DIVSI
Deutsches Institut
für Vertrauen und
Sicherheit im Internet

Max-Otto Baumann

Privatsphäre als neues digitales Menschenrecht?

Ethische Prinzipien und aktuelle Diskussionen

Diskussionsbeiträge

Deutsches Institut für Vertrauen und Sicherheit im Internet (Hrsg.)

Max-Otto Baumann

Privatsphäre als neues digitales Menschenrecht?

Ethische Prinzipien und aktuelle Diskussionen

DIVSI Diskussionsbeiträge 07

Herausgeber:
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Mittelweg 110 B, 20149 Hamburg

www.divsi.de

Redaktion:
Michael Schneider

Geleitwort

Privatsphäre ist ein Menschenrecht. Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte aus dem Jahre 1966, dem die meisten Staaten beigetreten sind, besagt, dass niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre oder seines Rufes ausgesetzt werden darf.

Menschenrechte sind unveräußerlich: Niemand darf darauf verzichten, auch nicht freiwillig, weil er sonst kein Mensch mehr sein könnte. Würde, Freiheit und Gleichheit sind ethische Prinzipien, die für alle Menschen gleichermaßen gelten.

Dennoch behaupten einige, im digitalen Zeitalter gäbe es keine Privatsphäre mehr. Das Zeitalter der Privatsphäre sei vorbei, sagt zum Beispiel Mark Zuckerberg. Das Berliner „Collaboratory Internet & Gesellschaft" behauptet, das Konzept der Privatsphäre sei wissenschaftlich überholt und technisch nicht mehr darstellbar. Eric Schmidt sagt voraus, immer mehr Menschen würden in Zukunft freiwillig auf ihre Privatsphäre verzichten. Tim Cook hingegen hat kürzlich erklärt, er fühle sich den Deutschen sehr nah, weil wir seine Ansichten zum Schutz der Privatsphäre teilen würden. „Wir lesen Ihre E-Mails nicht, wir lesen Ihre Textnachrichten nicht – und wir finden es inakzeptabel, wenn jemand das tut. Ich will auch nicht, dass jemand bei mir mitliest" (Interview mit „Bild am Sonntag" vom 1. März 2015, S. 15).

Andere sehen die Privatsphäre nicht nur durch kommerzielle Datensammler bedroht, sondern auch durch den Staat, durch die Geheimdienste. In vielen Ländern dieser Erde fordern Aktivisten gerade nicht die Aufgabe der Privatsphäre, wie das die „Post-Privacy-Spackeria" propagiert, sondern ein neues digitales Menschenrecht auf Privatsphäre, das das alte aktualisiert. Die einen setzen dabei auf eine Fortentwicklung des Völkerrechts, womöglich unter Moderation der Vereinten Nationen, die anderen eher darauf, „informationelle Selbstbestimmung" auch in einer Welt durchzusetzen, in der man praktisch nicht mehr leben kann, ohne Datenspuren zu hinterlassen. Während die einen den Nutzer ertüchtigen wollen, sich klug im Netz zu bewegen (Stichwort Medienkompetenz), glauben andere, dass das allein nicht genügt, sondern es für die Verarbeitung von Daten verbindliche Regeln geben muss, die alle einzuhalten haben.

Max-Otto Baumann, bis Anfang 2015 Mitarbeiter am John Stuart Mill Institut für Freiheitsforschung in Heidelberg, führt ein in diese Debatte um ein Menschenrecht auf Privatsphäre, das dem digitalen Zeitalter gerecht wird, und zeigt auf, wer sich an dieser Debatte beteiligt, die derzeit heftig tobt, und welche Argumente dabei vorgetragen werden. Er unterzieht diese Argumente einer kritischen Prüfung, inwieweit sie für eine ethische Begründung dieses „neuen" Menschenrechts taugen. Es handelt sich mithin nicht um eine juristische oder politische, sondern um eine philosophische Analyse.

Ein vergleichbarer Überblick über die aktuelle Diskussion über das neue, alte Menschenrecht der Privatsphäre ist mir nicht bekannt. Ihm sind viele Leserinnen und Leser zu wünschen, weil die Frage, wie wir Privatsphäre im digitalen Zeitalter definieren und durchsetzen wollen, eine Frage ist, die uns alle angeht. Bis Antworten auf diese Frage gefunden sind, dürfte noch eine Weile vergehen. Aber die Zeit drängt.

Göttrik Wewer
Hamburg, im Juni 2015

1. Privatsphäre im digitalen Zeitalter

Die digitale Revolution schreitet so rasant voran, dass unsere Sprache manchmal der Realität hinterherhinkt: So ergibt der Ausdruck „ins Internet gehen" heute kaum noch Sinn, denn das Internet ist zur Infrastruktur fast aller unserer alltäglichen Aktivitäten geworden: Kommunikation, Information, Einkauf, Unterhaltung, Kontoführung, politische Partizipation, Organisation, Jobsuche und vieles mehr finden heute in virtuellen Umgebungen statt, in denen wir mit unseren Profilen auch dann präsent bleiben, wenn wir gerade „offline" sind. Wer ein Smartphone mit sich führt, ist permanent „online".

Fast alle Wirkungen des Internets leiten sich daraus ab, dass es hilft, die Grenzen von Raum und Zeit zu überwinden. Schon in den 1950er-Jahren, als Telefon und Fernseher in die Haushalte kamen, konstatierte der Schriftsteller Max Frisch: „Wir sind Fernseher, Fernhörer, Fernwisser." Das gilt für die digitale Gesellschaft erst recht, vielleicht mit der Ergänzung, dass wir auch noch „Fernhandler" geworden sind. Dies bedeutet einerseits eine ungeheure Ausweitung unserer individuellen Autonomie, was sicherlich auch die Beliebtheit des Internets und seiner digitalen Applikationen erklärt. Auch die digitale Wirtschaft „brummt" und schafft Innovationen, Wachstum und Arbeitsplätze (vgl. Podesta 2014).

Aber wir sind auch verwundbar geworden. Unsere digitalen Existenzen weiten sich im virtuellen Raum ungeheuerlich aus, denn bei jeder digital mediatisierten Aktivität werden personenbezogene Daten gesammelt und gespeichert, oft in fremden Staaten. Es wird immer schwieriger, jene Informationen, die unsere Identität konstituieren, noch selbst kontrollieren zu können. Der vollständige Rückzug aus den digitalen Netzen ist keine Option mehr, man kann sich darin sprichwörtlich verfangen.

Vor allem kann man auf eine Art und Weise beobachtet und entblößt werden, wie das in vordigitaler Zeit undenkbar war, denn das „Fernwissen", und zunehmend auch das „Fernhandeln", findet auch in umgekehrter Richtung statt. Im Netz kursiert eine Karikatur, in der ein Nutzer auf den Bildschirm vor sich starrt, der die Linse eines riesigen Teleskops ist. Wer heute über eine Browser-Suche die weite Welt recherchiert, der muss damit rechnen, dass jemand anderes zeitgleich und gewissermaßen den Informationsfluss aufwärts tiefe Einblicke bis in unsere Psyche nimmt und aufgrund dieser Informationen entscheidet, welche Preise, Dienste oder Möglichkeiten wir bekommen oder eben nicht.

Die Digitalisierung hat noch lange kein Ende erreicht. Derzeit stehen wir an der Schwelle zum „Internet der Dinge", wodurch sich die Menge der freigesetzten personenbezogenen Informationen noch potenzieren wird. Die Folgen betreffen nicht nur unsere sozialen Beziehungen; hier kann am ehesten mit flexiblen Anpassungen an die neue Lebenswelt gerechnet werden. Weitaus problematischer ist, dass dem Internet dicht auf den Fersen in der Regel der Markt und der Staat folgen, also Gewinn- und Herrschaftsinteressen. Die Privatsphäre, bislang wesentliches Element einer gesellschaftlichen Machtbalance zwischen Individuen, Wirtschaft und Staat, ist dabei hinderlich, sie wird von Wirtschaft und Staat mehr oder weniger gezielt unterlaufen: „Collective investment in the capability to fuse data is many times greater than investment in technologies that will enhance privacy" (Podesta 2014: 54).

Diesem Ungleichgewicht kann eigentlich nur durch neue Regeln begegnet werden. Tatsächlich ist die digitale Revolution seit etwa einer halben Dekade, und besonders seit den Snowden-Enthüllungen im Jahr 2013, zu einem kontroversen politischen Thema geworden. Einerseits haben Staaten ihre digitalen Überwachungskapazitäten weiter ausgebaut, was insbesondere für die Länder des globalen Südens gilt. Gleichzeitig ist aber auch der Widerstand gewachsen. Der Europäische

Gerichtshof hat in seinem „Google-Urteil" das „Recht auf Vergessenwerden" geschaffen und auch die EU-Richtlinie zur Vorratsdatenspeicherung vorerst gestoppt. Die Generalversammlung der Vereinten Nationen (VN) hat eine Resolution zum Thema „Privacy In The Digital Age" verabschiedet. Das EU-Parlament hat seinen Entwurf für eine EU-Datenschutz-Grundverordnung beschlossen, während der EU-Ministerrat noch über einen eigenen Entwurf verhandelt.

Neu ist auch, dass Bürgerrechtsgruppen und Netzaktivisten sich 2014 erstmals oder mit neuer Energie für ein digitales Menschenrecht auf Privatsphäre ausgesprochen haben. Zwar reicht die wissenschaftliche Beschäftigung mit Privatsphäre sehr viel weiter zurück: Als Startschuss gilt die 1890 vorgetragene Forderung eines „Right To Be Let Alone" durch die beiden amerikanischen Juristen Samuel Warren und Louis Brandeis; die breite Öffentlichkeit wird seit der Ausbreitung der sozialen Medien (Facebook wurde 2004 eingeführt) durch einen teils recht alarmistischen Diskurs vor der digitalen „Zerstörung der Privatsphäre" gewarnt; wenig später kam die Sorge um die Bürgerrechte dazu. Vor diesem Hintergrund stellt die Forderung nach einem digitalen *Menschenrecht* auf Privatsphäre eine weitere Eskalationsstufe im Privatsphärendiskurs dar.

Der Ruf nach einem Menschenrecht ist eine moralische Forderung mit drei Ausrufezeichen. Er reflektiert das Gefühl, dass ein großes moralisches Übel zu weit um sich greift, gewissermaßen endemisch geworden ist. „Die Nadel des moralischen Kompasses unserer Zeit zittert", so Dave Eggers, der Autor des Bestsellers „The Circle"; „seit zehn Jahren sind wir in der Phase, in der sie sicheren Norden sucht." So mancher Kommentator artikuliert den Eindruck, dass der Mensch durch die Digitalisierung aus dem Mittelpunkt der Gesellschaft verdrängt wird. Die Forderung nach Menschenrechten ist die logische Antwort darauf: Menschenrechte schützen Individuen vor anderen Individuen und Institutionen, sie ermächtigen sie zu einem selbstbestimmten Leben (Mahoney 2008: 154). Ein digitales Menschenrecht auf Privatsphäre soll helfen, die gesellschaftliche Machtbalance im Lot zu halten, und ist insofern letztlich auch ein politisches Projekt, das gegen Widerstände durchgesetzt werden muss.

Vor diesem Hintergrund möchte die vorliegende Studie zwei Dinge leisten. Erstens soll die Forderung nach einem neuen digitalen Menschenrecht auf Privatsphäre zum Anlass genommen werden für eine ausführlichere Reflexion über die ethische Problematik der Privatsphäre im digitalen Kontext. Informationen bedeuten Einfluss, und so verschieben sich in der digitalen Revolution die Interessen der Akteure und die Art und Weise, wie man sich gegenseitig schadet und nützt. Die dabei auftretenden ethischen Konflikte bedürfen einer Erklärung, jedenfalls wenn man die normative Prämisse teilt, dass der Maßstab der Informationsgesellschaft letztlich im Wohl der Menschen liegt.

Für diesen Zweck wird die philosophische und informationsethische Literatur über die Privatsphäre aufgearbeitet, freilich unter dem Gesichtspunkt, das Feld der ethischen Probleme abzustecken, und weniger, den wissenschaftlichen Diskurs umfassend wiederzugeben. Es geht in diesem Kontext auch nicht darum, konkrete politische Handlungsempfehlungen zu generieren, etwa zu einer fairen Balance individueller und wirtschaftlicher Interessen.[1]

Zweitens sollen im empirischen Teil die im transnationalen Aktivistendiskurs vorgetragenen Forderungen nach einem neuen digitalen Menschenrecht auf Privatsphäre aufgegriffen, geordnet und zumindest in Ansätzen auch bewertet werden. Die Analyse konzentriert sich dabei auf etwa zehn kollektive und einzelne Aktivisten, was zwar eine kleine Zahl ist, aber genügt, um einen hinreichenden Überblick über den Diskurs und die darin artikulierten Positionen zu geben.

---

[1] Das Thema eines Menschenrechts legt uns auf eine Schutzperspektive in Bezug auf den Menschen fest – politische und wirtschaftliche Interessen sind aus diesem Blickwinkel notwendig sekundär. Wie viel Privatsphäre letztlich angemessen ist, d.h. wie stark dafür z.B. wirtschaftliche Interessen eingeschränkt werden dürfen, das ist eine Frage, die gesellschaftlich ausgehandelt werden muss.

Grundsätzlich lassen sich zwei Diskursfelder unterscheiden: In dem einen geht es unter Bezugnahme auf bereits existierendes Völkerrecht zum Schutz der Privatsphäre um die Kritik der staatlichen Massenüberwachung, wie sie durch Snowden bekannt wurde; im anderen sind, eher fern völkerrechtlicher Normen, die Wirtschaftsunternehmen das Ziel der Forderung nach einem neuen digitalen Menschenrecht. Die Berücksichtigung beider Felder scheint mir wichtig, weil erstens die Big-Data-Problematik in beiden Feldern ähnlich ist, weil zweitens die verschiedenen inhaltlichen Ansätze sich gegenseitig befruchten können und weil es drittens am Ende auch nur ein neues digitales Menschenrecht geben wird, jedenfalls sofern es überhaupt zu einer ‚Novellierung' des einschlägigen Völkerrechts kommt.

2. Die Ethik der Privatsphäre

2.1 Annäherung an einen schwierigen Begriff

Wenn die Deutschen sich über Verletzungen der Privatsphäre echauffieren, sollten sie besser noch einmal nachdenken, suggeriert der amerikanische Wissenschaftler James Whitman (2004): Denn was sei von solchen Empörungen zu halten, wenn es in dem Land keinen Anstoß errege, sich barbusig im Stadtpark zu sonnen? Schwer verständlich für einen US-Amerikaner. Auch würden die Deutschen das amerikanische Konzept der Privatsphäre nicht begreifen, das ein Bollwerk zum Schutz der individuellen Freiheit sei, vor allem in Gestalt der Unverletzlichkeit der Wohnung. Dass in den USA die sexuellen Verfehlungen von Politikern zum Skandal gemacht, dass Straftäter an den öffentlichen Pranger gestellt und die Überwachung der Telekommunikation toleriert würde, habe eigentlich wenig mit Privatsphäre zu tun, sondern sei Ausdruck einer funktionierenden demokratischen Öffentlichkeit.

Nicht nur im internationalen Vergleich, auch zwischen den Generationen liegen die Auffassungen über die Privatsphäre manchmal weit auseinander: Was für Jüngere oft selbstverständlich ist, z.B. das Teilen persönlicher Informationen in sozialen Online-Netzwerken, das Telefonieren in der Öffentlichkeit etc., erscheint älteren Semestern als sicherer Beleg eines Niedergangs der Privatsphäre.

Privatsphäre ist ein notorisch unscharfes Konzept (vgl. Solove 2002: 108 f.8). Trotzdem müssen wir den Versuch unternehmen, zu klären, was wir darunter verstehen. Dabei gibt die Frage, ob es so etwas wie ein digitales Menschenrecht auf Privatsphäre geben kann, bereits eine Richtung vor, in der wir suchen müssen: Erstens begründet ein Menschenrecht einen fundamentalen, universalen moralischen Anspruch; erforderlich ist also ein Privatsphärenkonzept, das an ein ebenso fundamentales menschliches Interesse ankoppelt und unabhängig von national-kulturellen Einfärbungen ist. Zweitens geht es hier um ein digitales Menschenrecht, weshalb das gesuchte Konzept sensibel sein sollte für Entwicklungen im Bereich von Big Data und Informationsgesellschaft.

Eine ausführliche Diskussion der umfangreichen Privatheitsliteratur kann hier nicht geleistet werden (vgl. für einen Überblick z.B. Westin 1970, Rössler 2001, Solove 2002). Ich verfahre unter Gesichtspunkten einer guten einführenden Orientierung lieber so, zunächst eine Abgrenzung gegenüber einem klassisch-alltäglichen Privatsphärenverständnis vorzunehmen und dann zwei wichtige, für unser Thema besonders relevante Konzepte vorzustellen. Sie sind wichtig, weil sich aus ihnen Aussagen ableiten lassen, (a) wodurch Privatsphäre verletzt wird, und (b) weshalb dies ein ethisches Problem ist (Gavison 1980: 423). Wie bei einer Zwiebel werden im Verlauf der Studie die sozial-kontingenten Aspekte der Privatsphäre Schicht für Schicht abgetragen, bis deren normativer Kern offenliegt.

In der Alltagssprache verstehen wir unter „Privatsphäre" einen Rückzugsraum gegenüber der Gesellschaft, der räumlich verstanden werden kann (Haus, Zimmer), aber auch informationell, insofern es Grenzen gibt, was andere Menschen legitimerweise über einen wissen dürfen; auch gewisse Entscheidungen sind Privatsache (vgl. Rössler 2001). Privatsphäre ist demnach durch Begriffe wie „Alleinsein", „Geheimnis", „Intimität" und „Selbstbestimmung" charakterisiert und grenzt sich von Öffentlichkeit als Sphäre verbindlicher Normen und gegenseitiger Sichtbarkeit ab. In einer solchen dichotomischen Konzeption von Privatsphäre und Öffentlichkeit kann noch gut zwischen „privaten" und „öffentlichen" Informationen unterschieden werden.

Schon recht früh, aber verstärkt mit dem Beginn der Informationsgesellschaft in den 1970er-Jahren wurden Privatsphärenkonzepte entworfen, die anders gestrickt sind und die sich nicht mehr bruchlos auf die Trennung von „privat" und „öffentlich" reduzieren lassen. Schon der Eintrag in einer Datenbank konstituiert ein rudimentäres Fremdbild der Person, das darüber entscheidet, wie andere (z.B. die Steuerbehörde) eine Person behandeln. Je mehr Aktivitäten des privaten Lebens in der

Quasi-Öffentlichkeit des Internets ausgeübt werden, desto weniger ist ein Rückzug in eine private Sphäre noch eine Option. Die „neuen" Privatsphärenkonzepte gründen daher auf dem Konzept der Information. Sie betrachten die Person als durch ihre Informationen konstituiert und sehen daher eine Verletzung der „informationellen Privatheit" auch als „eine Form der Aggression gegen die persönliche Identität" (Floridi 2005: 194).

Anders als im „right to be let alone" (Warren/Brandeis 1890), mit dem alles anfing, geht es bei der Privatsphäre heute also weniger um den Rückzug von der Gesellschaft als vielmehr um das selbstbestimmte Leben *innerhalb* der Gesellschaft, auch wenn dabei das „In-Ruhe-Lassen" noch eine wichtige Komponente ist. Im Paradigma der informationellen Privatheit gibt es nun zwei aufschlussreiche Ansätze, einen eher deskriptiven und einen normativen, die eine nähere Betrachtung verdienen.

Der deskriptive Ansatz ist mit dem Namen der amerikanischen Medienwissenschaftlerin Helen Nissenbaum (1998) verbunden. Er kann als Kritik des in den USA dominierenden Privatsphärenverständnisses gelesen werden, in dem zwar das Haus als sakrosankt gilt, aber die „Privatheit in der Öffentlichkeit", um die es Nissenbaum geht, keine Rolle spielt.[2] Folgendes Beispiel mag zeigen, um was es Nissenbaum geht: Man stelle sich vor, jemand würde in der Öffentlichkeit auf Schritt und Tritt begleitet und alle Aktivitäten würden peinlich genau protokolliert (was man einkauft, wohin man geht etc.). Allein aus diesen öffentlichen Daten ließen sich tiefe Einblicke in die Persönlichkeit gewinnen, die jede Vorstellung von Anonymität in der Öffentlichkeit zunichtemachen. Die Gefährdung der Privatsphäre liegt in dieser Perspektive überhaupt nicht darin, was Menschen selbst über sich preisgeben (das ist durch soziale Normen bestimmt, die sich womöglich gar nicht ändern), sondern sie liegt in der neuen Art der Beobachtung.

Diese Entblößung ist bei Nissenbaum indes nur die erste Stufe der Privatsphärenverletzung. Denn teilen wir nicht ständig Informationen mit mehr oder weniger fremden Personen der Öffentlichkeit (ein Begriff, den Nissenbaum sehr weit auslegt)? Der Arzt weiß in bestimmter Hinsicht über eine Person mehr als deren Ehepartner, der Lehrer mehr über einen Schüler als die Eltern etc. Nissenbaum betont daher, dass wir Informationen immer nur in bestimmten sozialen Kontexten teilen (Arztpraxis, Schule etc.). Privatheit liege daher in der „kontextuellen Integrität": Eine Verletzung der Privatsphäre liegt immer dann vor, oder besteht darin, dass Informationen aus einem sozialen Kontext in einen anderen gelangen, für den sie nicht bestimmt sind. Umfassende digitale Beobachtung, zentrale Speicherung und virtuelle Diffusion von Daten sind vor diesem Hintergrund ein großes Risiko für die Privatsphäre (dazu unten mehr).

Das andere, normative und praktisch sicherlich einflussreichere Konzept von Privatsphäre ist die „informationelle Selbstbestimmung". Wir sprechen von „normativ", denn es formuliert ein abstraktes Ideal, das dazu dient, den Wert der Autonomie zu schützen. Alan Westin, eine Koryphäe der Privatsphärenforschung (und ebenfalls ein US-Amerikaner), beschreibt in den 1960er-Jahren ein solches Konzept der informationellen Selbstbestimmung: „Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (zitiert aus Vitale 2014: 724). Das Recht auf Selbstbestimmung bedeutet nicht, dass ein Individuum volle Kontrolle über sein (digitales) Fremdbild hat; das würde mit der Freiheit anderer kollidieren, sich selbst ein Urteil bilden zu dürfen. Die Essenz der informationellen

[2] Im US-Privatsphärenrecht spielt die Doktrin der „reasonable expectaction of privacy" eine wichtige Rolle, die 1979 in dem Urteil „Smith v. Maryland" des Supreme Court geschaffen wurde. Danach sind Kommunikationsdaten (‚wer wen anruft') nicht geschützt, weil der Anrufer ja wisse, dass das Telefonunternehmen sie erfasst; es wird unterstellt, dass die Daten dann freiwillig geteilt würden (vgl. Podesta 2014: 32). Aus meiner Sicht ist das eine normativ sehr schwache Konzeption der Privatsphäre, die technologischen Entwicklungen widerstandslos nachgibt. Denn offensichtlich kann damit jede Privatsphärenverletzung durch die einfache Unterstellung legitimiert werden, dass der Nutzer ja mehr oder weniger Bescheid wisse.

Selbstbestimmung liegt vielmehr darin, selbst über die Preisgabe und die Verwendung personenbezogener Informationen entscheiden zu dürfen. Im Privatsphärenrecht der USA fand dieses Konzept zunächst keine Resonanz, wohingegen das deutsche Bundesverfassungsgericht in seinem Volkszählungsurteil 1983 ein „Recht auf informationelle Selbstbestimmung" geschaffen hat, das Grundrechtsrang hat. Praktisch erfüllt es sich im Wesentlichen in Einwilligungsregeln (z.B. durch Bestätigung der AGB).

Die beiden Privatsphärenkonzepte von „kontextueller Integrität" und „informationeller Selbstbestimmung" schließen sich nicht gegenseitig aus, sondern überlappen sich; das eine liefert eher eine Phänomenologie der Privatsphäre, das andere eine normative Orientierung. Mit Nissenbaum lässt sich verdeutlichen, welche Art von Daten unter die informationelle Selbstbestimmung fallen sollten.

Man unterscheidet zwischen Inhaltsdaten (Texte, Bilder) und Kommunikations-/Metadaten (Adressat einer Kommunikation, Aufenthaltsorte etc.); die einen werden bewusst geteilt, die anderen sind eher „digitales Abgas" (Podesta 2014: 2). Offenkundig fallen die in der „Öffentlichkeit" von digitalen Beobachtern aufgegriffenen Daten, die uns sehr weitgehend entblößen können, in die Kategorie der Metadaten. Der US-Fahdienstvermittler „Uber" konnte allein aus den Metadaten seiner Kunden, d.h. den Informationen über ihre Routen und Fahrzeiten, ableiten, welcher Kunde gerade sexuelle Affären habe (Frost 2015). Ein zeitgemäßes Privatsphärenkonzept darf deswegen nicht zwischen Inhalts- und Metadaten unterscheiden.

Mit dieser Einsicht können wir einen weiteren Pflock einschlagen zur Vermessung des Problemfelds Privatsphäre im digitalen Zeitalter. Es ist nämlich klar, dass diese Art der Privatsphärenverletzung auf dem Einsatz von Big-Data-Technologie beruht und daher fast ausschließlich von Wirtschaftsunternehmen und Staaten ausgehen kann. Weil Informationen unterschiedliche, teils subtile, teils handfeste Kontroll- und Steuerungsmöglichkeiten eröffnen, ändert sich im Zuge der digitalen Revolution die Stellung des Individuums gegenüber der Wirtschaft und dem Staat und damit das gesellschaftliche Machtgefüge insgesamt. Privatsphäre ist deswegen auch ein wichtiges Konzept des politischen Liberalismus, der Privatsphäre als ein für die individuelle Autonomie ganz zentrales Abwehrrecht gegenüber gesellschaftlichen und politischen Kräften sieht.

2.2 Normative Begründung des Rechts auf Privatsphäre

Allerorten lesen wir von einer akuten „Bedrohung" oder sogar „Zerstörung" der Privatsphäre im Zuge der digitalen Revolution, daher der dringende Appell, etwas zu ihrem Schutze zu tun. Allerdings bedeutet die Tatsache, dass etwas zerstört wird, nicht automatisch, dass es auch schutzwürdig ist. Im ständig ablaufenden gesellschaftlichen Wandel werden auch Dinge „zerstört", denen niemand nachtrauert, z.B. rigide Normen der Sexualität. Von einer ethisch bedenklichen Zerstörung der Privatsphäre kann nur gesprochen werden, wenn sich ihr Wert unabhängig von wandelnden gesellschaftlichen Praktiken begründen lässt. Dies ist umso wichtiger, als verschiedene Gesellschaften und Kulturen ganz unterschiedliche Privatsphärenverständnisse haben. Es bedarf also einer rationalen ethischen Klärung, was den Wert der Privatsphäre ausmacht.[3]

[3] Die Begründung von Menschenrechten ist ein schwieriges Feld: Eine glänzende, d.h. annähernd zwingende ethische Begründung läuft praktisch meist darauf hinaus, dass gerade nicht westliche Gesellschaften sich damit nicht identifizieren können. Alternativ können Menschenrechte als genuin politisches Projekt betrachtet werden, und um der praktischen Geltung willen kann auf eine theoretische Begründung verzichtet werden. Allerdings kann ohne ein ethisches Fundament ein solches Menschenrecht leicht durch andere Interessen gebeugt und verwässert werden. Das ist der tägliche Konflikt von VN-Menschenrechtsdiplomaten (Lohman 2010: 34; vgl. den Exkurs zum Universalitätsproblem unten).

Dies gilt insbesondere, wenn der Privatsphäre Menschenrechtsrang zugesprochen werden soll. Ein Recht qualifiziert sich als Menschenrecht, wenn es ein grundlegendes menschliches Interesse schützt. Menschenrechte kommen jedem Menschen qua seines Menschseins zu, und daher haben sie den Status eines moralischen Rechts: „Die Realität moralischer Rechte ist rein normativ und nicht institutionell – obwohl natürlich Institutionen geschaffen werden können, um sie zu schützen. Dass Menschen bestimmte Rechte haben, die respektiert werden sollten, ist eine moralische Forderung, die nur mit moralischen Argumenten abgestützt werden kann" (Nagel 2002: 33).

Welches „grundlegende menschliche Interesse" schützt die Privatsphäre? Die Fachliteratur hat bislang Privatsphäre nicht explizit im Kontext eines Menschenrechts behandelt, weshalb viele einschlägige Studien für den Zweck einer entsprechenden Begründung kaum weiterhelfen. Die wichtigsten, immer wieder anzutreffenden Argumente für Privatsphäre lauten: (a) sie ist eine grundlegende demokratische Norm; (b) sie schützt persönliche Beziehungen; (c) sie bietet emotionale Rückzugsräume und fördert mentale Gesundheit; (d) sie reduziert sozialen Konformitätsdruck; (e) sie bedeutet Freiheit und Autonomie („ein Mensch unter Beobachtung ist nicht frei"). Alle diese Argumente tragen substanziell zum Verständnis von Privatsphäre bei, aber nur das letzte ist m.E. hinreichend belastbar, um einen Menschenrechtsanspruch tragen zu können.

Man kann die ersten vier Argumente als funktionalistisch bezeichnen. Sie stützen jeweils ein anderes Interesse, das zwar intuitiv eingängig ist, aber begründungstheoretisch problematisch, weil das Recht auf Privatsphäre dann von diesem anderen Interesse abhängig wird. Zum Beispiel leuchtet die Verknüpfung von Privatsphäre und Demokratie unmittelbar ein, sie bedeutet aber, dass ein individuelles Recht (Privatsphäre) mit einem kollektiven Gut (Demokratie) begründet wird. Menschen in autokratischen Gesellschaften hätten dann kein Recht auf Privatsphäre, oder jedenfalls nur, insofern sie auch ein Recht auf Demokratie haben. In etablierten Demokratien ließe sich die Privatsphäre mit dem Argument einschränken, dass die Verteidigung der Demokratie eine Einschränkung der Privatsphäre erforderlich mache.

Die anderen Argumente sind eher deswegen problematisch, weil sie in keiner unmittelbaren Verbindung zu den Entwicklungen der digitalen Revolution stehen (vgl. Michelfelder 2014: 134). Die Überwachung durch die NSA gefährdet z.B. intime Beziehungen eher nicht, und dass die Menschen das Web 2.0, die Möglichkeiten des Self-Tracking und viele sonstigen Applikationen des Internets massenweise und mit sichtbarer Freude nutzen, spricht auch nicht dafür, dass emotionale Rückzugsräume wirklich gefährdet sind. Ein derartiger Begründungsversuch geriete also leicht in Widerspruch mit der subjektiven Realität ausgerechnet jener Menschen, deren Privatsphäre besonders gefährdet ist. Schließlich hilft es auch nicht, einfach mehrere Argumente zu bündeln.[4] Der begründungstheoretische Schuss mit der Schrotflinte ist schlechte Philosophie – Kritiker werden sich dann das schwächste Argument herausgreifen. (vgl. Michelfelder 2014: 133 f.).

Ideengeschichtlich wurzeln die Menschenrechte in der Naturrechtslehre, einer bis in die Antike zurückreichenden Denktradition, die sich mit dem Ideal der menschlichen Existenz beschäftigt. Zwar war auch die Naturrechtslehre immer ein Kind ihrer Zeit und dadurch nicht gegen unrühmliche Verfehlungen gefeit.[5] Dennoch haben wir aus dieser Tradition, aus ihrer Neuinterpretation durch die Aufklärung und durch die spätere, leidvolle Erfahrung der beiden Weltkriege eine moralische Konzeption

[4] Vgl. den Ansatz von Solove (2002), der sich auf Wittgensteins Konzept einer „Familienähnlichkeit" bezieht, um eine Reihe von Privatheitskonzepten zusammenzuführen.

[5] Noch bei Montesquieu ist das erste der Naturgesetze, wie die menschliche Vernunft sie diktiere, „jene Norm, die uns zum Schöpfer hinführt" (Montesquieu 1950: 81). Mit dem Bezug auf Gott wurden auch die Indianerkriege in Lateinamerika gerechtfertigt (Hinsch/Janssen 2006: 68).

der Person gewonnen, die heute ein hinreichend solides und universales Rechtfertigungsfundament für die Menschenrechte bietet.

Der Informationsethiker Rafael Capurro knüpft an die Tradition der Naturrechtslehre an, um den moralischen Wert der Privatsphäre offenzulegen. Dazu erinnert er an die seit der frühen Antike für die Philosophie ganz wichtige Unterscheidung vom Menschen als emotional-materiellem und als rationalem Wesen, aus der Immanuel Kant eine Begründung der Menschenwürde gewinnt: Der Mensch ist nicht allein kausal determiniert, sondern als vernunftbegabtes Wesen bewohnt er auch das „Reich der Zwecke" (Kant, zitiert aus Capurro 2005: 38). Damit ist gemeint, dass wir in einem metaphysischen Sinne frei sind, uns selbst Ziele und Prinzipien („Maximen") zu geben – wir sind also nicht von äußeren Zwängen bewegt, sondern auch von eigenen, inneren Gründen. Deswegen darf der Mensch nicht als Mittel, sondern muss als Zweck behandelt werden (vgl. Nida-Rümelin 2005: 154-159). Freiheit impliziert auch, dass wir Verantwortung für uns selbst und unsere Handlungen haben – eine Vorstellung, die sich tief in die kollektive Mentalität eingegraben hat. „This experience of human autonomy and universality, with all its ambiguities and limitations, is at the core, it seems to me, of what we mean when we say that we must protect privacy" (Capurro 2005: 40).

Der Wert der Privatsphäre wird mit diesem Ansatz auf den Wert von Freiheit oder, etwas praktischer gesprochen, Selbstbestimmung zurückgeführt. Der Schutz der Privatsphäre bedeutet den Schutz vor Zwängen, wie sie in jeder Gesellschaft, in der Wirtschaft und der Politik auftreten und die uns zu Mitteln für fremde Zwecke machen. Privatsphäre schafft einen Freiheitsraum, in dem wir von Gründen bewegt werden, es ist der Raum der menschlichen Selbstentfaltung (und weil sich Gründe nur im Austausch mit anderen bilden können, ist auch die freie Kommunikation ein wichtiger Aspekt der Privatsphäre).

Das ist alles sehr abstrakt. Jedoch sind in dieser auf Kant rekurrierenden moralischen Konzeption des Individuums drei konkretere moralische Ausgangspunkte zu erkennen, nämlich: Würde, Freiheit/Autonomie und moralische Gleichheit. Diese drei fundamentalen menschlichen Interessen bilden ein Rechtfertigungsfundament für jedes Menschenrecht, aber besonders auch für die Privatsphäre. Mit ihnen lässt sich begründen, warum Menschen unbedingt vor bestimmten Schäden zu schützen sind, welche eine Verletzung der Privatsphäre bedeutet (vgl. Mahoney 2008: 173).

WÜRDE

Vielleicht sollte der Spruch „Ein Mensch unter Beobachtung ist nicht frei" besser heißen „Ein Mensch unter Beobachtung hat keine Würde". Die Einschränkung der Freiheit hängt davon ab, ob der Betroffene sich subjektiv eingeschränkt fühlt (dazu unten mehr), aber Verletzungen der Würde tun dies nicht in derselben Weise. Jemand, der völlig exhibitionistisch lebt, erscheint uns würdelos, und jemandem, der sich einer Beobachtung nicht bewusst ist, weil er gewissermaßen durch die Blicke anderer „exhibitioniert" wird, dem würde man gerne eine Warnung zurufen. Aber nicht jede Beobachtung verletzt die Würde, ein Ehepartner darf zum Beispiel mehr sehen als ein Nachbar und der wiederum mehr als ein Geschäftspartner. Es kommt auf den Kontext an und darauf, wie eng sich der Beobachtete mit dem Beobachtenden identifiziert.

FREIHEIT/AUTONOMIE

Die absolute Freiheit ist bei Kant ein metaphysisches Konstrukt, aber in der Praxis steht der Autonomie (Selbstbestimmung) immer die Heteronomie (Fremdbestimmung) gegenüber. Freiheit ist also im praktischen Leben immer relativ. Sie hat wie ein Gletscher ein Nähr- und ein Zehrgebiet: Einerseits bedeutet Selbstbestimmung nicht nur, Ideen selbst zu fassen; es muss dies auch auf der Grundlage freien Denkens geschehen, weshalb jede Einschränkung der Kommunikation und jede Manipulation

von Denkwegen problematisch ist. Auf der anderen Seite ist Selbstbestimmung immer nur so viel wert, wie sie in praktisches Handeln umgesetzt werden kann.

GLEICHHEIT

Die moralische Gleichheit ist Ausgangspunkt jeder ethischen und politischen Theorie seit der Aufklärung. John Rawls' allgemeines Gerechtigkeitsprinzip lautet, dass Ungleichheiten nur erlaubt sind, wenn sie den Benachteiligten in der Gesellschaft dienen und vom Gemeinwohl her gerechtfertigt werden können (1975: 83). Privatsphäre schützt, insofern sie einen Schleier vor die gesellschaftlichen Ungleichheiten der Menschen zieht, vor vielfältiger Diskriminierung nach Maßstäben, die vielleicht nicht politisch legitimiert sind. Profilbildung dient umgekehrt genau dazu, diesen Schleier zu durchstoßen und Unterschiede zu erkennen, um ein Individuum dann auf dieser Grundlage zu behandeln.

Im alltäglichen Diskurs sprechen wir vom „Wert" der Privatsphäre, den es zu schützen gilt, aber wir wollen ja die Privatsphäre als Menschen*recht* begründen. Werte und Rechte sind, auch wenn sie eng miteinander verwoben sind, nicht dasselbe, und ein wenig Begriffsarbeit macht klar, was die „moralische Pointe" davon ist, von einem Recht zu sprechen (vgl. Hinsch/Janssen 2006: 73 f.): Werte stiften Sinn, sie können kollektiv geteilt, aber auch sehr individuell angenommen werden, woran man sieht, dass sie vor allem nach *innen* wirken. Rechte dagegen wirken nach *außen*: Ein Recht zu haben bedeutet, einen legitimen Anspruch gegenüber einem anderen zu haben. Dem eigenen Recht auf Privatsphäre korrespondiert also erstens die Pflicht des anderen, die eigene Privatsphäre zu respektieren. Zweitens ist damit auch das Recht auf eine bestimmte Organisation der Gesellschaft gegeben, welche sicherstellt, dass Pflichten nachgekommen wird. „Wenn wir von dem Recht einer Person sprechen, meinen wir damit, daß die Person von der Gesellschaft verlangen darf, im Besitz dieses Rechts [...] geschützt zu werden", so John Stuart Mill. Ein Recht kann, wie man mit einem kritischen Seitenblick auf das Konzept des „Selbstdatenschutzes" sagen kann, prinzipiell nicht den „eigenen Bemühungen überlassen" werden (Mill 1976: 93).

Findige Skeptiker eines Rechts auf Privatsphäre haben eingewandt, dass es eigentlich nichts schütze, was nicht bereits durch andere Freiheitsrechte geschützt werde (Persönlichkeitsrecht, Diskriminierungsverbot, Fairness-Gebot etc.). Wozu dann der Aufwand einer eigenen ethischen Begründung? Viele Privatsphärentheoretiker drehen das Argument allerdings herum und behaupten, dass Privatsphäre andere Rechte mit abstütze und teilweise sogar noch verstärke. So argumentiert Bruin (2010: 521-527), dass man nicht auf die moralische Verantwortung der anderen vertrauen könne, die eigenen Rechte zu respektieren. Das unbefugte Betreten eines Privathauses ist verboten, aber dennoch schließen wir ab, und das umso eher, je mehr Fremde an unserer Haustür des Weges kommen. In einer ähnlichen Spur behauptet auch Rössler, dass „die eigentliche Realisierung von Freiheit, nämlich autonome Lebensführung, nur möglich ist unter Bedingungen geschützter Privatheit" (Rössler 2001: 137-143). Von Foucault wissen wir, dass manchmal schon der „zwingende Blick" (Foucault 1976: 221) genügt, um Menschen ihre Freiheit zu rauben.

Es kann argumentiert werden, dass der Konnex von Privatsphäre und anderen Menschenrechten in der digitalen Gesellschaft besonders eng ist. Zum Beispiel ist es oft nicht möglich oder wäre mit unverhältnismäßigen Risiken verbunden, unter der Bedingung umfassender Online-Beobachtung bestimmte politisch brisante Informationen zu beziehen oder Meinungen zu äußern. Privatsphäre schützt also in digitalen Kontexten auch die Informations-, Meinungs-, und Versammlungsfreiheit, außerdem die Reisefreiheit (Sobel 2014). Der Politikwissenschaftler Henry Shue hat in den 1990er-Jahren das Konzept der „basic rigths" (1996: 19) geprägt, wonach einige Rechte grundlegender sind als andere.

Je mehr im Zuge der digitalen Revolution unser privates, soziales, wirtschaftliches und politisches Leben digital mediatisiert ist, desto größer sind auch die Angriffsflächen und desto eher erscheint die Privatsphäre als ein solches „Supergrundrecht", an dem eine Reihe anderer Rechte hängen.

Exkurs zur Universalität: Privatsphäre und nicht westliche Gesellschaften

Die auf Kants moralische Konzeption der Menschen zurückgehende Begründung der Menschenrechte beansprucht philosophische Universalität; Würde, Freiheit und Gleichheit sind so grundlegend, dass sie jedem Menschen zustehen. Sie konstituieren die menschliche Existenz. Gleichwohl bleibt dies eine theoretische Begründung, die wie die gesamte Tradition der Menschenrechte eng mit der westlich-abendländischen Kultur verknüpft ist. Nicht westliche Gesellschaften haben wegen eigener, teils ebenfalls jahrtausendealter philosophischer und gesellschaftlicher Traditionen deswegen häufig Vorbehalte. Daher stellt sich leicht die bei Max Frisch geschilderte missliche Situation ein, dass „jedesmal, wenn einer von uns beiden messerscharf denkt, überzeugt es den andern keineswegs" (in: Stiller 1965: 36).

Gerade in Bezug auf die Privatheit sind die kulturellen Unterschiede ausgeprägt. In den kollektivistisch geprägten asiatischen Moralvorstellungen kommt dem Individuum kein besonderer Wert zu: „[I]n Japan, it makes no sense to protect something that has only a negative value. On the contrary, as we see there, this something called ‚self' should be denied, not protected" (Capurro 2005: 42[6]). Ähnliches gilt für andere Kulturen der Welt, die nicht auf dem Wert des Individualismus gründen, sondern tendenziell dem sozialen Kollektiv Vorrang einräumen.

Vor diesem Hintergrund ist die oben bereits angedeutete Option relevant, dass Menschenrechte statt von den Werten her, die spaltend wirken, auch im Hinblick auf politische Ziele begründet werden können (vgl. Mahoney 2008: 158). Eine Mittelposition zwischen „frivolem Relativismus" und „moralischem Imperialismus" (Ernst/Sellmaier 2010: 11) nehmen Diskurstheoretiker wie Jürgen Habermas und Vertragstheoretiker wie John Rawls ein, die auf einen moralischen Konsens vernunftbegabter Menschen setzen.

In diesem Sinne können einige Gründe angeführt werden, weshalb Menschen jeder Kultur von einem Recht auf Privatsphäre profitieren: Erstens reguliert ein digitales Menschenrecht auf Privatsphäre nicht primär die sozialen, sondern die wirtschaftlichen und politischen Beziehungen eines Individuums. Zweitens wirkt Profilbildung im wirtschaftlichen Kontext individualisierend, was in kollektivistischen Gesellschaften problematisch ist. Drittens schützt Privatsphäre nicht nur Individuen, sondern auch Gruppen – man denke daran, wie z.B. in China unter Mao Familien zerstört wurden, weil Kinder zu Spitzeln des Staates wurden; in Palästina späht die israelische Besatzung die Intimsphäre der Palästinenser aus, um sie erpressbar zu machen. Das deutet auf einen vierten Faktor hin, nämlich dass Privatsphäre in kollektivistischen Gesellschaften helfen kann, das Gesicht zu wahren (vgl. Kitiyadisai 2005).

Praktisch bedeutet dies: Es wird gelingen müssen, eine nüchterne gemeinsame ▶

[6] Vgl. die Sonderausgabe des Journals „Ethics and Information Technology" (7/2005) zum Thema Privatsphäre in Asien.

▶ Sprache über das „zivilisatorische Minimum“ zu finden (Ernst/Sellmaier 2010: 8). Einen Anfang könnte man in der gemeinsamen Zurückweisung staatlicher Überwachung suchen – niemand möchte von fremden Staaten ausgespäht werden. Dass hierbei Mobilisierungspotenzial besteht, zeigt die gelungene Verabschiedung einer Resolution der VN-Generalversammlung, die zahlenmäßig von nicht westlichen Staaten dominiert wird, im Jahr 2014.; so lassen sich selbst Autokratien zumindest für ein öffentliches Bekenntnis zum Recht auf Privatsphäre bewegen.

2.3 Bedrohungen des Rechts auf Privatsphäre

Sind die Bedrohungen der Privatheit nicht selbstevident angesichts der ubiquitären Überwachung im digitalen Zeitalter? Die Auseinandersetzung mit den Bedrohungen der Privatheit bedeutet keine Abschweifung vom Thema. Vielmehr ist ein Verständnis jener Mechanismen, welche die Privatsphäre und die von ihr geschützten menschlichen Interessen verletzen, ein weiterer und wichtiger Baustein in der Begründung eines digitalen Menschenrechts auf Privatsphäre. Wir können die Privatsphäre nur dann effektiv schützen, wenn wir einen Begriff von ihren digitalen Bedrohungen haben.

Wie oben bemerkt, zählen unter dem Aspekt eines digitalen Menschenrechts wieder nur solche Bedrohungen, die grundlegende menschliche Interessen betreffen, weshalb bestimmte Praktiken, auch wenn sie im öffentlichen Diskurs als korrosiv für die Privatsphäre wahrgenommen werden, hier nicht relevant sind. Dazu zählen z.B. das Telefonieren im Zug und der Exhibitionismus in TV-Shows wie „Big Brother“ oder in sozialen Online-Netzwerken. Es handelt sich bei diesen Beispielen auch eher um eine freiwillige Preisgabe von Privatsphäre, d.h., es werden keine Privatsphären*rechte* verletzt, allenfalls bestimmte Normen der Öffentlichkeit (vgl. Rössler 2001: 141). Der Wandel mag als schmerzlich empfunden werden, aber was heute als empörende Verletzung sozialer Konventionen gilt, ist morgen vielleicht die neue Realität, während das Maß an individueller Freiheit gleich geblieben ist.

Die eigentliche Bedrohung der Privatheit spielt sich, folgen wir dem Konzept von Nissenbaum, weniger auf der Ebene dessen ab, was Individuen selbst tun, sondern was sich bei den technologischen und ökonomischen Entwicklungen tut. Die Beobachtung ändert sich, wird immer umfassender und leistungsstärker und kann Individuen heute auch in Zusammenhängen entblößen, wo die Privatsphäre bislang kaum zur Disposition stand. „Profiling“ bedeutet, dass personenbezogene Daten erhoben, aus ganz unterschiedlichen Quellen zusammengeführt und mit anderen Datenbeständen verglichen werden. Durch diese Art der Datenanalyse vollzieht sich ein qualitativer Sprung in der Beobachtung: „while isolated bits of information [...] are not especially revealing, assemblages are capable of exposing people quite profoundly“ (Nissenbaum 1998: 589).

Das war schon Ende der 1990er-Jahre richtig, als es die interaktiven sozialen Medien als Hauptdatenquelle noch gar nicht gab. Heute übersteigt die Menge der Daten *über* ein Individuum (Metadaten) bei weitem die Menge der Daten *von* einem Individuum (Inhaltsdaten) (Podesta 2014: 54). Immer billigere und leistungsfähigere Big-Data-Technologie kann immer größere Mengen von immer kleineren Datenfragmenten (Small Data) zusammenführen und daraus neuen Wert generieren, wobei

sich dieser Wert eben in der Eindringtiefe in die Privatsphäre bemisst.[7] Allein aus den Likes von Facebook-Nutzern kann mit hoher Treffsicherheit auf „sexuelle Orientierung, Alter, Geschlecht, ethnische Herkunft, religiöse und politische Orientierung, Intelligenz" geschlossen werden (Morgenroth 2014: 191). Es können auch Einblicke in das Gefühlsleben genommen werden, in Echtzeit.

Kritiker sehen darin eine „moralisch empörende" (Nussbaum 1998: 589) Verletzung der Privatsphäre. Allerdings könnte der notorische Skeptiker oder ein Anhänger der Post-Privacy-Bewegung (vgl. Heller 2011) einwenden, dass die Beobachtung *an sich* noch niemanden in seiner Freiheit einschränke, und daher auch nicht in seiner Würde. Ob man sich entblößt fühlt oder nicht, ist offenkundig wieder eine subjektive Sache.

Um das Schadenspotenzial von Privatsphärenverletzungen objektiver bestimmen zu können, hat der niederländische Philosoph Boudewijn de Bruin (2010) ein interessantes analytisches Konzept vorgeschlagen, welches Privatsphäre eng mit Freiheit verknüpft. Dazu löst er sich von der Perspektive der Entblößung des Individuums und richtet das analytische Augenmerk auf die Interaktion des Individuums mit anderen, von denen Freiheitseinschränkungen ausgehen können. Freiheit ist laut de Bruin dann eingeschränkt, wenn man etwas tun möchte, aber daran von jemandem gehindert wird (2010: 511). Der Zusammenhang von Privatsphäre und Freiheit hat laut de Bruin nun drei Stufen: (1.) die Enthüllung der Informationen über eine Person A gegenüber einem Akteur B; (2.) ein Einstellungswandel („belief change") bei B; (3.) eine Aktion, oder eine Disposition zur Aktion, von B gegenüber A, die ohne den Einstellungswandel nicht stattgefunden hätte.

Ein Beispiel könnte so aussehen: (1.) Der Staat erfährt durch Online-Überwachung, dass ein Individuum sich für Salafismus interessiert; (2.) der Staat glaubt in der Folge, dass von diesem Individuum ein Risiko für die öffentliche Sicherheit ausgeht; (3.) das Individuum kommt auf die No-Fly-Liste. Die Freiheit des Individuums wird dadurch verringert, denn es kann keine Flugreise mehr unternehmen. Nun könnte es freilich sein, dass das Individuum im Augenblick gar keinen Plan hat, eine Flugreise anzutreten, oder dass der Staat das Individuum vorerst doch nicht auf die No-Fly-Liste gesetzt hat. Trotzdem werde seine Freiheit eingeschränkt, sagt de Bruin, denn es genüge, wenn der Staat eine „Disposition" zur Handlung gegenüber dem Individuum habe, welche das Individuum in Rechnung zu stellen hat (2010: 514). Nach genau diesem Muster werde die Freiheit in totalitären Staaten eingeschränkt: Wer es nicht darauf ankommen lässt, kann auch im totalitären Staat unbehelligt leben, aber wir würden deswegen nicht sagen, dass eine solche Person frei ist. Der Versuch, von der Freiheit Gebrauch zu machen, würde einen mit hoher Wahrscheinlichkeit in Konflikt mit dem Staat bringen.

Zwei Dinge erscheinen an diesem Konzept wichtig: Erstens liegt das Problem einer Privatsphärenverletzung hier nicht im subjektiven Gefühl des Beobachtetwerdens *(jetzt)*, sondern darin, wie andere sich *(in Zukunft)* zu einem verhalten (ebd.: 517). Zweitens wird allein schon die Verletzung der Privatsphäre als ein Eingriff in die Freiheit des Individuums gewertet, auch ohne dass es zu einem objektiv nachweisbaren Schaden kommt.

Dieses Modell ist noch recht allgemein. Es erklärt auch viele niederschwellige Freiheitseinschränkungen, die in Gesellschaft immer vorkommen und im Rahmen einer fairen Balance von Freiheitsrechten auch legitim sind. Allerdings ergeben sich durch Big Data einige spezifische, ethisch problematische Freiheitseinschränkungen. Dies kann man sich auf allen drei Stufen von de Bruins Modell plausibel machen kann:

---

[7] Eine immer wieder interessante Quelle für die unternehmerische Perspektive auf Big Data sind Vorträge auf wirtschaftlich ausgerichteten Workshops, in denen das Potenzial von Big Data ganz ungebremst von normativen Sorgen angepriesen wird. Vgl. etwa http://de.scribd.com/doc/214813740/What-Big-Data-Means-for-PR-and-Why-It-Matters-to-Us (23.1.2015).

STUFE 1

Neu ist im Zeitalter der digitalen Revolution erstens, dass Informationen viel leichter in andere Kontexte übertragen werden können (vgl. Nissenbaum 1998), was auch bedeutet, dass sie an eine größere Zahl oft unbekannter anderer Akteure gelangen; Konsumdaten gelangen an Kreditauskunfteien, die Reiseroute an die Sicherheitsdienste etc. Entsprechend verändert sich die „gewusste Freiheit" (de Bruin 2010: 528) des Individuums, es wird immer unsicherer über seine Handlungsfolgen. Der zweite neue Aspekt hat mit dem Qualitätssprung der Datenverarbeitung zu tun. Die epistemologische Kraft der Profilbildung ermöglicht es, Dinge über ein Individuum zu wissen, welche die meisten Individuen freiwillig nicht von sich preisgeben würden und die sie manchmal auch gar nicht über sich selbst wissen. Big-Data-Unternehmen brüsten sich damit, Entscheidungen vorhersagen zu können, die das Individuum noch gar nicht getroffen hat. Dies eröffnet Möglichkeiten der Manipulation.

STUFE 2

Hier ist zunächst zu konzedieren, dass ein Einstellungswandel auch auf eine Freiheits*erweiterung* hinauslaufen kann, z.B. wenn durch Offenlegung gesunder Finanzen ein Kredit gewährt wird, den man sonst nicht bekommen hätte (de Bruin 2010: 515). Doch die im Kontext von Big Data vorgenommenen Einstellungswandel sind häufig anderer Natur, insofern sie im Hinblick auf bestimmte Zwecke des Datenverarbeiters vorgenommen werden. Niemand bekommt personalisierte Werbung, weil jemand bei der Erreichung von eigenen Zwecken helfen möchte, sondern weil dies den Zwecken des Unternehmens dient (Nissenbaum 1998: 590). Im Einzelfall mag dies in Ordnung sein, aber wenn eine Vielzahl gesellschaftlicher Interaktionen auf diese Weise rationalisiert wird, zehrt dies an den moralischen Ressourcen der Gesellschaft (z. B. indem Normen der Reziprozität, Solidarität und des Respekt durch strategisches Kalkül ersetzt werden).

Man spricht in diesem Zusammenhang auch vom „verschwindenden Anderen" (Lyon 2001: 179): Einerseits sinkt mit zunehmender Effizienz von Big-Data-Technologie, die etwa einem Polizisten sagt, wer verdächtig sein könnte, die Möglichkeit, sich in Betroffene hineinzuversetzen; andererseits ist es für diese schwieriger, Rechte gegenüber einem anderen geltend zu machen, wenn der nur tut, was das System ihm sagt. Ein einschlägiges ethisches Problem sind falsche Daten zu einer Person, von denen das Individuum vielleicht gar nicht weiß oder, falls doch, die es nicht oder nur sehr aufwendig korrigieren kann.

STUFE 3

Einmischung kann in verschiedenen Formen auftreten, z.B. ganz subtil im „Nährgebiet" der Autonomie, wenn infolge einer Echtzeit-Profilbildung Gefühle erfasst und manipuliert werden – „the kind of interference that many would identify as being the most morally disagreeable of privacy invasions" (Mitchfelder 2001: 135) – oder sehr manifest im Zehrgebiet der Autonomie, z.B. wenn über den Zugang zu Dienstleistungen, Gütern und Möglichkeiten entschieden wird. Dies schränkt *möglicherweise* die Freiheit ein (im Einzelfall kann sie auch erweitert werden), ganz *sicher* aber den Grundwert der moralischen Gleichheit. Denn Profilbildung hat etwas inhärent Diskriminierendes: Sie ermöglicht ja gerade eine individuelle Behandlung. Bürgerrechtsaktivisten befürchten, dass sich im Internet neue Formen des „Redlining" herausbilden (Podesta 2014: 46), dass also bestimmte Gegenden oder gesellschaftliche Gruppen schlechter behandelt werden. Dadurch können Prinzipien der bürgerlichen Gleichheit unterlaufen werden, für deren Verletzung es im vordigitalen Zeitalter noch keine Grundlage gab.

2.4 Ethische Konzepte zum Schutz der Privatsphäre

Nachdem Begründungen und Bedrohungen der Privatsphäre skizziert wurden, stellt sich die Frage, wie ein (Menschen-)Recht auf Privatsphäre im Kontext von Big Data konzipiert werden kann. Die im politischen Diskurs immer wieder ins Spiel gebrachten Konzepte von „Selbstdatenschutz" und technischen Lösungen scheiden hier aus, weil sie außerhalb der Rechtsperspektive liegen. Innerhalb eines rechtebasierten Ansatzes lassen sich grob zwei Paradigmen unterscheiden: Das eine setzt auf maximale individuelle Kontrolle über die eigenen Daten und wird in Bezug auf die Wirtschaft diskutiert; das andere nimmt die Datenverarbeiter in die Pflicht und kommt primär gegenüber Staaten zur Anwendung.

Das Paradigma der individuellen Kontrolle

Das Paradigma der Kontrolle (im Deutschen „informationelle Selbstbestimmung") beruht auf der Idee, dass die autonome Einwilligung der Nutzer die beste Legitimation für eine Datenerfassung und -auswertung darstellt, welche zwar die Privatsphäre verletzen mag, nicht aber das *Recht* auf Privatsphäre. Ein Recht auf ein bestimmtes Gut und der individuelle Umgang damit sind zwei unabhängige Dinge, z.B. darf man seine eigene Sicherheit riskieren, was jedoch keinesfalls bedeutet, dass man damit sein Recht auf körperliche Unversehrtheit verwirken würde. Die Einwilligung des Datensubjekts schützt die Privatsphäre, weil sie ein moralisch transformativer Akt ist (vgl. Schermer et al. 2014: 172): Das gewaltsame Betreten eines fremden Hauses wäre eine Verletzung des Rechts auf Privatsphäre der Bewohner, aber wenn ein Fremder *eingeladen* wird, das Haus zu betreten, konstituiert dieselbe Handlung keine Verletzung des Rechts auf Privatsphäre.

Das praktische Pendant zur „Einladung" besteht im Wesentlichen in der Bestätigung von AGB, wodurch die Zustimmung zur Datenerfassung und -verarbeitung erteilt wird. Sowohl das amerikanische als auch das europäische Datenschutzrecht gründen auf dem Prinzip der Einwilligung (engl. „consent").

Allerdings gäbe es nicht den ganzen Diskurs um ein neues digitales Menschenrecht, wenn nicht mit der Einwilligung einige grundsätzlichere ethische Probleme überhaupt erst anfangen würden. Unter welchen Bedingungen kann die Einwilligung als autonomer Akt gewertet werden? Was wäre, wenn der eingeladene Gast Freunde mitbringt, sich schlecht benimmt, zu lange bleibt? Offenkundig bedarf das Konzept der Selbstbestimmung weiterer Kriterien, damit es seine moralische Wirkung tut. Schermer et al. nennen vier Kriterien (2014: 172 ff.):

- **INFORMATION:** Nur wenn das Datensubjekt angemessen informiert ist über die Verwertung seiner Daten, über bestimmte Risiken sowie die Gegenleistung, kann von einem fairen Tausch gesprochen werden.
- **ZWANGLOSIGKEIT:** Eine erzwungene Einwilligung ist per definitionem keine autonome Entscheidung und legitimiert daher nichts.
- **ABSICHT:** Die Einwilligung darf nicht unterstellt werden, nur weil sie in einem bestimmten Kontext üblich ist, es muss vielmehr eine bewusste Einwilligung sein.
- **SPEZIFIZITÄT:** Je unklarer es ist, worauf sich die Einwilligung konkret bezieht, desto schwächer ist ihre legitimatorische Wirkung.

Diese vier Kriterien begründen komplementäre Pflichten an die Datenverarbeiter, die in der Bereitstellung von Einwilligungsoptionen, der Transparenz im Sinne adäquater Information und der Vertragstreue liegen. Allerdings bestehen Zweifel, ob das Modell der Kontrolle noch praxistauglich ist. Infrage steht weniger, ob die Unternehmen ihren Pflichten nachkommen (dieses Problem könnte

durch verbesserte Rechtsdurchsetzung gelöst werden), sondern ob die Datensubjekte in der Lage sind, ihre Rechte in einer bedeutungsvollen Art und Weise auszuüben (dieses Problem kann nicht durch Compliance-Druck gelöst werden).

Umfragen belegen immer wieder, dass AGB nicht gelesen werden, dass also Einwilligung uninformiert geschieht. Die Menschen wissen auch nur selten, wer welche Daten über sie hat (vgl. Podesta 2014: 51). Damit ist die Prämisse der Einwilligung, nämlich die bewusst-autonome Entscheidung, verletzt. Zwar könnte man dies der Unfähigkeit oder Faulheit der Nutzer selbst anlasten. Massenhaftes Versagen deutet jedoch auf eine Überforderung hin, und dann verschiebt sich die Verantwortung. Wenn sich etwa im Straßenverkehr die schweren Autounfälle an einer bestimmten Kurve signifikant häufen, dann geht die moralische Verantwortung dafür von den einzelnen Fahrern auf die Straßenbehörde über; der Fahrer wird vom „moralischen Subjekt", das handelt und haftet, zum „moralischen Objekt", das geschützt werden muss.

An dieser Stelle lohnt sich ein Blick auf die Strukturen der digitalen Ökonomie. So ist generell fraglich, ob angesichts der technischen und ökonomischen Komplexität der Datenerfassung und -auswertung einerseits die Unternehmen ihrer Informationspflicht überhaupt noch nachkommen können und ob andererseits, wenn dies der Fall wäre, die Nutzer noch eine Chance hätten, diese Informationen zu verarbeiten. Alle AGB zu lesen, würde durchschnittlich 244 Stunden im Jahr dauern (Schermer et al. 2014: 177). Dabei sind Schwierigkeiten im Verständnis des juristischen Jargons nicht berücksichtigt.[8] Legitimationsprobleme ergeben sich ferner beim Kritierium der Spezifizität. Ein für den US-Präsidenten angefertiger Bericht über Big Data resümiert: „As a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data."[9] Wenn die Innovation von Big Data gerade in der Zusammenziehung von Daten aus verschiedenen Quellen liegt und wenn die immer elaborierteren Algorithmen Betriebsgeheimnis sind, dann wird eine individuelle und bewusste Zustimmung dazu praktisch unmöglich.

Dennoch sprengen diese Probleme das Paradigma der Selbstbestimmung nicht zwangsläufig, sie belasten es nur bis an die Schmerzgrenze. Tatsächlich gesprengt wird die Selbstbestimmung hingegen dann, wenn die Manipulation von Entscheidungen der Zweck der Datenverarbeitung ist. Es heißt häufig: „Der Nutzer zahlt mit seiner Privatsphäre." Oft geht es aber gar nicht um einen Tausch, sondern die Profilbildung wird *gegen* den Kunden verwendet; der Interaktionstyp ist dann eher der einer Täuschung. Wer etwa einen Apple-Laptop für Online-Bestellungen nutzt, bekommt unter Umständen Preise, die bis zu 50 % höher als normal ausfallen, weil die Verwendung von Apple auf einen gewissen Wohlstand schließen lässt. Denkbar ist auch, dass Preise entsprechend dem aktuellen emotionalen Befinden angesetzt werden. Der ausgespähte Nutzer zahlt also zwei Mal, mit seiner Privatsphäre *und* mit seinem Geldbeutel. Solche Praktiken der Profilbildung sind inkompatibel mit dem Prinzip der Nutzerselbstbestimmung, denn Einwilligung würde hier Selbstschädigung bedeuten.

Es gibt noch einen zweiten Einwand von derselben Klasse: Autonome Entscheidungen implizieren Wahlmöglichkeiten, aber diese können durch die autonomen Entscheidungen anderer Akteure reduziert werden. So ist der Fall denkbar, dass all jene, die positive Diskriminierung erwarten können (z.B. die Gesunden im Fall einer Versicherung), sich mit der Preisgabe ihrer Privatsphäre einen Vorteil erkaufen, was dann aber die kleinere Gruppe derjenigen unter Druck setzt, die aus guten Gründen ihre Privatsphäre nicht preisgegeben haben. Für sie ist dann das Kriterium der Zwanglosigkeit verletzt. Ihnen droht negative Preisdiskriminierung, ob sie einwilligen (und ein problematisches Verhalten

[8] Die Autoren fürchten daher den paradoxen Effekt, dass eine Verschärfung der Informationspflichten, wie sie in der neuen EU-Datenschutz-Grundverordnung vorgesehen ist, das Datenschutzniveau senken könnte.

[9] White House, Report to the President: Big Data and Privacy: A Technological Perspective, 2014, www.whitehouse.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy (22.1.2015).

sichtbar wird) oder nicht (und dieses unterstellt wird). Das Recht auf informationelle Selbstbestimmung versagt hier im Schutz der Privatsphäre, weil die Privatsphäre auch ein kollektives Gut sein könnte (vgl. Regan 1995): Entweder alle haben sie, oder niemand hat sie.

Das Paradigma der verantwortlichen Datenverarbeitung

Der andere Ansatz basiert dagegen auf dem verantwortlichen Umgang mit Daten: „Focusing on responsible use [...] holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection" (Podesta 2014: 56). Die Metapher hier wäre nicht der Gast im Haus, sondern die Leihgabe: Wer ein Ding leiht, der übernimmt auch die Verantwortung dafür, d.h., er haftet für eventuelle Schäden. Die Metapher hinkt zwar, insofern Daten nicht nur geliehen werden, sondern daraus neue Datenprodukte entstehen, aber auch in diesen liegt noch immer ein Stück der Identität des Datensubjekts, das deswegen auch verletzt werden kann durch die Datenverarbeitung.

Es gibt einen Bereich außerhalb der Datenschutzgesetze, in dem dieser Ansatz schon länger gebräuchlich ist, nämlich die staatliche Überwachung von Bürgern. Eine Legitimation der Privatsphärenverletzung durch individuelle Zustimmung scheidet hier logischerweise aus (der potenzielle Terrorist kann nicht gefragt werden), weswegen die Rechtfertigung der Privatsphärenverletzung über allgemeine Prinzipien erfolgen muss.

Um eine solche Kompensation von direkter Einwilligung in den Blick zu bekommen, bietet sich ein Rekurs auf die ethische Theorie des „Gerechten Krieges" an[10], deren Kriterien im Völkerrechts- und Aktivistendiskurs sehr präsent sind (dazu unten mehr). Die Ethik des „Gerechten Krieges" besagt nicht, dass es einen gerechten Krieg gibt (bzw. die gerechte Verletzung der Privatsphäre); eine Verletzung der Rechte einzelner, unschuldiger Menschen ist immer ungerecht. Dieses moralische Dilemma, d.h. der Konflikt von grundlegenden Rechten, ist der Ausgangspunkt der Ethik des „Gerechten Krieges". Sie bietet eine Reihe von sehr restriktiven Kriterien, anhand derer abgewogen werden kann, wann die Verletzung eines individuellen Rechts gerade noch zu rechtfertigen ist (oder bereits nicht mehr).

Diese Kriterien sind: Gerechter Grund, Notwendigkeit, Proportionalität, Erfolgsaussicht und legitime Autorität (teilweise werden noch weitere Kriterien angeführt, die in unserem Kontext aber nicht relevant sind). Wir werden sie unten ausführlicher diskutieren, für den Augenblick interessiert uns ihr moralischer Status. Sie sind nichts anderes als Forderungen der praktischen Rationalität, die jedem vernunftbegabten Menschen einleuchten sollten. So ist es z.B. unmittelbar einsichtig, dass ein Menschenrecht nur im Namen eines gerechten Grundes eingeschränkt werden darf, und ebenso, dass der Schaden einer Rechtsverletzung nicht größer als der Nutzen sein darf.

Allerdings ist diese Art der kasuistischen Ethik nicht gegen Kritik gefeit. Niemand Geringeres als Immanuel Kant hat die Lehre des „Gerechten Krieges" verspottet, weil sie nie eine Regierung davon abgehalten habe, einen Krieg zu führen (Hinsch/Janssen 2006: 60). Wichtiger ist für Kant, eine Rechtsordnung zu finden, welche die Beziehungen zwischen den Akteuren verlässlich regelt. Aus dieser Überlegung ergibt sich in Bezug auf den Privatsphärenschutz kein Widerspruch zu den genannten Prinzipien, sondern es kommt vielmehr noch ein weiteres zu: dass nämlich eine Einschränkung der Privatsphäre in dem Maße, wie sie nicht auf Selbstbestimmung gegründet werden kann, nur auf der Basis von Gesetzen erfolgen darf. Dies gilt in erster Linie für die staatliche Überwachung von Bürgern im virtuellen Raum. Darüber hinaus hat der Staat aufgrund der moralischen Drittwirkung auch die

[10] Vgl. für eine gute Einführung Hinsch/Janssen (2006); Nardin (1996).

Pflicht, einen entsprechenden gesetzlichen Rahmen, der die genannten Kriterien beinhaltet, für die Wirtschaft zu schaffen.

Tatsächlich lassen sich auch einige Parallelen zwischen der Ethik des „Gerechten Krieges" und dem deutschen Bundesdatenschutzgesetz ziehen: Der legitime Grund könnte im Interesse des Nutzers liegen; die Notwendigkeit hat eine Parallele zur Zweckbindung; die Proportionalität zur Datensparsamkeit bzw. dem Prinzip „Privacy by default"; die legitime Autorität könnte Pflichten des Datensammlers dahingehend begründen, dass nur Daten sammeln und verarbeiten darf, wer durch technische und organisatorische Maßnahmen auch ihre Sicherheit gewährleisten kann.

Bislang und in absehbarer Zukunft gilt für den Bereich der Wirtschaft das Paradigma der Kontrolle bzw. der informationellen Selbstbestimmung. Ein digitales Menschenrecht auf Privatsphäre würde Staaten und Unternehmen aber dieselben Schutzpflichten auferlegen. Gerade in Bezug auf den Bereich der Wirtschaft könnte dies als paternalistisch verstanden werden, was auch schon für Kompromisslösungen gelten würde, z.B. das „Nudging" (Schermer et al. 2014: 179 ff.). Allerdings ist die Grenze zwischen Paternalismus und staatlichen Schutzleistungen, auf die Bürger ein Recht haben, fließend. Wenn mit der Privatsphäre tatsächlich ein Menschenrecht auf dem Spiel steht, wird man eher nicht von Paternalismus sprechen.

3. Akteure und Positionen: Der transnationale Privatsphären-Aktivismus

3.1 Methode und Überblick zum Feld der Aktivisten

Die digitale Revolution und in ihrem Zuge die Gefährdung der Privatsphäre sind längst nicht mehr nur ein akademisches Thema. Es gibt mittlerweile einen breiten gesellschaftlichen Diskurs, in dem sich weit mehr Aktivisten zu Wort melden, als in dieser Studie aufgegriffen werden können. Der Initiative „Necessary and Proportionate"[11] zum Beispiel haben sich mehr als 400 NGOs weltweit angeschlossen. Es ist also eine Auswahl erforderlich. Das Ziel sollte dabei zum einen sein, die diskursiven „heavy hitters" zu identifizieren, zum anderen sollte möglichst auch ein angemessen breites Spektrum der aus ethischer Sicht relevanten Positionen abgebildet werden.

Methode und Auswahl

Die Auswahl der Beiträge erfolgt daher unter zwei Gesichtspunkten. Das erste Aufgreifkriterium ist der explizite Bezug auf ein neues digitales Menschenrecht auf Privatsphäre. Diese Einschränkung ist dem Thema geschuldet. Sie ist insofern nicht ganz unproblematisch, als damit viele interessante, aber weniger öffentlichkeitsheischende Diskussionsbeiträge nicht erfasst werden. Denn das Recht auf Privatsphäre ist in fast allen Staaten der Welt gesetzlich anerkannt und es gilt prinzipiell auch für den virtuellen Raum, weshalb es nicht zwingend notwendig ist, ein ganz neues, digitales Menschenrecht zu fördern, um den Schutz der Privatsphäre zu verbessern.

Allerdings geht es in diesem Abschnitt auch um etwas anderes: Denn der manchmal etwas ostentative Menschenrechtsbezug signalisiert den Wunsch nach politischer Mobilisierung, und Menschenrechte waren ja schon immer, und auch primär, ein politisches Projekt. Wir isolieren also durch das Kriterium des Menschenrechtsbezugs jenen Diskurs, der die Speerspitze der transnationalen Bewegung bildet und der, vielleicht noch besser als die philosophischen Überlegungen, Aufschluss über gesellschaftliche Befindlichkeiten und die Richtung einer zukünftigen Entwicklung gibt.

Zweitens wurden nur solche Beiträge aufgegriffen, welche eine gewisse Relevanz im Sinne von Prominenz und Einfluss bieten, von denen also, mit anderen Worten, erwartet werden kann, dass sie die Richtung des Menschenrechtsdiskurses mitbestimmen. Es wurden daher keine Blogs, keine Leserkommentare etc. gesichtet. Prominenz kommt vor allem einzelnen Personen zu, wie etwa dem Erfinder des World Wide Web, Tim Berners-Lee, während beim Einfluss vor allem die (finanzielle, juristische) Schlagkraft größerer zivilgesellschaftlicher Organisationen zählt.

Das Who's Who der Aktivisten und ihre Themen

Nach einer ursprünglich umfangreicheren Recherche wurde ein knappes Dutzend Dokumente von NGOs und Aktivisten aufgegriffen. Es mag sein, dass diese sich anderswo auch zu anderen Aspekten der digitalen Revolution geäußert haben. Im Vordergrund stehen hier aber weniger die Aktivisten selbst, d.h., es soll nicht ein lexikalischer Überblick über das Akteursfeld gegeben werden. Ziel ist es vielmehr, die Aktivisten-Kampagne unter dem Gesichtspunkt der ethisch relevanten Positionen aufzuarbeiten, und dabei genügen die eher wenigen Beiträge bereits für eine inhaltliche Sättigung. Sie sollen im Folgenden überblicksartig vorgestellt werden.

---

[11] https://en.necessaryandproportionate.org (14.02.2015).

Ein wichtiges Diskursfeld bilden jene Beiträge, die auf eine Neuauslegung bereits existierenden Völkerrechts setzen, um dadurch die staatliche Massenüberwachung einzuschränken. Ausgelöst wurde dieser Diskurs durch die Staaten selbst: Nach den Snowden-Enthüllungen verabschiedete die VN-Generalversammlung im Herbst 2013 eine von Deutschland und Brasilien eingebrachte Resolution unter dem Titel „Privacy In The Digital Age"[12], in welcher u.a. auch die damalige VN-Menschenrechtskommissarin *Navi Pillay* beauftragt wurde, einen Bericht über den Schutz der Privatsphäre im Kontext der Online-Massenüberwachung anzufertigen. Damit war das Feld für eine Neuinterpretation der existierenden Menschenrechtsartikel eröffnet. Einige größere Zivilrechtsorganisationen haben im Rahmen eines begleitenden Konsultationsprozesses substanzielle, teils auch gemeinsame Studien eingebracht, andere haben sich unabhängig davon in den öffentlichen Diskurs eingemischt.

Der Mitte 2014 erschienene Bericht von Navi Pillay („The right to privacy in the digital age") ist selbst zu einem Referenzpunkt der Debatte geworden. Für Pillay, eine ehemalige südafrikanische Richterin, hat laut eigenem Bekunden die Verteidigung der Privatsphäre denselben Stellenwert als Menschenrechtsthema wie der Genozid in Ruanda im Jahr 1994, an dessen juristischer Aufarbeitung sie beteiligt war. In ihrem Bericht kommt sie zu dem Schluss, dass die staatliche Massenüberwachung ein eklatanter Verstoß gegen das existierende Völkerrecht ist, weil sie ausländische Bürger diskriminiere, weil sie unverhältnismäßig sei und weil sie nicht durch Gesetze gedeckt sei.

Diese Position wird von einigen großen Organisationen geteilt, die sich auch an dem VN-Konsultationsverfahren beteiligt haben. Eine davon ist die 1990 gegründete britische NGO *„Privacy International" (PI)* mit Sitz in London. Bekannt geworden ist sie vor allem durch die jährliche Vergabe der „Big Brother Awards", mit denen Behörden, Unternehmen und Einzelpersonen ausgezeichnet werden, „who have excelled in the violation of our privacy."[13] Daneben hat PI gemeinsam mit dem „Electronic Privacy Information Center"[14] einige Rankings des Schutzniveaus der Privatsphäre in allen europäischen und elf weiteren Ländern erstellt. Außerdem führt PI mit ihren 17 Mitarbeitern Musterklagen, macht Lobbyismus und Öffentlichkeitsarbeit.

PI hat sich in einer gemeinsamen Stellungnahme mit sechs weiteren namhaften Institutionen[15] am VN-Konsultationsprozess beteiligt. Darin wird betont, dass Inhalts- oder Kommunikationsdaten gleichermaßen privatsphärenrelevant seien und entsprechend *jede* Datensammlung eine Verletzung der Privatsphäre konstitutiere (PI et al. 2014: 2). Über diese Stellungnahme hinaus tritt PI immer wieder als vehementer Fürsprecher für ein universales Menschenrecht auf Privatsphäre auf, das auch in wirtschaftlichen Kontexten zu gelten habe. So heißt es beim Internetauftritt von PI: „Privacy is essential to human dignity and autonomy in all societies. Privacy is at the cross-section of technology and human rights. The right to privacy is a qualified fundamental human right – meaning that if someone wants to take it away from you, they need to have a damn good reason for doing so."[16]

Ein weiterer namhafter „Big Player" der Menschenrechtsszene ist die ebenfalls 1990 ins Leben gerufene US-amerikanische Bürgerrechtsorganisation *„Electronic Frontier Foundation" (EFF)* mit Sitz in San Francisco. In ihrem Führungsstab sitzt u.a. *John Perry Barlow*, der für seine „Declaration of the Independence of Cyberspace" (1996) bekannt ist. Mit rund 70 Mitarbeitern und einem Budget von knapp 70 Mio. Dollar entfaltet die EFF eine vergleichsweise hohe Schlagkraft. Sie macht nicht nur

[12] VN-Dokument A/C.3/68/L.45, 1. November 2013.

[13] www.bigbrotherawards.org (15.2.2015).

[14] https://epic.org (15.2.2015).

[15] Das sind: APC, Article19, Human Rights Watch, World Wide Web Foundation, access, Electronic Frontier Foundation.

[16] www.privacyinternational.org (15.2.2015).

Öffentlichkeitsarbeit, sondern ist auch mit Musterklagen im Bereich Lobbyismus und in der Politikberatung aktiv.

Die EFF hat gemeinsam mit der Organisation *„Article19"* die oben erwähnte Initiative „Necessary and Proportionate" gestartet, die 13 „Internationale Prinzipien für die Anwendung der Menschenrechte auf die Kommunikations-Überwachung" propagiert. Diese Prinzipien sind recht kurz gehalten, weshalb eine längere Hintergrundanalyse dazu publiziert wurde, auf welche ich mich im Folgenden beziehe. Das Vorgehen in dieser Hintergrundanalyse ist eher juristisch-konservativ und besteht darin, aus völkerrechtlich relevanten Gerichtsurteilen („Case Law") Prinzipien für eine zeitgemäße und restriktive Auslegung geltender Völkerrechtsnormen zu gewinnen und zu erhärten.

Das Problem sei, dass existierendes Datenschutzrecht, wie es maßgeblich vom Europäischen Gerichtshof für Menschenrechte (ein Gericht des Europarats) und dem Europäischen Gerichtshof (EUGH) geschaffen wurde, noch zu deutlich zwischen Inhalts- und Metadaten unterscheide und diese unterschiedlich schütze: „it is clear that existing distinctions between metadata and content are no longer sound and that a fresh approach is necessary in order to protect individual privacy in a digital age" (EFF/Article19, 2014: 12). Damit vertreten auch EFF und Article19 ein zeitgemäßes Konzept von informationeller Privatheit. Allein schon die Sammlung von Metadaten verletze die Privatsphäre der betroffenen Personen (ebd.: 13).

Eine dritte und schon traditionsreiche Institution ist die 1920 gegründete *„American Civil Liberties Union" (ACLU)* mit Sitz in New York, die dem politischen Liberalismus nahesteht und für verschiedene Bürgerrechte kämpft, darunter auch die Privatsphäre. Mit einem Budget von knapp 40 Mio. EUR gehört sie sicherlich zu den „heavy hitters". Sie führt eine Kampagne zum Thema „Protecting Civil Liberty Rights in the Digital Age". Bei ihrem Internetauftritt heißt es: „Things we once thought could only happen in far-away enemy states or distant dystopias are suddenly happening here in America." Eine Diagnose, die durch das Privatsphärenranking von PI bestätigt wird: Die USA werden darin als „endemische Überwachungsgesellschaft" auf einer Ebene mit China eingeordnet.

Auch die ACLU gibt sich in ihrer ausführlichen Stellungnahme zum VN-Konsultationsprozess eher völkerrechtskonservativ, d.h., sie fordert kein neues Menschenrecht, sehr wohl aber einen neuen „Generalkommentar 16" zu Artikel 17 des „Internationalen Pakts über bürgerliche und politische Rechte", oder kurz „Zivilpakt", welcher die Privatsphäre schützt. Der Generalkommentar ist für die Menschenrechtserklärung, was der Talmud für die Thora und die Sunna für den Koran ist: Er gibt an, wie der sehr knappe Originaltext anzuwenden ist, und ist daher, auch wenn er nicht verbindlich ist, von hoher praktischer Bedeutung. Der existierende Generalkommentar wird aus zwei Gründen für unzureichend gehalten: Erstens könnten durch neue Technologie auch aus öffentlich verfügbaren Metadaten individuelle Profile erstellt werden (ACLU 2014: 15); Meta- und Inhaltsdaten dürften nicht mehr unterschiedlich geschützt werden, denn der Effekt der Datensammlung sei beide Male derselbe (ebd.: 18, 32). Zweitens gäbe es eine immer engere „symbiotische" Beziehung von Privatsphäre und dem Recht auf Meinungsfreiheit, Versammlungsfreiheit und anderen Menschenrechten, und dem müsse in der Bewertung von Privatsphärenverletzungen Rechnung getragen werden (ebd.: 3, 9).

Neben diesen drei großen Institutionen, die mit juristisch fundiertem Sachverstand aufwarten, beteiligen sich auch eine Reihe weiterer Gruppen, Plattformen und Einzelindividuen am Aktivistendiskurs über ein digitales Menschenrecht auf Privatsphäre. Für sie steht meist der wirtschaftliche Bereich im Vordergrund, in dem es um die Stärkung von Nutzerrechten gegenüber Unternehmen geht.

Eine gewisse öffentliche Wahrnehmung hat in diesem Bereich die *„Internet Rights and Principles Coalition" (IRPC)* erreicht. Es handelt sich dabei um eine Dialogplattform, die 2008 aus dem „Internet Government Forum" der VN hervorging und die von einer Handvoll Leuten, vor allem Akademikern, aber auch Vertretern von Firmen, organisiert wird. Sie hält regelmäßig Treffen ab, bringt Berichte heraus

und möchte damit eine Art Katalysator für den internationalen Diskurs über Privatsphäre sein. Ihre beiden wichtigsten Beiträge sind „The 10 Internet Rights & Principles" (2014a) und ein längerer, auch auf Deutsch publizierter Kommentar dazu unter dem Titel „Die Charta der Menschenrechte und Prinzipien für das Internet" (2014b). Beide verfolgen die „Vision einer menschenrechtsbasierten Internetumgebung" (ebd.: 7). Es wird explizit ein Recht auf „Privacy and Data Protection" gefordert und dahingehend expliziert, dass es nicht nur die Freiheit von Überwachung beinhalte, sondern auch das Recht auf Verschlüsselung und Anonymität – eine Forderung, die im VN-Diskurs nirgends erhoben wird.

Ein weiterer Beitrag zum Privatsphärendiskurs kommt vom *„Forum d'Avignon"*, bei dem es sich um einen französischen Think Tank handelt, der versucht, Wirtschaft und Kultur zusammenzubringen. Das Forum beschäftigt sich mit drei Themenschwerpunkten, einer davon lautet „Innovation und Digitales". Im Herbst 2014 wurde in diesem Kontext die „Preliminary Declaration of the Digital Human Rights" vorgestellt, die im Wesentlichen ein digitales Menschenrecht auf Privatsphäre begründet. Gleich im ersten Prinzip wird unter dem treffenden Begriff der „Digitalen DNA" festgehalten, dass personenbezogene Daten nicht von ihrem Träger gelöst werden können: „Every human being's personal data, in particular digital data, conveys information on his cultural values and private life. Personal data cannot be reduced to a commodity."

Im fünften Prinzip wird explizit ein Recht auf Privatsphäre formuliert: „Everyone has the right to respect for his dignity, private life and creative works, and shall not be discriminated against on the basis of access to his personal data and the use made thereof. No private or public entity may use personal data to manipulate access to information, freedom of opinion or democratic procedures." Diese Begründung ist für die vorliegende Studie interessant, weil sie erstens die Rolle der Privatsphäre in einem größeren gesellschaftlichen Kontext betrachtet und zweitens vor allem auf den wirtschaftlichen Bereich zielt.

Einige sehr interessante Beiträge kommen auch von Einzelpersonen. Unter ihnen sticht der Erfinder des World Wide Web *Tim Berners-Lee* hervor. Er ist Direktor des von ihm 1994 gegründeten „World Web Consortium", einer Organisation, die eher technische Lösungen für die Vision eines freien Internets entwickelt, und der 2009 ebenfalls von ihm gegründeten „World Wide Web Foundation", die sich für die „vision of an open Web available, usable, and valuable for everyone"[17] einsetzt. Berners-Lee ist ein gefragter Redner zu dem Thema (der Honorare verlangt, für die man auch einen ehemaligen US-Präsidenten bekommen kann). Er fordert eine „Magna Charta" für das Internet, um nicht nur den Schutz der Privatsphäre zu verbessern, sondern überhaupt eine offene und faire Gesellschaftsordnung zu gewährleisten – ein Aspekt, der in einer moralischen Begründung eines Rechts auf Privatsphäre nicht fehlen sollte.

Mit dem Blogger *Enno Park* soll ein Einzelkämpfer aufgegriffen werden, der als solcher freilich eine typische Erscheinung für das digitale Zeitalter ist, in dem auch Individuen einen direkten Zugang zur (digitalen) Öffentlichkeit haben. Park fordert unter dem Aspekt eines digitalen Menschenrechts insbesondere ein Recht auf „Pseudonymität", das sich gegen den Klarnamenzwang richtet. Pseudonyme sind zweifellos ein elementares ethisches Problem: Wie zieht man die Grenze zwischen dem Recht auf Unbekanntsein in der Öffentlichkeit und dem Recht der anderen, zu wissen, an wem sie sind? Nur wenige der oben genannten Aktivistengruppen erwähnen die Pseudonymität.

Eine politische Mobilisierung wäre nichts, wenn sie nicht die Schriftsteller auf ihrer Seite hätte. Schriftsteller sind professionelle Beobachter der Gesellschaft, sie spüren latenten Spannungen nach, und manchmal entwerfen sie Utopien oder Distopien, welche das kollektive Denken prägen. George Orwells Roman „1984" ist längst eine Chiffre für die Überwachungsdiktatur geworden. In diesem

[17] http://webfoundation.org (15.2.2015).

Zusammenhang ist es bemerkenswert, dass Ende 2013 eine Gruppe renommierter Autoren in Reaktion auf die Snowden-Enthüllungen eine Petition unter dem Titel „Die Demokratie verteidigen im digitalen Zeitalter" veröffentlicht hat.[18] Mehr als 560 Autoren aus der ganzen Welt haben den Aufruf unterzeichnet.

Die Schriftsteller stellen fest: „Dieses existenzielle Menschenrecht [auf Privatsphäre] ist inzwischen null und nichtig, weil Staaten und Konzerne die technologischen Entwicklungen zum Zwecke der Überwachung massiv missbrauchen. Ein Mensch unter Beobachtung ist niemals frei; und eine Gesellschaft unter ständiger Beobachtung ist keine Demokratie mehr. Deshalb müssen unsere demokratischen Grundrechte in der virtuellen Welt ebenso durchgesetzt werden wie in der realen."

Ein besonders prominenter Autor ist *Dave Eggers*, dessen 2014 erschienener Roman „The Circle" wie Orwells „1984" eine Dystopie der Überwachungsgesellschaft entwirft und der schnell zum Weltbestseller avancierte. Der Orwell'sche Überwachungsstaat beruht auf zentraler Beobachtung und Steuerung, aber bei Eggers entfaltet sich die Tyrannei infolge absoluter Transparenz durch gegenseitige soziale Kontrolle. Eggers begnügt sich nicht damit, ein neues digitales Menschenrecht zu fordern, sondern er hält den Menschen auch den Spiegel vor, indem er ihnen die Arglosigkeit demonstriert, mit welcher sie sich in den Sog des Internets ziehen lassen. Dadurch lädt er zu einer etwas anderen Art der moralischen Reflexion über die digitale Revolution ein.

3.2 Die Ethik der staatlichen Massenüberwachung

Als am 6. Juni 2013 die britische Zeitung „The Guardian" die ersten von Edward Snowden geleakten Dokumente publizierte, war die Empörung der Öffentlichkeit vorprogrammiert. Mit einer Überwachung solchen Orwell'schen Ausmaßes hatte niemand gerechnet. Gleichwohl äußerten abgeklärte Kommentatoren schon bald, dass Überwachung nun einmal die Aufgabe der Geheimdienste sei und sich im digitalen Zeitalter eben auch auf den virtuellen Raum erstrecken müsse. Jeder Staat tue dies, und die USA machten es eben etwas besser. So war es eine Sache, sich über ein großes Unrecht zu empören, aber eine andere, auch zu einem argumentativ gesicherten Urteil über die NSA-Überwachung zu gelangen.

Mittlerweile sehen wir klarer. Die genannten Bürgerrechtsorganisationen haben ausführliche Bewertungen der Massenüberwachung vorgelegt, um Einfluss auf den VN-Meinungsbildungsprozess zu nehmen. Sie fordern kein neues digitales Menschenrecht auf Privatsphäre, sondern arbeiten überwiegend rekonstruktiv, insofern sie aus verschiedenen Völkerrechtsquellen (Generalkommentar, Dokumente des Menschenrechtsrats, Urteile internationaler Gerichte) Rechtsprinzipien gewinnen, anhand derer sich die Online-Massenüberwachung beurteilen lässt. Im Wesentlichen handelt es sich dabei um Kriterien, wie sie auch in der Ethik des „Gerechten Kriegs" diskutiert werden..

Die Dokumente ähneln sich daher in Struktur und Inhalt, auch wenn die Begrifflichkeit jeweils eine etwas andere ist. Im Folgenden nehme ich den Ausgangspunkt daher bei der Initiative „Necessary and Appropriate"[19] und deren Interpretation durch die EFF und „Article19", wobei abweichende oder ergänzende Bezugnahmen selbstverständlich mit eingeflochten werden.

---

[18] www.change.org/p/die-demokratie-verteidigen-im-digitalen-zeitalter (15.2.2015).

[19] Diese 13 Prinzipien sind: Legalität, Legitimes Ziel, Notwendigkeit, Adäquatheit, Proportionalität, kompetente rechtliche Autorität, ordentlicher Prozess, Nutzerbenachrichtigung, Transparenz, Öffentliche Kontrolle, Integrität von Kommunikation und Computersystemen, Garantien für internationale Kooperation, Sicherungen gegen unberechtigten Zutritt.

Über einen Punkt herrscht indes absolute Übereinstimmung: nämlich dass Artikel 17 des Zivilrechtspakts, welcher die Privatsphäre schützt[20], wie jedes Menschenrecht universal gilt, d.h. auch extraterritorial. Gerät ein Individuum unter den Einfluss eines Staates, so hat dieser Staat Menschenrechtspflichten gegenüber diesem Individuum. „Individuals subject to surveillance by a foreign State Party are within the power of that State Party" (ACLU 2014: 34). Ebenso herrscht Konsens, dass bereits die Datensammlung und -speicherung eine Verletzung der Privatsphäre der betroffenen Individuen konstituiert, selbst wenn kein Mensch sich über die entsprechenden Daten beugt (ebd.: 36). Mit anderen Worten: Beobachtung ist Einfluss, und Einfluss begründet Verantwortung. Im Folgenden geht es nun darum, unter welchen Bedingungen solche Verletzungen des Menschenrechts auf Privatsphäre noch verantwortbar sind.

Gerechter Grund

Eine Verletzung von Rechten kann nur legitim sein, wenn sie einem Zweck dient, der mindestens so schwer wiegt wie das verletzte Recht – alles andere würde die moralische Ordnung auf den Kopf stellen. Allerdings ist erstaunlich unklar, was im Kontext der Massenüberwachung ein gerechter Grund ist. Die Europäische Menschenrechtskonvention (1950) nennt in Artikel 8 auch den „Schutz der Moral" und das „wirtschaftliche Wohl eines Landes" als gerechte Gründe. Tatsächlich scheinen im Sicherheitsbegriff der USA wirtschaftliche Interessen eine wichtige Rolle zu spielen, während gerade Diktaturen gerne mit dem Schutz der öffentlichen Moral argumentieren. Nicht erlaubt wären wohl nur die Überwachung zur Kontrolle politischer Feinde, zur Unterdrückung und Verfolgung von Minderheiten und zur Eintreibung von Steuern[21].

Etwas konkreter sind die „13 Prinzipien" von „Necessary and Proportionate". Laut ihnen qualifizieren sich als „legitimes Ziel" (das ist nur ein anderer Begriff für den gerechten Grund) „legale Interessen von überragender Bedeutung, die in einer Demokratie wichtig" sind. Konkretisiert wird dies nicht. Pillay nennt in ihrem Bericht, welcher die Völkerrechtslage zusammenfasst, „nationale Sicherheit", „Terrorismusabwehr" und „other crimes" (2014: 8; vgl. auch Omand et al. 2012: 43). Noch restriktiver ist die EFF, die ein Urteil des Bundesverfassungsgerichts aus dem Jahr 2008 aufgreift, wonach „life, limb or liberty of a person" gefährdet sein müssen oder „public goods, the endangering of which threatens the very bases or existence of the state, or the fundamental prerequisites of human existence" (zitiert aus EFF 2014: 19 f.). Der erste Aspekt impliziert eine Art moralische Äquivalenz, wonach also die Verletzung eines Menschenrechts mit dem Schutz mindestens gleichrangiger Menschenrechte begründet werden muss (Leib, Leben, Freiheit).

Nehmen wir dieses Äquivalenz-Kriterium ernst, so erscheinen alle anderen Gründe und besonders die „öffentlichen Güter" als problematisch, denn es handelt sich dabei erstens um kollektive Güter, die sich zweitens nur über längere Begründungsketten auf individuelle Menschenrechte zurückführen lassen. Was überhaupt der Wirtschaft dient oder schadet, ist selbst unter Ökonomen umstritten. Am ehesten gelingt die Reduktion auf ein Menschenrecht noch bei der nationalen Sicherheit, denn es gibt nach Kant auch ein Menschenrecht auf Staat, insofern nur der Staat die Menschenrechte garantieren kann.

---

[20] Artikel 17 des „Internationalen Pakts über bürgerliche und politische Rechte" (1966) lautet: „Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden."

[21] So selbstverständlich dies klingt: Das britische Gesetz „Regulation of Investigatory Powers Act 2000 (RIPA)" sieht darin einen gerechten Grund für Überwachung (Omand et al. 2012: 42).

Doch was konstituiert eine Gefährdung der nationalen Sicherheit, und ist damit auch gleich der Staat gefährdet? Die EFF greift eine Stellungnahme des UN-Sonderberichterstatters für die Meinungsfreiheit Frank LaRue auf, der das Konzept der nationalen Sicherheit als äußerst vage kritisiert, denn damit könnten z. B. auch Journalisten ins Visier genommen werden (2014: 19). Das tiefere Problem ist wohl, dass die Nation und ihre Sicherheit beides soziale Konstrukte sind, die nicht in derselben Weise verletzt werden können wie ein Ding. Nationen haben den Verlust von Territorium überstanden (z.B. Deutschland im zweiten Weltkrieg), und auch der Tod vieler Menschen (die USA durch 9/11) scheint den Fortbestand des Staates überhaupt nicht zu gefährden. Unterstellt man weniger drastische Verletzungen der nationalen Sicherheit, so könnte ein Gegenargument lauten, dass die Werte und Gesetze eines Landes täglich zigfach verletzt werden, wobei diese Verletzungen von den Sicherheitsdiensten und der Justiz in der Regel gut bewältigt werden. Zwar kann eine Gesellschaft auch in ihrer „ontologischen Sicherheit" verletzt werden, z.B. wenn infolge von Terrorismus die Angst das öffentliche Leben beeinträchtigt. Aber das Sicherheitsgefühl liegt schon wieder nahe am vagen Kriterium der „öffentlichen Moral"; manchmal schüren Politiker diese Angst auch selbst, wenn es ihren Interessen dient.

Diese Überlegungen zeigen, dass der gerechte Grund ein sehr missbrauchsanfälliges Kriterium ist und vielleicht gerade deswegen von der Politik teils recht exzessiv in Anspruch genommen wird. In ethischer Betrachtung kommt man mit dem gerechten Grund aber ohnehin nicht sehr weit: Denn selbst wenn der gerechte Grund gegeben wäre, könnte eine Überwachungsmaßnahme noch an allen weiteren Kriterien scheitern.

Abwägungsbedingung

Die Kriterien der Notwendigkeit, Proportionalität und Aussicht auf Erfolg lassen sich unter dem Begriff der Abwägung zusammenfassen. Im amerikanischen Völkerrechtsdiskurs wird statt Abwägung auch davon gesprochen, dass Überwachung nicht „willkürlich" sein dürfe, was aber auf dasselbe hinausläuft. Zwar ist auch die Abwägung immer vage: Denn ist es nicht utopisch, Nutzen und Schäden präzise zu messen bzw. überhaupt erst vorhersagen zu wollen? Darauf kommt es jedoch nicht an, im Alltag treffen wir ständig ethische Entscheidungen, ohne absolute Gewissheit zu haben. Im Wesentlichen kann daher gefordert werden, dass die „positiven Folgen eines [...] Eingriffs in die [Privatsphäre] seine negativen Folgen *bei weitem* übertreffen werden" (Hinsch/Janssen 2006: 89).

Alle aufgegriffenen Kommentare stimmen überein, wenngleich aus leicht unterschiedlichen Gründen, dass eine Massenüberwachung, wie sie von der NSA betrieben wird, diese Abwägungsbedingung nicht erfüllt und als „willkürlich" zu gelten hat.

Die EFF sieht das Kriterium „Aussicht auf Erfolg" als grundlegend an: „A measure which is inherently incapable of achieving the stated objective, or which is demonstrably grossly ineffective in achieving it, cannot ever be said to be ‚appropriate', ‚necessary', or, ‚proportionate'" (EFF 2014: 21). Diese Anwendung des Kriteriums ist allerdings ein wenig irreführend, denn ein Mittel darf nicht allein in Bezug auf den Zweck abgewogen werden. Eine solche Zielerreichungsrationalität würde bedeuten, dass eine zu 100 % erfolgreiche Überwachung, die jeden potenziellen Terroristen ans Licht bringt, automatisch legitim wäre. Output-Legitimität könnte außerdem als Aufforderung an die Geheimdienste verstanden werden, ihre Überwachungskapazitäten noch weiter auszubauen.

Das Kriterium der Notwendigkeit bedeutet, dass ein Mittel über den Erfolg hinaus auch dasjenige Mittel sein, das am „wenigsten intrusiv" ist (Pillay 2014: 9; EFF 2014: 20). Für die ACLU versagt an diesem Punkt die Rechtfertigung der Massenüberwachung: Diese sei „an arbitrary interference with the right to privacy, as it does not represent the least intrusive means of achieving particular aims" (ACLU 2014: 39).

Der hier ins Spiel gebrachte Begriff „Intrusivität" verweist darauf, dass bei der Abwägung immer auch der potenzielle Schaden einer Maßnahme in Rechnung zu stellen ist. Ein Schaden an der Privatsphäre unschuldiger Menschen entsteht bereits durch die Erfassung ihrer personenbezogenen Daten. So zitiert die EFF ein Urteil des Europäischen Gerichtshofs für Menschenrechte, wonach bereits die Speicherung von DNA eine „unproportionale Einmischung" in das Privatleben der betroffenen Individuen darstelle (2014: 21). Der Bericht von Navi Pillay bringt treffend auf den Punkt, was Notwendigkeit und Proportionalität bedeuten: „It will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened" (Pillay 2014: 9). Eine Überwachungsmaßnahme kann also notwendig sein, um ein Ziel zu erreichen, aber sie kann dennoch am Kriterium der Proportionalität scheitern.

Die Metapher mit dem Heuhaufen verweist darauf, dass unter dem Gesichtspunkt der Proportionalität nicht allein das zahlenmäßige Verhältnis der wenigen „Treffer" gegenüber den vielen unschuldig Erfassten problematisch ist, sondern es müssten auch die Kollateralschäden mitbilanziert werden. Die können beträchtlich sein, wenn die Privatsphäre tatsächlich eine Art „Supergrundrecht" wäre. Ein von Berners-Lee initiierter offener Brief an die Open Government Partnership protestiert gegen die staatliche Überwachung, weil dadurch die Meinungs-, Informations- und Versammlungsfreiheit beeinträchtigt würden, die ebenfalls Menschenrechtsstatus haben.[22] Das Deutsche Institut für Menschenrechte hat in eine ähnliche Kerbe geschlagen und gegen das Antiterrordatei-Gesetz eingewandt, dass die Speicherung von „Befürwortern" eine abschreckende Wirkung auf die Meinungsfreiheit und politische Partizipation habe (2014b; vgl. auch ACLU 2014: 40).

Pillay stellt in Rechnung, dass eine Überwachung heute, welche die zukünftige Überwachung erschwere oder verteuere, kontraproduktiv sei und auch dieser Effekt in die Kosten-Nutzen-Bilanz eingehen müsse. Privacy International gibt zu bedenken, dass Massenüberwachung zwangsläufig Unsicherheit erzeuge, weil eine so enorme Datensammlung nicht mehr beherrscht und gesichert werden könne: „The very quantity and nature of the information being collected renders such a system inherently unsafe" (PI 2014: 18). Die EFF argumentiert, dass die NSA durch den Einbau von Hintertüren die Sicherheit und das Vertrauen im Netz insgesamt beschädige. „Just as it would be unreasonable for governments to insist that all residents of houses should leave their doors unlocked just in case the police need to search a particular property, or to require all persons to install surveillance cameras in their houses on the basis that it might be useful to future prosecutions, it is equally disproportionate for governments to interfere with the integrity of everyone's communications in order to facilitate its investigations" (EFF: 2014: 29).

Recht und Öffentlichkeit

Bislang haben wir die *ethischen* Aspekte der Überwachung in den Blick genommen und die (völker-)-rechtliche Ebene ausgeklammert. Allerdings kann die Gesetzmäßigkeit einer Privatsphärenverletzung selbst eine Forderung der Ethik sein. Einer der schärfsten Kritiker der Lehre des „Gerechten Krieges" war, wie schon erwähnt, Kant, der angemerkt hatte, dass es bislang „kein Beispiel gibt, dass jemals ein Staat durch Argumente wäre bewogen worden, von seinem Vorhaben abzustehen" (zitiert aus Hinsch/Janssen 2006: 60). Auf ethische Argumente allein sollte eine Menschenrechtsverletzung nicht gegründet werden (das Dilemma einer rein ethischen Beurteilung ist wohl, dass entweder eine vage Abwägung akzeptiert wird oder dass für jedes Kriterium weitere, noch detailliertere Kriterien

[22] www.opengovpartnership.org/blog/blog-editor/2013/12/20/letter-ogp-governments (11.2.2015)

aufgestellt werden, die dann am Ende vielleicht nicht mehr restriktiv, sondern plötzlich wieder permissiv wirken).

Es bedarf noch einer anderen „Zutat", die gegenüber Regierungen eine höhere Kraft des Faktischen hat, nämlich Recht und Öffentlichkeit. Kant ist der Begründer der Idee von der Herrschaft des Rechts. Der Eintritt in den Rechtszustand ist für Kant eine ethische Pflicht, weil nur so die Hobbes'sche Konfliktspirale von Angst und Selbstverteidigung überwunden werden kann. Wenn mich ein Polizist in Erfüllung seiner Ordnungsfunktion anhält, schränkt das meine Freiheit in der Regel nicht ein; darf jeder Mitbürger bei jedem Verdacht dies tun, wäre ein massiver gesellschaftlicher Freiheitsverlust zu befürchten. Legalität hat also nicht nur einen Frieden stiftenden, sondern wie die Einwilligung auch einen moralisch transformativen und die individuelle Freiheit sichernden Effekt.

So lässt sich die Forderung der EFF nach der „Legalität" einer Überwachungsmaßnahme als Gebot der Herrschaft des Rechts einordnen (2014: 14 ff.). Dabei seien, wie u.a. im Rekurs auf die Rechtsprechung des Europäischen Gerichtshofs gezeigt wird, an das Recht zusätzliche Kriterien zu stellen, nämlich Klarheit, Zugänglichkeit und Berechenbarkeit (im Sinne vorhersehbarer Effekte des eigenen Handelns) und Spezifizität/Präzision (ebd.: 15; vgl. auch ACLU 2014: 20-23). Geheime Regeln oder Interpretationen dieser Regeln, d.h. die legalen Tricks, die Regierungen anwenden zur Legalisierung von Überwachungsmaßnahmen, sind angesichts dieses Kriteriums vergebliche Liebesmühe. Sie erreichen, so die EFF, nicht die „Qualität von Recht" (2014: 16; vgl. auch Pillay 2014: 10).

Für die EFF scheitert die Rechtfertigung der Massenüberwachung an der mangelnden Spezifizität der rechtlichen Legitimation: „By its very nature, mass surveillance does not involve any form of targeting or selection, let alone any requirement on the authorities to show reasonable suspicion or probable cause" (2014: 22). Auch die ACLU kommt auf dieser Grundlage zu einer kategorischen Ablehnung der Legitimität von Massenüberwachung (2014: 23): „Bulk mass surveillance with no grounds for such suspicion would, logically and obviously, fail such a test." Massenüberwachung „ought to be entirely prohibited", wolle man an Artikel 17 des Zivilpakts festhalten (ebd.: 26).

Das Kriterium der Herrschaft des Rechts ist schließlich mit den Prinzipien der Gewaltenteilung und der Öffentlichkeit verbunden. Die EFF fordert, dass nur eine „kompetente rechtliche Autorität, die unabhängig von der Regierung handelt und im Einklang mit den rechtlichen Verfahren", die Entscheidungen zur Überwachung treffen dürfe (2014: 21). Der parlamentarischen Kontrolle könne man nach der Erfahrung von 9/11 nicht mehr trauen, weil damals die Abgeordneten leichtfertig individuelle Rechte zugunsten der nationalen Sicherheit aufgegeben hätten (ebd.: 23). Außerdem müssten die geschädigten Individuen die Möglichkeit haben, sich rechtlich zu wehren, was voraussetze, dass sie innerhalb einer gewissen Frist über eine an ihnen erfolgte Überwachung informiert werden (ebd.: 25).

3.3 „Digitale Souveränität": Kontrolle für den Nutzer

Ein völlig anderes Feld im Aktivistendiskurs über ein neues digitales Menschenrecht bilden jene Sorte von Beiträgen, welche Konzepte der Kontrolle und der „informationellen Selbstbestimmung" artikulieren. Alle diese Konzepte kreisen um die Einwilligung: Datenverarbeitung ja, aber man möchte bitte schön gefragt werden. Wenn der Mensch tatsächlich im Mittelpunkt der digitalen Gesellschaft stehen soll, so liegt es dem Paradigma der Kontrolle folgend nahe, die Datenverarbeitung radikal im Wollen und Entscheiden der Menschen zu verankern. Souverän ist, wer entscheiden kann, und digitale Souveränität bedeutet dann, selbst über die Verwendung der eigenen Daten entscheiden zu können.

Die Beiträge in diesem Diskursfeld knüpfen an keine existierenden Völkerrechtsnormen an, sondern fordern, dass die informationelle Selbstbestimmung in den Rang eines neuen digitalen

Menschenrechts auf Privatsphäre erhoben wird. Gemeinsam ist ihnen auch, dass sie nicht, wie der klassische Liberalismus, auf den Staat als potenziellen Bedroher der individuellen Freiheit fokussiert sind, sondern auf private Wirtschaftsunternehmen.

Das Prinzip der Einwilligung

Das Forum d'Avignon gründet in der „Preliminary Declaration of the Digital Human Rights" den Schutz der Privatsphäre auf die Zustimmung: „Any exploitation of the data or creative works of any individual requires his free, prior, informed, time-limited and reversible consent."[23] Auch die IRPC sieht die Essenz des Privatsphärenschutzes im Prinzip der Zustimmung: „Jede Person hat das Recht auf Datensouveränität. [...] Wer auch immer persönliche Daten anderer Personen benötigt, muss die informierte Zustimmung der betroffenen Person Daten einholen" (2014b: 19). Gleiches gilt für die Schriftsteller, die in ihrer Petition das Recht fordern, „for all people to determine, as democratic citizens, to what extent their personal data may be legally collected, stored and processed, and by whom; to obtain information on where their data is stored and how it is being used".

Die vom Forum d'Avignon angeführten Kriterien der Zustimmung sind am differenziertesten, werden aber leider nirgends interpretiert. Versuchen wir daher selbst eine Problematisierung: Die „freie" Zustimmung ist natürlich das normative Fundament des Rechts auf informationelle Selbstbestimmung. Allerdings verbinden sich mit diesem Kriterium auch die größten Schwierigkeiten: Wenn Menschen immer schon in soziale, wirtschaftliche und politische Strukturen eingebunden sind, dann ist auch ihre Autonomie immer schon beschränkt – wie „frei" ist etwa ein Jugendlicher, ein allseits beliebtes soziales Online-Netzwerk *nicht* zu nutzen? Analytisch betrachtet liegt das Problem darin, dass Rechte ein Gegenüber verpflichten, aber in diesem Fall, d.h. vor einer Registrierung, noch gar keine Beziehung zwischen Nutzer und Anbieter besteht. Es wäre absurd, dem Anbieter Freiheitseinschränkungen eines ihm noch unbekannten Kunden vorzuwerfen. Sofern hier tatsächlich Handlungsalternativen fehlen, liegt dies mehr an der Organisation des Marktes (Monopole) als an einzelnen Unternehmen, weshalb das Recht auf *freie* Zustimmung eher den Staat verpflichtet, entsprechende Rahmenbedingungen herzustellen.

Die anderen vier Kriterien formulieren dagegen Pflichten, die sich unmittelbar an den Diensteanbieter richten. „Vorausgehende Zustimmung" bedeutet, dass eine Entscheidung getroffen wird, bevor potenzielle Kunden Zeit und Arbeit in eine Registrierung gesteckt haben. Die übliche Praxis, bei einer Online-Bestellung als *letzten* Schritt noch die AGB zu akzeptieren, erscheint vor diesem Hintergrund fragwürdig. Das Kriterium „informiert" erfordert, dass das Datensubjekt Klarheit über die Verwendung seiner personenbezogenen Daten hat. Die IRPC spricht von Informationen bezüglich „des Inhalts, Zwecks und Speicherorts, der Dauer und Art des Zugangs, der Abfragemöglichkeiten und der Korrektur der persönlichen Daten" (2014b: 19). Dieser Forderung entspricht eine komplementäre und u.a. auch vom Forum d'Avignon angemahnte Transparenzpflicht der Anbieter.

Die beiden Kriterien einer „zeitlich begrenzten" und „reversiblen" Einwilligung gehören zu den innovativeren Vorschlägen im Datenschutzdiskurs. Sie liegen im Vorfeld eines Löschungsrechts, wie es die IRPC fordert (2014b: 19). Ethisch betrachtet kommen sie dem grundlegenden menschlichen Interesse entgegen, sich permanent selbst zu entwickeln. Soziale Realität ist immer im Fluss, entweder die Persönlichkeit ändert sich oder die gesellschaftliche Umwelt, und dann müssen auch die

[23] Einige Kommentatoren haben sich daran gestört, dass die Menschenrechtserklärung des Forum d'Avignon personenbezogene Daten mit kreativer Arbeit gleichsetzt, denn damit werde unter der Hand das Copyright in den Rang eines Menschenrechts erhoben. Gut möglich, dass darin die Wirtschaftsnähe des Forum d'Avignon zum Ausdruck kommt. Die Zustimmungsproblematik betrifft dies aber nicht.

Datenregime so flexibel sein, dass die digitalen Fremdbilder nicht eingefroren und damit zu Karteileichen werden.

Außerdem trägt eine befristete und reversible Einwilligung einer völlig neuen Situation in der digitalen Welt Rechnung, die tendenziell nicht den Nutzer, sondern den Datenverarbeiter begünstigt. Heute reicht bereits der einmalige Kontakt, z.B. eine Online-Bestellung, um eine Beziehung mit einem Unternehmen herzustellen, die dann aber kein definiertes Ende hat, vergleichbar mit dem Verlassen eines Ladens nach Abschluss eines Kaufs. Eine befristete Einwilligung würde der Akkumulation von Daten Grenzen setzen und damit die Position der Nutzer stärken.

Kontrolle auch nach der Einwilligung

„Digitale Souveränität" kann sich nicht allein in der autonomen Einwilligung erfüllen. In einem solchen „One Shot Game" würde sich das Recht, Kontrolle über die eigenen Daten zu haben, darin erschöpfen, diese Kontrolle in einem Tausch freiwillig aufzugeben. Solange ein Unternehmen personenbezogene Daten eines Kunden speichert, hat es Einblicke in dessen Privatsphäre, und deshalb fordern die meisten Aktivisten unveräußerliche Kontrollrechte, die auch nach dem Zeitpunkt der Einwilligung noch gelten. Schon das eben genannte Prinzip der „Reversibilität" ist im Grunde ein solches nachgelagertes Kontrollrecht.

Der Mehrwert eines solchen unveräußerlichen Kontrollrechts mag auf den ersten Blick nicht ersichtlich sein. Eine Analogie aus anderen, alltäglichen Zusammenhängen ist schwer zu finden: Wenn ich meinem Schneider die Telefonnummer freiwillig mitgeteilt habe, um bei Fertigstellung der Reparatur einen Rückruf zu erhalten, habe ich vermutlich keinen Anspruch, diese Information zu kontrollieren. Anders wäre die Situation aber, wenn der Schneider ein Spitzel ist, der Informationen an den Staat weitergibt, welcher damit zum eigentlichen Datenverarbeiter wird. In diesem Fall macht ein permanentes Kontrollrecht Sinn, wobei dieser Fall im digitalen Ökosystem wohl mehr die Regel als die Ausnahme ist. Kreditauskunfteien, Marketingfirmen etc. sind solche sekundären Datenverarbeiter, die enormen Einfluss auf Individuen haben, die bei ihnen überhaupt keine Kunden sind.

Forderungen nach einem Recht auf Kontrolle, das sich auf die Daten im „Maschinenraum" bezieht, kommen vor allem wieder aus dem europäischen Raum. So lautet beim Forum d'Avignon das vierte Menschenrechtsprinzip „Right of Inspection: Everyone has the right to inspect and control his personal data, including that resulting from his behavior and objects connected to him." Was mit „kontrollieren" gemeint ist, wird nicht weiter erklärt. Aber wir wissen, dass schon ein bloßes Sich-Informieren eine Form des „zwingenden Blicks" ist, insofern Missstände aufgedeckt und eine Firma in Misskredit gebracht werden könnte. Ein darüber hinausgehendes Kontrollrecht bestünde darin, falsche Daten korrigieren zu können; es gibt viele drastische Beispiele, wie Menschen aufgrund fehlerhafter Daten, oder sogar einer Verwechslung von Identitäten, massive Nachteile erleiden (vgl. Garfinkel 2000: 25-29).

Die IRPC fordert, wie bereits angesprochen, nicht nur das Recht auf eine Abfrage von Daten, sondern auch ein Löschungsrecht (2014b: 19): Wer einen Gast in sein Haus lässt, der muss ihn auch wieder hinauswerfen können, sonst ist er nicht Herr im Haus. Der Aufruf der Schriftsteller verlangt, dass „ein Bürger seine Daten löschen lassen kann, falls sie *illegal* gesammelt und gespeichert wurden" (meine Hervorhebung). Das kommt jenen Unternehmen entgegen, welche Datenschutz-Gesetze umsetzen; sie kämen in die Bredouille, wenn Kunden rechtmäßig geteilte Daten nach eigenem Belieben jederzeit zurückrufen könnten. Von einem „Recht auf Vergessenwerden", wie es der Europäische Gerichtshof 2014 in seinem „Google-Urteil" geschaffen hat, spricht keiner der untersuchten Texte.

Kritik der informationellen Selbstbestimmung

Das Paradigma der informationellen Selbstbestimmung steht durch den direkten Bezug zur individuellen Autonomie auf einem starken normativen Fundament. Gleichwohl wurden in den letzten Jahren immer lautere Zweifel angemeldet, ob es sich im Kontext von Big Data noch einlösen lasse. Die Zweifel kommen weniger von den Aktivisten selbst als von einzelnen Kommentatoren mit Nähe zur Wissenschaft. Einer davon ist Viktor Mayer-Schönberger, der Vordenker des „Rechts auf Vergessenwerden". Er hält die informationelle Selbstbestimmung für „tot". Bei den enormen Mengen an Daten, welche jeder Mensch heute freisetze, oft unbewusst, und der Komplexität von Big-Data-Märkten und -Technologien sei es illusorisch, noch anzunehmen, der Einzelne könne eine bedeutungsvolle Kontrolle über seine weitverstreuten Daten ausüben[24]: „The naked truth is that informational self-determination has turned into a formality devoid of meaning and import. [...] Protection for the consumer should not depend on the ability to comprehend what's going on with her data and ability to take action."[25]

Eine weitere kritische Stimme ist der Datenschutz-Experte, Rechtsanwalt und Blogger Eduardo Ustaran. Auch er hält es für eine Überforderung der Autonomie von Nutzern, wenn sie ihre Daten selbst kontrollieren müssten:

„Pretending that we can take a view in any meaningful way as to how information about us is gathered, shared, and used by others is wishful thinking. We cannot even attempt to recognize what personal information is being made available by us in our daily comings and goings, so how could we possibly decide whether to consent or not to every possible use of that information? [...] Any legal regime that puts the onus on individuals (who are meant to be protected by that regime) is bound to be wrong. The onus should not be on us to decide whether a cookie may reside in our computer when hardly anyone in the real world knows what a cookie does. What the law should really do is put the onus on those who want to exploit our information by assigning different conditions to different degrees of usage, leaving consent to the very few situations where it can be truly meaningful."[26]

Auch Ustaran vertritt damit die im theoretischen Teil bereits aufgegriffene Forderung (vgl. Schermer et al. 2014), dass Zustimmung auf jene Bereiche reduziert werden müsse, in denen sie relevant und realisierbar ist, während der Rest durch generelle Erlaubnisse und Verbote zu regeln wäre. Vielleicht liegt der grundsätzliche Fehler der informationellen Selbstbestimmung darin, dass Ziel und Methode verwechselt werden: Die individuelle Autonomie zu schützen, indem sie zugleich in Form von Wissens- und Entscheidungskompetenz in Anspruch genommen wird, erinnert ein wenig an das Abenteuer des Baron Münchhausen, der sich an den eigenen Haaren selbst aus dem Sumpf zieht.

[24] https://privacyassociation.org/news/a/yes-consent-is-dead-further-continuing-to-give-it-a-central-role-is-danger/ (22.1.2015).

[25] www.privacyassociation.org/news/a/keynote-forget-notice-and-choice-lets-regulateuse (22.1.2015).

[26] www.linkedin.com/pulse/20140327085821-24251273-the-evolution-of-consent (20.1.2015).

3.4 Weniger Kontrolle, besserer Schutz? Regulierung der Datenverarbeitung

Die bislang aufgegriffenen Beiträge zu einem digitalen Menschenrecht auf Privatheit fallen in zwei Gruppen – jene, die staatliche Überwachung strikten Kriterien unterwerfen möchten, und solche, die Datensammlung im wirtschaftlichen Kontext betrachten und ein Maximum an Nutzer-Selbstbestimmung ermöglichen möchten. Dazwischen klafft eine Lücke: Nur wenige Aktivisten fordern, und meist auch eher nebenbei, dass auch die wirtschaftliche Datenverarbeitung prinzipiellen Einschränkungen zu unterwerfen sei, die bei einer Einwilligung nicht zur Disposition stehen. Ein solcher Ansatz geht in die von Ustaran und Mayer-Schöneberger geforderte Richtung, die Datenverarbeitung selbst zu regulieren, ergänzend oder sogar anstelle einer Regulierung der Nutzer-Unternehmen-Beziehung.

Das stärkste Plädoyer für allgemeine Datenschutzprinzipien findet sich bei der IRPC. Sie fordert „Mindeststandards bei der Benutzung persönlicher Daten":

„Wenn persönliche Informationen erforderlich sind, darf nur das Minimum an notwendigen Daten gesammelt werden, und das nur für den kürzesten notwendigen Zeitraum. Daten müssen gelöscht werden, wenn sie nicht mehr länger für den Zweck, für den sie gesammelt wurden, notwendig sind" (2014b: 19).

Wirklich neu sind diese Forderungen allenfalls in einem internationalen Kontext; das deutsche Bundesdatenschutzgesetz kennt die Prinzipien der „Datensparsamkeit" (§ 3 a), der „Zweckbindung" (§ 28 Abs. 1) und der „Löschungspflicht" (§ 35, 2) schon länger. Es sind vor allem Datenschutzpraktiker, welche nicht zustimmungsbasierte Datenschutzgrundsätze propagieren. So fordert die „Madrid Resolution", die 2009 auf einer Weltkonferenz der staatlichen Datenschutzbeauftragte verabschiedet wurde, u.a. die Prinzipien der Legalität, Zweckbindung, Proportionalität, Datenqualität und Rechenschaftspflicht (Madrid-Resolution 2009: 10-13). Auch eine bereits 1980 von der OECD verabschiedete und 2013 nochmals aktualisierte Datenschutz-Richtlinie formuliert ähnliche Kriterien, unter anderem auch zur Datensicherheit (vgl. OECD 2013: 23), die sich nicht vollständig auf eine Nutzerzustimmung zurückführen lassen.

Man erkennt darin einige der weiter oben in Anlehnung an die Ethik des „Gerechten Krieges" diskutierte Kriterien. Entscheidend ist am Ende, wie diese Grundsätze ausgelegt werden. Wenn etwa der Zweck einer Datensammlung nicht nur die Abwicklung einer einmaligen Dienstleistung ist, sondern die Optimierung der Kundenbindung, so könnte die Dauer einer Datenverarbeitung potenziell bis zum Lebensende des Kunden reichen. Eine strenge Auslegung im Sinne des Privatsphärenschutzes würde einige für die Unternehmen schmerzliche Begrenzungen bei den gängigen Praktiken der Datenverarbeitung bedeuten.

Das wirtschaftsnahe „Center for Democracy and Technology", eine amerikanische NGO[27], warnt vor einem „Datenpaternalismus" (2014: 8-9), wenn das Prinzip der Nutzer-Selbstbestimmung zugunsten einer stärkeren Verantwortung der Unternehmen aufgeweicht würde. Es sieht darin eine Einschränkung der Nutzer-Autonomie. Inwiefern allerdings solche Konflikte von Autonomie und Paternalismus tatsächlich bestehen, wird nicht thematisiert. Mit einiger Plausibilität lässt sich wohl sagen, dass dieser Paternalismus eher die wirtschaftliche Freiheit betrifft als die Autonomie der Nutzer.

[27] Das 1994 gegründete „Center for Democracy and Technology" hat rund 30 Mitarbeiter und ein beachtliches Budget von knapp über 4 Mio. Dollar. Es beschreibt sich auf seiner Website zwar als „champion of global online civil liberties and human rights, driving policy outcomes that keep the Internet open, innovative, and free". Da es jedoch fast ausschließlich von Internetkonzernen finanziert wird, ist eine gewisse Skepsis angebracht. Der Schwerpunkt dürfte eher darauf liegen, das Internet für die Wirtschaft „offen, innovativ und frei" zu halten.

Die richtige Balance von wirtschaftlicher Freiheit und individuellem Privatsphärenschutz zu finden, ist eine Aufgabe, die jede Gesellschaft für sich lösen muss. Wer allerdings die Forderung nach einem *Menschenrecht* auf Privatsphäre erhebt, der hat sich im Prinzip schon für Letzteres entschieden, denn der Spielraum für die Einschränkung fundamentaler moralischer Rechte ist generell nicht groß. Die Privatsphären-Aktivisten jedenfalls sehen bislang die wirtschaftliche Freiheit im Vorteil. Dave Eggers, der unten ausführlicher besprochen wird, stellt zum Thema Privatsphäre und Big Data fest: „Wir haben alles reguliert, die Luftfahrtindustrie, die Pharmaindustrie, wir haben Regeln für Nahrungsherstellung, für Wasser, all diese Dinge haben wir erfolgreich reguliert. Nur diesen einen Bereich lassen wir komplett ungeregelt." Der Vergleich ist ein starkes Instrument ethischer Überlegungen: Wenn wir von einem allgemein akzeptierten Prinzip abweichen (hier: Verbraucherschutz), dann ist diese Abweichung in besonderer Weise begründungspflichtig.

Eine technische Regulierung dürfte sich zwar als schwierig erweisen. Es ist ein ehernes Gesetz, dass jede Software Fehler hat, weshalb ein digitales Produkt nicht wie eine Bohrmaschine geprüft und mit einem CE-Kennzeichen versehen werden kann. Allerdings kann eine Regulierung auch bei der Marktstruktur ansetzen. Monopole unterlaufen die digitale Souveränität, weil sie Wahlmöglichkeiten einschränken. Wir kommen hier also auf die Feststellung zurück, dass ein Menschenrecht zu haben bedeutet, ein Recht auf eine gesellschaftliche Organisation zu haben, die der Realisierung dieses Menschenrechts entgegenkommt.

Mangelnde Regulierung beeinträchtigt die Nutzersouveränität auch auf andere Weise: Sie können ohne klare Regeln nicht klagen, d.h. die Ressourcen des Rechtsstaats nicht in Anspruch nehmen. Laut Informationen des Deutschen Instituts für Menschenrechte ist derzeit die Möglichkeit eines rechtlichen Vorgehens gegen Datenschutzverletzungen stark eingeschränkt. Gründe dafür seien stark fragmentierte oder gänzlich fehlende Gesetze, ein Mangel an kompetenten Anwälten und Richtern und ein häufig zu geringer Streitwert. „In der Folge bleiben zahlreiche Rechtsfragen in Ermangelung von Präzedenzfällen ungeklärt. Derartige Leitentscheidungen würden aber nicht nur Gerechtigkeit im Einzelfall herbeiführen, sondern auch die Rechtslage für vergleichbare Fälle präzisieren helfen" (DIM 2014a: 2).

Es ist ein Teufelskreis: Ohne Recht kein Klagen, aber ohne Klagemöglichkeit auch keine Rechtsentwicklung. Wenn die digitale Souveränität ausgerechnet beim Recht endet, zeigt dies, dass wir in der Praxis noch weit von einem Menschenrecht auf Privatheit entfernt sind.

3.5 Einzelkämpfer für ein digitales Menschenrecht auf Privatsphäre

Während sich die bisher referierten Forderungen in überwiegend vertrauten Bahnen bewegen – die einen mehr im Hinblick auf das VN-Völkerrechtssystem, die anderen mehr in Bezug auf europäisches Recht –, bringen einige Einzelkämpfer auch neue Aspekte eines digitalen Menschenrechts auf Privatsphäre ins Spiel. Bei diesen etwas unkonventionellen Beiträgen schwingen auch Visionen des „guten Lebens" im digitalen Zeitalter mit.

Enno Park und das Recht auf Pseudonymität

Enno Park ist ein deutscher Autor, Blogger und Kommunikationsberater. In einem Interview mit der „ZEIT", das schon ein paar Jahre zurückliegt, bezeichnet er Pseudonymität als ein digitales

Menschenrecht.[28] Diese Forderung, die mit dem Klarnamenzwang kollidiert, richtet sich an die Unternehmen der Internetwirtschaft, insbesondere Google. In einem Kunstprojekt nutzte er seinen echten Namen für sein Google+-Profil, aber was er dort von sich preisgab, war alles erfunden. Damit protestierte er gegen Googles Praxis, immer mehr Daten zu sammeln und zusammenzuführen.

Park leitet das Recht auf Pseudonymität aus dem Konzept der informationellen Selbstbestimmung ab. „Ein Mensch muss Hoheit über seine Identitäten haben dürfen und Hoheit darüber, welche öffentlich als zusammenhängend dargestellt werden und welche separat, quasi geheim bleiben sollen." Das betreffe z.B. Homosexuelle, Revolutionäre und andere, die ihre Interessen in der Öffentlichkeit nicht mit Klarnamen verfolgen können, ohne unverhältnismäßige Gegenreaktionen zu riskieren. In einem Leserkommentar wird angefügt, dass auch Beamte, die zu politischer Neutralität verpflichtet sind, ohne Pseudonyme sich online nicht politisch äußern könnten. Hinter dem Recht auf Pseudonymität steht der Gedanke, dass, wenn der virtuelle Raum Funktionen der klassischen Öffentlichkeit übernimmt, es den Menschen möglich sein muss, in den virtuellen Raum zu folgen – und zwar ohne auf ihren Rechten sitzenzubleiben. Weil Google, Facebook & Co. Öffentlichkeit bzw. deren digitale Infrastruktur herstellen, werden sie zum Adressaten eines Rechts auf Pseudonymität.

Zwar kann ein Nutzer derzeit nicht wirklich daran gehindert werden, sich unter einem Pseudonym zu registrieren. Aber ein Recht auf Pseudonymität würde auch bedeuten, dass Pseudonyme von einem Unternehmen unter Androhung von Strafe nicht aufgedeckt werden dürfen, sondern vielmehr aktiv geschützt werden müssen.

Ein immer wieder anzutreffender Einwand gegen Pseudonymität lautet, dass es ohne Klarnamenzwang zu einem Verfall der Sitten im virtuellen Raum käme, weil Akteure nicht mehr haftbar gemacht werden könnten für ihre Beiträge. Die oft wüsten Leserkommentare bei Online-Zeitungen scheinen einen solchen Sittenverfall zu bestätigen. Allerdings sind Sitten ein recht vages Konzept. Aus einer Menschenrechtsperspektive scheint es fragwürdig, das Freiheitsrecht der Pseudonymität durch das eher ästhetische Interesse an einem gepflegten Online-Dialog einzuschränken, den zu lesen niemand verpflichtet ist.

Pseudonymität ist mit Anonymität verwandt, dem Nichtbekanntsein. Kann das Unternehmen ein Pseudonym seinem Träger zuordnen, so schützt Pseudonymität nur gegen soziale andere. Kennt indes nur der Träger selbst sein Pseudonym, so geht es praktisch über in Anonymität. Diese kollidiert mit dem Geschäftsmodell der Internetwirtschaft und könnte deswegen ein wirksames Instrument zum Schutz der Privatsphäre sein. Wenn Park sagt, der einzige wirkliche Grund für den Klarnamenzwang bestehe im Gewinninteresse der Unternehmen und nicht in der Vision einer tugendhaften Online-Lebenswelt, so scheint er eigentlich ein Recht auf Anonymität zu fordern.

Eine interessante Perspektive zur Pseudonymität und Anonymität findet sich bei der israelischen Rechtsphilosophin Ruth Gavison (1980), die darin einen starken Hebel zum Schutz der Privatsphäre erblickt: Man stelle sich vor, jemand ruft in einer Menschenmenge „Hier ist der Präsident!" – es wäre um dessen Privatsphäre sofort geschehen (ebd.: 432). Unerkannt zu bleiben unterbindet Aufmerksamkeit, und die ist für Gavison der größte Feind der Privatsphäre: „What protects privacy is not the difficulty of invading it, but the lack of motive and interest of others to do so" (ebd.: 469). Heute investieren Staat und Unternehmen große Summen in Technologien der De-Anonymisierung, die Aufmerksamkeit, die sie ihren Bürgern und Nutzern dadurch schenken, hat beinah präsidentiellen Charakter. Unter einem Recht auf Anonymität wäre die Entwicklung solcher Fähigkeiten, die das Motiv des Beobachtens überhaupt erst erzeugen, problematisch.

---

[28] www.zeit.de/digital/datenschutz/2011-10/ennomane-google-klarnamen (6.2.2015).

Das Menschenrecht auf Anonymität wird auch von anderen Aktivisten gefordert, z.B. vom Forum d'Avignon in seiner digitalen Menschenrechtserklärung: „Everyone has the right to the [...] protection of his anonymity when he so requests." Auch die IRPC fordert es als einen Aspekt des Rechts auf Privatsphäre, verbunden mit dem Recht auf verschlüsselte Kommunikation (2014a: 2). Bislang wurde Verschlüsselung eher als eine Sache für politikferne Nerds betrachtet, zunehmend aber auch als Element des „Selbstdatenschutzes" für jedermann. Dabei wird sträflich übersehen, dass auch die beste Technik des Selbstdatenschutzes einen wunden Punkt hat, der darin besteht, dass die Politik sie einfach verbieten kann. Der britische Premier David Cameron hat unlängst die Absicht bekundet, dies mit der Verschlüsselung zu tun.

Dave Eggers und die Moral von der Geschichte

Der Autor des Weltbestsellers „The Circle" hat im Interview mit der FAZ eine „neue Erklärung der Menschenrechte, über die Rechte von Individuen im digitalen Zeitalter und über den Schutz unserer Privatsphäre" gefordert.[29] Dieses Recht auf Privatsphäre müsse beinhalten, „sein digitales Profil zu kontrollieren, sein digitales Ich, seine Einkaufsgeschichte, seine Daten. All die Dinge, die jetzt zu Geld gemacht werden, ohne darüber zu informieren, ohne Kontrolle. Heute ist es pseudolegal, diese Daten zu sammeln und zu verkaufen. Man hat nicht das Recht, es zu verbieten."

Eggers' Klage über die vom Datensubjekt selbst nicht kontrollierbare Kommodifizierung und Kommerzialisierung der Privatsphäre erinnert an eine Zeit vor der Aufklärung, als Menschen im absolutistischen Staat noch wenig Rechte hatten. Die These des britischen Philosophen John Locke, dass der Mensch ein Eigentum an sich selbst habe und an den Dingen, die er sich durch Arbeit aneigne, war in diesem Kontext revolutionär: „[E]very man has a property in his own person", so Locke (zitiert aus Solove 2002: 1112). Diese These ist auch heute wieder interessant, denn wenn das Individuum durch seine Informationen konstituiert ist, dann kann argumentiert werden, dass es, ähnlich wie beim Urheberrecht, auch ein Eigentumsrecht an seinen Informationen hat. Deswegen verbietet sich deren kommerzielle Vermarktung ohne Einwilligung der Person.

Zwar ist eine solche Konzeption der Privatsphäre angreifbar. Es ließe sich argumentieren, dass der Wert der Daten erst durch die Big-Data-Verarbeitung zustande kommt, sodass ein Unternehmen mit derselben Begründung einer „Aneignung durch Arbeit" ein Besitzrecht auf die Daten des Individuums erheben könnte (vgl. Solove 2002: 1113). Mit Eggers kann diese Schraube aber gedanklich noch ein Stück weitergedreht werden, auch wenn er das selbst nicht so sagt: Denn wenn die Unternehmen personenbezogene Daten bearbeiten, die eben nicht vom Individuum abzulösen sind, so bearbeiten sie zugleich auch das Individuum mit, und das untergräbt dessen Recht auf die eigene Person.

Ähnliche Überlegungen haben sicherlich auch andere angestellt. Eggers ist indes einer der wenigen, welcher die digitale Überwachung in den Begriffen einer moralischen Orientierungslosigkeit beschreibt, die nicht nur in Bezug auf Wirtschaftsunternehmen sichtbar wird, sondern auch im gesellschaftlichen Umgang der Menschen miteinander. So beklagt er die zunehmende private Überwachung, z.B. wenn die Menschen allerorten Minikameras installieren würden oder wenn ein E-Mail-Programm den Sender darüber informiere, ob eine Nachricht gelesen wurde. Zu denken wäre auch an Techniken wie die neue „Google Glas"-Brille – es sind gewissermaßen digitale Kleinwaffen, welche die Nutzer selbst einsetzen, die aber eine Massenüberwachung der anderen Art darstellen und ebenfalls freiheitseinschränkende Wirkung haben können.

---

[29] www.faz.net/aktuell/feuilleton/buecher/fuer-eine-neue-erklaerung-der-menschenrechte-der-autor-dave-eggers-im-gespraech-13089419-p2.html (29.12.2014).

In seinem Roman beschreibt Eggers eine global dominierende Internetfirma, die eine Ideologie der absoluten Transparenz propagiert, um das Leben der Menschen offener, ehrlicher und fürsorgender und die Politik demokratischer zu machen. Die Menschen sind begeistert. Damit möchte uns Eggers den Spiegel vorhalten. Die Situation ist gefährlich, weil ein Ungleichgewicht eingetreten ist von mangelndem gesellschaftlichen Problembewusstsein einerseits und einem wachsenden Missbrauchspotenzial andererseits. Derzeit kontrollieren relativ wenige Unternehmen einen enormen Bereich der digitalen Infrastruktur, und es sei daher „nicht schwer, sich vorzustellen, wie sich die aktuelle Lage entwickeln könnte, wenn sich diejenigen, die die Schleusen kontrollieren, entschließen, ihre Macht zu missbrauchen".

Es ist also eine Sache, ob und wie stark bestimmte Menschenrechte heute bereits verletzt werden. Die andere Sache ist, dass sie jederzeit noch viel massiver verletzt werden könnten. Die Gesellschaft ist in einem prekären Zustand, weil bislang alles gut ging, aber eigentlich ist sie ohne „moralischen Kompass" zu weit in fremdes Terrain marschiert und deshalb nicht mehr – um Eggers' Gedanken mit Kant zuzuspitzen – im Zustand gesicherter Rechte. Um die Menschen aus ihrer Lethargie zu reißen, bräuchte es, so Eggers, einen „moralischen Schock": „Wie vor vielen Jahren, als in Schottland das Schaf geklont wurde. Da gab es einen riesigen Aufschrei, auch unter Wissenschaftlern, und kurz darauf Gesetze auf der ganzen Welt, die das Klonen von Menschen verbieten. Nur so kann man es verhindern."

Tim Berners-Lee und das offene Netz

Tim Berners-Lee ist seit seiner Erfindung des World Wide Web der Idee eines offenen, den Menschen dienenden Internets verpflichtet. Daran erinnert er heute erneut, 25 Jahre nach der Einführung des „www" im Jahr 1990 und nachdem klar wurde, wie wirtschaftliche und staatliche Interessen das Internet mittlerweile dominieren. Berners-Lee fordert nicht weniger als eine digitale „Magna Carta"[30], um die derzeitige weitgehende Rechtlosigkeit im Internet zu beenden, die meist zu Lasten der Individuen geht. Die englische Magna Carta aus dem Jahr 1215 gilt als ein Vorläufer verbriefter Menschen- und Freiheitsrechte sowie als Meilenstein von Demokratie und Rechtsstaat.

Prinzipiell neue Menschenrechtsinhalte bietet Berners-Lee nicht an; seine Forderung nach einer Magna Carta ist zuvorderst ein politisches Statement. Sie geht allerdings insofern über die beschriebenen Beispiele hinaus, als sie, ähnlich wie Eggers, aber weniger alarmistisch, mit dystopischen Szenarien einer Gesellschaft begründet wird, die weit hinter ihre eigenen politischen Standards zurückzufallen droht. Im Kern ist sein Argument, dass die Privatsphäre zu derjenigen Stellschraube geworden ist, welche die grundlegenden Normen der Gesellschaft reguliert.

Der Abbau der Privatsphäre bereite einer willkürlichen Diskriminierung den Weg. So müsste in Zukunft sichergestellt sein, „[that] I can communicate with everybody and I won't find my packets suddenly delayed because I go to an abortion site and my ISP provider disapproves of abortions". Das wäre ein Fall davon, dass Unternehmen ihre Macht missbrauchen und die „Schleusen" selektiv dicht machen. Demokratisch ausgehandelte Normen und Freiheiten könnten so niederschwellig unterlaufen werden. Es bräuchte daher Vorkehrungen, damit „the internet is neutral politically from the point of view of race, colour, creed, sexual preference – all the things where we do not discriminate". Letztlich wird dadurch die moralische Gleichheit geschützt, die eine Grundnorm moderner Demokratien ist.

In dieser Spur macht Berners-Lee auch darauf aufmerksam, dass ein offenes Internet, in dem die Privatsphäre gesichert ist, nicht nur eine Voraussetzung für die Geltung der klassischen

[30] www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web (15.12.2014).

Freiheitsrechte ist, wie sie im schon Zivilrechtspakt verankert sind. Dieses Argument vertreten auch andere. Berners-Lee geht weiter und stellt auch einen Bezug von Privatsphäre und jenen kollektiven Gütern her, ohne welche einige der Menschenrechte der sogenannten „zweiten Generation", wie sie im „Sozialpakt" (1966) verankert sind, nicht realisiert werden könnten. „Unless we have an open, neutral internet we can rely on without worrying about what's happening at the back door, we can't have open government, good democracy, good healthcare, connected communities and diversity of culture." So betrachtet ist, wie man anfügen könnte, die Privatsphäre nicht nur ein Aspekt der Bürgerrechte, sondern sie müsste auch ein Thema der Sozialdemokratie sein.

In modernen, hoch ausdifferenzierten Gesellschaften sind viele Interessen, Prozesse und Güter rechtlich geschützt und/oder reguliert. Das gilt für alle Bereiche der Gesellschaft, insbesondere die Wirtschaft. Sie klagt häufig über eine Überregulierung, die das Wachstum behindere, aber Berners-Lee erinnert auch daran, dass gerade kommerzielle Interessen wie das Copyright sehr gut geschützt seien – so „gut" jedenfalls, dass Menschen für Rechtsverstöße im Gefängnis landen würden. Vergleichbare Sanktionen gäbe es im Bereich der Demokratie und der Privatsphäre hingegen bislang nicht. „None of this has been set up to preserve the day to day discourse between individuals and the day to day democracy that we need to run the country."

4. Realisierungschance eines neuen Menschenrechts

Abschließend sollen die zentralen Punkte der Studie noch einmal zusammengebunden und dabei einige Probleme reflektiert werden, die weniger die ethischen Überlegungen als vielmehr den Aspekt der politischen Mobilisierung betreffen, der in der bisherigen Argumentation eher ausgeblendet wurde. Letztlich sind die Menschenrechte ja immer auch ein politisches Projekt.

Zwei weit auseinanderliegende Positionen

Der Diskurs über ein neues digitales Menschenrecht auf Privatsphäre hat zwei voneinander unabhängige Schwerpunkte. In Bezug auf die staatliche Überwachung wirkt der von Deutschland und Brasilien angestoßene VN-Prozess als Katalysator einer transnationalen Kampagne. Ein wirklich neues Menschenrecht wird darin nicht gefordert und wäre wohl auch nicht erforderlich. Navi Pillay resümiert in ihrem Bericht, dem von niemandem widersprochen wurde: „International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data" (2014: 15). Das Problem besteht nicht in fehlenden Völkerrechtsnormen, sondern in deren zeitgemäßer Interpretation und Durchsetzung.

Der andere Schwerpunkt des Diskurses betrifft den Bereich der wirtschaftlichen Datenverarbeitung. Der Befund ist sehr ähnlich: Viele der Forderungen nach einem digitalen Menschenrecht auf Privatsphäre greifen Datenschutz-Prinzipien auf, insbesondere das Recht auf „informationelle Selbstbestimmung", die im europäischen Kontext schon relativ gut realisiert sind. Auch hier liegt das zentrale Problem in der „Compliance". Ganz neue inhaltliche Aspekte finden sich im Diskurs der Aktivisten nicht, auch wenn einige der ins Feld geführten Stichworte Anlass für interessante ethische Reflexionen bieten.

Die beiden Diskurse, die völlig konträre Ansätze zum Schutz der Privatsphäre verfolgen (Verantwortung beim Nutzer vs. Verantwortung beim Datenverarbeiter), laufen bislang parallel. Soll es tatsächlich ein neues Menschenrecht auf Privatsphäre im digitalen Zeitalter geben, müssten die beiden Ansätze irgendwann miteinander verbunden werden. Dabei scheint mir die Ausweitung des existierenden Völkerrechts (und damit des Prinzips, dass der Datenverarbeiter die Verantwortung für den Schutz der Privatsphäre hat) auf den Bereich der Wirtschaft sinnvoller, als andersherum mit dem Konzept der Kontrolle zu einem internationalen Menschenrecht aufzuschließen bzw. ein ganz neues zu bilden – zumal von Experten mittlerweile auch grundlegende Zweifel angemeldet werden, ob das Konzept der Kontrolle nicht schon der Vergangenheit angehöre.

Ein deutscher Sonderweg?

Es überrascht ein wenig, dass deutsche Aktivisten im transnationalen Diskurs über ein neues digitales Menschenrecht auf Privatsphäre praktisch nicht vertreten sind. Woran liegt das? Es könnte zum einen mit dem relativ hohen Datenschutzniveau in Deutschland zu tun haben, was einerseits den Problemdruck reduziert, andererseits vielleicht zu einer gewissen Scheu vor einer als zu plakativ empfundenen Menschenrechtsrhetorik führt. Über einen mangelnden öffentlichen Diskurs über die Gefährdung der Privatsphäre kann man sich in Deutschland ansonsten nicht beklagen.[31]

[31] Vgl. Schaar (2014), Aust/Amman (2014), Albrecht (2014), um nur einige wenige Beispiele zu nennen.

Andererseits fällt auf, dass hierzulande die digitale Herausforderung auch anders diskutiert wird, nämlich eher unpolitisch. Konzepte des Selbstdatenschutzes und besonders die Medienkompetenz sind nicht nur eine tragende Säule der Datenschutz-Strategie der Bundesregierung, wie dies etwa aus dem Koalitionsvertrag und der Digitalen Agenda hervorgeht, sondern sie werden auch im zivilgesellschaftlichen Bereich immer wieder artikuliert. Tagungen zum Thema Privatsphäre enden gerne mit der Forderung, die Medienkompetenz der Bürger zu stärken.

Doch bei aller Wertschätzung der liberalen Tugend des wehrhaften Bürgers könnte die oben referierte Kritik am Konzept der Kontrolle auch Anlass sein, sich in Deutschland stärker mit den ethischen und politischen Dimensionen von Privatsphäre auseinanderzusetzen, statt das Thema in den Bereich der (Jugend-)Bildung zu verschieben. Spätestens wenn der Staat versucht, im Namen der Sicherheit mit der Verschlüsselung auch ein Stück weit Privatsphäre zu verbieten, wie dies derzeit in Großbritannien angedacht wird, hat auch die exzellenteste Medienkompetenz keinen Wert mehr in Bezug auf den Schutz der Privatsphäre.

Politische Realisierungschancen – ein steiniger Weg zum neuen Menschenrecht

Die Studie hat die Forderung nach einem digitalen Menschenrecht auf Privatsphäre nicht unter politischen Gesichtspunkten betrachtet (geschweige denn unter juristischen). Ein paar abschließende Stichworte genügen, um zu zeigen, dass der Weg zu einer Novellierung des völkerrechtlichen Privatsphärenschutzes steinig sein wird. Generell können „Treiber" und „Bremser" einer völkerrechtlichen Kodifizierung eines neuen digitalen Menschenrechts auf Privatsphäre unterschieden werden.

Als Treiber ist bislang nur die Zivilgesellschaft erkennbar, – in einer offenen Demokratie, in der das Volk die politische Agenda mitbestimmt – zwar kein geringer Faktor, allerdings hält sich die politische Empörung in Grenzen, sie hat bislang eigentlich nur unmittelbar nach den Snowden-Enthüllung mobilisierend gewirkt (und auch nur in Bezug auf die staatliche Massenüberwachung). Ein bremsender Faktor liegt darin, dass bislang nur solche Rechte zu Menschenrechten gemacht wurden, die innerhalb der westlichen Staaten bereits überwiegend realisiert waren. Ein derartiger Normenexport ist beim Thema Privatsphäre nicht möglich – Privacy International stuft z.B. die USA als eine endemische Überwachungsgesellschaft ein. Dazu kommen praktische Probleme, die damit zusammenhängen, ein sehr fluides Feld abschließend zu regeln. Ein Menschenrecht auf Privatheit wird niemals den Grad an Differenzierung erreichen wie z.B. die geplante EU-Datenschutz-Grundverordnung.

Im internationalen Bereich dürfte nicht nur das Sicherheitsinteresse westlicher Staaten bremsend wirken. Es steht auch die Glaubwürdigkeit der westlichen Vorreiterrolle beim Thema Menschenrechte auf dem Spiel. Westliche Staaten dürften schwerlich einem Menschenrecht zustimmen, das einen normativen Standard schafft, der dann von Autokratien gegen sie gerichtet werden kann. Das gesamte Menschenrechtsregime könnte dadurch in Schieflage geraten. Der Punkt ist freilich, dass dies infolge einer weltweiten Bewusstseinsbildung zum Schutz der Privatsphäre auch ohne ein formales Menschenrecht geschehen könnte. In diesem Fall wäre es politisch klug, ähnlich wie beim Thema Nuklearwaffen Bemühungen um eine sukzessive Einhegung der Privatsphärenverletzungen einzuleiten.

5. Quellen- und Literaturverzeichnis

Quellen:

American Civil Liberties Union (2014): Privacy Rights in the Digital Age. A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union, New York.

Center for Democracy and Technology (2014): Letter to the Federal Trade Commission, January 10, 2014, www.cdt.org (25.1.2015).

Deutsches Institut für Menschenrechte (2014a): „Zugang zu Datenschutz-Rechtsbehelfen in EU-Mitgliedstaaten" – eine Studie der EU-Grundrechteagentur. Hintergrundinformationen zur Forschung in Deutschland (ohne Autor), Bonn.

Deutsches Institut für Menschenrechte (2014b): Neufassung des Antiterrordateigesetzes: Gesetzgeber muss Menschenrechtsschutz ernst nehmen, in: aktuell 2/2014, Autor: Eric Töpfer, Bonn.

Electronic Frontier Foundation/Article 19 (2014): Necessary & Proportionate. International Principles on the Application of Human Rights Law to Communications Surveillance.

Fischermann, Thomas (2011): „Pseudonymität ist ein digitales Menschenrecht", Interview mit Enno Park, in: ZEIT Online, www.zeit.de/digital/datenschutz/2011-10/ennomane-google-klarnamen (5.1.2015).

Forum d'Avignon (2014): Preliminary Declaration of the Digital Human Rights, http://sandbox.spintank.fr/index-en.php (16.2.2015).

Internet Rights and Principles Coalition (2014a): 10 Internet Rights & Principles, http://internetrightsandprinciples.org/site/campaign/.

Internet Rights and Principles Coalition (2014b): Die Charta der Menschenrechte und Prinzipien für das Internet, Dynamische Koalition für Internet-Rechte und -Prinzipien – Internet Governance Forum der Vereinten Nationen.

Kiss, Jemima (2014): An online Magna Carta: Berners-Lee calls for bill of rights for web, in: The Guardian, 12.3.2014, www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web (15.12.2014).

Madrid Resolution (2009): International Standards on the Protection of Personal Data and Privacy, www.privacycommission.be/en/node/3887 (12.1.2015).

OECD (2013): Exploring Data-Driven Innovations as a New Source of Growth. Mapping the Policy Issues Raised by „Big Data", OECD Digital Economy Papers, No. 222, OECD Publishing, http://dx.doi.org/10.1787/5k47zw3fcp43-en.

Omand, David/Bartlett, Jamie/Miller, Carl (2014): „A balance between security and privacy online must be struck …", Demos: London, www.demos.co.uk.

Pillay, Navi (2014): The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights, VN-Dokument A/HRC/27/37, 30.6.2014.

Podesta, John (2014): Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, Washington, D.C.

Privacy International (2014): OHCHR consultation in connection with General Assembly Resolution 68/167 „The right to privacy in the digital age", gemeinsam mit: Access, Electronic Frontier Foundation, Article 19, Association for Progressive Communications, Human Rights Watch, World Wide Web Foundation.

Ustaran, Eduardo (2014): The evolution of consent, www.linkedin.com/pulse/20140327085821-24251273-the-evolution-of-consent (15.2.2015).

Weidermann, Volker (2014): Wir brauchen eine neue Erklärung der Menschenrechte, Interview mit Dave Eggers, in: FAZ, www.faz.net/aktuell/feuilleton/buecher/fuer-eine-neue-erklaerung-der-menschenrechte-der-autor-dave-eggers-im-gespraech-13089419-p2.html (29.12.2014).

Writers Against Mass Surveillance (2013): A Stand for Democracy in the Digital Age, www.change.org/p/a-stand-for-democracy-in-the-digital-age-3 (16.2.2015).

Literatur:

Albrecht, Jan Philipp (2014): Finger weg von unseren Daten! Wie wir entmündigt und ausgenommen werden, Knaur: München.

Aust, Stefan/Amman, Thomas (2014): Digitale Diktatur, Econ: Berlin.

Birrer, Frans A. J. (2005): Data mining to combat terrorism and the roots of privacy concerns, in: Ethics and Information Technology, Vol. 7, S. 211-220.

Brey, Philip (2005): Editorial introduction – Surveillance and privacy, in: Ethics and Information Technology, Vol. 7, S. 183-184.

Bruin, Boudewijn De (2010): The Liberal Value of Privacy, in: Law and Philosophy, Vol. 29 (5), S. 505-534.

Capurro, Rafael (2005): Privacy. An intercultural perspective, in: Ethics and Information Technology, Vol. 7, S. 37-47.

Deutsches Institut für Menschenrechte (2014): „Zugang zu Datenschutz-Rechtsbehelfen in EU-Mitgliedstaaten" – eine Studie der EU-Grundrechteagentur. Hintergrundinformationen zur Forschung in Deutschland, hrsg. vom DIM: Berlin.

Erk, Christian (2012): What makes a Right a Human Right? The Philosophy of Human Rights, in: Schweidler, Walter (Hrsg.): Human Rights and Natural Law. An Intercultural Philosophical Perspective, Academia: Sankt Augustin, S. 101-131.

Ernst, Gerhard/Sellmaier, Stephan (Hrsg.): Universelle Menschenrechte und partikulare Moral, Kohlhammer: Stuttgart.

Ess, Charles, (2005): „Lost in translation?" Intercultural dialogues on privacy and information ethics (Introduction to special issue on Privacy and Data Privacy Protection in Asia), in: Ethics and Information Technology, Vol. 7, S. 1-6.

Ess, Charles/Thorseth, May (2008): Kant and information ethics, in: Ethics and Information Technology, Vol. 10, S. 205–211.

Floridi, Luciano (2005): The ontological interpretation of informational privacy, in: Ethics and Information Technology, Vol. 7, S. 185-200.

Foucault, Michel (1976): Überwachen und Strafen. Die Geburt des Gefängnisses, Suhrkamp: Frankfurt a. M.

Garfinkel, Simon (2000): Database Nation. The Death of Privacy in the 21st Century, O'Reilly & Associates: Sebastopol.

Gavison, Ruth (1980): Privacy and the Limits of Law, in: The Yale Law Journal, Vol. 89 (3), S. 421-471.

Hinsch/Janssen (2006): Menschenrechte militärisch schützen. Ein Plädoyer für humanitäre Interventionen, Bundeszentrale für politische Bildung: Bonn.

Kitiyadisai, Krisana (2005): Privacy rights and protection: foreign values in modern Thai context, in: Ethics and Information Technology, Vol. 7, S. 17-26.

Lyon, David (2001): Facing the future: Seeking ethics for everyday surveillance, in: Ethics and Information Technology, Vol. 3, S. 171-181.

Mahoney, Jon (2008): Liberalism and the Moral Basis for Human Rights, in: Law and Philosophy, Vol. 27 (2), S. 151-191.

McDonagh, Maeve (2013): The Right to Information in International Human Rights Law, in: Human Rights Law Review, Vol. 13 (1), S. 25-55.

Michelfelder, Diane P. (2001): The moral value of informational privacy in cyberspace, in: Ethics and Information Technology, Vol. 3, S. 129-135.

Mill, John Stuart (1976 [1871]): Der Utilitarismus, Reclam: Stuttgart.

Montesquieu, Baron de (1950): Vom Geist der Gesetze, Walter de Gruyter & Co: Berlin.

Morgenroth, Markus (2014): Sie kennen dich! Sie haben dich! Sie steuern dich! Die wahre Macht der Datensammler, Droemer: München.

Myskja, Bjorn K. (2008): The categorical imperative and the ethics of trust, in: Ethics and Information Technology, Vol. 10, S. 213-220.

Nagel, Thomas (2002): Concealment and Exposure & Other Essays, Oxford University Press: Oxford.

Nardin, Terry (Hrsg) (1996): The Ethics of Peace and War. Religious and Secular Perspectives, Princeton University Press: Princeton.

Nida-Rümelin, Julian (2005): Über menschliche Freiheit, Reclam: Stuttgart.

Nissenbaum, Helen (1998): Protecting Privacy in an Information Age: The Problem of Privacy in Public, in: Law and Philosophy, Vol. 17 (5/6), S. 559-596.

Regan, Priscilla M. (1995): Legislating privacy: Technology, Social Values and Public Policy, University of North Carolina Press

Rössler, Beate (2001): Der Wert des Privaten, Suhrkamp: Frankfurt a. M.

Schaar, Peter (2014): Wie wir in Zukunft unsere Daten schützen, Aufbau Verlag: Berlin.

Sobel, Richard (2004): The Right To Travel And Privacy: Intersecting Fundamental Freedoms, in: The John Marshall Journal of Information Technology & Privacy Law, Vol. 30 (4), S. 639-666.

Solove, Daniel J. (2002): Conceptualizing Privacy, in: California Law Review, Vol. 90 (4), S. 1087-1155.

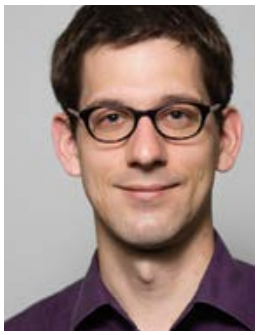
The Madrid Resolution (2009): International Standards on the Protection of Personal Data and Privacy, International Conference of Data Protection and Privacy Officers, Madrid.

Vitale, Marco Quiroz (2014): Control Over Personal Data, Privacy And Administrative Discretion In Europe And The USA: The Paradox Of Italian „Data Protection Authority", in: The John Marshall Journal of Information Technology & Privacy Law, Vol. 30 (4), S. 721-756.

Westin, Alan F. (1970): Privacy and Freedom, Atheneum: New York.

Whitman, James Q. (2004): The Two Western Cultures of Privacy: Dignity Versus Liberty, in: Faculty Scholarship Series, Paper 649, Vol. 113, S. 1151-1221, http://digitalcommons.law.yale.edu/fss_papers/649.

Über den Autor



Dr. Max-Otto Baumann
geb. 1982

Dr. Baumann studierte in Heidelberg Politikwissenschaft, Philosophie und Physik und wurde im Fachbereich Internationale Beziehungen promoviert. Von 2012 bis 2015 war er Akademischer Mitarbeiter am John Stuart Mill Institut in Heidelberg im Projekt „Öffentlichkeit und Privatheit in der Digitalen Revolution". Nun forscht er am Deutschen Institut für Entwicklungspolitik (DIE), Bonn.

DIVSI Veröffentlichungen

Studien

Milieu-Studie zu Vertrauen und Sicherheit im Internet, 2012, Aktualisierung 2013
Meinungsführer-Studie: Wer gestaltet das Internet?, 2012
Entscheider-Studie zu Vertrauen und Sicherheit im Internet, 2013
Studie zu Freiheit versus Regulierung im Internet, 2013
U25-Studie: Kinder, Jugendliche und junge Erwachsene in der digitalen Welt, 2014
Studie zu Bereichen und Formen der Beteiligung im Internet, 2014
Braucht Deutschland einen Digitalen Kodex?, 2014
Wissenwertes über den Umgang mit Smartphones, 2014
Daten: Ware und Währung, 2014
U9-Studie: Kinder in der digitalen Welt, 2015
Beteiligung im Internet – Wer beteiligt sich wie?, 2015

Diskussionsbeiträge

Dominic Völz, Timm Christian Janda: Thesen zur Netzpolitik – Ein Überblick, 2013
Christina Heckersbruch, Ayten Öksüz, Nicolai Walter, Jörg Becker, Guido Hertel:
Vertrauen und Risiko in einer digitalen Welt, 2013
Göttrik Wewer: Digitale Agenda 2013–2017: Netzpolitik im neuen Deutschen Bundestag, 2013
Miriam Meckel, Christian Fieseler, Jan Gerlach: Der Diskurs zur Netzneutralität, 2013
Dominic Völz, Timm Christian Janda: Netzpolitik in Deutschland – Wahlprogramme,
Koalitionsvereinbarung, Regierungserklärung, 2014

Bücher

Thomas Fischermann, Götz Hamann: Zeitbombe Internet, Gütersloher Verlagsgruppe, 2012
Hans Peter Bull: Netzpolitik – Freiheit und Rechtsschutz im Internet, Nomos Verlag, 2013
Utz Schliesky, Christian Hoffmann, Anika D. Luch, Sönke E. Schulz, Kim Corinna Borchers:
Schutzpflichten und Drittwirkung im Internet – Das Grundgesetz im digitalen Zeitalter,
Nomos Verlag, 2014