezieht sich einerseits auf die Anwendungen selbst – kontingente Intermediäre sind hier explizit nicht Teil der verteilten Anwendungsstruktur – und andererseits auf die zu kommunizierenden Daten – diese werden nach dem Ermessen der beteiligten Endpunkte

verschlüsselt, so dass Intermediäre darauf keinen Zugriff haben. Dieser Forderung folgend sollten Anwendungen möglichst so spezifiziert werden, dass sie potentiell Ende-zu-Ende-basiert umsetzbar sind, und entsprechende Standards sollten dem nicht unnötig im Wege stehen.

Ebenso muss es aber auch möglich sein, Anwendungen so zu gestalten, dass Intermediären – sowohl explizit aufgerufenen als auch transparent intervenierenden – eine unterstützende Rolle in der Ausgestaltung der Funktionalitäten zufällt. Weder sollte also Ende-zu-Ende-Verschlüsselung von Daten obligatorisch (technisch oder rechtlich) sein, noch sollte die potentielle Rolle von Intermediären unnötig eingeschränkt werden durch rechtliche Vorgaben oder Standards in dieser Hinsicht. Um dies auch dann zu einer sinnvollen Option für Endnutzer zu machen, wenn es um sensible private Daten geht und Intermediäre als nur bedingt vertrauenswürdig gelten können, müssen technisch-architektonische Lösungen umgesetzt werden, die die Machtbalance zwischen Endnutzern und Intermediären auch in diesem Szenario wahren. Eine gangbare und zu fördernde Entwicklung in dieser Hinsicht ist Multihoming, also die gleichzeitige Kommunikation über unterschiedliche Internetzugänge, so dass einzelne Intermediäre keinen Zugriff auf die vollständige Kommunikation der fraglichen Anwendung haben.

Big Data

Weder Potentiale noch Risiken großer Datensammlungen lassen sich ex ante bestimmen. Beide können immens sein. Die inhärenten Risiken müssen dringend in den Blick genommen werden.

Tags: Aggregation

Während sich die öffentliche Diskussion um Privatheit auf die Preisgabe von persönlichen Informationen konzentriert, wird nicht ausreichend thematisiert, wer die Kontrolle über persönliche Informationen hat.

Der derzeitige Datenschutz und die klassische »Information Privacy« sind ungenügende Konzepte, um die informationelle Selbstbestimmung zu adressieren, da sie sich auf sichere und transparente Datensammlung und Verarbeitung konzentrieren. Hinzu treten müssen Konzepte, ethische Modelle und rechtliche Rahmenbedingungen, um die Wirkungen, die die Nutzung von Informationssystemen mit sich bringen, im Bezug auf Diskriminierung, »Social Sorting« und andere Beeinträchtigungen der persönlichen Freiheiten und gesellschaftlichen Werte zu verstehen und neu zu verhandeln.

Grundsätzlich wissen wir um die Disruptivität von datenbankübergreifenden Verknüpfungen von Datensätzen. Durch das Internet werden Vollerhebungen mit hoher Datendichte ständig vorgenommen, was neue Dimensionen für die Auswertungsmöglichkeiten evoziert. Statistische Verfahren können aus großen Datenbeständen Aussagen über zukünftige, erwartbare menschliche und gesellschaftliche Verhaltensweisen generieren. So hilfreich und wichtig solche Prognosen für etwa politische Entscheidungsprozesse sind, so gefährlich sind sie auch, wenn sie manipulativ eingesetzt werden. Das Recht adressiert diese Frage bisher nicht, eine politische Strategie um die Implikationen ist bisher nicht vernehmbar, eine öffentliche Debatte findet bisher nicht oder kaum konzentriert und wahrnehmbar statt.

Toleranz

Toleranz gewinnt in der digitalen Gesellschaft weiter an Bedeutung und sollte vom Kindergarten an »gelehrt« werden.

Tags: Kompetenz

Die Möglichkeit mehr über andere und ihre Eigenschaften zu erfahren wird der Gesellschaft und all ihren Akteuren ein Mehr an Toleranz abverlangen. Während wir heute eigentlich nur wenig über unsere Mitmenschen, Mitarbeiter, Vorgesetzten und Freunde wissen, werden in der Zukunft auch uns bislang verborgene Seiten technisch einfacher zugänglich sein. Konstitutiv für ein Funktionieren der Gesellschaft wird daher sein, dass es Lösungen für den Umgang mit diesem Mehr an Wissen über die anderen gibt.

Reiz des Privaten

Eine Welt mit Privatsphäre ist interessanter als eine ohne.

Tags: Kompetenz

Nehmen wir an, Post-Privacy wäre ein natürlicher Zustand, der verschiedene Vorteile mitbringt. Nehmen wir weiter an, die Konstruktion von Privatheit und deren technische Umsetzung stellt einen künstlichen Eingriff, eine Einschränkung des Informationsflusses dar. Selbst dann lohnt es, Privatheit zu ermöglichen, weil sie das Leben reicher und sinnvoller macht.

Es ist menschlich und wünschenswert, Informationen exklusiv mit einer kleinen Gruppe zu teilen. Private Informationen bzw. Geheimnisse anderer bedeuten für den Betroffenen Unwissenheit oder unvollständiges Wissen. Diese Uninformiertheit kann unter anderem zu zwei Effekten führen: Überraschungen und Fehlentscheidungen, also Entscheidungen, die ich bei vollständiger Datenlage anders getroffen hätte. Dass Überraschungen das Leben bereichern können, ist offensichtlich: Man stelle sich nur »totale Transparenz« bei einem Pokerspiel vor. Langweilig. Aber auch das Geburtstagsgeschenk und der Abenteuerurlaub verlieren an Reiz. Scheinbare Fehlentscheidungen tragen ebenfalls erheblich zu einem erfüllten Leben bei: Rückblickend lässt sich oft feststellen, dass ich manche Person nie näher kennengelernt, manche Orte nie besucht, manche Aktivität nie unternommen hätte, wenn ich vorher alles über sie hätte erfahren können; denn nur zu oft entscheide ich mich für das Bekannte, Vertraute, Passende. Gerade die unerwarteten, nicht ganz passenden Begegnungen sind es aber, die das Leben lebenswert machen.

Umkehrschluss: Eine Welt ohne Privatsphäre, ohne Geheimnisse, mit totaler Information ist zwar möglich, vielleicht auch effizient, vielleicht sogar in mancherlei Hinsicht optimal. Aber sie ist letztlich langweilig und vielleicht sogar sinnlos.

2 Privatheit und Öffentlichkeit: Seitenblicke

2.1 Der Innenminster: Interview mit Hans-Peter Friedrich

Hans-Peter Friedrich (CSU) ist seit 2011 Bundesminister des Inneren

»Grundsätzlich muss natürlich jeder selbst entscheiden, wie viel er von sich selbst im Internet preisgeben möchte.«

Foto: CC BY-SA, Henning Schacht

Was zeichnet die verfügbaren Daten/Informationen aus? Was ist das qualitativ Neue der Daten?

Wissen ist Macht. Und der kostbare Rohstoff, aus dem das Wissen gemacht wird, ist die Information. Lange Zeit hatte nur ein eng begrenzter Kreis von Personen Zugang zu Informationen. Bücher und Zeitungen waren – global betrachtet – nur für eine Minderheit zugänglich. Das ist heute anders. Das Internet hat den Zugang zu Informationen und Daten »demokratisiert«: Wissen ist heute praktisch überall, jederzeit und für jedermann verfügbar. Das Internet ist eine kollektive Informationsquelle, aus der sich jeder bedienen kann – vorausgesetzt er hat Zugang zu Computer und Netz.

Und diese Informationsquelle sprudelt lebhaft: Täglich – ja sekündlich – füllt sich das Internet mit neuen Informationen – mit Wissen über die Welt und mit Wissen über uns. Das hat viele positive Folgen. Wenn ich zum Beispiel an mein Studium zurückdenke, dann kommt mir das vor wie ein

Blick in eine andere Welt: wir Studenten mussten oft stundenlang in Bibliotheken recherchieren, um Gerichtsurteile und Fachaufsätze zu einem bestimmten Thema herauszusuchen. Und wenn man Pech hatte, war die relevante Seite zuvor von einem anderen Kommilitonen herausgerissen worden. Hinzu kam: Manche Bücher waren nicht immer verfügbar. Mitunter mussten sie in anderen Bibliotheken bestellt werden. Eine Wartezeit von einer Woche war dann normal. Heute hingegen sind viele dieser Informationen oftmals nur einen Mausklick entfernt.
Neu ist auch die Schnelligkeit, mit der das Internet Entwicklungen und Ereignisse in der ganzen Welt verbreiten kann. Wenn wir vom »global village«, vom globalen Dorf, sprechen, dann ist das Internet so etwas wie der virtuelle Dorfplatz dieses globalen Dorfs. Und dieser virtuelle Dorfplatz verändert nicht nur die Art und Weise der Berichterstattung. Wir alle kennen die Bilder vom Tahrir-Platz. Das Internet transportierte sie in Sekundenschnelle um die ganze Welt – ungefiltert und höchst individuell kommentiert, mit enormen Auswirkungen auf die Entwicklungen vor Ort und in der Region.

Wer entscheidet im Einzelfall, wo die Grenzen zwischen Öffentlichem und Privatem verlaufen? (Gesellschaftliche Perspektive)
Grundsätzlich muss natürlich jeder selbst entscheiden, wie viel er von sich selbst im Internet preisgeben möchte. Der Einzelne kann dies tun, indem er etwa seine Einstellungen in einem sozialen Netzwerk festlegt und seinen Freundeskreis definiert. Manchmal liegt es aber eben auch nicht in meiner Hand, z. B. wenn ich eine öffentliche Diskussionsveranstaltung besuche, mich zu Wort melde und die Veranstaltung später ins Netz gestellt wird. Von der Dokumentation der Diskussion profitieren wir letztlich wieder alle. Insofern wird die Grenze zwischen Privatem und Öffentlichem auch durch das öffentliche Interesse bestimmt. Wir müssen uns wahrscheinlich daran gewöhnen, dass wir durch das Internet auch ein Stück weit zu einer öffentlichen Person werden. Wichtig ist es, die Balance zu halten und auch der Privatheit Raum zu geben.

Welche Wechselwirkungen bestehen zwischen Identität und Öffentlichkeit und welche Spielarten gibt es? (Gesellschaftliche Perspektive)
Das Internet – so sagen die Experten – vergisst nichts. Es dokumentiert dauerhaft und öffentlich. Das ist nichts Schlechtes. Viele von uns werden im Internet alte Schulfreunde wiederentdeckt oder festgestellt haben, dass man mit der alten Sandkastenfreundin heute über drei Ecken beruflich zu tun hat. Wie stets, gibt es aber auch hier zwei Seiten einer Medaille: Denn im Internet finden sich unter Umständen auch Jugendsünden, alte Kontakte und Aktivitäten, an die man ungern erinnert werden möchte. Und die Gewichtung all dieser Mosaiksteinchen übernimmt die Suchmaschine. Das führt zu der Frage: Wie kann ich das Bild, das von mir gezeichnet wird, beeinflussen oder wieder gerade rücken? Die Wechselwirkungen zwischen Identität und Öffentlichkeit sind mitunter enorm facettenreich. Das Bundesministerium des Innern hat sich dieser interessanten Fragen mit dem Ideenwettbewerb »Vergessen im Internet« angenommen (www.vergessen-im-internet.de). Jeder ist eingeladen, sich hieran bis zum 31. Januar 2012 zu beteiligen.

Wo ist Ihnen Anonymität wichtig? (Individuelle Perspektive)
Anonymität ist mir dort wichtig, wo sie dem Schutz von Menschen dient. Gerade Beratungsstellen und Einrichtungen der Seelsorge müssen Anonymität garantieren können, da Menschen in Not sich ihnen nicht anvertrauen würden, wenn sie ihre Identität preisgeben müssten. Anonymität hat ihren Platz auch in Bereichen des Lebens, in denen es ein schützenswertes Vertrauen gibt, das nicht enttäuscht werden darf. Anonymität ist überall dort richtig, wo das Gegenüber kein berechtigtes Interesse an der Kenntnis meiner Identität hat.
Ein allgemein gültiges Recht auf Anonymität gibt es in unserer Gesellschaft nicht. Denn das Recht, zu wissen, mit wem man es zu tun hat, ist auch schützenswert. Das hat etwas damit zu tun, dass man Verantwortung

übernimmt für das, was man tut und sagt. Ich empfinde es – gerade auch angesichts unserer jüngeren Geschichte – als ein wertvolles Gut, dass jeder von uns heute in politischen Debatten mit offenem Visier streiten kann und mit seinem Namen für die eigene Meinung einstehen kann. Und dieses wertvolle Gut sollten wir auch auf dem virtuellen Dorfplatz nicht preisgeben.

2.2 Der Medienwissenschaftler: Interview mit Stefan Münker

Stefan Münker ist Medienwissenschaftler am Institut für Medienwissenschaft und Musikwissenschaft der Humboldt Universität Berlin, Publizist und unter anderem Autor von »Emergenz digitaler Öffentlichkeiten. Die Sozialen Medien des Web 2.0.«

»Die Grenze zwischen Öffentlichem und Privatem war nie starr. Ihr Verlauf hängt zudem immer davon ab, was in einem jeweiligen historischen und kulturellen Kontext als öffentlich und was als privat gilt.«

Was zeichnet die verfügbaren Daten/Informationen aus? Was ist das qualitativ Neue der Daten?

Abgesehen von der Tatsache, dass das Spektrum verfügbarer Daten in seiner medialen und technischen Diversität (von mesopotamischen Keilschrifttafeln zu digitalen Speichermedien) noch nie so groß war wie heute, ist das Spezifische gerade der im Netz digital verfügbaren Informationen ihre unspezifische Verfügbarkeit. Zu immer mehr Personen, Institutionen und Themen sind immer mehr Informationen in zerstreuten Dateien an verschiedensten Orten des Netzes gespeichert und dabei längst jedem zentralen Zugriff entzogen. Vielleicht mehr noch als die gigantische Menge der flottierenden Daten ist das Maß ihrer Zerstreuung das qualitativ Neue – weil es sie ebenso verfügbar wie unverfügbar macht.

Was für technische Möglichkeiten bestehen, mit diesen Daten umzugehen?

Es gibt viele Möglichkeiten, digitale Informationen zu verwerten. Am interessantesten erscheint mir die beliebige Reproduzierbarkeit und (Re-) Kombinierbarkeit von Daten. Dieser Prozess schafft die Voraussetzung für innovative Gestaltung und Kreativität.

Was sind die wesentlichen Veränderungen von Öffentlichkeit?

Die klassische Öffentlichkeit der modernen Gesellschaft war ein Produkt der Massenmedien. Zeitung und Zeitschrift, Radio oder Fernsehen wiederum sind Medien der Öffentlichkeit im doppelten Sinn: Sie sind als Mittel zur Artikulation von Öffentlichkeit zugleich Mittel zur Herstellung einer von ihnen unterschiedenen und unabhängigen Öffentlichkeit – der Öffentlichkeit der Leser, Hörer und Zuschauer, die im Diskurs über die gelesenen, gehörten oder gesehenen Informationen Meinungen ebenso austauschen wie bilden.

Anders als die elektronische Öffentlichkeit der Massenmedien hat die digitale Öffentlichkeit keine Leser, Hörer oder Zuschauer, die von ihr prinzipiell zu unterscheiden wären. Die Differenz: Hier sind die Medien, dort sind die Menschen – diese Differenz lässt sich in einem medialen Umfeld, das durch die Partizipation von aktiven Teilnehmern erst entsteht, eben nicht mehr machen.

Die vielleicht wichtigste Konsequenz der heute sichtbaren Veränderungen lautet: Während die durch Massenmedien institutionell konstituierte Öffentlichkeit in erster Linie als Vermittlungsinstanz zwischen den getrennten gesellschaftlichen Sphären von Politik, Ökonomie und Zivilgesellschaft gewirkt hat (und so auch noch fortwirkt), sind die im Netz entstehenden Öffentlichkeiten zum einen (noch) nur selten institutionell verankert, zum anderen und vor allem vermitteln sie nicht zwischen getrennten gesellschaftlichen Sphären – sie vermischen diese vielmehr. Die Öffentlichkeit im Netz fördert die Durchlässigkeit bestehender Grenzen ebenso wie die Transparenz starrer Strukturen – und sie bringt dadurch das etablierte Gefüge der gesamten Gesellschaft durcheinander.

Wer entscheidet im Einzelfall, wo die Grenzen zwischen Öffentlichem und Privatem verlaufen?

Die Grenze zwischen Öffentlichem und Privatem war nie starr. Ihr Verlauf hängt zudem immer davon ab, was in einem jeweiligen historischen und kulturellen Kontext als öffentlich und was als privat gilt. Die historische und kulturelle Variabilität ist enorm – und tatsächlich wird das Begriffspaar aufgrund der gegenwärtigen Entwicklungen im und durch das Internet in neue Konstellationen gebracht.

Für die Entscheidung im Einzelfall ist das relevant insofern, als eben die Frage, ob eine preisgegebene Information als privat überhaupt gilt, längst nicht gesellschaftsweit (geschweige denn weltweit) konsensual beantwortet wird.

Vor diesem Hintergrund gilt: Im Einzelfall entscheidet einerseits der jeweilige gesellschaftliche Akteur (ein Publikationsmedium etwa, oder ein soziales Netzwerk) durch die an Bedingungen geknüpfte Vergabe von Zugangsoptionen über Publikationsoptionen – und legt z. B. in seinen Geschäftsbedingungen dabei fest, was ihm als veröffentlichbar überhaupt gilt. Alles andere bleibt per Ausschluss privat. Andererseits hat der private Akteur (als Nutzer eines Netzwerks beispielsweise) die Möglichkeit, im Einzelfall Exklusionsoptionen wahrzunehmen (opt-out Regeln, o. ä.), und mit dem Widerspruch zur Veröffentlichung bestimmter Daten ihre Privatheit für sich persönlich zu definieren.

Welche Wechselwirkungen bestehen zwischen Identität und Öffentlichkeit und welche Spielarten gibt es?

Welche Identität? Die der Gesellschaft – oder die ihrer Mitglieder? Die Art und Weise einer jeweiligen Gesellschaft ist ebenso abhängig von wie konstitutiv für die Art und Weise ihrer jeweiligen Öffentlichkeit. Verändern können sie sich nur gemeinsam. Für die individuellen Mitglieder einer Gesellschaft ist die jeweilige Öffentlichkeit ein elementares Medium zur Teilhabe – an Informationen ebenso wie an Diskussionen. Die Art der Öffentlichkeit entscheidet über die Art der Teilhabe: passiv wie zu Zeiten der Massenmedien oder (potentiell) aktiv wie im digitalen Netz. Wer sich

als Teil einer Gesellschaft zugleich über die Teilhabe an dieser identifiziert, für den ist jeder Wandel der Öffentlichkeit ein entscheidender Faktion seiner Identitätsbildung.

Welche (Arten von) Informationen willst Du freigeben? An wen? Warum?

Persönliche Informationen zu filtern und ihre Freigabe zu kontrollieren ist Teil der Art von Identitätsmanagement, die eine immer größere Bedeutung in unserer immer vernetzteren Welt spielt. Die Kompetenz dazu freilich scheint mir bei vielen, gerade auch vielen jungen Akteuren deutlich unterentwickelt.

Ich persönlich gebe Informationen sehr freigebig, aber zugleich stark gefiltert und ebenso kontrolliert preis – d. h. verschiedene Daten und Datenarten in verschiedenen Kontexten und Gruppen.

An welchen Orten/Portalen gibst Du Daten preis?

Müsste es hier nicht umgekehrt heißen: an welchen Orten gibt man keine Daten preis?

An welchen Informationen über mich hat die Öffentlichkeit ein berechtigtes Interesse?

»Die« Öffentlichkeit gibt es nicht. Deswegen kann es auch keine eine Öffentlichkeit geben, die ein berechtigtes Interesse an irgendwelchen Informationen hat. Dennoch: Die Öffentlichkeit hat ein berechtigtes Interesse an Information über einzelne Individuen überhaupt nur dann, wenn diese Informationen auch gesellschaftlich relevant sind.

2.3 Die Bloggerin: Interview mit Danah Boyd

Foto: CC BY, Joi Ito

Die US-amerikanische Medienforscherin und Bloggerin Danah Boyd ist Expertin für Online-Kultur und soziale Medien.

»In face-to-face encounters, our interactions are »private by default, public through effort.« With mediated technologies, the defaults are inverted. Interactions are »public by default, private through effort.«

What is the function of the public sphere and what are its requirements in terms of privacy?

The public sphere is where society is created and maintained. It is where people stop being individuals and become part of a society. It is the site of civilization. The public sphere is created through the imagination, ideas, and actions of people working towards a greater good.

Privacy is a social process by which people maintain the intimate. Privacy exists only to the degree that people have agency and the ability to control a social situation. The public sphere exists when people have agency and are willing to give up control. Without agency, neither exist.

The public sphere does not rely on an expulsion of the intimate. It does not require that everything be made transparent. And, more importantly, it does not mean that we need to erode the agency of individuals. In fact, that destroys the public sphere too. There is plenty of room to carve out privacy in society even when there is a healthy public sphere.

The problem is that these words – public (adj), public (government) public sphere, publics, publicity, privacy, private (commercial), private (adj), etc. – all look like they are the same but they are not; they refer to different conceptions and, of course, even educated folks disagree on their essence.

What information about myself is of legitimate interest to the public?

People are interested in gossip, but that does not mean that their interest is legitimate to the health of a public sphere. But keep in mind that there is a difference between a public and the public sphere. Increasingly, we are seeing commercialized publics where the economics of capitalism are driving the »interests.« And we have always seen social publics where people's curiosity and desire to hold power over others drives their eavesdropping. But that is not a public sphere.

What (kinds of) information do you want to make accessible and to whom?

The reason why privacy is confusing at this point in history is that the very idea of access is getting reworked. In face-to-face encounters, our interactions are »private by default, public through effort.« Publicizing a conversation takes effort and so we only share the things that we think are appropriate (or the juicy gossip that we want to share even though we're violating social norms). With mediated technologies, the defaults are inverted. Interactions are »public by default, private through effort.« In other words, what we share in a mediated environment is easily accessible – either by those we intend or by those who get access through unexpected means. Sharing is much easier because content is easily replicable online. And it is persistent by default. All of this changes how we think about privacy.

But the point here is that access means something very different in a mediated environment than it does in an unmediated environment. And what it means to reveal is also different. For example, I do not have a choice but to reveal my race, gender, height, and approximate age in physical environments. I may try to obscure it or modify it but I do not really have a lot of choices there. Online, I cannot avoid revealing other things …

What information do you want to keep secret? From whom and why?

Secrecy is the process of purposeful non-disclosure to specific people. What I keep »secret« changes depending on the audience. Keep in mind... it is ALL about audience and context for all of these issues.

And what do you want to know about others (curiosity)?

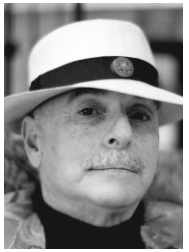
There are many different reasons to want to know things about others. Sometimes, it is a matter of curiosity. Sometimes, it is so that we can find common ground so that we can relate (this is critical for the public sphere). Sometimes, it is to exert power over someone (this is what destroys the public sphere). Our incentives drive the kinds of information that we want to know.

Where is anonymity important to you?

Anonymity has a bad rap these days because it is assumed that it is always about concealing information. Sometimes, it is simply about creating a space where you have the right to be let alone. There are times and places when I love being recognized; there are times and places where it is a pain in the ass. This is true for many people. Personally, I love the ability to be able to be anonymous in public; I can put my guard down, even when all I am trying to do is read a book in a cafe. I do not have to keep a smiley face or be my work self. And that can be a serious relief. That is a mundane reason to want anonymity but it is important to recognize. Anonymity is more politically important – especially when we're talking about the public sphere – when you think about what it means to speak truth to power. Whistle blowing is one that we can never forget.

→ Weitere Gedanken zu dem Thema finden Sie unter Anderem in dem Artikel »Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies« unter http://www.danah.org

2.4 Der Social-Media-Pionier: Interview mit Howard Rheingold



Howard Rheingold is known as the inventor of the term »virtual community«, the first executive editor of the online edition of the Wired Magazine »HotWired« and visiting lecturer for the communication department of the Stanford University.

»Many people are unaware to which degree their self-expressions are available to many people they don't know.«

Is the Internet a rather private or public space?
The default is definitely a public space. Unless you take strong technical measures to insure privacy, whatever you post is going to be reproducible, distributable and potentially online forever. You can't get much more public than that.

On his understanding of the term »publics«:
Of course there is a lot of political theory about »the public sphere« and one of the arguments that have come up is that there is not just one public sphere. Originally, Habermas' public sphere was the traditional political and intellectual discourse of the (European) »bourgeois public«. It was essentially white, middle class males, however especially over the last 50 years we have of course seen people, who are not white, not middle class and not male, influencing public opinion. Those movements have been called »counter-publics«.
Feminism, and gay and lesbian movements are good examples of people who were left out of what was considered the public sphere, and who made their own counter-public, by forming their own »gender publics«.

The civil rights movement is another example of people forming their own public. They created a public in the sense of various media – from face-to-face to publications of various kinds.
What is increasingly important to the formation of publics is the access to communication – Now that is not just print and broadcast but all the media that are available online. The formation of publics is much easier and more rapid and fluent than it ever was before. The plurality of the public spheres depends on the plurality of the contributions.

How the rapid growth of social media is confusing many people and how individuals are using the Internet as a tool to build their identity:
There is a certain degree of confusion among many people. They often don't know when they do things online when it is public and when it is not. I think there is an illusion of privacy. This is because people are in the comfort of their private homes when they are participating online. Many people are unaware to which degree their self-expressions are available to many people they don't know.
I think that the Internet has brought some changes to what we traditionally understand as »identity«. For most of history, physical presence has been regarded as our frame and limit to marketing our identity. So, the presentation of self depended on who was visible in the physical environment. However, over time it has extended to an invisible environment where people are not physically present. This was first true for people of public interest like politicians and artists but is now true for everybody. Today our identities are available in the form of text and multimedia to the whole world. Nevertheless, you can modify how you present yourself according to what particular forum you interact in. There are all these social clusters that one participates in and they are somewhat collapsed on the Internet in a way we can't completely analyze yet.

What is perceived as private and public and how to enable people to take advantage of these new conditions?
The reasons for violating ones privacy can be divided into embarrassment and control. If somebody can see you naked that might be considered embarrassing and as some kind of a breach of privacy. But that does not necessarily give the people who see you naked control over you. On the other hand, if the state or a private individual is able to surveil you and to obtain private information about you that enables them to influence or even control your behavior in some way – That is a very serious danger.
Education is the most effective and the most practical way to equip people. There is a group of people who voluntarily provide sensitive information. The famous drunken college photo on Facebook is a good example of that can be harmful to them when applying for a job. I think the best way is to teach the children. Like taking them to the sidewalk and showing them how to cross the street in order to equip them for a life in the automobile age. This is because young people need to be equipped for life before they get online.
I think there needs to be education about the degree of how information about them is available on the Internet and how it can impact their lives, and about what control they have, if any – Are there any privacy controls in the social network service that they are using? What kind of self-restraint on their own behavior is appropriate – in what circumstances, for what reasons? It is fairly simple to educate people about the difference between privacy as embarrassment and privacy as control but they are not really discussed. They are not among the facts of life that parents talk to their kids about. This all happened very rapidly and with extremely rare exceptions, I don't see it at schools.

How should, and how can the enabling and educating of people be implemented into policy?
Other than international agreements on what is widely agreed to be criminal behavior, a lot of problems have to do with cultural differences regarding norms. Norms of privacy are very different from place to place.

There are places like Japan were people share a very dense living-space. Hence special norms about pretending and acting as if you can't hear one another have developed.

If there was a general political agreement about regulating the Internet (of course the internet is international and growing in all different countries all with their own laws) states could try to control their own citizens. Luckily it is very difficult (near to impossible) to make some kinds of general regulations.

Furthermore, the danger of states manipulating and controlling the thoughts and speech of citizens are so much greater then the dangers of unregulated speech (including privacy infringements). So overall I think, the idea to create some kind of international regulation is really a threat to the generative creativity and the use of the Internet for political purposes. I think that education is most important to equip people to use the net to contribute to society while also enabling individual privacy solutions.

We have seen that play out in China, Iran and in the Middle East where people who are seeking freedom of expression use the Internet to organize, and the state uses regulation of the Internet to try to control that expression. That is the great danger when you have some kind of international regulation other than, as I said, on criminal activities.

Regulating the Internet raises the question of anonymity and (governmental) surveillance:

In terms of anonymity and openness the distinction must be made between the Internet in general and any particular forum on the Internet. Of course a particular forum on the Internet can institutionalize it's own rules – for instance that you have to have a verified identity. People who have verified identities have proven to become more reasonable in their statements online. Most of the unacceptable »drive-by comments« don't have verified and identifiable names.

Having said that, I think there are several very strong examples where it is important to be anonymous. There are whistleblowers e.g. exposing corruption and dangers for the public safety, and they need to have protection. There are individuals who seek to escape substance abuse and who help others to escape substance abuse – they require anonymity. Another example are victims of domestic abuse. Political dissidents are perhaps the most important example it is important to be able to speak freely without the fear of state punishment for statements about political positions. I think there are very strong arguments for maintaining a place of anonymity and not executing technical measures that prohibit it. States already have a lot of tools to use surveillance on their citizens.

The main idea of David Brin's book »The Transparent Society« says that we cannot stop complete surveillance anymore, so the best thing we can do is to make the collected data accessible for everyone thereby surveiling the surveiller:

This is an interesting idea philosophically but how much will anybody be willing to bet that states are going to give up the asymmetry of surveillance that they have. I'm not optimistic that the authorities are going to allow this to happen. If there is some kind of technical invention that enables you to see the officials while they are watching you that might be a really good idea – I just practically don't see it happen.

Also, when Brin wrote that, we did not have the automatic facial recognition software that we have now. Not only do we have the surveillance cameras in most urban areas, but those cameras can actually identify people automatically. There is a great danger in that ability of the state to identify individuals. But even if the people have the ability to surveil back – Who are they going to surveil?

2.5 Der Science-Fiction-Autor: Interview mit Bruce Sterling

Foto: CC BY, Robert Scoble

Der Science-Fiction Autor und Mitbegründer des Cyberpunk lehrt derzeit Internet Studies und Science Fiction an der European Graduate School in Saas-Fee.

»I take more interest in the emergent and the defunct, personally. For instance: what happens to all the MySpace data once the enterprise finally winks out?«

What are the (new) characteristics of internet-based data/ information? What attributes of the data are qualitatively new?
The size of the data sets and the arrival of big commercial silo operations like Apple, Facebook, Amazon, Google. Also the rise of state-supported hacking operations.

What are the most interesting technological possibilities to make use of this data?
People tend to be formally interested in technological possibilities that make a lot of money. I take more interest in the emergent and the defunct, personally. For instance: what happens to all the MySpace data once the enterprise finally winks out?

Where are, and where aren't opportunities to shape good use from a technological point of view?
The moguls hold all the cards here. Intelligence agencies might be able to steal some of the cards. There just are not a lot of tools left for politicians or activists. Events are outpacing reaction. Imagine you were a member of the Egyptian elite asking this question two years ago.

Who is to draw the line between public and private (in different contexts)?
It looks to me like the »revolving door« there has been knocked off the hinges and trampled; »private« enterprise can buy all the »public« it wants. Once again I think the key issue here is the behavior of the ultra-wealthy; they are able to maintain at least some lines of obscurity around their behavior, so, how do they manage it?

How does identity depend on publicness?
That is a good question. If I am Robinson Crusoe these days, do I exist, even in my own eyes?

What information do you want to keep secret? From whom? Why? And what do you want to know about others (curiosity)?
I would say that I am mostly interested in protecting the confidences of other people; I do not want to embarrass sources, who trusted me. I also make it an ethical point not to distribute information about committing illegal activities.
I would say the guys who most concern me are Balkan nationalist vigilantes who would like to harm my spouse for her political activism. It is an active threat but, to tell the truth, it does not make a lot of difference in daily behaviour.
Since I travel a lot, immigration officials are of some concern.
I am curious about all kinds of odd things, but mostly as source material for fiction or journalism: I have never been keen to »intrude« on anyone's so-called »private« life.

At which places/ on which platforms do you disclose information?
My blog, Twitter, FlickR, on email lists, and of course through banking, passports and credit cards.

Where is anonymity important to you?
As an author I am a fan of pseudonymity.

3 Privatheit und Öffentlichkeit: Schlüsselbegriffe

3.1 Historischer Wandel von Privatheit und Öffentlichkeit

»Privat« und »öffentlich« sind historisch und kulturell bedingte Vorstellungen, die sich in der menschlichen Geschichte ständig gewandelt und an konkrete Gegebenheiten menschlichen Lebens angepasst haben. Wenn wir also verhandeln was unter Bedingungen zunehmender Vernetzung sinnvoller Weise »privat« und was »öffentlich« ist, lohnt es sich zu bedenken, dass es auf diese Frage keine immer und überall gültigen Antworten gibt. Unser kurzer historischer Abriss beschreibt einige wesentliche Wandlungen der Vorstellungen von Öffentlichkeit und Privatheit ab. Orientierungspunkte sind dabei die Medienrevolutionen Sprache, Schrift, Buchdruck (und in der Folge Massenmedien) und Vernetzung einhergehen. Beispielhaft haben wir zwei zentrale Elemente herausgegriffen, um diese Wandlungen zu illustrieren – das »Bild des Einzelnen als Abbild« und die »architektonische Ordnung des öffentlichen Raumes«. Die Abbildungen von Individuen verdeutlichen, wie der Einzelne und sein Einfluss auf das Ganze wahrgenommen und gedeutet wurden. Natürlich bleibt diese Darstellung skizzenhaft und selektiv, deutlich wird jedoch die Geschichte eines permanenten Wandels, von Aushandlungsprozessen und Umkehrungen.

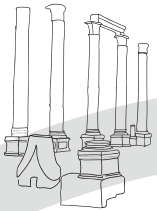
SPRACHE

Frühe Darstellungen von Menschen sind generisch, Höhlenmalereien stellen oft Tiere und Menschen dar, aber eben nicht als konkrete einzelne. Das Individuum verschwindet mehr oder weniger in der Gruppe. Dies entspricht der weitgehend geteilten Lebenswelt, in der es kaum private Rückzugsmöglichkeiten gegeben haben dürfte.

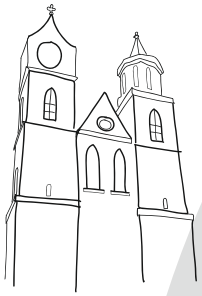
Die Urform der Gemeinschaft symbolisiert das Lagerfeuer, um dass sich Menschen versammeln. Diese gemeinsame Versammlung um einen kommunikativen Punkt bildet den Ausgangspunkt menschlicher Gemeinschaft.

SCHRIFT

Später werden zum Beispiel in Grabmalereien durchaus konkrete Personen dargestellt und historische Ereignisse festgehalten. Allerdings wird die Identität der Personen nicht durch phsyische Ähnlichkeit hergestellt, sondern vor allem über Symbole, die Position und Rolle des Dargestellten bezeichnen. Individuelle Darstellungen fokussieren auf die soziale Rolle einer Person. Im Mittelalter prägen Abbildungen religiöser Ereignisse und Personen die Kunst.

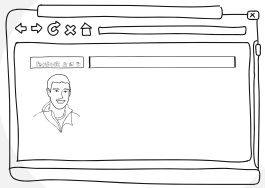


Im antiken Griechenland firmiert die Agora, auf der sich die Bürger versammeln eine zentrale Rolle – und diese Idealvorstellung von Demokratie wirkt bis heute fort.
Doch schon im römischen Forum findet sich das Muster einer stärker hierarchischen, weniger diskursiven Form politischer Öffentlichkeit. Und in beiden Formen existieren Aktivitäten, die dem Zugriff dieser politischen Öffentlichkeit entzogen sind und dennoch beobachtbar und publik sind. Das Private findet auch hier schon »öffentlich« statt.



Im Mittelalter wird die Religion zum Bezugspunkt öffentlicher Ordnung, nicht nur durch die häufige Gleichsetzung kirchlicher und weltlicher Autorität, sondern auch durch die zentrale Stellung von Kirchen und Klöstern im öffentlichen Raum. Hier kommen Menschen zusammen und religiöse Rituale und Begründungszusammenhänge stellen Gemeinschaft her.

VERNETZTE GESELLSCHAFT



Die zunehmende Vernetzung löst die bekannten Grenzen zwischen privat und öffentlich auf. Dieser neuerliche Wandel drückt sich auch darin aus, dass sich das Private weiter ausdifferenziert. Neue, nichtpolitische Form von Öffentlichkeit gewinnen an Bedeutung, in denen der einzelne nicht länger nur oder auch nur vorwiegend vor staatlichem Zugriffe geschützt werden will.

Die Vernetzung ist dabei sowohl Chance als auch Gefahr: Gefahr, weil erlernte Muster für den Schutz von Informationen nicht mehr Funktionieren; Chance, weil neue Formen von Kooperation und Kommunikation möglich werden. Beides sinnvoll abzuwägen ist die Herausforderung.

BUCHDRUCK

Mit der Renaissance bekommt die Abbildung von Individuen einen grundsätzlich neuen Charakter – es geht um die Abbildung bestimmter Personen in möglichst großer Wirklichkeitstreue. Porträts bedeutender Personen rücken das Individuum in den Mittelpunkt. Die Vorstellung entsteht, dass der Einzelne nicht nur über seine soziale Rolle am gemeinsamen Leben teilhat, sondern individuelle Rechte, Eingriffsmöglichkeiten und Interessen hat. Gleichzeitig entsteht eine neue mediale Sphäre, die durch den Buchdruck ermöglicht wird. Die Darstellung nach außen gewinnt dadurch neue Dynamik. Erst unter diesen Bedingungen entwickelt sich langsam auch die moderne europäische Vorstellung von Privatsphäre.

Im Italien der Renaissance steht erneut der Marktplatz für das erstarkende Bürgertum und sein politisches, öffentliches Auftreten. Mit der Verbreitung der Demokratie findet dieser öffentliche Raum in Parlamentsgebäuden Ausdruck und manchmal, wie in Washington D.C. im Layout ganzer Städte.

MASSENMEDIALE GESELLSCHAFT

Begleitet wird dies durch die Entwicklung einer medialen Öffentlichkeit, Zeitungen und Journale, später Radio und Fernsehen. Gleichzeitig entsteht eine Sphäre der geschützten Privatheit, wobei dieser Schutz vor allem ein Schutz vor staatlichem Zugriff ist. Öffentlichkeit wird verstanden als die politische Öffentlichkeit der gemeinsame Angelegenheiten.
Beide Sphären bereichern und ergänzen sich, ihre Trennung wird als zentral für Demokratie und Freiheit gesehen.

Mit der Fotografie gewinnt auch die Darstellung nach außen eine neue Dimension – es geht zunehmend darum die eigene Außenwahrnehmung zu steuern. Durch digitale Medien erhält nun sowohl der Schutz der Privatsphäre, der ein relativ junges Phänomen ist, als auch die Darstellung des Einzelnen nach außen eine neue Dynamik.

3.2 Anonymität, Pseudonymität und Identität

So wie die Unterscheidung in physischen und Cyberspace, also reale und virtuelle Welt, durch die Vermischung und Verknüpfung beider Bereiche obsolet wird, so sehr stellt diese Verknüpfung auch eine Herausforderung für unser gesellschaftliches Konstrukt von Identität, Zurechenbarkeit, Anonymität und Meinungsfreiheit dar. Die Beziehung zwischen Identität und Anonymität im digitalen Zeitalter ist vielschichtig: Auf der einen Seite sind die Plattformen – hier verstanden als soziotechnische Umgebungen, die so etwas wie Identität stiften können – nie zuvor so zahlreich gewesen, nie so umfassend dokumentiert und analysiert worden wie heute. Die Menge der anscheinend an unsere Realidentität digital gekoppelten und zu ihr in Relation gesetzten, in Form gebrachten Informationen hat durch die Digitalisierung (und Vernetzung durch das Internet) Ausmaße erreicht, die zuvor kaum vorstellbar waren.

Zugleich ist über das Internet theoretisch ein Grad an Anonymität möglich, der neu ist. Am Ende können bei bestimmten Anonymisierungsverfahren weder die aufgerufene noch die angefragte Partei, aber auch nicht die in die Übermittlung Eingebundenen ohne zusätzliche Referenzinformationen wissen, woher eine Anfrage ursprünglich stammte.

Was verändert sich also im digitalen Zeitalter? Die historisch gewachsene Relation zwischen einem Menschen und seiner Aktion unter Zuhilfenahme der Beschreibung, der Deskription, in Form eines Namens verliert an Bedeutung. Das namensbasierte Konzept der Identität ist primär eines der Unterscheidung, und es funktioniert nur in sehr kleinen Kreisen: wenn Michael Müller und Petra Schmidt nicht in ihrem Umfeld auf einen identischen (sic!) Namen treffen, respektive die sie kennenden Personen nicht in die Verlegenheit zweier gleichlautender Namen gebracht werden. Und dennoch lassen sich die beiden Namenszwillinge unterscheiden.

Nichts ist mehrfach in der Welt – keine zwei Objekte sind identisch, nicht einmal digitale Kopien, selbst wenn sie identischen Inhalt verkörpern, was sich spätestens in ihrem jeweiligen Umfeld, ihren Beziehungen zur Umwelt abbilden und beschreiben lässt. Nur: Die digitale Welt unterliegt nicht der gleichen Verknüpfungsdichte wie die materielle. Nutzer Michael Müller ist von Nutzer Michael Müller in der reduzierten digitalen Deskriptionsdichte nicht zu unterscheiden. Denn digitale Originalität und damit auch Identität ist nicht anhand ihrer selbst von ihrer Kopie, einem gleichförmigen Original oder einer Kopie eines anderen identischen Originals zu unterscheiden.

Anonymität und Pseudonymität sind im digitalen Kontext Reduktionen einerseits der bereits vorliegenden wie auch andererseits der theoretisch möglichen Verknüpfungen. Und die digitale Umwelt ist die im ersten Schritt reduzierteste aller denkbaren Umwelten. Erst die Deskription erzeugt Muster, die so etwas wie individuelle Eindeutigkeit, etwas Identitätsartiges erzeugen können. Statt anhand *eines* eineindeutigen Merkmals (so wie sie die ab Geburt vergebene Steuer-ID oder die Personenkennzahl PKZ in der DDR darstellt) verknüpfen sich viele Elemente zu einem gemeinsamen Muster, das dann eine oder mehrere Identitäten konstituieren kann.

Wir sind im Netz grundsätzlich keine identifizierbaren Identitäten sondern abstrakte Teilnehmer. Wir können uns als eine reale oder künstliche Identität ausgeben und entwickeln; und durch Verknüpfungen mit weiteren Informationen lässt sich die Wahrscheinlichkeit erhöhen, dass dies glaubwürdig erscheint. Ob es sich dabei um eine reale, eine fiktive oder auch mehrere Personen/Identitäten (so wie unter dem Kollektivpseudonym *»Bernd«* des deutschen Imageboards Krautchan oder *»Anonymous«* des englischsprachigen Vorbilds 4chan) handelt, ist vorerst – d. h. ohne weitere Deskriptoren zurate zu ziehen – nicht aufzulösen.

- **Identität** heißt, Originalität durch Referenzierung plausibler zu machen.
- **Pseudonymität** heißt, Originalität oder Identität vorzutäuschen/einzuschränken, indem ein Drittes eingeführt wird, über dessen Verknüpfung

mit dem Subjekt und seiner Identität im Übrigen das Subjekt im Grundsatz frei entscheiden kann bzw. diese durch Dritte vornehmen/einschränken lässt.

- **Anonymität** heißt, die Referenzierung zu unterdrücken/nicht zuzulassen/abzuschneiden.

Wie also verhalten sich diese drei zueinander?

These 1: Absolute Anonymität existiert online nicht.

These 2: Eineindeutige Identität existiert online nicht.

These 3: Echte Pseudonymität existiert online nicht.

Das klingt im ersten Moment erstaunlich. Anonymität ist genaugenommen die Nichtzuordnungsfähigkeit eines Objektes oder einer Handlung zu einem bestimmten Subjekt. Pseudonymität ist die begrenzte Zuordnungsfähigkeit, die Herstellung einer Relation zwischen beiden Elementen unter Zuhilfenahme eines Tertiums, eines synthetischen Zuordnungsobjekts, das weder mit dem Subjekt noch mit seinen Handlungen identisch ist. Doch was ist diese Identität? Identität selbst ist per Definition nur ein Common Sense/Common Denominator für ein Subjekt: Anhand einer oder mehrerer Zuweisungen wird jemand oder etwas *identifiziert* (zur Verwendung des Subjekt-Begriffs: Hansen/Pfitzmann 2010, v0.34: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml).

Alle drei sind grundsätzlich legitim und in unterschiedlichen Kontexten wünschenswert bzw. bedenkenswert.

Identität und das Internet

Identität erfüllt klassisch zwei Funktionen: Zum einen ist sie für uns selbst die Summe unserer Vorstellung vom »Ich«, die Summe der Selbstwahrnehmung. Sie ist die Selbsteinordnung des Individuums in seine Umwelt, gebunden an Erfahrungen, Körper, soziale Interaktion – die Identifikation des Ich in der Welt. Dies ist die höchstpersönliche Komponente von Identität.

Der Psychologe Erik Erikson machte in den 1970ern darauf aufmerksam, dass wir nicht mit einer ausgebildeten Identität geboren würden, sondern sich diese erst im Laufe unseres Lebens bilden würde. Diese Identität würde durch den spielerischen Umgang und die Beobachtung, die Reflexion unserer Umwelt in der Wahrnehmung unserer selbst erst zu einer autonomen Identität führen. Erikson nahm an, dass die Identitätsbildung aus der eigenen Perspektive mit dem Erwachsenwerden abgeschlossen sei, was in statischeren früheren Lebenswirklichkeiten durchaus denkbar, aus heutiger Perspektive jedoch eher unzutreffend scheint: Der Zeitraum der Identitätsfindung wird allgemein als auch mit dem sogenannten Erwachsenwerden nicht abgeschlossen angesehen, sondern ist ein stetiger Prozess der Kumulation, der mit zunehmendem Alter gefestigt wird. Dabei ist ein nicht zu kleiner Teil unserer Identitätsbildung und Identitätsabbildung an offensichtliche oder auch unterschwellige Anforderungen unserer Umwelt gekoppelt: So wie die Selbstdarstellung als Teil einer Familienzugehörigkeit, einer regionalen Abstammung oder der sozialen Verhältnisse Anforderungen an uns stellt, so sehr kann mit diesen auch spielerisch umgegangen und Identität gebildet werden. Der höfischen Etikette, dem rheinischen oder brasilianischen Karneval und dem Knigge ist gemein, dass sie Anforderungen postulieren, dem Einzelnen dabei entweder ihre Ausgestaltung überlassen oder ihre Einhaltung einfordern.

Konsequenterweise forderte Erikson entsprechend eine Art Moratorium für die Zeit der Identitätsfindung. Auch das Internet ermöglicht in der Theorie ein Moratorium: die Entkoppelung der eigenen von dargestellten, selbstgewählten Identitäten in einem abgeschlossenen Raum wie zum Beispiel in Spielwelten. Doch das ist heute nur noch zum Teil wahr: An vielen Stellen werden Verknüpfungen als Identitätsreferenz angefordert. Entsprechend wird durch die Zunahme automatisierter Wiedererkennungsmechanismen wie Gesichts- und Mustererkennung ein derartiges Moratorium deutlich erschwert, ein Moratorium im Sinne Eriksons findet nicht mehr statt. Sherry Turkle beschreibt

die Beschränkung so: »Viele dieser Erfahrungen beginnen mit dem Registrieren per Kreditkarte.« Sofern nicht Mechanismen anbieterseitig unterstützend eingesetzt werden, ist ein Moratorium zur Identitätsbildung künftig kaum noch vorstellbar: Wie eine Schildkröte ihren Panzer ihr Leben lang mit sich herumträgt, tragen wir unsere digitale(n) Identität(en) mit uns herum.

Ob und wie gezielt getrennt gehaltene Identitäten künftig überhaupt noch getrennt gehalten werden können, ist überaus fraglich. Dies bedeutet, dass nicht der mittelbare und unmittelbare Personenbezug, sondern die Profilbildung als solche in den Mittelpunkt der Überlegungen gestellt werden muss: Wie kann eine Trennung von gezielt getrennt gehaltenen Identitäten gesichert werden?

Die eigenen Identitätsmerkmale zu offenbaren, kann stets nur ein relativer Vorgang sein, bezogen auf einen sich stetig wandelnden Prozess, da es sich um ein »Moving Target« handelt: Die Summe der Zuschreibungen verhält sich zum Subjekt, wie sich dieses zu seiner Umwelt verhält bzw. diese zu ihm. Analog gilt dies auch für die jeweiligen Teilidentitäten, die wir anderen offenbaren und aus deren Reaktionen wir hieraus selbst wieder reflektierend eigene Annahmen über unser Selbst treffen.

Identität als Identifikation

Zu dem »Ich« gesellt sich also die zweite Funktion: die Wahrnehmung durch die anderen. Dies sind in erster Linie Zuschreibungen, wie wir sind, was wir sind. Diese Dimension dient der Identifikation durch andere (Menschen, Institutionen, Vertragspartner), zur Wiedererkennung und zur Einschätzung des Gegenübers. Wir empfangen im Laufe unseres Lebens Zuschreibungen, von der Geburtsurkunde über das Abschlusszeugnis bis hin zum finalen Akt der Sterbeurkunde, die an unsere Identität gebunden sind. Ein anderer attestiert uns Eigenschaften, etwa dass wir etwas tun können – oder manchmal auch nicht. Eine extrem negative Zuschreibung ist etwa eine strafrechtliche Verurteilung, von der das Bundesverfassungsgericht feststellt, sie treffe (neben der Zumessung einer Strafe) ein »sozialethisches Unwerturteil« (BVerfGE 96, 245, 249). Konsequenz einer solchen Zuschreibung ist regelmäßig langfristige soziale Stigmatisierung als »vorbestraft«. Auch die Frage, ob und wie eine Art *informationelle Resozialisierung* möglich sein kann, ist bislang ungeklärt (BVerfGE 35, 202, 233f.). Ist ein Anrecht auf ein künftiges oder auch rückwirkendes Vergessen, also beispielsweise die Entfernung von Namensnennungen in digitalen Archiven heute durchsetzbar? Ist, was einmal öffentlich war, der Öffentlichkeit per Norm entziehbar? Oder handelt es sich dabei um eine Art rückwirkende Geschichtsfälschung? Der Fall einer früheren Hamburger Rotlichtgröße, die rückwirkend die Nennung eines gängigen und selbstverwandten Pseudonyms, das nunmehr von ihr selbst als diskriminierend erachtet wird, aus den Archiven getilgt sehen will, ist dabei wohl nur der Auftakt der schwierigen Grenzziehung zwischen dem Anspruch der Öffentlichkeit auf konsistente Bewahrung auch vergangener Öffentlichkeiten einerseits und dem Recht auf Identitätsautonomie des Einzelnen andererseits.

Die Nachvollziehbarkeit von Identität ist im Alltag oft erst in bestimmten Situationen relevant. Wir melden uns am Telefon mit Namen, oft auch selbst dann, wenn wir schon sehen, wer uns anruft, da wir seine Nummer gespeichert haben. Jedes Einander-Vorstellen, mit dem Ziel, dass man einander kennenlernt, ist eine Preisgabe einer Teilidentität. Wir versprechen uns davon im positiven Sinne etwas. Wenn wir uns ausweisen, gibt es in bestimmten Situationen einen positiven Anreiz: Wir möchten gegebenenfalls nicht, dass jemand anderes an unserer Stelle agiert. Es gibt also ein natürliches Bestreben, die Deutungshoheit über die eigene Identität zu bewahren. Hierin dürfte zum Beispiel auch der Kern der vielfältigen Bestrebungen liegen, rechtliche Schritte gegen unwillkommene Presseveröffentlichungen zu ergreifen.

Nun ist Identität kein monolithischer Block. Wir alle nutzen jeden Tag Teilidentitäten: Für den Bäcker sind wir eine andere Person als für unsere Eltern, für unsere Kinder, unsere Kollegen. Und für alle könnten wir im jeweiligen Kontext identifizierbar sein. Doch was ist hier die Rolle des Internets?

Aggregation von Identitätsaspekten

Das Netz kann zur Aggregation aller einzelnen Zuschreibungen führen, die von uns existieren. Wer will, kann aus den Puzzlestücken verschiedene Elemente rekombinieren. Da ist beispielsweise der Personaler zu nennen, der den Namen des Bewerbers in eine Suchmaschine eingibt oder auf sozialen Netzwerken nachschaut, ob die vor ihm liegende Bewerbungsidentität mit der auffindbaren Online-Identität übereinstimmt. Nur wer durch Zufall einen Namen trägt, der ihn auf Grund bekannterer Namensvettern vor der Auffindbarkeit bewahrt, kann hier auf Unschärfe hoffen.

Identitätskontexte neuer Teilöffentlichkeiten

Zugleich bietet uns das Netz eine Möglichkeit, die in dieser Form zuvor noch nicht da war. Wir können uns, entgrenzt von räumlichen Barrieren, in Kontexten bewegen, in denen wir zuvor nicht hätten unterwegs sein können. Wer heute mit australischen Hundezüchtern oder bayrischen Laienschauspielern diskutieren will, kann dies tun. Wir sind zu Beginn stets nur »ein Computer im Internet«, mit dessen Hilfe wir Dinge tun können. Mit seiner Hilfe suchen wir uns die Teilöffentlichkeiten, die uns interessieren, für uns Relevanz entfalten. In diesen jeweiligen Kontexten sind wir ab dem Zeitpunkt, an dem wir von unserer reinen Beobachterrolle abrücken, wieder mit einer Teilidentität – die abgesehen vom Faktor Zeit nicht zwangsläufig an unsere existierenden weiteren Teilidentitäten gebunden sein muss – in die Teilöffentlichkeiten integriert.

Pseudonymität

Nun stehen wir vor der Frage, welche Identität wir im Netz verwenden wollen und können, also welche Voraussetzungen anbieterseitig gegeben sind. Der Gesetzgeber hat in Deutschland den Intermediären verhältnismäßig hohe Hürden gesetzt, wenn diese eine pseudonyme und anonyme Nutzung unterbinden wollen.

Pseudonymität erfüllt mehrere Funktionen. Beispielsweise verführen nicht alle Hobbys und Vorlieben dazu, sie unter dem realen Namen auszuüben, und nicht jeder möchte jederzeit für jedermann ohne weiteres Wissen identifizierbar sein. So wie wir auf der Straße zwar erkannt werden können, wenn uns jemand bereits kennt, so verhält es sich auch im Netz: Wir können Namen wählen, die weniger markant sind als unsere eigenen, echte Namen anderer Personen, reine Phantasienamen oder Mischformen.

Durch die geringe Verknüpfungsdichte und die zu Beginn geringe Zahl an Relationen zwischen unseren verschiedenen Teilidentitäten können wir selektiv vorgehen und in unterschiedlichen Kontexten unterschiedlich auftreten. Pseudonyme bieten auf diese Weise auch die Möglichkeit für Kollektive, unter einem gemeinsamen Namen aufzutreten. Diese Autonomie ist Schutz für den Einzelnen – vor gesellschaftlicher Ächtung, vor Verfolgung und Willkür.

Pseudonymität schützt dabei immer nur begrenzt und vor bestimmten Akteuren: Tatsächlich sind viele Nutzer spätestens dann wieder identifizierbar, sobald ein gewisses Maß an Relationen vorliegt. Wir sprechen von Pseudonymität im Netz dann, wenn technisch oder durch Zugriff auf Relationen die Rückverfolgung zur Person des Nutzers möglich ist, der den Rechner bedient. Folge dieser Verknüpfung ist, dass die synthetische Identität, die mit dem Pseudonym verknüpft ist, wieder mit einem Subjekt verknüpft werden kann: Die Trias Subjekt – Pseudonym – Identität schrumpft (jedenfalls aus der Perspektive derjenigen, die die Zuordnung kennen) wieder zur klassischen Zuordnung von Subjekt und Identität.

»Drive-by«-Kommentare von »Pseudo-Anonymen«

Die Möglichkeit der Pseudonymität erfordert dabei auch vom Nutzer ein gerüttelt Maß an Selbstdisziplin. Die Freiheit, so auftreten zu können, wie einem beliebt, ist insbesondere in den teils hitzig geführten Diskursen auf Onlineplattformen nicht immer frei von der Perfidie des Zwergenkönigs

Alberich aus der Nibelungensage: Solange er seine Tarnkappe trug, konnte ihm kaum jemand gefährlich werden. Zudem verwechseln auch manche Internetnutzer Pseudonymität mit Anonymität. Nur ist beispielsweise die Technik der vergleichenden Gesichts-, Stimm- und Texterkennung mittlerweile so weit fortgeschritten, dass sie unter Umständen tatsächlich auf den Urheber schließen lässt. Auch hier befinden wir uns noch eher am Anfang denn am Ende der Entwicklung.

Reputation oder Identifizierbarkeit?

Pseudonymität bewegt sich also im schwierigen Spannungsfeld technischer oder sozialer Auflösbarkeit der vordergründigen Unerkennbarkeit – im Sinne einer Unmöglichkeit der Zuordnung zu einem Subjekt und seiner »wahren« Identität – einerseits und der Freiheit, selbstbestimmt seine Identitäten und Identitätsbausteine pflegen zu können, zwischen Schutzbedürfnis des Einzelnen und Missbrauchsmöglichkeiten. Gerade Letztere beruhen allerdings unter den Gegebenheiten von Pseudonymität primär auf der Fehlannahme der Nichtrückverfolgbarkeit. Grundsätzlich anders verhält es sich jedoch bei der dritten Form:

Echte Anonymität

Wenn wir nicht ohne Weiteres und nicht für jedermann identifizierbar sein möchten, können wir uns in die Anonymität begeben. Anonymität bedeutet, dass niemand uns mit derzeit denkbaren Mitteln identifizieren könnte. Es ist das Wesen dieser Nichtrückverfolgbarkeit, dass es einiger technischer Hilfsmittel bedarf, um uns von unserem Tun zu trennen. Denn grundsätzlich sind wir im digitalen Raum nicht anonym unterwegs, wir sind oft bloß noch nicht für die Gegenseite identifiziert – was spätestens unser Internetanbieter auflösen könnte. Um dies zu verhindern, gibt es Schutzmechanismen: technische Hilfsmittel, bei denen durch Erzeugung von verschlüsseltem Datenrauschen, das nicht von »echtem« Verkehr unterscheidbar ist, der Internetverkehr vieler Nutzer so weit durcheinandergewürfelt wird, dass am Ende nicht mehr klar ist, wer was getan hat, sondern nur, dass jemand etwas getan hat. Die Zuordnung zum Einzelnen geht im Schwarm der die meiste Zeit kryptierten Anfragen irreversibel unter.

Zudem gibt es die Möglichkeit, Rechner Dritter für eigene Zwecke zu nutzen, etwa die Ressourcen von Anonymisierungsdiensten oder auch die unbekannter anderer (hierauf beruht etwa die Unzahl von Spam-E-Mails, die regelmäßig aus »Botnetzen« ferngesteuerter, mit Schadsoftware infizierter Rechner verschickt werden). Auch die Nutzung fremder Netzwerke ist Teil mancher Anonymisierungsstrategie, ob nun durch virtuelle Leitungen oder durch physische Nutzung, zum Beispiel über unsichere Funknetze oder die Internet-Sharing-Funktionen unsicherer mobiler Endgeräte.

Technisch ist Anonymität im digitalen Kontext also möglich. Allerdings funktioniert sie nicht fehlerfrei. Wir hinterlassen breite Spuren, wenn wir das Netz nutzen, allein durch die Geräte, die wir verwenden, und durch unser Verhalten. De-Anonymisierung ist nicht unmöglich, solange genug Referenzobjekte und Untersuchungsgegenstände vorhanden sind, um am Ende mit hoher Wahrscheinlichkeit beim Einzelnen anzugelangen. So wie Profiler in Kriminalbehörden Rückschlüsse aus verwendeten Buchstaben in zusammengeklebten Erpresserbriefen (im Internetzeitalter etwas außer Mode gekommen), verwendetem Papier, Stil und Erpresstem ihre Rückschlüsse ziehen, so lässt sich dies softwaretechnisch gleichermaßen mit vordergründig anonymen oder auch mit pseudonymen Handlungen vollziehen. Ein Beispiel aus dem späten analogen Zeitalter hierfür ist die Ergreifung von Theodore Kaczynski, des sogenannten Unabombers, dessen Bombenpost in den USA fast 20 Jahre lang Furcht und Schrecken auslöste. Dessen Fahndungsprofil war irgendwann so verfeinert, dass der Bruder des Täters ihn darin erkannte, obwohl der Gesuchte alle zur Verfügung stehenden Mittel ausgeschöpft hatte, um seine Identifizierung zu vermeiden. Da die Menschen einen immer größeren Teil ihres Lebens mit digitalen Spuren versehen, ist die Wahrscheinlichkeit einer De-Anonymisierung in den vergangenen Jahren deutlich gestiegen: Die Analyse ist einfacher geworden.

Herausforderungen und Chancen

Die beschriebenen Transformationen von Identitätsaspekten im Netz stellen unsere Gesellschaft vor wesentliche Fragen: Wie viel Identifizierbarkeit, Anonymität und Pseudonymität sind notwendig, um zielführende Diskurse und Prozesse in demokratischen Gesellschaften zu ermöglichen? Ist die Identifizierbarkeit nicht ausschließlich das Privileg der Gruppe der »*white male heterosexuals*«? Können für diese anwendbare Regeln tatsächlich ein würdevolles, selbstbestimmtes Leben für alle in einer heterogen-pluralistischen Gesellschaft ermöglichen?

Sowohl Identität als auch Pseudonymität oder Anonymität sind wesentliche Elemente des demokratischen Meinungsbildungs-, Meinungsfreiheits- und politischen Willenbildungsprozesses. Der Schutzraum von Anonymität ist dabei nicht nur für das wohl unmittelbar einleuchtendste Beispiel des Whistleblowing und die Möglichkeit einer anonymen Anzeige bei den Strafverfolgungsbehörden unverzichtbar. Die gesamte Meinungsfreiheit – unter die der Europäische Gerichtshof für Menschenrechte auch das Whistleblowing subsumiert – hängt davon ab, ob wir unsere Auffassung, unsere Beobachtungen und unsere Schlussfolgerungen frei äußern können. Selbst wenn die Meinungsfreiheit in Europa und Deutschland traditionell nicht der gleichen Schrankenlosigkeit unterliegt, wie sie ihr beispielsweise in den USA zugestanden wird, ist sie als konstitutives Element demokratischer Prozesse in den vergangenen Jahrzehnten und mit dem Wandel hin zur digitalen Informationsgesellschaft in ihrer Relevanz und auch in der rechtlichen Betrachtung ihrer Rolle eher gestärkt denn geschwächt worden.

Anonymität spielt auch dort eine wesentliche Rolle, wo die Aufdeckung der realen Identität unmittelbare und nicht-rechtstaatliche, aber auch dort wo sie individuelle soziale und wirtschaftliche Folgen jenseits des Justiziablen nach sich ziehen kann. Allein die Möglichkeit der Aufdeckung der Identität kann dabei zu einer Einschränkung der Meinungsfreiheit und damit zur vorweggenommenen Selbstbeschränkung in Erwartung möglicher Sanktionen führen.

Dies kann unter Umständen gewollt sein, beispielsweise um die Zurechenbarkeit einer Äußerung zu einem Absender zu ermöglichen, was in bestimmten, vor allem wirtschaftlichen und Verwaltungsprozessen logisch erscheint. Ein anonym erstellter Haftbefehl, ein anonymer Bundeskanzler, ein anonym verfasstes Gerichtsurteil – es ist offensichtlich und unzweifelhaft, dass Anonymität dem Staat anders als seinen Bürgern grundsätzlich nicht zusteht. Hier ist die Nachvollziehbarkeit als höherwertiges Gut einzuschätzen. Beispielsweise zeigt die Debatte um Namensschilder für Polizisten die Schwierigkeiten staatlicher Nichtzuordbarkeit auf: Kann ein Akteur im Staatsdienst ein Recht auf Nichterkennbarkeit haben? In der Regel ist dies zu verneinen, doch gibt es natürlich auch hier Bereiche, in denen die reale Identität mit gutem Grund verschleiert werden muss. Eine vollständige Anonymisierung hingegen widerspräche auch hier dem Anspruch der Verantwortlichkeit gegenüber den Bürgern.

Während für staatliche Akteure also Pseudonymität als maximale Stufe möglich sein kann, muss dem Bürger auch die Möglichkeit einer vollkommen anonymen Meinungsäußerung gegeben sein – im digitalen Umfeld ist dies eine Herausforderung.

Insbesondere für den Bereich geschäftlicher Interaktion ist die Debatte um Anonymität und Pseudonymität in der digitalen Welt noch nicht sehr weit fortgeschritten. Während es uns normal erscheint, den Alltagseinkauf bei Barzahlung ohne Angabe jedweder Identität zu tätigen, erscheint es offenbar bislang gleichermaßen normal, bei jedem Zahlvorgang im digitalen Raum umfassenden Identifikationsmechanismen zuzustimmen.

In der sozialen Interaktion spielt die Verwendung von mehr oder minder stark getrennten Teilidentitäten eine wesentliche Rolle. Zwar findet ein wesentlicher Teil der in den Alltag integrierten Onlinekommunikation der Nutzer unter dem bürgerlichen Namen statt. Doch erst die Möglichkeit einer Trennung von dieser ermöglicht die unbeschwerte, selbstbestimmte Teilnahme an Diskursen und sozialer Interaktion, beispielsweise für Studenten

oder Absolventen der katholischen Theologie an GayRomeo, die Teilnahme in Online-Selbsthilfegruppen, aber auch dem egalitären, weil nicht an die sonstige Identität gekoppelten, Diskurs. Wäre ein als solcher identifizierbarer Bankvorstand noch in der Lage, gleichermaßen an einem politischen Onlinediskurs teilzunehmen?

Ein Aspekt des Umgangs mit diesen »anderen Teilidentitäten« ist deren soziale Akzeptanz. Während es in bestimmten Kreisen – wie zum Beispiel bei akademischen Konferenzen – verpönt ist, Pseudonyme zu verwenden, sind diese in anderen Kontexten umso üblicher. Da ein Diskurs jedoch nur zustande kommt, wenn zwei oder mehr Parteien miteinander interagieren, obliegt die Akzeptanz des unter Pseudonym Agierenden durch die Mitdiskutanten deren individuellem Urteil.

Wer nicht mit offensichtlichen Pseudonymen interagieren möchte, wird hierzu in der digitalen Welt nicht gezwungen. Ob und wie Identitäten miteinander agieren, entspricht daher am ehesten der sozial normierten Technik von Vertrauensketten, dem Web-of-Trust, bei dem das Vertrauen der Teilnehmer untereinander und nicht die formale Deskription der Identität im Mittelpunkt stehen. Ein solches Web-of-Trust besteht aus einen System von Bürgen: Dadurch, dass Individuen sich untereinander Vertrauenswürdigkeit bescheinigen, können andere Individuen auf diese als »*trustworthy*« eingestuften Relationen vertrauen. Zugleich ist dies natürlich auch anfällig: Wer beliebigen Entitäten vertraut, gefährdet die Integrität des gesamten Systems. Der Vorteil eines Web-of-Trust liegt darin, dass es nicht auf eine externe Referenz angewiesen ist – die Teilnehmer selbst referenzieren untereinander, und ob sie dies gegenüber realen oder virtuellen Identitäten/Entitäten tun, ist dabei zweitrangig.

Historisch gibt es zahlreiche Beispiele, welche die Entkoppelung von »realer« Identität und Reputation, also der Anerkennung der Werke, der Ideen und der Tätigkeiten durch andere, als keineswegs neu erscheinen lassen. Ob Autoren, Staatsmänner oder Kulturschaffende: ihre Reputation ist primär durch die ihnen zugeschriebenen Kompetenzen oder Inkompetenzen, durch die externe Zuschreibung von Attributen und die Wertschätzung oder Missbilligung, das Vertrauen oder Misstrauen geprägt – nicht durch einen einzelnen Wert.

3.3 Transformation der Öffentlichkeit durch das Internet

Welche Eigenschaften und Institutionen sollten in unserer Gesellschaft im Bezug auf öffentlichen Diskurs und private Rückzugsräume geformt werden? Nachdem mit fortschreitender Industrialisierung Entfremdung (z. B. von der Arbeit) und soziale Isolation (in Großstädten), ja sogar der »*death of the public man*«, attestiert und analysiert wurden, schwingt das Pendel jetzt scheinbar zurück und es wird ein Übermaß an sozialen und öffentlichen Verbindungen in den sozialen Medien problematisiert.

Dabei ist zunächst bemerkenswert, dass sich technisch-professionelle Systeme, die das Thema Privatheit überhaupt nicht »mitdachten«, zunehmend zu soziotechnologischen Lebensräumen entwickeln. In diesem Prozess lernen Ingenieure erst langsam durch transdisziplinäre Zusammenarbeit, den sozialen Nutzungskontext von Anfang an zu bedenken. Die Perspektive der Rechts- und Sozialwissenschaften, die Privacy als einen Wert in sich selbst verstehen, welcher Freiheit, aber auch entsprechende Verantwortlichkeit mit sich bringt, wird zunehmend auch bei der Konzeption soziotechnischer Systeme berücksichtigt.

Vor dem Hintergrund der Auswirkungen des Internets auf das Verständnis von Privatheit ist es wichtig, auch den Wandel von Öffentlichkeit zu untersuchen und kritisch zu hinterfragen. In diesem Abschnitt soll (1.) auf die Auswirkungen des Internets auf die politische oder bürgerliche Öffentlichkeit eingegangen werden, um emergente Prozesse zu verdeutlichen, und (2.)

deren (mögliche) Rolle bei der Herstellung einer idealtypischen bürgerlichen Öffentlichkeit im Habermas'schen Sinne verdeutlicht werden.

Vom Stammtisch bis zur ePetition – Was verändert das Netz?

Die Rolle der bürgerlichen Öffentlichen hat sich in der Zeit zwischen Diskussionen der Intellektuellen der »Bohème« in Wiener und Londoner Kaffeehäusern zu Beginn des 18. Jahrhunderts bis zu den heute allgegenwärtigen Cafés, die durch kostenfreie Internetzugänge die Möglichkeit eröffnen, sich in einer global vernetzten Öffentlichkeit zu bewegen, ständig gewandelt. Treibende Kraft dieses Wandels waren immer die Medien, die im Prozess individueller und öffentlicher Meinungsbildung als Medium und Faktor fungierten, in denen also öffentliche Meinungen transportiert oder erzeugt wurden. Analoge Massenmedien wie Tageszeitungen versetzen Gesellschaften in die Lage, komplexe gesellschaftliche Diskurse zu führen und somit die öffentliche Meinung zu beeinflussen. Auch spätere, elektronische Massenmedien wie das Radio und Fernsehen weisen dieses Merkmal auf und trugen dazu bei, dass sich immer größere Teile der Gesellschaft an der Öffentlichkeit beteiligten und somit potenziell Teil der öffentlichen Diskussion werden konnten. Andererseits führte die Entwicklung eben dieser Massenmedien dazu, dass eine Abhängigkeit zwischen der Teilhabe an der öffentlichen Debatte und den verfügbaren Medien entstand. Es bestand die Gefahr, dass die Meinungen derjenigen, über die nicht berichtet wird, ungehört verklingen, bevor das nächste Thema den öffentlichen Diskurs bestimmt. Die Kommunikatoren in den klassischen Massenmedien entschieden in signifikantem Umfang darüber, welche Informationen überhaupt den Status einer relevanten Nachricht erhalten. Hier werden zwei Besonderheiten der analogen Medien deutlich: Einerseits kommt den Mittlern des öffentlichen Diskurses in den Massenmedien eine zentrale Rolle zu, andererseits bieten diese Medien wenig Möglichkeiten zur aktiven und schnellen Partizipation über einen begrenzten Kreis von Akteuren hinaus. Demgegenüber stand das Bedürfnis nach selbstbestimmter Kommunikation. Und das Internet trat mit dem Anspruch auf, dieses soziale Bedürfnis in allen Varianten, Eins-zu-vielen, Viele-zu-eins, Eins-zu-eins, Wenige-zu-eins usw., gegenüber dem hierarchischen Eins-zu-vielen-Format der Massenmedien zu erfüllen.

Trotz der Möglichkeiten der Erweiterung des Öffentlichen durch die Entwicklung sehr vieler lokaler und spezialisierter Massenmedien lässt sich während des 20. Jahrhunderts speziell in hoch industrialisierten Gesellschaften eine Schwächung der Öffentlichkeit feststellen. In *»Bowling Alone: The Collapse and Revival of American Community«* beschreibt Robert D. Putnam die Folgen dieses Rückzugs ins Private und die damit einhergehende Senkung des Sozialkapitals, dem gesellschaftlichen Vorteil, der aus Interaktionen und Zusammenarbeit von Individuen entsteht. Putnam führt diesen Rückzug auf die Individualisierung der Freizeit durch Massenmedien wie Fernsehen oder das Internet zurück. Auch die US-amerikanische Politikwissenschaftlerin Pippa Norris schreibt 2000: *»The common view in American politics is that the public turns off, knows little, cares less and stays home.«*

Die Anfänge des Internets wurden von der liberalen Diskussionskultur der frühen Netznutzer (vor allem Akademiker und Techniker) bestimmt, und das frühe Internet bestand zum großen Teil aus Diskussionen auf Mailinglisten und Foren, die verschiedenste Formen von Öffentlichkeiten und Communities of Interest hervorbrachten (siehe auch das Interview mit Howard Rheingold, der als einer der Ersten das Netz als soziales Ökosystem beschrieb). Nachdem die Entwicklung in den späten 1990er Jahren dann hin zu einer eher statischen Informationsvermittlung geschäftlicher und institutioneller Akteure ging, brachte das sogenannte Web 2.0 den Austausch der Nutzer wieder in den Vordergrund.

Das soziale Internet – Idealtyp des öffentlichen Raums?

Durch das Internet wurden die Zugangshürden zum öffentlichen Diskurs so weit gesenkt, dass es für einen weitaus größeren Personenkreis möglich wurde, sich ohne die vormaligen Einschränkungen wie Ort und Zeit zu beteiligen. Der neu entstandene soziotechnologische Lebensraum ermöglichte es

außerdem, mit einer von physischen Identitäten getrennten *»calculated co-presence«*[12] am öffentlichen Diskurs teilzunehmen. Das führt dazu, dass die Trennung zwischen dem Medium und dem Nutzer immer durchlässiger und eine Unterscheidung zwischen dem realen Selbst und dessen Repräsentation im Netz zunehmend aufgehoben wird. Ohne großen Aufwand kann jeder publizieren, also die klassische Rolle der Medien einnehmen. Durch das Internet haben auch diejenigen politischen Akteure eine Chance zur Artikulation, denen solche Möglichkeiten bislang verwehrt waren. Gegenüber traditionellen Massenmedien ist das Internet durch ein deutlich höheres Maß an »Durchlässigkeit« zwischen den Ebenen der Massenmedien und den Rezipienten gekennzeichnet. So verweisen etwa Weblogs durch Links auf die Websites traditioneller Medien, und umgekehrt richten auch reichweitenstarke Anbieter ihre Aufmerksamkeit auf das Web 2.0. Hierdurch entsteht ein kommunikatives Wechselspiel zwischen den klassischen Medien und der sich kommunikativ betätigenden »Bürgergesellschaft«, welches das strenge »Gatekeeping« beim Zugang der massenmedialen Öffentlichkeit entfallen lässt. Die die herkömmliche Medienwelt prägenden starren Grenzen zwischen Medien und Nutzern werden im Internet zunehmend durchlässiger. Neben die durch klassische Medien verfassten Öffentlichkeiten (»Medienöffentlichkeiten«) treten nun »Gegenöffentlichkeiten«, die auf der kommunikativen Partizipation des Einzelnen und anderer Akteure beruhen und welche die Bedeutung sowie die Machtfülle der klassischen Medien relativieren. Hier wird deutlich, dass sich die Bedeutung der Privatsphäre ändert und personenbezogene Daten eine immer größere öffentliche Bedeutung haben.

Durch diese Entwicklungen wurde der öffentliche Raum und die Art, wie und von wem in ihm interagiert wird, grundlegend verändert. Durch die rasende Verbreitung der Internetnutzung können mittlerweile auch Gruppen, die bis vor Kurzem kaum oder keinen Zugang zu diesem Medium hatten, die partizipativen Elemente des Internets (meist über internetfähige Mobiltelefone) nutzen. Andererseits lassen sich auch beim Internet Ausgrenzungsprozesse feststellen, da bisher nicht alle gesellschaftlichen Gruppen gleichermaßen an den sozialen Anwendungen des Internets teilhaben.

Jürgen Habermas beschreibt in »Strukturwandel der Öffentlichkeit« drei institutionelle Kriterien für die bürgerliche Öffentlichkeit. Um die permanente öffentliche Diskussion unter Privatleuten zu ermöglichen, müssen demnach die prinzipielle Ebenbürtigkeit, Themenoffenheit und Unabgeschlossenheit des Teilnehmerkreises gewährleistet sein. Anhand dieser Kriterien lassen sich einige Phänomene der Internetöffentlichkeit aufzeigen und diskutieren.

- ***Ebenbürtigkeit***

Das erste Kriterium lässt sich für das Internet durchaus als erfüllt bezeichnen, wenn man davon ausgeht, dass Ebenbürtigkeit durch die Abwesenheit fester Hierarchien und Rollen erzeugt wird. Mittlerweile hat ein weitaus größerer Personenkreis als zu der Zeit der herkömmlichen elektronischen Medien die Möglichkeit, sich aktiv an öffentlichen Debatten zu beteiligen. Durch die zunehmende »Demokratisierung der Produktionsmittel des öffentlichen Diskurses« werden vermehrt auch die Inhaber politischer oder wirtschaftlicher Macht gezwungen, an dieser Form der Öffentlichkeit teilzunehmen. Hier wird deutlich, dass die prinzipielle Ebenbürtigkeit »… nicht etwa die Gleichheit des Status voraussetzt, sondern von diesem überhaupt absieht«.[13] Durch die Qualität der Beiträge, die Häufigkeit der aktiven Teilnahme am öffentlichen Diskurs oder den Grad der Bekanntheit der einzelnen Teilnehmer entstehen natürlich auch in den Foren des Internets verschiedene Reichweiten. Trotzdem ermöglicht das Social Web prinzipiell jedem Nutzer, unabhängig von der gesellschaftlichen Stellung außerhalb des Internets, die Teilnahme an Diskussionen.

12 Varnelis, K. (Hrsg), 2008: *Networked Publics,* Cambridge et al.: MIT Press. Verfügbar unter http://networkedpublics.org.

13 Habermas, Jürgen, 1990 [1962]: Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft. Frankfurt am Main: Suhrkamp.

• *Unabgeschlossenheit des Teilnehmerkreises*

Die gesellschaftliche Stellung spielt auch eine wichtige Rolle bei der Frage nach der Unabgeschlossenheit des Teilnehmerkreises der Internetöffentlichkeit. Auch hier gilt, dass die Struktur des Internets prinzipiell für jeden offen ist und viele der sozialen Anwendungen darauf ausgelegt sind, dass niemand von der Nutzung ausgeschlossen wird. Andererseits können innerhalb der einzelnen Foren sehr wohl Teilnehmer vom öffentlichen Diskurs ausgeschlossen werden, indem beispielsweise Kommentare gelöscht werden oder Teile der Diskussion in geschlossenen Gruppen geführt werden. Obwohl viele dieser Hürden der Qualität des Diskurses dienen, wird damit die Unabgeschlossenheit des Teilnehmerkreises außer Kraft gesetzt. Außerdem ist es für viele gesellschaftliche Gruppen (noch) nicht möglich, sich an der Öffentlichkeit im Internet zu beteiligen. Abgesehen von der Tatsache, dass ganze Völker durch Zensur oder durch mangelnde Infrastruktur von der Teilnahme an der Internetöffentlichkeit ausgeschlossen sind, ist es beispielsweise für ältere oder bildungsferne Gruppen noch immer schwierig, diese Technologie in vollem Umfang zu nutzen. Deshalb ist es wichtig, den Umgang mit diesen Medien (nicht nur an Schulen) zu lehren, die weitere Verbreitung dieses Mediums an alle gesellschaftlichen Gruppen zu fördern und zu verstehen, welche Möglichkeiten und Gefahren durch diese neue Form der Öffentlichkeit in vormals privaten Lebensbereichen entstehen können.

• *Themenoffenheit*

Das Kriterium der Themenoffenheit wird durch das Internet im hohen Maße erfüllt. Doch der Rückzug in abgeschlossene Diskursräume im Netz kann der Fragmentierung der medialen Öffentlichkeit in eine Vielzahl von Teilöffentlichkeiten Vorschub leisten. Beim Netzaktivismus zeigt sich, dass diese Themenoffenheit eine Chance für ein Wiedererstarken der politischen Öffentlichkeit darstellt. Mit Hilfe des Internets können gesellschaftliche Randgruppen öffentliches Interesse wecken und sich besser organisieren. Das Erstarken der Öffentlichkeit wird beispielsweise bei der ePetition des Deutschen Bundestags oder bei der Rolle von sozialen Netzwerken wie Twitter oder Facebook zur Organisation des Sturzes von Husni Mubarak Anfang 2011 deutlich. Für die gesellschaftliche Diskussion ist allerdings wichtig, dass die Vielzahl an veröffentlichten Standpunkten auch ein Publikum erreicht. Die automatisierte Personalisierung von Suchergebnissen oder Statusmeldungen in sozialen Netzwerken kann zu einer »Filterblase«[14] führen, welche einerseits dazu beiträgt, dass die einzelnen Nutzer schneller die Informationen erhalten, die sie im Moment benötigen; andererseits wird dadurch vielen Themen die Möglichkeit genommen, in einer breiten Öffentlichkeit diskutiert zu werden.

In der zusammenfassenden Betrachtung der institutionellen Kriterien der Internetöffentlichkeit wird deutlich, dass die Struktur des Internets durchaus eine themenoffene und allen zugängliche Öffentlichkeit von einander ebenbürtigen Nutzern zulässt. Allerdings ist es ausgesprochen wichtig, dass diese Möglichkeiten auch umgesetzt werden. Ansonsten besteht die Gefahr, dass sich diese Öffentlichkeit zu einer Ansammlung geschlossener Foren entwickelt. Insbesondere in der Diskussion um die Rolle der individuellen Privatsphäre im Zuge der Entwicklung des Internets muss auf die Gefahren für politisch aktive Nutzer hingewiesen werden, wie sie beispielsweise von autoritären Regierungen ausgehen. Schon heute wird die Auswertung von Handydaten, Tweets und Kommentaren in sozialen Netzwerken von vielen Staaten genutzt, um beispielsweise Oppositionelle ausfindig zu machen oder Demonstrationen zu unterbinden. Allen, die zu den Diskussionen im Internet beitragen, muss klar sein, dass die generelle Offenheit der meisten Foren auch für all jene gilt, die den Kommentatoren schaden könnten.

Auch wenn viele der Funktionen sozialer Anwendungen im Internet bereits von »klassischen« Medien wie Tageszeitung oder Fernsehen erfüllt wurden, kann durch die Einfachheit der Nutzung und die große Anzahl an Nutzern

14 Eli Pariser über die Filterblase (englisch):
http://www.ted.com/talks/view/lang/eng//id/1091

von einer neuen Qualität des öffentlichen Diskurses gesprochen werden. Die Ursache der von Robert Putnam beschriebenen sozialen Isolation war die Tatsache, dass die aktive Teilnahme am öffentlichen Diskurs in den vorhandenen Medien weder vorgesehen noch praktisch umsetzbar war. Für die Internetöffentlichkeit stellt sich nun die Frage, ob die Einfachheit der Beteiligung nicht dazu beiträgt, dass das Netz zu einem Trägermedium einer Kakophonie der Monologe (beispielsweise durch belanglose Statusupdates) wird. Wenn die Kulturtechnik Onlinediskurs von einem Großteil der Gesellschaft verstanden und beherrscht wird, lassen sich konstruktive, dialektische und zielführende Diskurse entwickeln, ohne dabei die Themenoffenheit und Unabgeschlossenheit des Teilnehmerkreises der Internetöffentlichkeit zu gefährden.

3.4 Geheimnisse im Internet

Die Welt ist voller Geheimnisse: Das Geschäftsgeheimnis, das Bankgeheimnis, das Beichtgeheimnis, das Arztgeheimnis, das Anwaltsgeheimnis und viele weitere haben sogar rechtliche Anerkennung gefunden. Aber auch außerhalb rechtlicher Normen gibt es einen weiten Bereich kulturell anerkannter Schutzräume, in denen ein Weitertragen einer Information jenseits des Kreises der Eingeweihten als Vertrauensbruch wahrgenommen wird. Oftmals gibt es auch für diese Räume Schutzvorschriften, die unterbinden sollen, dass ein Geheimnisbruch durchgeführt wird. So schützt das Telekommunikationsgeheimnis das am Telefon vertraulich gesprochene Wort. Aber selbst ein heimlich geführter Flirt, ein Gespräch in vertraulichem Kreise dringt nur dann an eine größere Öffentlichkeit, wenn sich einer der Beteiligten entscheidet, dies eben genau dorthin zu bringen.

Mit anderen Worten: Auch die verschiedenen Begriffe und Typen von Geheimnissen unterliegen zwar den individuellen Empfindungen des Subjekts, sind überdies zugleich zumindest teilweise normativ verobjektiviert. Es gibt darüber hinaus jedoch freilich auch ethisch normative Typen des Geheimnisses, deren Bedeutung und Bruch in der Familie, der Freundschaft oder einem anderen sozialen Gefüge interaktiv definiert wird.

Sucht man nach Regeln, die einen Geheimnisbruch gegen den Willen der Geheimnisträger durchsetzen wollen, wird man mit wenigen Ausnahmen nahezu ausschließlich im Strafprozessrecht fündig. Ansonsten gilt: Was ein Einzelner oder eine Gruppe für sich behalten will, darf dort verbleiben.

Dieser Geheimnisschutz hat eine wichtige Funktion, so paradox es klingt: Er ermöglicht Kommunikation. Denn nicht mit jedem Satz, jeder Handlung, jedem Gedanken möchte man später, vielleicht zudem dekontextualisiert, konfrontiert werden. Der Schritt an die Öffentlichkeit soll in der Regel ein bewusster sein (dürfen).

Diesem Verständnis steht das Internet als größtmögliche Öffentlichkeit gegenüber. Zeitlich und örtlich potentiell unbegrenzt, weitgehend durchsuchbar (»Query-Öffentlichkeit«) ist sie selbst vom klassischen Öffentlichkeitsbegriff, der Veröffentlichung in der Zeitung oder dem Statement auf einer öffentlichen Veranstaltung, abzugrenzen. Im Vergleich zu Ersterem muten die Letzteren nahezu wie geheime Räume an. (Was sie freilich nicht sind, denn hier hat ja in der Regel der bewusste »Schritt« an die Öffentlichkeit stattgefunden.)

Neben dieser unbegrenzten Öffentlichkeit, die für das Geheimnis im vorgenannten, weiten Verständnis eine Bedrohung darstellt und damit auch die geschützte Kommunikation zu gefährden droht, findet noch ein zweiter paradigmatischer Wechsel statt: Durch die Transformation eines Großteils der Kommunikation in die Netze wird der faktische Schutz intransparent. Während der Empfängerkreis eines Gesprächs in kleiner Runde für alle Beteiligten erkennbar ist und ein hohes Maß an Sicherheit und Vertrauen gewährt, dass die Information zunächst nur diesen erreicht, verschleiert die

Technik vielfach weitere mögliche Rezipienten einer Information. Auch wenn wir im Alltag nicht davon ausgehen, dass unser E-Mail-Provider unsere Nachrichten liest (geschweige denn, dass er ein Interesse daran haben könnte), so bleibt doch für den aufmerksamen Nutzer immer ein erhebliches Fünkchen Ungewissheit, was mit der Information passiert: Eine Datenpanne und offen stehende Archive (vgl. Wikileaks) oder eine bewusste Entscheidung derjenigen, die die technische Kontrolle haben, eine vermeintlich kleine Öffentlichkeit einer größeren, entgrenzten zu öffnen (so geschehen im Newsnet), droht bei der Nutzung derzeitiger Infrastrukturen, die insofern die derzeitigen kulturellen Konventionen nur schlecht oder zumindest unvollständig abbilden.

Nun soll hier nicht den diskreten Gesellschaften, Geheimbünden und Verschwörungen das Wort geredet werden. Eine moderne, demokratische Gesellschaft lebt auch von einem großen Maß an Transparenz bezüglich der Handlungen ihrer Akteure. Entscheidungen zur gesellschaftlichen Entwicklung gewinnen potentiell an Qualität, wenn ihnen weitreichendes Faktenwissen zugrunde liegt. Das Internet bietet mit seinen Speicher- und Auswertungsmöglichkeiten hierfür immense Potentiale, die auch kulturelle Wandelungsprozesse mit sich bringen. Ein unbedachtes Aufgeben geschützter Kommunikationsräume allerdings birgt erhebliche Risiken individueller wie gesamtgesellschaftlicher Natur.

4 Exkurse

4.1 Smart Grid und Datenschutz

Auf welche Herausforderungen Datenschutz und informationelle Selbstbestimmung oft treffen, soll ein Beispiel aus der Praxis illustrieren. Smart Grids, intelligente Stromnetze, sollen helfen, den Stromverbrauch zu senken und den Übergang zu erneuerbaren Energien erleichtern. Das sind gesellschaftliche Ziele, gegen die kaum jemand etwas einzuwenden haben dürfte. Auf der anderen Seite aber erfassen Smart Grids auch permanent personenbezogene Daten.

Was ist das Smart Grid?

Das Smart Grid stellt im Wesentlichen eine um Kommunikationsfähigkeit angereicherte Energieversorgungsinfrastruktur dar. So beinhaltet es auf allen Netzebenen Lastmesser, welche den aktuellen Netzstatus in Echtzeit weitergeben.

Für Konsumenten ist der spannendste und relevanteste Teil des Smart Grids das Smart Metering. Die Grundlage hierfür sind elektronische Stromzähler, die über eine zusätzliche Kommunikationseinheit bidirektional kommunizieren können. Der Stromverbrauch kann dabei potentiell sekundengenau gemessen und weitergegeben werden. Außerdem können z. B. Preisinformationen vom Lieferanten in den Kundenhaushalt übermittelt werden.

Ziel und Begründung

Das Ziel von Smart Grids und Smart Meterings ist es, die Energieversorgung effizienter zu gestalten. In der derzeitigen Energieversorgungsarchitektur wird

der für die Netzstabilität zwingend erforderliche jederzeitige Ausgleich von Erzeugung und Verbrauch maßgeblich von der Steuerung der Angebotsseite, d. h. der Energieproduktion, gewährt. Die Nachfrage, d. h. der Energieverbrauch, wird als gegeben angenommen. Man spricht hier auch von verbrauchsorientierter Erzeugung.

Mit der Variabilität der Versorgung durch erneuerbare Energien – insbesondere sind hier Wind und Sonne zu nennen – ist jedoch auch eine stärkere Flexibilität auf der Nachfrageseite notwendig, da die Netzstabilität und der Ausgleich zwischen Produktionskapazität und Nachfragemenge mangels Steuerbarkeit von Wind und Sonne nicht mehr auf der Produktionsseite aufgelöst werden können. Zumindest zu einem gewissen Anteil soll daher in Zukunft auch das Prinzip des erzeugungsorientierten Verbrauchs verfolgt werden. Hierzu sind Smart Meter jedoch unerlässlich.

Der einfachste Fall der Nutzung von Smart Metern zur Verbrauchsbeeinflussung sind Tarife, bei denen der pro Kilowattstunde zu zahlende Strompreis über die Zeit variiert. Neben der vergleichsweise einfachen Abhängigkeit von der Uhrzeit wird aber auch an solche Tarife gedacht, deren Preis sich aufgrund der jeweils aktuellen Erzeugung aus regenerativen Quellen (Wind, Sonne) dynamisch verändert: Zu Zeiten mit vergleichsweise hohem Verbrauch – also beispielsweise an einem trüben, windarmen Herbsttag um die Mittagszeit – wäre dann der Strompreis hoch, während er zu Zeiten hoher Erzeugung bei gleichzeitig vergleichsweise geringem Verbrauch – also z. B. wenn nachts ein Starkwindgebiet über Norddeutschland hinweg zieht – deutlich niedriger wäre. Derartige dynamische Tarife stellen eine Möglichkeit dar, dem oben beschriebenen Problem zu begegnen, dass sich Erzeugung und Verbrauch bei zunehmender Integration regenerativer Stromquellen mangels Steuerbarkeit von Wind und Sonne immer schwerer in Ausgleich bringen lassen.

Weiterhin werden mit der Einführung von Smart Metering und sog. In-Home Energy Displays konsistente Energieeinsparungen verbunden. Langzeitstudien kommen hier zu divergierenden Ergebnissen von 3 %[15] bis 15 % Verbrauchseinsparung allein durch die Echtzeitinformation des Energieverbrauchs.

Rechtlicher Rahmen

Seit dem 01. 01. 2010 sind laut Energiewirtschaftsgesetz (EnWG) alle Neubauten sowie alle Gebäude, die einer größeren Sanierung unterzogen werden, mit Smart Metern auszustatten, soweit dies technisch möglich und wirtschaftlich sinnvoll ist. Nach der aktuellen Novelle des EnWG sind nunmehr ab spätestens 01. 01. 2013 in allen Haushalten intelligente »Messsysteme« – also elektronische Zähler, die über die Fähigkeit zur bidirektionalen Fernkommunikation verfügen – zu installieren, soweit dies technisch möglich und wirtschaftlich sinnvoll ist. Bei Neubauten, umfangreichen Sanierungen und bei Kunden mit einem Jahresverbrauch von mehr als 6.000 kWh entfällt zudem die Übergangsfrist und der Vorbehalt »sofern wirtschaftlich sinnvoll«, sodass diese Kunden zukünftig ausnahmslos mit intelligenten Messsystemen ausgestattet werden, sofern dies technisch möglich ist. Als technisch möglich wiederum gilt der Einbau, wenn Messsysteme, die den gesetzlichen Anforderungen entsprechen, zu denen u. a. auch zu definierende Schutzprofile des BSI gehören, am Markt verfügbar sind.

Ist nun ein intelligentes Messsystem bei einem Kunden installiert, dann werden die Messdaten nach derzeitiger Rechtslage in einer bestimmten Auflösung regelmäßig an den Messstellenbetreiber gesendet. Dieser sendet sie dann an den Verteilnetzbetreiber, der die Daten – ggs. nach vorheriger Aufbereitung – an den jeweils zuständigen Lieferanten weiterleitet. Außerdem sendet der Verteilnetzbetreiber aggregierte Daten an den Übertragungsnetzbetreiber, der darauf aufbauend die Bilanzierung von Verbrauch und Erzeugung vornimmt. Optional ist zudem z. B. zu Informationszwecken eine *zusätzliche*

15 http://www.stadtwerke-bochum.de/index/energiewelt/energie/energienews/115000.html

direkte Datenübertragung vom Messstellenbetreiber zum Lieferanten möglich, abrechnungs- und bilanzierungsrelevante Daten müssen jedoch immer über den Verteilnetzbetreiber laufen.

Herausforderung für die Gesellschaft

Die sich mit der Einführung von Smart Grids insbesondere an der Schnittstelle von Technik, Recht und Gesellschaft ergebende zentrale Herausforderung für die (Informations-) Gesellschaft soll nun überblicksweise dargestellt werden. Besonders deutlich wird diese Herausforderung im Bereich des Datenschutzes bzw. des Rechts auf informationelle Selbstbestimmung. Grundsätzlich stellen nämlich Energiemessdaten personenbezogene Daten dar, aus denen sich – je nach Auflösung – zumindest potentiell Aussagen zum Verhalten und zur Haushaltsausstattung eines einzelnen Elektrizitätsnutzers ableiten lassen.[16]

Zielkonflikte

Gleichzeitig ist es zur Erreichung der mit der Einführung von Smart Grids verfolgten Ziele – nämlich der Steigerung der Energieeffizienz im Stromnetz – aber unerlässlich, dass unterschiedliche Beteiligte Zugriff auf hochaufgelöste Messdaten haben. Der Lieferant eines Kunden benötigt diese Daten, um dynamische, z. B. wetterabhängige Tarife überhaupt ordnungsgemäß abrechnen zu können, was wiederum zwingend notwendige Voraussetzung für einen weiteren Ausbau regenerativer Energiequellen ist. Der lokale Verteilnetzbetreiber benötigt ebenfalls hochaufgelöste Messdaten um die Herausforderungen, die mit einem zunehmenden Ausbau erneuerbarer Energien und insbesondere mit der zukünftig zu erwartenden Etablierung von Elektromobilität einhergehen werden, überhaupt beherrschen zu können. Der Übertragungsnetzbetreiber wiederum benötigt hochaufgelöste Echtdaten, um auch unter den Bedingungen von zunehmend volatiler Erzeugung und dynamischer Lastverlagerung auf Kundenseite einen stabilen Netzbetrieb garantieren zu können.

Optionsraum

Schon hier werden die vielfachen Zielkonflikte zwischen Datenschutz, Klimaschutz und Versorgungssicherheit deutlich, die in diesem Bereich zukünftig eingehend zu diskutieren sein werden. Teilaspekte lassen sich sicher durch die konkrete technische Ausgestaltung der Systeme lösen. So reicht es für viele Anwendungsfälle beispielsweise aus, lediglich pseudonymisierte oder mittels Aggregation anonymisierte Messdaten zu verwenden.[17] An der für bestimmte Anwendungsfälle bestehenden Notwendigkeit des Zugriffs auf höher aufgelöste, personenbezogene Messdaten sowie an deren prinzipiellem Vorliegen ändert dies jedoch nichts. Zudem soll in Zukunft neben dem heutigen Energiekernmarkt auch ein neuer Markt für unterschiedlichste, auf Energiemessdaten basierende Zusatzdienste entstehen. Die auf einem derartigen Markt in Zukunft angebotenen Dienste können auch für den einzelnen Kunden durchaus einen echten Mehrwert bedeuten, lassen sich jedoch schon aus prinzipiellen Gründen nicht vorhersehen, geschweige denn bewerten.

Deshalb stellt sich wie bei jeder risikobehafteten Tätigkeit die Frage, wie sich der Staat in diesem Zielkonflikt positionieren muss. Auf der einen Seite könnte man meinen, dass die Marktkräfte hier schon einen gerechten Ausgleich

16 Einen anschaulichen Einstieg vermittelt bspw. Quinn, E. L. (2009): Privacy and the New Energy Infrastructure, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731. Mit steigender Auflösung der vorliegenden Messdaten lassen sich auch teilweise deutlich detailliertere Aussagen treffen. So ist es bspw. Studenten des Hasso-Plattner-Instituts der Univer-sität Potsdam gelungen, anhand der Verbrauchssignatur eines Kaffeevollautomaten den georderten Kaffee zu bestimmen. Vgl. hierzu http://epic.hpi.uni-potsdam.de/Home/InMemoryRealTimeEnergyManagement.

17 Vgl. hierzu bspw. die jeweiligen Abschnitte zur »Datensparsamkeit« der Beiträge in Raabe, Pallas, Lorenz, Weis, Boesche (Hrsg., 2011): Datenschutz in Smart Grids.

herbeiführen, wie dies in der allgemeinen Debatte um den (globalen) Rechtsrahmen für das Internet vertreten wird. Auf der anderen Seite könnte man staatliche Detailregelungen fordern, wie sie z. B. für den Bereich der sozialen Netzwerke immer wieder verlangt werden, weil der Staat sich auch im Internet schützend vor seine Bürger stellen müsse.

Lösungsansatz

Zur Lösung dieser Frage müssen aus rechtlicher Perspektive in jedem Fall die Rahmenbedingungen der Einführung von Smart Metering mit berücksichtigt werden. Mit der Novelle des Energiewirtschaftsgesetzes im Jahre 2011 besteht hier erstmalig die staatlich gesetzte Pflicht eines jeden Bundesbürgers, dessen jährlicher Stromverbrauch eine bestimmte Schwelle überschreitet, eine IKT-Schnittstelle in seinem Haushalt zu installieren. Daraus erwächst ein besonderer Schutzauftrag des Staates für seine Bürger, weil er mit der verpflichtenden Einführung der Kommunikationsschnittstellen selbst ein Risiko setzt und in der klassischen Perspektive des Datenschutzes gesetzliche Maßnahmen hoher Regulierungsdichte zu erwarten wären. Auf der anderen Seite verlangen zukünftige (noch unbekannte) Effizienzmaßnahmen auf Basis der Strommessdaten die größtmögliche Offenheit für Innovationen vom Gesetzgeber. Während das letztgenannte Ziel also eine innovationsoffene Gesetzgebung mit möglichst geringer Regulierungsdichte (bzw. hohen Freiheitsgraden für die Marktenfaltung) verlangt, folgt aus dem kollidierenden Recht der Sicherung der informationellen Selbstbestimmung der Auftrag für detailreiche ordnungsrechtliche Maßnahmen, welche die etablierten datenschutzrechtlichen Prinzipien in den gesetzlichen Rahmen implementieren.

Die zentrale Herausforderung an den Gesetzgeber besteht also darin, ein modernes bereichsspezifisches Datenschutzrecht zu entwickeln, das wahrhaft technologieneutral gestaltet ist, anpassungsfähig auf neue Architekturen und Rollen reagiert, die hergebrachten Prinzipien des Datenschutzes optimiert, aber gleichwohl wegen der teilweise erheblichen Investitionsentscheidungen auch Rechtssicherheit gewährleistet.

Da das Smart Grid gleichzeitig auch den Übergang zwischen der klassischen Ansehung des Datenschutzes in geschlossenen IKT-Systemen und der Offenheit des Internets markiert, kommt diesem Satz durchaus eine gewisse Allgemeingültigkeit zu.

4.2 Privatheit und Öffentlichkeit als Gegenstand gesellschaftlicher Aufmerksamkeitsdynamiken

Im zweiten Jahrzehnt dieses Jahrhunderts befinden wir uns mitten in einer gewaltigen gesellschaftlichen Umwälzung im Hinblick auf die integrale Einbindung des Menschen in das soziotechnologische System des Internets. Die Frage ist kaum mehr, ob wir Teil dieses Raumes sein möchten – wir sind es längst. Egal ob wir eine Flugreise unternehmen oder ein Ferngespräch führen: unsere physische Umgebung und traditionellen Technologien konvergieren mehr und mehr im »Cyberspace«. Während also die Verknüpfung unserer Lebenswelten mit dem Internet in vollem Gange ist, stellt sich die substantielle Frage, wie wir die Balance zwischen Privatheit und Öffentlichkeit halten.

Beispiele wie die öffentliche Erregung um Google Street View in Deutschland zeigen, wie schwer diese Balance für grundsätzlich neue Dienste und Anwendungen zu finden ist. Und sie zeigen vor allem auch, wie schwer es ist, unaufgeregte, gut informierte und nachhaltig ausgerichtete Debatten dazu zu führen. Anders ausgedrückt: Ähnlich dem Gartner-Hype-Zyklus[18] folgt die öffentliche Erregung über neue internetbasierte Produkte auch im Hinblick auf mögliche »Datenschutzprobleme« einer Dynamik der Über- und

18 http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

Untertreibung, bevor sie sich auf einem realistischen Niveau einpegelt. Während also etwa Google Street View noch zu scharfen Kritiken führte, wurde die Ankündigung von Microsofts weitgehend äquivalentem Streetside-Dienst deutlich entspannter aufgenommen.

Im Folgenden möchten wir mittels vier Mini-Fallstudien einen Überblick zu verschiedenen Technologien geben, die sich auf unterschiedlich frühen Stufen der hypothetisierten Aufregungskurve einordnen lassen: von dem mit signifikanten Unsicherheiten verbundenen Anfangsstadium einer Technologie (Phase 1 von 5) bis hin zu einem Mittelstadium, in dem Nutzen, Kosten und Risiken aus praktischer Sicht verstanden werden (ca. Phase 3 von 5). Unser Ziel ist es dabei nicht, vollständige Fallstudien zu präsentieren oder gar Vorhersagen zur weiteren Entwicklung im frühen Stadium befindlicher Technologien zu treffen, sondern das Feld für mögliche weitere Arbeit am Thema grob zu skizzieren, indem wir unsere »Privatheit-und-Öffentlichkeit-Aufregungskurve« mit Leben füllen. Perspektivisch ist es dann unser Ziel, einschlägige Artefakte und Institutionen bezüglich ihres Einflusses auf den Umgang mit potentiell sensiblen Daten zu beleuchten, und zwar möglichst bevor die Debatte primär durch medial getriebene »übersteigerte Erwartungen« und »Desillusionierung« geprägt wird.

Erste Prototypen: Beispiel dezentrale soziale Netzwerke

Dezentrale soziale Netzwerke lassen sich am besten als logisches Gegenstück zu den populären zentralisierten Diensten à la Facebook und Twitter begreifen. Mittels offener Schnittstellen und einer verteilten Architektur verbleiben Kontrolle und Zugangsregulierung zu Inhalten und Funktionen des Dienstes bei den Nutzern, deren Daten ja, wie auch bei zentralen Netzwerken, die Ausgangsbasis jeglicher »sozialer« Funktionen des Dienstes sind. Je nach Netzwerk- und Sicherheitskonzept des Systems kann dabei ein Nutzer selbst einen Server betreiben und somit nicht nur mit seinem »Profil« und seinen Interaktionen, sondern auch funktional Teil des sozialen Netzwerks sein. Mittlerweile existiert eine Reihe solcher dezentralen, auf diversen offenen Standards basierenden Systeme[19], auch wenn diese in ihrer Verbreitung noch vergleichsweise unbedeutend sind. Noch hat es kein System geschafft, die Einstiegshürden für die breite Masse an Endanwendern hinreichend niedrig zu gestalten und dabei einen mit existierenden zentralisierten Systemen vergleichbaren Mehrwert zu liefern.

Durch die Verteilung der Netzwerkarchitektur geben dezentralisierte soziale Netzwerksysteme den Nutzern also die prinzipiell wünschenswerte Möglichkeit, ihre Daten selbst zu verwalten und den Zugriff von Dritten darauf – anders als etwa beim zentralisierten »Klassiker« Facebook – selbst zu steuern.[20] Andererseits kann eine verteilte Architektur, die von Nutzern betrieben wird, strukturelle Sicherheitsprobleme nach sich ziehen, da beliebige Personen einen Teil des Netzwerks betreiben können. Die Abwesenheit einer zentralen Instanz kann zudem zu Problemen bei der Durchsetzung gesellschaftlicher Normen und Rechtsgrundsätzen führen (Stichwort illegales Filesharing in P2P-Netzen). Dezentralisierte soziale Netzwerke können also zwar in einem sehr realen Sinne die informationelle Selbstbestimmung der Nutzer fördern und ihre Abhängigkeit von einem zentralen System beseitigen, erzeugen jedoch auch ganz eigene Herausforderungen im Spannungsfeld zwischen Privatheit und Öffentlichkeit sowie Nutzen und Kosten, die bislang nur in Ansätzen verstanden sind.

Beginnende Aufregung: Beispiel Gesichtserkennung

In den letzten Jahren verbreitete sich im Internet die Möglichkeit, Fotos mit abgegrenzten Personenkreisen, aber auch mit der Weltöffentlichkeit zu teilen.

19 Siehe für einen Überblick http://www.w3.org/2005/Incubator/federatedsocialweb/wiki/Software und http://en.wikipedia.org/wiki/Distributed_social_network#Comparison_of_projects. Viele dieser Projekte sind expe-rimenteller Natur, einige jedoch auch schon relativ weit gediehen – siehe etwa Jappix oder Friendika.

20 Siehe etwa die offenen Authentifizierungsstandards OAuth and WebID.

Dazu kommt die mittlerweile ernst zu nehmende Technologie, Gesichter innerhalb von Fotos zu identifizieren. In der Tat experimentieren Sicherheitsbehörden in Zusammenarbeit mit Spezialanbietern schon länger mit Diensten, die Bilder von Überwachungskameras in Flughäfen oder an strategisch wichtigen öffentlichen Plätzen in Echtzeit auswerten und via Gesichtserkennungssoftware mit Bildern aus polizeilichen Datenbanken vergleichen.

Eine breitere Ausweitung dieser Technologie hin zu den Lebenswelten von Endnutzern scheint also nur noch eine Frage der Zeit. Erste soziale Netzwerke haben Gesichtserkennung in ihre Dienste integriert, begleitet von erheblichem Medienecho. Im Hinblick auf Fragen zur Bedrohung von Privatheit befinden wir uns in einer Phase anschwellender Aufregung: Denn wie damit umgegangen werden kann/muss, dass die Identität von potentiell jedem – egal ob in Videos, auf einer Party oder einer Demonstration – in Erfahrung gebracht werden kann, bleibt derzeit noch fraglich. Anonymität als Ausgangspunkt zwischenmenschlicher Beziehungen würde der Vergangenheit angehören, die Folgen für unser Verständnis von Privatheit und Öffentlichkeit wären immens. Rechtlich durchzusetzende Verbote/Gebote sowie technische Einschränkungen des potentiell Machbaren könnten angezeigt sein. Solange sich kein Gleichgewicht zwischen gesellschaftlichen Normen, technischen Möglichkeiten und kommerziellen Nutzungen abzeichnet, wird die Unsicherheit im Umgang mit der Technologie Gesichtserkennung groß bleiben.

Konsolidierung praktischer Erfahrungen:
Beispiel ortsbasierte Internetdienste

Das Internet ist mittlerweile für weite Teile der Bevölkerung – mindestens aber die sogenannten »Digital Natives« – zum integralen Bestandteil von mobiler Kommunikation geworden, eine Domäne, die bislang lediglich durch Sprachtelefonie und Kurznachrichten (SMS) geprägt war. Durch die Verknüpfung von Geolokation (Standortbestimmung in Echtzeit und ohne zwingendes Zutun der Anwender) und internetbasierten Diensten ergeben sich völlig neue Anwendungsszenarien des Internets. Dass dabei mit Aufenthalts- und Bewegungsprofilen im Sinne des klassischen Datenschutzbegriffs personenbezogene oder -beziehbare Daten über Endanwender anfallen, liegt in der Natur der Sache.

Welche gesellschaftlich relevanten Probleme zu Privatheit und Öffentlichkeit daraus tatsächlich erwachsen, hängt von der konkreten Anwendung ab. Insgesamt ist das Feld der Vorteile von ortsbasierten Diensten relativ gut abgesteckt; es scheint derzeit, als ob der Anwendungsbereich solcher Dienste in der Tat recht eingeschränkt ist – es finden sich dort Navigation, »Augmented Reality«, zunehmend auch »soziale« Netzwerke. Die fragwürdigen oder potentiell abträglichen Aspekte scheinen ebenso überschaubar – Stichwort Geofencing. Echte Killapplikationen jenseits von ortsbasierter Werbung sind bislang nicht in Sicht, und gesellschaftliche Normen zum Umgang mit dem personenbezogenen Datum »aktueller Aufenthaltsort« sind erst im Entstehen. Der Weg aus dem »Tal der Enttäuschung« hin zum »Pfad der Erleuchtung« steht uns hier also noch bevor.

Fazit

Die vorgestellten Beispiele für internetbezogene Technologien und Produktentwicklungen gehen mit ganz unterschiedlichen gefühlten, realen und potentiellen Auswirkungen im Bereich Privatheit und Öffentlichkeit einher. Es scheint uns plausibel, ein Modell von »stark exponentiell gedämpfter Schwingung mit Annäherung an eine Gleichgewichtslage« für die unterschiedlichen Dimensionen gesellschaftlicher Aufregung zu diesen Fragen auf solche Artefakte und Entwicklungen anzuwenden. Eben wegen der Vielzahl relevanter Dimensionen und Abhängigkeiten in einem solchen theoretischen Gebilde jedoch bleibt es freilich zu diesem Zeitpunkt unklar, ob derartige Diskussionen einen signifikanten Einfluss auf gesellschaftliche Aufregungsdynamiken haben können. Als Analyseansatz indes liefern sie einen sinnvollen Beitrag zur Betrachtung von Internettechnologien und deren Implikationen zu Privatheit und Öffentlichkeit.

5 Literaturempfehlungen

Zu Beginn der vierten Initiative des Internet & Gesellschaft Co:*llaboratory* wurden die Experten darum gebeten, jeweils drei Artikel, Blogs oder Videos zum Thema Privatheit und Öffentlichkeit für die Knowledge Base vorzuschlagen und ihre Auswahl mit einem kurzen Kommentar zu begründen. Auf diese Weise konnten über 50 Literaturempfehlungen zusammengetragen werden, die auf www.collaboratory.de aufrufbar sind. Für den Abschlussbericht haben wir einige Quellen ausgewählt die einen groben Überblick zum Wandel von Privatheit und Öffentlichkeit ermöglichen sollen.

→ Boyd, S. (2010). Publicy Defined, and some Background.

Kurzzusammenfassung

Anhand der Definition von »Publicy« erläutert Stowe Boyd die Probleme, die bei der Verwendung verschiedener Begriffe für Öffentlichkeit bei der Auseinandersetzung mit Privatheit auftreten können.

Expertenkommentar

Publicy beschreibt den Wandel der Wahnehmung von Privatheit in social networks.

URL

http://www.stoweboyd.com/post/771781382/publicy-defined-and-some-background

→ Jarvis, J. (2010). The german paradox – privacy, publicness and penises.

Kurzzusammenfassung

In diesem Vortrag auf der re:publica 2010 geht der US-amerikanische Journalist Jeff Jarvis auf die kulturellen Unterschiede in der Bewertung von Privatheit ein. Insbesonderer im Kontext globaler Produkte wie Google Street View sei es nötig, diese Unterschiede zu berücksichtigen.

Expertenkommentar

In einer Keynote auf der Re:Publica 2010 beschreibt Jeff Jarvis humorvoll den deutschen Umgang mit zwischen Prüderie und gemischter Sauna.

URL

http://www.youtube.com/watch?v=pSqyEXLkrZ0

→ OpenDataCity. (2010). Verräterisches Handy. ZEIT ONLINE.

Kurzzusammenfassung

Der grüne MdB Malte Spitz hat seine Vorratsdaten von der Telekom eingeklagt und mit frei im Netz verfügbaren Informationen von Twitter etc. verknüpft. Daraus wurde eine Animation erstellt, die es möglich macht, über einen Zeitraum von sechs Monaten einen detaillierten Einblick in sein Leben zu erhalten.

Expertenkommentar

Vorratsdaten visualisiert. Zeigt plastisch, wie genau unser tägliches Leben automatisiert erfasst werden kann – Grimme Online Award 2011.

URL

http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

→ Solove, D. J. (2008). »I've Got Nothing to Hide« and Other Misunderstandings of Privacy. San Diego Law Review, Seite 745 – 772.

Kurzzusammenfassung

In diesem Aufsatz wird das »Ich habe nichts zu verbergen« Argument analysiert, welches häufig im Zusammenhang mit Überwachungsprogrammen gemacht wird. Daniel J. Solove konzeptualisiert dazu zunächst Privacy, um auf dieser Basis das Argument zu problematisieren.

Expertenkommentar

Solove betrachtet dieses Argument im Detail und beleuchtet die möglichen Probleme, die sich daraus ergeben.

URL

http://www.gab.ro/wp-content/uploads/2010/02/nothing-to-hide.pdf

---

→ Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. The Yale Law Journal, 113(6), Seite 1151 – 1221.

Kurzzusammenfassung

In diesem Artikel geht James Q. Whitman auf die unterschiedliche Wahrnehmung von Privatheit in verschiedenen westliche Kulturen ein. Diese führen unter Anderem zu andauernden Auseinandersetzungen über den Schutz von Kundendaten zwischen der Europäischen Union und den USA.

Expertenkommentar

Der Text von Whitman stellt eine äußerst wertvolle Grundlage für das Verständnis der Unterschiede zwischen der europäischen und der amerikanischen Interpretation von »Privacy« dar. Außerdem räumt er mit dem Missverständnis auf, der Kern des amerikanischen Privacy-Verständnisses wäre bei Warren/Brandeis zu finden – deren Sichtweise ist nämlich eindeutig europäisch geprägt.

URL

http://www.yalelawjournal.org/pdf/113-6/WhitmanFINAL.pdf

6 Ablauf der vierten Initiative

Es gibt wenige Länder, in denen so intensiv, ja fast schon konfrontativ über das Verhältnis zwischen Privatheit und Öffentlichkeit diskutiert wird wie in der Bundesrepublik Deutschland. So entstehen international maßgebliche Debattenbeiträge, die die gesellschaftliche Verortung von Privatheit und Öffentlichkeit erst möglich machen.

Hier knüpfte das Co:*llaboratory* mit seiner vierten Initiative Privatheit und Öffentlichkeit im April 2011 an. Losgelöst vom Tagesgeschäft der Teilnehmer sollte dieses schwierige Verhältnis unter die Lupe genommen werden. Die Vorarbeit hierfür begann im kleinen Kreis, bestehend aus Bernd Lutterbeck, Rafael Capurro, Hubertus Gersdorf, Max Senges, Philippe Gröschel, Henning Lesch, Jan Schallaböck und Falk Lüke, schon im Sommer 2010. Die groben Umrisse der Initiative wurden festgelegt; außerdem wurde die Fragen diskutiert, ob die Teilnehmer überhaupt miteinander in ein konstruktives Gespräch kommen könnten oder ob die Differenzen gar so groß sind, dass die Kommunikation allein schon schwierig wird. Diese Unsicherheit blieb bis zum ersten Treffen vorhanden – aber eine Idee war geboren: Statt im Hier und Heute verhaftet zu bleiben, sollte die Gruppe, ähnlich der jüngsten Co:*llaboratory*-Initiative (Thema Urheberrecht), die Diskussion mit einem virtuellen Zukunftspunkt verknüpfen – dem Jahr 2035. Für diese Zeit »in ferner Zukunft« sollten hypothetische Referenz-Szenarien entwickelt werden, die jeweils unterschiedliche Entwicklungen der »Koordinaten« Privatheit und Öffentlichkeit zugrunde legen.

Am 1. April 2011 fand der erste Workshop in der Berliner Vertretung der E-Plus-Gruppe statt. Noch während der Vorstellungsrunde beherrschte Skepsis den Raum: Mit wem hat man es hier zu tun? Aus der Expertengruppe, hochkarätig und interdisziplinär aus Wissenschaft, Wirtschaft und Zivilgesellschaft besetzt, konnte jede und jeder Wissen und Vorstellungen zu

Privatheit und Öffentlichkeit einbringen. Die Runde begann mit einer Vielzahl von Fragen:
Wie viel Paternalismus darf, muss, kann wünschenswert sein? Sind Daten Macht oder Algorithmen? Welche Rolle spielen heute und in Zukunft Anonymität, Pseudonymität und (multiple) Identität? Sind Daten ein Rohstoff? Sind die aktiv von uns gegebenen Daten künftig überhaupt noch relevant? Oder erzeugen wir nicht alle einen stetigen Datenstrom, der viel genauere Aussagen über uns, unser Verhalten und unsere Vorlieben trifft? Wie viel Öffentlichkeit braucht das Netz – und wie viel ein funktionierendes Gemeinwesen? Welche Rollen spielen gesellschaftliche und kulturelle Konventionen bei der Abwägung zwischen privat und öffentlich?

Um das Spannungsfeld etwas systematischer anzugehen, teilten wir es in drei Fragenkomplexe: (1) gesellschaftliche, (2) individuelle und (3) technische Aspekte.

Mit diesem Ansatz und unseren Fragen stellten wir uns im April 2011 den Teilnehmern des Internetkongresses re:publica'11. In der lebhaften und vielfältigen Diskussion wurde deutlich, dass sich die Beteiligten nur schwer von der aktuellen Debatte lösen konnten. Kaum jemand schien willens oder in der Lage, das Thema in einem größeren Kontext (»bigger picture«) zu betrachten.

Auch aufgrund dieser Erfahrungen fällten wir bereits im Rahmen unseres ersten Workshops die Entscheidung, unsere Fragen auch an Experten außerhalb des Co:*llaboratory* zu richten. Die dabei entstandenen Interviews finden Sie in diesem Bericht zu finden.

Mit unserem zweiten Expertenworkshop gastierten wir bei der Stiftung Neue Verantwortung. Dort wurde intensiv diskutiert, ob und wie Szenarien beschreibbar wären, die im Jahr 2035 spielen und in denen die Gesellschaft verschiedene Richtungen im Verhältnis zwischen Privatheit und Öffentlich-

keit eingeschlagen hat. Mit einer Vielzahl an Storyboard-Ideen zeigten die Expertinnen und Experten ihre Kreativität. Auch im Jahr 2035 werden die Menschen, der Erwartung unserer Runde nach, weder perfekt noch grundsätzlich gut sein. Während der Erstellung der Szenarien fiel jedoch auf, dass ein brauchbarer Überblick zum Verhältnis zwischen Privatheit und Öffentlichkeit, zwischen ihren Ausprägungen und ihren Problemen bislang fehlt. Dies zu versuchen nahmen wir uns für unseren Bericht nun vor. Ziel sollte es des weiteren sein, der Gesellschaft die Gestaltungshoheit in Bezug auf Privatheit und Öffentlichkeit wiederzugeben. Der Workshop entwickelte dazu eine Vielzahl an Handlungsoptionen und -empfehlungen.

Im Juni öffnete sich die Expertenrunde dann erstmals auch nach außen: Die Initiative war zu Gast in der Hauptstadtrepräsentanz der Deutschen Telekom. Während dieses dritten Workshops näherten wir uns einem weiteren großen Themenblock: dem von uns so getauften Bereich des Lexikons und der Landkarte der Phänomene. Dahinter stand die Frage, ob und wie Privatheit und Öffentlichkeit und die das Spannungsfeld zwischen ihnen beschreibenden Phänomene sich zueinander verhalten.

Hierzu luden wir drei Gäste ein: Prof. Dirk Heckmann, Prof. Karl-Heinz Ladeur und Dr. Jan Schmidt. Zunächst beteiligten sie sich aktiv an der Tagesdiskussion und gaben beim anschließenden Co:*llaboratory*-Abend dem Expertenkreis und Gästen mit Vorträgen (zu finden auf unserem YouTube-Kanal) weiteren Input für Diskussionen über Ansätze und Perspektiven – beispielsweise ob persönliche Informationen wie informationelle Güter behandelt werden sollten oder ob wir tatsächlich die Kontrolle über unsere Daten verlieren oder sie nicht vorauseilend einfach aufgeben.

Konnte die Vielzahl der aufgeworfenen Fragen und selbstgestellten Aufgaben in nur noch zwei verbleibenden Workshops geklärt werden? Unmöglich. Spontan wurde ein weiteres Workshopwochenende einberufen: In der idyllischen Abgeschiedenheit Brandenburgs traf sich ein knappes Dutzend der Experten, um mit größtmöglicher Intensität Landkarte und Lexikon der Phänomene, Szenarien und Denkanstöße voranzubringen, was gut gelang. Spätestens ab diesem Brandenburg-Workshop ging die Arbeit schnell voran: In Telefonkonferenzen wurden die Maßgaben für die Szenarien gemeinsam entwickelt, erste konsistente Storyboards entworfen, die Kommunikation zwischen den Präsenztreffen nahm zu. Zurück in Berlin konsultierten wir einen Mann, der gerade bei der Entwicklung von Szenarien für die ferne Zukunft ein ausgewiesener Experte war: Dr. Karlheinz Steinmüller, Science-Fiction-Autor und Gesellschafter der Zukunftsberatung Z-Punkt.

Der vierte Workshop in der Berliner Vertretung von CSC stand vor der anspruchsvollen Aufgabe, die bisher entwickelten, diversen Bausteine wie ein Puzzle zusammen zu fügen. Mit den Ergebnissen gingen wir schließlich im September 2011 in den Abschlussworkshop in der Landesvertretung Sachsen-Anhalts. Trotz der gleichzeitig entbrannten Debatte um den europäischen Rettungsschirm und den Papstbesuch in Deutschland war das Interesse an unserer Initiative groß – fast 50 Personen aus Wirtschaft, Wissenschaft, Zivilgesellschaft, Politik und Verwaltung nahmen an unserer ganztägigen Veranstaltung teil. Unser Ziel war es, im Gespräch mit weiteren Experten und erstmals auch unter Beteiligung von Politik und Verwaltung die im Laufe eines halben Jahres entstandenen Ansätze zu prüfen. Die Resonanz floss in die Erstellung des nun vor Ihnen liegenden Berichts ein. Mit neuen Einblicken bereicherte uns die Hamburger Medienpsychologin Prof. Sabine Trepte: Sie stellte die Studienergebnisse des von ihr geleiteten Forschungsclusters »Young Scholars Network on Privacy and Web 2.0« vor.

Wenn man auf die Zusammenarbeit des vergangenen halben Jahres zurückblickt, fällt auf, wie gut die Expertinnen und Experten nach einer anfänglichen »Schnupperphase« miteinander ins Gespräch kamen und zu konkreten Ergebnissen, konstruktivem Kon- wie Dissens gelangten. Am Ende liegt ein Bericht vor, der das komplexe Spannungsfeld zwischen Privatheit und Öffentlichkeit so grundlegend analysiert wie dies wohl nur mit diesem transdisziplinären Kreis möglich war. Es wurde gestritten, um echte Kompromisse gerungen und Falsche wurden vermieden. Die Resultate widersprechen

einander zum Teil diametral, was die Vielfalt der Ansätze und Meinungen widerspiegelt und zum Nachdenken anregen soll. Die vorliegenden Ergebnisse werden entsprechend nicht von jedem Experten in jedem Punkt geteilt. Doch alle am Ende des Berichts aufgeführten Teilnehmer haben konstruktiv in gemeinschaftlicher Anstrengung zu dieser vierten Initiative des Co:*llaboratory* beigetragen; sie haben sich die Zeit genommen, um innezuhalten und einen neuen Blickwinkel auf das größere Ganze zu suchen. Ob uns das gelungen ist, das entscheiden am Ende Sie: als Leser dieses Berichts.

7 Expertenkreis der vierten Initiative

Ahmet Emre Açar studierte Informatik an der HU Berlin und Kommunikationswissenschaft an der TU Berlin. Als Kollegiat der Alcatel SEL Stiftung für Kommunikationsforschung beschäftigt er sich mit den Auswirkungen neuer Informations- und Medientechnologien. Mit seiner Design Thinking Agentur hilft er Unternehmen bei der Entwicklung neuer Produkte und Dienstleistungen.

Dr. Matthias Bärwolff promovierte in Ingenieurwissenschaften und ist Mitbegründer der Open-Source-Jahrbuch-Reihe, dem Standardwerk zu den diversen gesellschaftlichen Aspekten von freier Software. Zur Zeit ist Matthias ehrenamtliches Mitglied im IEEE Computer Society History Committee und arbeitet als freier Berater und Autor in Berlin.

Ulf Buermeyer ist Richter in einer großen Strafkammer am Landgericht Berlin und ehemaliger wissenschaftlicher Mitarbeiter des Bundesverfassungsgerichts. Seine Forschungsschwerpunkte sind Grundrechte im Spannungsfeld von Freiheit und Sicherheit, Datenschutz, Persönlichkeitsschutz und das Telekommunikationsgeheimnis. Er gestaltet seit Jahren das strafrechtliche eJournal HRRS mit und bloggt privat zu verfassungs- und strafrechtlichen Fragen.

Prof. Dr. Rafael Capurro ist Professor (em.) an der Hochschule der Medien Stuttgart, Direktor des Steinbeis-Transfer-Institut Information Ethics (STI-IE), Präsident des International Center for Information Ethics (ICIE) und Distinguished Researcher in Information Ethics an der School of Information Studies der University of Wisconsin-Milwaukee, USA. Zudem ist er Editor-in-Chief der International Review of Information Ethics (IRIE).

Susanne Dehmel ist Juristin und leitet beim BITKOM den Bereich Datenschutz, Wettbewerbs- und Verbraucherrecht. Sie war unter anderem verantwortlich für die Koordinierung des Datenschutzkodex für Geodatendienste.

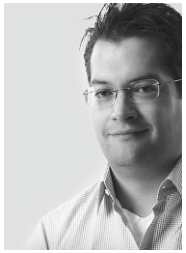
Prof. Dr. Hubertus Gersdorf ist Inhaber der Gerd Bucerius-Stiftungsprofessur für Kommunikationsrecht und Öffentliches Recht an der Universität Rostock, sachverständiges Mitglied der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages und Mitglied des Beirats der Gesellschaft zum Studium strukturpolitischer Fragen. Er arbeitet als Dozent an dem Europa-Institut der Universität des Saarlandes, an der Bucerius Law School Hamburg, an der Hamburg Media School (HMS) und an der Universität Bonn. Von 2002 bis 2008 fungierte er als (sachverständiges) Mitglied der Kommission der Gemeinsamen Stelle Digitaler Zugang (GSDZ) der Direktorenkonferenz der Landesmedienanstalten (DLM).

Philippe Gröschel ist Mitglied im Vorstand der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter und Jugendschutzbeauftragter. Er war verantwortlich für Medienpolitik bei den VZ-Netzwerken (schülerVZ, studiVZ und meinVZ). Momentan arbeitet er als Government Relations Manager und Jugendschutzbeauftragter bei Telefonica.

Seda Gürses studierte Internationale Beziehungen und Mathematik an der Universität Redlands (USA), Informatik an der Humboldt Universität zu Berlin und promovierte am Lehrstuhl für Informatik an der Katholischen Universität Leuven. Momentan forscht sie zu Computersicherheit und industrieller Kryptographie (COSIC) an der K. U. Leuven. Ihr Schwerpunkt liegt hierbei auf der Entwicklung von neuen Instrumenten für Privatsphäre und Identitätmanagement unter Berücksichtigung der unterschiedlichen Anforderungen informationsverarbeitender Systeme.

Stephan Hansen-Oest ist Fachanwalt für IT-Recht. Er ist beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich) und als Legal Expert für das European Privacy Seal (EuroPriSe) akkreditiert. Stephan berät Unternehmen bei der Bewältigung der alltäglichen Herausforderungen im Umgang mit personenbezogenen Daten und strategisch im Hinblick auf künftigen Entwicklungen im deutschen und internationalen Datenschutz.

Ulrike Höppner ist als promovierte Politikwissenschaftlerin an der Goethe Universität Frankfurt a. M. tätig und forscht dort zu Fragen von Transparenz und Geheimnis in der internationalen Politik. Sie interessiert sich besonders für die Notwendigkeit des Privaten für das Funktionieren der Öffentlichkeit aus der Sicht der politischen Theorie und Ideengeschichte.



Andreas Jungherr ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Politische Soziologie der Universität Bamberg. Er forscht zu den Auswirkungen von Online-Kommunikation auf politische Meinungsbildung und die Vermittlung politischer Inhalte. Er veröffentlichte Arbeiten zur Nutzung der e-Petitionenplattform des Deutschen Bundestags, zur Struktur von Kommunikationsnetzwerken auf der Microblogging-Plattform Twitter und Online-Kampagnen im Bundestagswahlkampf 2009.

Als Rechtswissenschaftler und Informatiker, bewegt sich **Christoph Kappes** seit über 20 Jahren im Spannungsfeld zwischen IT-Technologie, Geschäftsmodellen und Innovation. Heute ist er als Berater für Online-Strategien und operative Spezialaufgaben tätig. Er schreibt für Fachzeitschriften, ist freier Mitarbeiter der F.A.Z. und Mitherausgeber des Mehrautorenblogs Carta.

Ulrich Klotz, Dipl.-Ing., nach Forschungs- und Entwicklungsarbeiten in Computerindustrie und Werkzeugmaschinenbau befasste er sich seit den achtziger Jahren beim Vorstand der IG Metall mit dem Themenfeld Computer und Zukunft der Arbeit. Daneben war er Stiftungsprofessor an der Hochschule für Gestaltung in Offenbach, Beirat und Gutachter für das BMBF und Kanzleramt. Er ist Autor von ca. 300 teilweise preisgekrönten Veröffentlichungen zum Thema Arbeit, Technik und Innovation.

Henning Lesch ist Jurist und als Rechtsanwalt in Berlin zugelassen. Derzeit arbeitet er als Leiter Recht und Regulierung für den eco – Verband der deutschen Internetwirtschaft. Er beschäftigt sich vor allem mit den Themenbereichen Recht und Regulierung sowie Internet Governance auf nationaler und internationaler Ebene.

Falk Lüke ist der Projektmanager der vierten Initiative des Co:*llaboratory.* Der studierte Politikwissenschaftler ist Journalist für Technologie- und Politikthemen in Berlin, war beim Bundesverband der Verbraucherzentralen für Datenschutz zuständig, arbeitete davor bei einer Agentur und als festangestellter Redakteur.

Prof. Dr. Bernd Lutterbeck ist Berater öffentlicher und privatwirtschaftlicher Institutionen. Von 1978 bis 1984 war er Beamter beim Bundesbeauftragten für den Datenschutz in Bonn und ist seit 1984 Professor für Wirtschaftsinformatik an der Technischen Universität Berlin. Seit 1995 ist Bernd Inhaber der Jean Monnet Professur der Europäischen Union für humanwissenschaftliche Fragen der europäischen Integration an der Technischen Universität Berlin.

Florian Marienfeld hat Technische Informatik an der TU Berlin studiert und arbeitet als wissenschaftlicher Mitarbeiter beim Fraunhofer FOKUS – Institut für offene Kommunikationssysteme. In der Arbeitsgruppe »Trust in networked environments« untersucht er Vertrauenswürdigkeit und Vertraulichkeit in Kommunikationsräumen.

Matthias Niebuhr ist Fachanwalt für IT-Recht. Er ist Leiter Recht der MyHammer Holding AG in Berlin und zudem betrieblicher Datenschutzbeauftragter mehrerer Gesellschaften. Zuvor beriet er als Rechtsanwalt in Hamburg Unternehmen zum Internet- und Medienrecht und war Senior Legal Counsel bei AOL Deutschland.

Prof. Dr. Frank Pallas ist Gastprofessor für Datenschutz und Informationsökonomik an der TU Berlin und forscht gleichzeitig am Karlsruher Institut für Technologie zu technisch-rechtlichen Fragen des Smart Grids und der Elektromobilität. Den Schwerpunkt seiner Tätigkeiten bilden die Integration von Informatik, Neuer Institutionenökonomik und Rechtswissenschaft sowie die sich hieraus ergebenden Implikationen für IT-bezogene Regulierung.

Martina Pickhardt studierte Wirtschaftsinformatik an der FH Flensburg und hat maßgeblich den Aufbau des eCommerce Bereiches bei Oracle Deutschland bestimmt. Heute ist Martina als selbstständige Beraterin in den Themen CRM, Targeting und Personalisierug tätig. Ihr Interessensschwerpunkt liegt dabei auf Transparenz und Selbstbestimmung durch den Endbenutzer.

Dr. Cornelius Puschmann ist Sprach- und Informationswissenschaftler an der Heinrich-Heine-Universität Düsseldorf und beschäftigt sich mit dem Verhältnis von Öffentlichkeit und Privatheit im Rahmen des entstehenden Social Semantic Webs. Außerdem untersucht Cornelius den Einfluss der Digitalisierung auf die Wissenschaft (Open Access).

Dr. Oliver Raabe ist Forschungsgruppenleiter für »Energieinformationsrecht und Neue Rechtsinformatik« am Institut für Informations- und Wirtschaftsrecht (IIWR) im Karlsruher Institut für Technologie (KIT). Seine Forschungsschwerpunkte liegen insbesondere in den datenschutzrechtlichen Herausforderungen des »Internet der Dienste« und des »Smart Grid«. Zudem befasst er sich mit regulierungstheoretischen Fragen von komplexen IKT-Infrastrukturen.

Jan Schallaböck ist Jurist und forscht als Mitarbeiter des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) zu Datenschutz- und Datenschutztechnologien. Sein Arbeitsgebiet ist insbesondere die internationale Standardisierung, insbesondere in der ISO, hin und wieder aber auch in der IETF, dem W3C und der ITU. Er war außerdem Koordinator des European Privacy Open Space und Initiator und Organisator der Konferenz »Federated Social Web Europe 2011«.

Der Kulturwissenschaftler **Michael Seemann** arbeitet zur Zeit an seiner Doktorarbeit über philosophische Theorien des Archivs. Er gründete twitkrit.de und die Twitterlesung, organisierte verschiedene Veranstaltungen und betreibt den Podcast wir.muessenreden.de. Vor einem Jahr begann er das Blog CTRL-Verlust und er schreibt unregelmäßig für verschiedene Medien wie RollingStone, ZEIT Online, c't und das DU Magazin.

Dr. Max Senges arbeitet in Googles Policy Team in Berlin als Bindeglied zum akademischen Bereich und der Zivilgesellschaft. Er ist vor allem verantwortlich für Kooperationen mit Akademikern, NGOs und Kollegen aus der Internet-Community. In den letzten 10 Jahren war er mit akademischen, staatlichen und privaten Organisationen in den Bereichen Wissensmanagement, e-Learning und Internet Governance tätig.

Sebastian Sooth arbeitet in verschiedenen netzpolitischen Arbeitsgruppen und ist Projektmanager bei Wikimedia Deutschland – Gesellschaft zur Förderung Freien Wissens. Im von ihm mitinitiierten Netzwerk atoms&bits beschäftigt Sebastian sich mit der Frage, wie wir die Möglichkeiten, die das Netz und die neue Version der Kultur des Selbermachens bieten, für freiere gemeinsame Arbeits- und Lebensmodelle nutzen können.

Martin Spindler studierte Politikwissenschaften in Heidelberg und lebt und arbeitet seit 2009 in Berlin. Er ist Marktanalyst bei Verivox GmbH und arbeitet mit Fokus auf Smart Metering und SmartGrid und das »Internet der Dinge«. Er ist Mitbegründer der Cognitive Cities Conference.

8 Über das Internet & Gesellschaft Co:*llaboratory*

Das Co:*llaboratory* ist eine offene Kollaborationsplattform (Community of Practice) und entwickelt sich laufend weiter. Es soll folglich in seiner Form, seinen Prozessen und seinen Ergebnissen für Einflüsse aus verschiedensten Richtungen offen sein. Das Co:*llaboratory* bringt Experten aus verschiedensten Bereichen zusammen, um die Veränderungen der digitalen Welt zu analysieren und zu erläutern, welche Nutzen wir für unsere Gesellschaft aus den Entwicklungen des Internets ziehen können.

Damit will das Co:*llaboratory* einen Beitrag zum gesellschaftlichen Diskurs in Deutschland leisten und dabei zu aktuellen Debatten beitragen, beispielsweise zu Verfassungsbeschwerden, Petitionen oder zur Arbeit der Enquête-Kommission »Internet & Digitale Gesellschaft« des Bundestages. Durch das Co:*llaboratory* können Expertenmeinungen aus dem Netz für eine breitere Öffentlichkeit übersetzt und der gesellschaftliche Pluralismus abgebildet werden. Fachbeiträge, Berichte und Empfehlungen münden dabei in Argumente und Positionen, die ein Motor für Diskussionen oder Aktionen sein können.

Das Co:*llaboratory* organisiert sich in mehrmonatigen Initiativen bestehend aus zivilgesellschaftlichen, akademischen und privatwirtschaftlichen Experten. Auf Fachveranstaltungen (Workshops, Barcamps, etc.) werden zusätzlich im offenen Austausch mit Politikern und Vertretern der Verwaltung die zuvor identifizierten Themen diskutiert und gegebenenfalls Handlungsoptionen erarbeitet. Langfristig angelegte Ohus (Arbeitsgruppen) zu verwandten Themen und eine Discussion Paper Series ergänzen die Formate, die das Co:*llaboratory* als Plattform bietet.

Prinzipien

- Das Co:*llaboratory* ist eine unabhängige und transparente Diskussions- und Kollaborationsplattform.

- Das Co:*llaboratory* ist dem öffentlichen Interesse verpflichtet. Folglich bringen sich die Experten freiwillig und unabhängig ein, um ausgewogene Positionen und Initiativen zu erarbeiten.

- Das Co:*llaboratory* dient der deutschen Internet-Community als Katalysator, Sprachrohr und Brücke für Politik und öffentliche Verwaltung.

- Das Co:*llaboratory* will technische, rechtliche und soziologische Veränderungen der digitalen Gesellschaft beobachten und Stakeholdern dieser Entwicklungen zuhören. Es kann die Veränderungen durchdenken, diskutieren und so zur Lösung offener Fragen beitragen.

- Das Co:*llaboratory* bündelt umfassendes Fachwissen, um die zukünftige, vom Internet mitgeprägte Entwicklung der Gesellschaft einschätzen zu können. Wichtige Themen sollen frühzeitig vom Co:*llaboratory* erkannt und in den öffentlichen Diskurs eingebracht werden.

- Das Co:*llaboratory* ist offen für Themenvorschläge von außen und platziert sich an Schlüsselstellen im Netz, um solche Vorschläge anzuregen.

- Das Co:*llaboratory* zielt darauf ab, die ganze Bandbreite der internetpolitischen Diskurse pragmatisch, informell und konstruktiv aufzuarbeiten und ggf. ausgewogene Handlungsoptionen vorzustellen.

Besuchen Sie das
Internet & Gesellschaft Co:llaboratory auf

www.collaboratory.de
www.youtube.com/Collaboratory

ISBN 978-3-9503139-3-2