“You Have Zero Privacy Anyway – Get Over It”[1]
Von «Personal Privacy Management» zu «Network Publicy Governance»

Andréa Belliger & David J. Krieger

Scott McNealy, damaliger CEO von Sun Microsystems, erklärte 1999 einer Gruppe von schockierten Journalisten: «You have zero privacy anyway. Get over it» (Sie haben sowieso keine Privatheit. Lassen Sie das Thema hinter sich). Er konnte damals nicht ahnen, wie oft dieser Satz in den kommenden Jahren zitiert werden sollte.[2] Die Aussage McNealys drückt eine Haltung aus, die schon damals viele vertraten und die heute aktueller denn je ist. Ängste und Unsicherheit angesichts des Verlustes der Privatheit und die damit zusammenhängenden Folgen für Individuen und die Gesellschaft sind allgegenwärtig. Angesichts von Entwicklungen wie dem Web 2.0, Social Media, Big Data, kommerzielles Profiling und dem immer stärkeren Ruf nach einer datengetriebenen Gesellschaft steht die Sorge um Privatheit und Datenschutz im Fokus. Es scheint, als ob eine datengetriebene Gesellschaft und die vielversprechenden Möglichkeiten, die die Nutzung von Daten in allen Bereichen mit sich bringen, unweigerlich die Preisgabe persönlicher Informationen und den «gläsernen Menschen» erfordern. Auf der anderen Seite werden immer strengere Datenschutzregulationen wie z.B. die Datenschutz-Grundverordnung der EU, die im Mai 2018 in Kraft trat, implementiert. Der Eindruck entsteht, dass Privatheit und Datenschutz als Bollwerk und letzter Widerstand gegen eine ungehinderte Sammlung und Nutzung persönlicher Daten verstanden wird. Es scheint, als ob hier zwei Welten aufeinanderprallen, einerseits die neue digitale Welt, in der Daten als das «neue Öl» gelten, als Quelle von Wertschöpfung und Innovation, und andererseits die alte Welt, in der das Zurückhalten und die Geheimhaltung von Information als Garanten von Freiheit, Autonomie und Menschenwürde betrachtet werden.

Natürlich gab es Datenschutz auch 1999 als McNealy dessen Nutzlosigkeit erklärte. Es stellt sich aber die Frage, inwiefern es zutrifft, dass Privatheit in der digitalen Welt tatsächlich kaum noch zu retten ist und wir es tatsächlich aufgeben sollten, dies zu versuchen. Man könnte nämlich dem ersten Satz von McNealy, bei dem es um den Verlust der Privatheit geht zustimmen, ohne dies aber beim zweiten Satz, dass wir die Privatheit hinter uns lassen sollten, ebenfalls zu tun. Ganz im Gegenteil sollten wir gerade auf dem Hintergrund einer zunehmenden Bedrohung der Privatheit, alles daransetzen, Daten zu schützen und Privatheit wiederherzustellen. Es stellt sich vielmehr die Frage, was der zweite Satz von McNealy eigentlich bedeutet. Was heisst „Get over it“? Wenn Privatheit nicht gerettet werden kann, *wie* sollen wir Privatheit hinter uns lassen? Wohin sollen wir gehen und auf welchen Wegen, wenn der Weg zurück in die Welt der Geheimnisse und der Intransparenz nicht mehr gangbar ist? Natürlich werden diese Fragen erst dann wichtig, wenn es sich tatsächlich herausstellt, dass Datenschutz nicht funktioniert, wirtschaftlich kontraproduktiv ist oder letzten Endes nicht einmal das ist, was Menschen möchten. Wer will schliesslich auf die vielfältigen Vorteile der Datennutzung, wie z.B. personalisierte Produkte und Dienstleistungen in den Bereichen inklusiv Gesundheit, Bildung und Forschung verzichten? Privatheit ist mit einem Paradox konfrontiert. Das gut dokumentierte «Paradox der Privatheit» (Privacy Paradox) beschreibt, dass Menschen zwar

[1] “Sie haben sowieso keine Privatheit. Lassen Sie das Thema hinter sich”
[2] https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

sagen, sie seien über den Verlust von Privatheit besorgt, aber ganz anders handeln und ihre eigenen Daten freiwillig preisgeben.[3]

"You have zero privacy anyway."

In Bezug auf die Behauptung, dass Privatheit tot ist, spricht einiges dafür, dass alle Versuche, Daten zu schützen oder geheim zu halten, vergebens sind, oder wenigstens ineffektiv. Kaum ein Tag vergeht ohne Medienberichte über die neueste Datenschutzverletzung, ein Datenleck oder ein Datenhack. Kein Informationssystem und keine Datenbank, egal ob es sich um den Heim-PC, Firmen- oder gar Regierungsinfrastruktur handelt, scheint sicher zu sein. Cyberattacken, ob kriminell oder politisch motiviert, nehmen rasant zu.[4] Es ist zudem anzunehmen, dass das, was in den Medien bekannt wird, nur die Spitze des Eisbergs ist und viele Datenverluste gar nicht erst gemeldet oder entdeckt werden. Hinzu kommt die Tatsache, dass die Täter kaum eruiert werden können und wenn sie ausnahmsweise mit grossem Aufwand gefunden werden, nicht belangt werden können. Sicherheitsexperten geben zu, dass alles gehackt werden kann, wenn genügend Aufwand und Ressourcen zur Verfügung stehen. Privatheits- und Datenschutzregulationen ändern daran wenig.[5]

Hacking ist natürlich illegal und man könnte darauf hoffen, dass mit noch mehr IT-Sicherheitsanstrengungen oder besserer Gesetzgebung dem Datendiebstahl Einhalt geboten werden könnte. Aber auch wenn alle Sicherheitslücken gestopft werden könnten, ist Privatheit immer noch in Gefahr, da es neben der illegalen die legale Sammlung persönlicher Daten gibt. Kommerzielles Profiling ist seit vielen Jahren gang und gebe.[6] Daten-Broker wie Acxiom und Oracle, um nur zwei aus einer Vielzahl an Unternehmen zu nennen, sind darauf spezialisiert, personenbezogene Daten aus vielen verschiedenen Quellen zu sammeln, zu aggregieren und insbesondere zwecks gezielter Werbung oder für Themen des Risikomanagements weiter zu verkaufen. Acxiom behauptet stolz 5000 Datenpunkte von über 700 Millionen Menschen zu besitzen. Diese Daten beziehen sich auf Alter, Geschlecht, Bildungstand, Arbeitssituation, politische Ansichten, Beziehungsstatus, Familienstatus, Anzahl Kinder, Ethnizität, Religion, Gesundheit, Konsumverhalten, Hobbies, Mediennutzung, Darlehen, Einkommen, Fahrzeugbesitz und -nutzung, Immobilien, Finanz- und Versicherungsinformationen, Kredite, , Konsum von Alkohol und Tabak, Social Media-Nutzung, Wohnsituation, etc.[7] Die Praktiken der Datenbroker wurden in letzter Zeit wegen des «Skandals» um die Nutzung von Facebook-Daten durch die Firma Cambridge Analytica während des Wahlkampfes von Donald Trump in den USA und im Kontext des Brexit in der Öffentlichkeit diskutiert. Obwohl Datenbroker behaupten, ganz legal zu handeln und Datenschutzregulierungen zu achten, steht der grossangelegten Datenanalyse durch Korrelation der Daten aus unterschiedlichen Quellen und der De-Anonymisierung bzw. Re-Identifizierung nichts im Wege und individuelle Personen können problemlos identifiziert werden.[8]

---

[3] Vgl. dazu die Literatur zum Thema Privacy Paradox z.B. Barnes (2006); Norberg/Horne/Horne (2007); Brandimarte/Acquisti/Loewenstein (2012).

[4] https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

[5] Vgl. dazu Wikipedia zu Sicherheitslücken https://en.wikipedia.org/wiki/Vulnerability_(computing). Siehe auch https://www.washingtonexaminer.com/fbi-reminds-us-that-everything-can-be-hacked.

[6] Vgl. dazu den Bericht von W. Christl, "Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions," Cracked Labs, Vienna, June 2017. http://crackedlabs.org/en/corporate-surveillance

[7] Vgl. dazu den Bericht von Christl (2017: 64).

[8] Vgl. dazu Wikipedia https://en.wikipedia.org/wiki/De-anonymization.

Aber auch wenn persönliche Daten nicht durch Hacking oder kommerzielles Profiling in die Öffentlichkeit gelangen, so häufig doch dadurch, dass man persönliche Daten freiwillig und selbst preisgibt. In den verschiedenen Sozialen Medien, Communities, Foren, Apps und auf Plattformen werden Daten und Informationen ohne Bedenken preisgegeben. Diese Daten und Informationen werden oft von den Plattform- und Dienstleistungsprovidern als Teil ihres Geschäftsmodells an Partner oder Dritte weiterverkauft. Auch wenn neue Datenschutzrichtlinien wie die Datenschutzgrundverordnung (DSVGO) der Europäischen Union Firmen und Organisationen dazu zwingen, Transparenz bezüglich dieser Praktiken zu schaffen und den Nutzern die Möglichkeit eines *Opt-out* (Abmeldung) zur Verfügung zu stellen, ist nicht zu erwarten, dass viele Menschen diese Option wählen, da sie dadurch die Vorteile personalisierter Produkte und Dienstleistungen verlieren. Man wird vermutlich nicht einmal weniger Spam erhalten, da die Emailadressen längst im Netz zu kaufen sind. Personalisierte oder «smarte» Werbung wird als viel angenehmer, nützlicher und wirksamer empfunden als traditionelle Werbung, die ohne irgendwelchen Informationswert auf dem Prinzip der Aufmerksamkeitsgenerierung basiert. Wenn Facebook, Twitter und andere Plattformen sich heute bei der Beteuerung der Konformität mit den neuen Datenschutzregeln der EU gegenseitig überbieten, ist man als Nutzer einerseits dankbar für eine gewisse Transparenz, aber nach wie vor sehr bewusst, dass die meisten Menschen mit der Nutzung der Daten durch die Plattformbetreiber wohl einverstanden sind. „Smart" ist halt einfach besser. Und – von Smartphones bis smartem Marketing – ist es die Sammlung und Nutzung personenbezogener Daten, die den Unterschied zwischen smart und nicht-smart ausmacht.

Nimmt man Hacking, kommerzielles Profiling und die Selbstpreisgabe persönlicher Daten und Information zusammen, dann ist es schwierig McNealy zu widersprechen, wenn er behauptet, man habe in der Tat keine Privatheit. Wenden wir uns also der Frage zu, was dieses «Get over it» bedeutet. Was bedeutet es, dass wir keine Privatheit haben und dass demzufolge die Idee eines Rechts auf Privatsphäre eher Traum als Wirklichkeit ist? Vielleicht bedeutet es, dass wir heute tatsächlich in einer anderen, einer digitalisierten Welt leben, die sich von der alten, analogen Welt, in der Freiheit, Autonomie und Menschenwürde auf der Geheimhaltung von Information basierten, unterscheidet. Hat möglicherweise die digitale Transformation nicht nur die Voraussetzungen, sondern auch die Notwendigkeit geschaffen, Privatheit anders zu konzipieren als in der westlichen Moderne und der Industriegesellschaft?[9]

Die drei Disruptionen

Obwohl es viele verschiedenen Interpretationen der Digitalisierung gibt, und obwohl es eigentlich zu früh ist, die Konturen der digitalen Gesellschaft umfassend und präzis nachzuzeichnen, ist es möglich, mindestens drei «Disruptionen» zu beschreiben, durch die die alte Welt der Industriegesellschaft durch die Digitalisierung grundsätzlich transformiert worden ist. Die erste betrifft die Art und Weise wie Information und Wissen strukturiert und geordnet werden. Die Ordnung des Wissens hat sich durch die Digitalisierung tiefgreifend verändert. Die zweite Disruption betrifft die Ordnung der Gesellschaft. Die Art und Weise wie kooperatives Handeln in der Gesellschaft, d.h. in Organisationen zustande kommt, hat sich verändert. Die Netzwerkgesellschaft ist in vielen Aspekten anders organisiert als die Industriegesellschaft. Hierarchische, top-down gesteuerte Organisationsformen werden durch verteilte Netzwerkorganisationen abgelöst. Die dritte Disruption der digitalen Transformation betrifft das Selbstverständnis des Menschen. Das Menschenbild der digitalen Welt ist anders als das der Industriegesellschaft und grundsätzlich anders als das Menschenbild der

[9] Vgl. Belliger/Krieger 2018.

europäischen Moderne. Das autonome, rationale Subjekt steht nicht mehr im Zentrum der Welt. Der digitale Mensch erlebt und deutet seine Existenz, Subjektivität und Identität anders als dies mindestens seit dem 18. Jahrhundert im Westen der Fall war. Betrachten wir diese drei Disruptionen etwas genauer.

In seinem Buch «Too Big to Know» (2012) beschreibt David Weinberger die Ablösung eines für die Industriegesellschaft kennzeichnenden hierarchischen, begrenzten, exklusiven Informations- und Wissensregimes durch eine neue nicht-hierarchische, unbegrenzte, komplexe, inklusive und öffentliche Wissensordnung. Er bezeichnet diese neue Ordnung von Wissen in Abgrenzung zur hierarchischen Wissenspyramide als «Cloud». In der Cloud gibt es unendlich viele Informationen, die aber weder von Gatekeepern, Autoritäten, Institutionen oder Experten auf Wahrheit oder Zuverlässigkeit geprüft werden, noch ausschliesslich über eine strenge Zugangs- und Nutzungskontrolle zur Verfügung stehen. Was bisher nur Experten und Autorisierten vorbehalten war, steht jetzt allen offen. Mehr noch, auch die Mittel für die Produktion und Verteilung von Information liegen für wenig Kosten und Aufwand in den Händen aller. Dies bedeutet einerseits eine bisher ungeahnte Ermächtigung, da Wissen Macht bedeutet und die Macht des Wissens nun in den Händen aller liegt, andererseits kann Macht, wie das immer der Fall war, nun auch von allen, nicht nur den Eliten, missbraucht werden. Dies erklärt, warum «Fake News», alternative Fakten und Filterblasen prägende Merkmale des gegenwärtigen Informationsökosystems sind.

Damit haben wir nicht nur ein Problem mit dem Thema «Wahrheit», da nun jeder seine eigene Wahrheit in der Cloud findet, sondern auch die Möglichkeit zur sehr einfachen Gemeinschaftsbildung unter Gleichgesinnten und in Gruppen. Soziale Medien wie Facebook oder Twitter erlauben es, sogenannte «Echo Chambers» (Echokammern) zu bilden, in denen der Austausch von Information fast ausschliesslich zwischen Gleichgesinnten geschieht. Solche online Communities geben nur Zugang zu jenen Informationen, die die Ansichten der Mitglieder bestätigen. Dabei verfügt nicht nur jede Gruppe ihre je eigenen «Fakten», jede Gruppe entwickelt zudem auch ihre eigenen Methoden und Kriterien, Wahrheit, Zuverlässigkeit und richtige Nutzung von Information zu bestimmen. Alle – Klimaschutzgegner, Flacherdler und Verschwörungstheoretiker aller Art – finden ihren Platz und ihre Anhänger in der Cloud. In Anlehnung an Ludwig Wittgensteins bekannte Bemerkung, dass die Grenzen der eigenen Sprache die Grenzen der eigenen Welt sind, könnte man heute sagen, dass die Grenzen der eigenen Gruppe die Grenzen der eigenen Welt sind. Es gibt heute keine gesamtgesellschaftlich gültigen und allseits anerkannten Kriterien für die Feststellung von Wahrheit. In der neuen Wissensordnung, der Cloud, gibt es keine verbindlichen Methoden der Wahrheitsfindung und demnach keine gesamtgesellschaftliche „Rationalität“.[10] Jeder hat nicht nur seine eigenen «Fakten», sondern ebenso seine eigene «Rationalität».[11]

Die zweite disruptive Transformation betrifft die Art und Weise wie Menschen sich organisieren und zusammenschliessen, um durch kooperatives Handeln gemeinsame Ziele zu erreichen. Die bürokratisch und hierarchisch organisierte Industriegesellschaft wird von einer nicht-hierarchischen Netzwerkgesellschaft abgelöst.[12] Traditionelle bürokratisch strukturierte Organisationen werden zu Netzwerken. Netzwerke können nicht durch top-down kontrollierte Kommunikation gesteuert werden, sondern sie verteilen Entscheidungs- und Handlungskompetenzen unter lose gekoppelten Einheiten, die raum- und zeitunabhängig operieren. Traditionelle Unterschiede und Grenzen, wie

[10] Diese Fragmentierung von Wissen und der Relativismus von Weltanschauungen kann auch als konsequentes Resultat postmoderner Kritik und Dekonstruktion betrachtet werden.
[11] Habermas (1997) gründet die Möglichkeit von Rationalität in gemeinsam akzeptierten Kriterien für Wahrheit, Richtigkeit und Wahrhaftigkeit. Fehlen solche gemeinsam akzeptierten Kriterien, ist «rationale» Argumentation unmöglich und Konflikte sind nur durch nicht-rationale Mitteln, sprich Gewalt, lösbar.
[12] Vgl. Castells (2017), Belliger/Krieger (2016).

jene zwischen öffentlich-rechtlichen Organisationen, die durch demokratische Prozesse legitimiert werden, privaten Unternehmen oder zivilgesellschaftlichen Organisationen lösen sich auf. Netzwerke bestehen aus vielen verschiedenen Arten von Organisationen, haben keine klaren Grenzen, sind dezentral, nicht territorial begrenzt und agieren auf globaler Ebene. Eine globale Netzwerkgesellschaft stellt uns vor neue Probleme in Bezug auf Regulierung. Fragen der Legitimität und Verantwortung müssen anders gestellt und beantwortet werden als dies in der Industriegesellschaft der Fall war. Netzwerke lassen sich nicht wirksam mit den Mitteln regulieren, die für hierarchische und bürokratische Organisationen entwickelt wurden. Neue Formen der Regulierung müssen gefunden werden. Diese neuen Ansätze werden heute vor allem unten dem Stichwort «Governance» diskutiert. Wir kommen darauf zurück.

Die digitale Transformation greift schliesslich tief in das Selbstverständnis des Menschen ein und verändert die Art und Weise wie Subjektivität, Freiheit, Autonomie und Menschenwürde empfunden und gedeutet werden. Es ist kein Zufall, dass Privatheit und Datenschutz zu heiss diskutierten Themen geworden sind. Nicht mehr «Privacy», sondern «Publicy» ist, um es mit den Worten von Stowe Boyd zu sagen, der Grundzustand der vernetzten Gesellschaft. «Publicy» ist nicht mit Publizität zu verwechseln. Es handelt sich nicht um einen durch Medien forcierten öffentlichkeitswirksamen Zustand, sondern um eine grundlegende Transformation weg vom Verständnis des Menschen als ein privates Individuum hin zu einem «informationellen Selbst».[13] Der Mensch wird, wie Floridi (2014) es zum Ausdruck bringt, ein «Inforg», d.h. ein Wesen, das aus Information besteht. Und weil Information in Netzwerken lebt, d.h. in Netzwerken entsteht und Netzwerken gehört, löst sich das klar begrenzte Individuum der europäischen Moderne auf in verschiedene Identitäten, die in verschiedenen Netzwerken und Kontexten agieren. Damit entfällt eine eindeutige Definition von Freiheit, Autonomie oder Menschenwürde, denn das Verständnis dieser Ideen hängt von der jeweiligen Gemeinschaft oder dem jeweiligen Netzwerk ab. Privatheit kann nur noch «kontextuell» und Netzwerk abhängig definiert werden.[14] Was jeweils als «private» oder «persönliche» Information betrachtet wird, hängt sowohl von der jeweiligen Situation, als auch von den kontextuellen Erwartungen und Regeln darüber ab, wie mit dieser Information umgegangen werden soll. Es ist auf diesem Hintergrund fragwürdig, ob die bis anhin grundlegende Unterscheidung zwischen «öffentlich» und «privat» noch Sinn macht und ob überhaupt ein allgemeingültiges Recht auf Privatheit noch definiert werden kann.[15]

Enttäuschte Hoffnungen – Filterblasen, Echokammern, Amplifikation, Geschwindigkeit, Monetarisierung und Ausbeutung von Information, Netzwerkeffekte

Die drei Disruptionen, die die digitale Transformation mit sich bringt, gründen alle auf in der Dynamik des Internets. Auch die gegenwärtigen Diskussionen um Privatheit und Datenschutz finden auf dem Hintergrund der Probleme statt, die aus dieser Dynamik entstehen. Lange Zeit war die neue digitale Welt, trotz kritischer Stimmen, mit grossen Hoffnungen und utopischen Visionen verbunden. Dies hat sich in den letzten Jahren geändert. Die ursprünglichen Hoffnungen auf eine bessere Zukunft, auf die Durchsetzung von Demokratie oder nachhaltige Wirtschaftsmodelle, wurden Anlass zur Sorge. Die Probleme, die nun in den Vordergrund gerückt sind, lassen sich unter verschiedenen Aspekten

[13] Vgl. Belliger/Krieger (2018). Der Megatrend «Individualisierung» sollte nicht als Rückkehr zur freien Subjektivität der Aufklärung oder zum radikal individualisiertem Subjekt des Existenzialismus verstanden werden, sondern als «Personalisierung» aufgrund von Integration des Subjektes in Informationsnetzwerken. Siehe https://www.zukunftsinstitut.de/artikel/mtglossar/individualisierung-glossar/.
[14] Siehe Nissenbaum (2004).
[15] Experten sind unisono der Meinung, dass es keine allgemeingültige Definition von Privacy gibt.

betrachten. Sprach man früher hoffnungsvoll vom Vorteil des Informationszugangs für alle, dem Empowerment von online Communities, den Wettbewerbsvorteilen der Schnelligkeit, der Innovationskraft von Netzwerkorganisationen und von den neuen Möglichkeiten des sozialen und politischen Engagements, so stehen heute Themen wie Filterblasen, Echokammern, die störenden Auswirkungen der Amplifikation, die Gefahren der Geschwindigkeit, der ausbeuterischen Monetarisierung und der politischen Exploitation von Daten und Information im Fokus. Das Aufkommen des Populismus, die Wahl von Donald Trump und der Erfolg von Brexit bereiten Sorgen und schüren Ängste, dass die digitale Transformation eher Fluch denn Segen ist. Auch wenn nicht alle diese Probleme direkt mit Privatheit zu tun haben, so ist der gegenwärtige Privatheitsdiskurs weitgehend durch diese Ereignisse und Ängste bestimmt. Privatheit wird oft als Lösung zum Problem eines scheinbar aus den Rudern gelaufenen Internets verstanden. Können aber Privatheit und Datenschutz tatsächlich die Lösung sein oder sind wir nicht vielmehr mit einer völlig neuen Situation konfrontiert, die nach neuen Lösungen verlangt?

Betrachten wir zuerst das Filterproblem. Die unvermeidbare Notwendigkeit der Anwendung von Filtern bei der Suche und Nutzung von Information entsteht aus der Tatsache, dass die Cloud mit den Worten von David Weinberger *«too big to know»* ist. Das Internet konfrontiert uns mit einer Überfülle an Information, die nur durch Filter oder Moderation verständlich und nutzbar gemacht werden kann. Das Problem besteht nicht darin, wie die Filterblasenwarner meinen, dass wir zu wenig Information bekommen, sondern dass wir von zu viel Information überflutet werden. Ohne Filter wäre die neue Informationswelt nichts weiter als Rauschen. Weder Suchdienste noch Social Media-Plattformen, die nutzergenerierten Inhalt verwalten, sind blosse Kanäle ohne Priorisierung, Selektion oder Weiterverarbeitung von Information, denn die Überkomplexität von zu viel Information muss auf irgendeine Art und Weise reduziert werden. Und da die traditionellen Autoritäten, Experten und Institutionen, die in der Industriegesellschaft diese Rolle ausübten nicht mehr funktional sind und weil die traditionelle Gatekeeping-Funktionen bezüglich Wahrheit und Zuverlässigkeit von Information nicht mehr vorhanden sind, ist es an jeder und jedem einzelnen, in eigener Verantwortung seine eigenen Filter anzuwenden.[16]

Filter betreffen vor allem die Suche nach Information und können manuell oder automatisch funktionieren. Wir filtern Informationen manuell, wenn wir Suchanfragen formulieren, gewisse Informationsquellen abonnieren oder diese bewusst aus den Suchergebnissen ausschliessen. Algorithmen nutzen unser Suchverhalten und andere Informationen über uns, um automatisch Information für uns zu filtern. Der Erfolg von Google zeigt, wie wirksam, aber auch wie komfortabel automatisches Filtern ist. Die Schattenseite dieses Komforts: wenn man lediglich mit Information konfrontiert wird, die mit der eigenen Haltung und Meinung übereinstimmt, entstehen Filterblasen. Konträre Meinungen und Informationen werden manuell und zunehmend automatisch ausgefiltert. Im Kontext des persönlichen Konsumverhaltens ist dies kein Problem, da es durchaus Vorteile hat, genau das Produkt zu finden, an dem man interessiert ist. Handelt es sich aber um politische Kommunikation, sieht die Sache etwas anders aus. Manuelles und automatisches Filtern von Information, so die Befürchtung, untergrabe öffentliche, demokratische Debatten, die unabdingbar des Wissens um und der Auseinandersetzung mit verschiedenen Meinungen und Standpunkten bedürfen. Durch Filter, so führen Kritiker ins Feld, geht der für eine gesunde Demokratie nötige Pluralismus verloren.

[16] Das ist auf jedem Fall die Haltung der grossen Plattformen, die Aufgaben der Qualitätskontrolle den Usern überlassen wollen. Vgl. Gillespie (2018) für eine ausführliche Diskussion der moderierenden Tätigkeiten der grossen Internetplattformen.

Diese Kritik übersieht jedoch, dass eine rein «objektive» Debatte, die alle Standpunkte gleichermassen berücksichtigt und gleichbehandelt, ein Mythos ist. Schon vor dem Zeitalter der Digitalisierung wurden politische Meinungen durch gefilterte Informationen gebildet. Viele Massenmedien waren und sind bis heute parteipolitisch gefärbt. Nicht alle Standpunkte und Meinungen konnten sich in der Vergangenheit in den Median präsentieren. Und so etwas wie eine die Gesamtgesellschaft umfassende politische Debatte hat nie wirklich stattgefunden. Übersehen wird zudem, dass Pluralismus eigentlich das Problem und nicht die Lösung ist. Die Cloud bietet so viele Informationen, so viele Standpunkte und so viele Wahrheiten, dass es ohne Filter eigentlich keine Information gibt. Erst Filter bringen Ordnung ins Chaos und machen aus Rauschen Information. Eine objektive, rationale Erwägung verschiedener Informationen oder deliberative politische Prozesse ohne Filter sind kaum möglich. Im Blick auf das Thema Privatheit wird Filtern vorgeworfen, dass sie, da sie unsere Interessen abbilden, nicht nur für kommerzielles, sondern auch für politisches Profiling genutzt werden. Je mehr Information über uns im Netz vorhanden ist, desto besser kann diese Information für politisch motivierte Kommunikation «missbraucht» werden. Mangels strenger Regulierungen im Bereich von Privatheit, so die Argumentation, werde persönliche Information zu Manipulationszwecken genutzt. Dies ist auch der vermeintliche Skandal seitens Cambridge Analytica. Filterblasen sind aber nicht das einzige Problem. Das Filtern von Information führt zu einem verwandten, ebenso häufig diskutierten Problem des gegenwärtigen Informationsökosystems, en sogenannten Echokammern.

Bei der Suche nach Information sind wir nie ganz auf uns alleine gestellt. Im Kampf gegen die Informationsflut bietet uns das Netz die Möglichkeit, uns online mit Gleichgesinnten in Gruppen und Communities zusammenzutun.[17] Gemeinschaftsbildung zu fast jedem beliebigen Thema und Interesse funktioniert nicht nur in den Social Media, sondern in verschiedensten online Communities auf diversen Plattformen. Entscheidend dabei ist, dass man selber bestimmt, mit wem man es zu tun haben möchte. Ich wähle meine Facebook-Freunde selber aus und entscheide, wem ich auf Twitter folge. Das Netz ermöglicht damit nicht nur eine neue und vielversprechende «Sharing Economy», neue Formen des sozialen und politischen Handelns oder Selbsthilfegruppen zu alle nur erdenklichen Themen, sondern fördert, so die Meinung der Kritiker, auch den Umstand, dass wir uns vermehrt nur noch mit Menschen austauschen, die die gleichen Meinungen und Haltungen wie wir selber vertreten. Dadurch entstehen so genannte Echokammern, abgekapselte Informationsräume, die gegenüber anderen Meinungen, Kritik seitens Andersdenkender und gegenüber nicht-konformen Informationen abgeschottet sind. Im Wirtschaftskontext scheint dieser Umstand wiederum weniger als Problem betrachtet zu werden. Marken beispielsweise haben ihre Fanclubs und bieten Kunden die Möglichkeit, an Produktentwicklung und an Marketingthemen kreativ mitzuwirken. Rating-Plattformen dienen als Zugang zu Produkten und Dienstleistungen. Für die politische Kommunikation sieht dies aber ganz anders aus. Community-Bildung führe, so die kritischen Stimmen, zu einer gefährlichen Fragmentation der Öffentlichkeit und zur Polarisierung von ideologisch divergenten Gruppierungen. Dieses Problem wird dadurch verschärft, dass jede Gruppe nicht nur ihre eigenen Werte und Meinungen, sondern ebenso ihre eigenen «Fakten» hat. Fakten gründen auf Methoden der Wahrheitsfindung. Wenn nun jede Gruppe ihre eigenen Methoden hat, um Wahrheit von Unwahrheit zu unterscheiden, gibt es keine objektive, für alle verbindlichen Fakten mehr. Ohne objektive Fakten bleiben lediglich subjektive Meinungen und somit kaum mehr Möglichkeiten, Meinungskonflikte mit Hinweis auf etwas, das für alle gilt, zu schlichten. Von einer gesamtgesellschaftlichen Öffentlichkeit kann auf diesem Hintergrund eigentlich nicht mehr gesprochen werden, eher vielleicht von verschiedenen Öffentlichkeiten und dem unvermeidlichen

[17] Vgl. Shirky (2008).

Kampf aller gegen alle.[18] Als Gegenmassnahme zu dieser Entwicklung wird immer lauter nach Privatheit und Datenschutz gerufen, da Anonymität es zumindest etwas schwieriger macht, geeignete Mitglieder für Communities oder Opfer für Troll-Attacken zu finden.

Ein dritter, kritischer Aspekt der digitalen Welt, ist die so genannte Amplifikation. Amplifikation bezeichnet die «verstärkte» oder «virale» Verbreitung und damit überproportionale Wirkung bestimmter Information im Netz. Wegen des freien Informationsflusses in den globalen Netzwerken kann jede Information, ob wahr oder falsch, ob aus «autoritativen» Quellen oder nicht, ohne jede Kontrolle beliebig oft wiederholt und verteilt werden. Jede Information, nicht nur die Erzeugnisse autoritativer Massenmedien, kann prinzipiell viele Millionen Menschen erreichen. Auf der einen Seite verleiht das Netz jeder und jedem ganz im Sinne von Empowerment eine Stimme und die Möglichkeit, weit über lokale Grenzen hinaus gehört zu werden, auf der anderen Seite aber wird es möglich, dass Verschwörungstheorien und Fake News ebenso verbreitet werden. Auf diese Weise können Falschinformation «verstärkt» werden, «viral» gehen und eine Wirkung entfalten, die im vordigitalen Medienregime undenkbar gewesen wäre. Allein die Tatsache, dass sie vielfach und auf verschiedene Kanälen wiederholt wird, verleiht Information, auch wenn sie explizit als irreführend oder gar falsch bezeichnet ist, Bedeutung und eine Art «Wahrheit», allein aus dem Grund, dass so viele darüber reden. Durch diese besondere Dynamik des Internets sind Trolle, Unruhestifter aller Art und gezielte Cyberattacken in der Lage Personen, Organisationen und auch Nationen Schaden zufügen.

Ein Beispiel der unglaublichen und negativen Wirkung von Amplifikation ist die Meldung, dass ein Pastor einer kleinen Kirche in einem unbekannten Dorf im Süden des US Bundesstaates Florida über Twitter und YouTube ankündete, er werde den Koran verbrennen. Verschiedene Gruppen, die sich für religiösen Frieden einsetzen, erhielten Kenntnis davon und baten via Internet, dass er von seinem Vorhaben ablasse. Die Diskussion weitete sich aus und nationale sowie internationale Medien erfuhren davon. Es intervenierten schliesslich das Weisse Haus, das Aussenministerium und die Regierung von Afghanistan. In verschiedenen muslimischen Ländern kam es in der Folge zu gewalttätigen Ausschreitungen.[19] Es gibt Zahlreiche Beispiele und Geschichten dieser Art von Shitstorms, Mobbingfällen, «Fake News» oder der Verbreitung von Verschwörungstheorien mit dramatischen politischen Folgen. Die Dynamik viraler Kommunikation und Amplifikation ist neu und wäre so unter dem Informationsregime der Industriegesellschaft nicht denkbar gewesen. Entsprechende Informationen wären bereits von den institutionellen Gatekeepern herausgefiltert und wirkungslos gemacht worden.[20] Die Mechanismen, durch die Information verstärkt wird, sind bekannt und werden durchaus auch ganz bewusst eingesetzt, um persönliche, wirtschaftliche und oder politische Vorteile zu erlangen oder Schaden anzurichten. Auch in diesem Zusammenhang wird das Thema Privatheit angeführt, mit dem Ziel dadurch Opfer zu schützen und Gruppenbildung zu verhindern. Ob Privatheit tatsächlich eine wirksame Lösung zu problematischen Formen der Amplifikation darstellt, ist höchst fragwürdig, denn Menschen werden freiwillig zu Anhängern von Gemeinschaften, die z.B. Verschwörungstheorien vertreten oder als Trolle funktionieren, und es ist undenkbar, sämtliche öffentlichen Information über Zielpersonen und anvisierte Opfer geheim zu halten.

[18] Vgl. Latour (2017).

[19] https://en.wikipedia.org/wiki/Dove_World_Outreach_Center_Quran-burning_controversy.

[20] Interessanterweise werden heute Stimmen aus dem professionellen Journalismus laut, die eine Rückkehr zur Watchdog- und Gatekeeping-Funktion der Medien befürworten. Vgl. z.B https://medium.com/@gabrielletutheridge/what-is-the-role-of-gatekeeping-journalists-in-today-s-media-environment-2034a30ba850. Vgl. Gillespie (2018) für ein Plädoyer für die Gatekeeping-Verantwortung von Plattformen durch Moderation.

Der vierte Aspekt des gegenwärtigen Informationsökosystems, der nicht nur Vorteile, sondern auch Nachteile und Probleme mit sich bringt, ist die unglaubliche Geschwindigkeit, mit der Information generiert und verbreitet wird. Ob aktuelle News, Finanztransaktionen, online Einkaufen oder Logistik, Schnelligkeit ist ein Merkmal von Qualität, ein Wettbewerbsvorteil, ein «Game Changer» und zum Imperativ in allen Bereichen und Branchen geworden. Dass der Zwang zur Geschwindigkeit zu Problemen führen kann, zeigen Beispiele aus der Finanz- und Medienbranche. Mit dem Aufkommen der Bürgerberichterstattung («Citizen Reporting»), bei der Nachrichten von Menschen, die direkt vor Ort über aktuelle Ereignisse mittels Smartphone via Social Media Kanäle wie Facebook oder Twitter berichten, generiert und verteilt werden, sind die grossen Medienunternehmen unter Druck geraten diese Information aufzunehmen und so schnell wie möglich über ihre Netzwerke und Kanäle weiter zu verbreiten. Dies führt zu fehlerhafter Berichterstattung, da die Zeit und die Personalressourcen für Nachforschungen über den Wahrheitsgehalt, die Zuverlässigkeit oder die Vollständigkeit der Meldung weitgehend fehlen. Diese Situation erhöht das Risiko von Fehlern bei der Berichterstattung, die im Nachgang nur schwer zu korrigieren sind. In der Finanzbranche haben die Vorteile schneller Börsentransaktionen dazu geführt, dass Algorithmen auf Hochleistungsrechnern, die physisch möglichst nah an den Börsen platziert werden, im Millisekunden Takt automatisiert Transaktionen ausführen. Dies führt zu sogenannten Blitzabstürzen («Flash Crashes») und anderen Verzerrungen der Finanzmärkte und stellt ein nicht zu unterschätzendes Risiko für die Gesellschaft dar.[21] Privatheit und Datenschutz könnten unter Umständen dazu beitragen, das Sammeln und die Nutzung von Daten im Allgemeinen zu verlangsamen und damit der ungebremsten Geschwindigkeit der digitalen Welt entgegenwirken.

Auf Schnelligkeit ausgelegte Automatisierungsprozesse in der Medien- und der Finanzbranche sind Beispiele dafür, wie Information monetarisiert werden kann. Auch wenn Privatheit und Datenschutz auf den ersten Blick wenig mit dem automatisierten Handel an der Börse zu tun haben, gibt es viele Formen der Monetisierung und Ausbeutung von Information, die aufgrund der Digitalisierung zu besonderen Problemfeldern geworden sind. Es ist hinlänglich bekannt, dass Daten als das neue Öl bezeichnet werden, als wertvollster Rohstoff der digitalen Ökonomie. Aus Daten können nicht nur für die Gesellschaft wichtige Erkenntnisse gewonnen werden, aus Daten lässt sich Geld machen und Macht erlangen, etwa durch die Entwicklung und Vermarktung personalisierter Produkte und Dienstleistungen. Je mehr man über seine Kunden weiss, desto wirksamer und profitabler kann man neue Produkte und Dienstleistungen entwickeln und anbieten. Zielgerichtetes Marketing («Targeted Marketing») hat zum Ziel, möglichst viele Informationen über prospektive Kunden zu sammeln und auszuwerten. Datenbroker wie Acxion oder Oracle sammeln so viele Daten über so viel Personen wie nur möglich, um diese dann aggregiert als Kundenprofile an andere Unternehmen weiter verkaufen zu können. Onlinehändler wie Amazon, soziale Netzwerke wie Facebook oder Suchmaschinen wie Google verdienen alle ihr Geld mit zielgerichteter Werbung. Solange Werbung die Haupteinnahmequelle vieler netzbasierter Geschäftsmodelle ist, wird das Kundenprofiling von enormer Bedeutung bleiben. Auch wenn Kritiker das kommerzielle Profiling als skandalöse Monetarisierung persönlicher Daten bezeichnen, so ist es doch so, dass die meisten Menschen smarte personalisierte Werbung allgemeinem, unspezifischem Spam vorziehen. Die Vorteile personalisierter Produkte und Dienstleistungen beim Einkaufen, bei der Bildung oder in der Medizin sind unbestritten und fast jede Nation hat heute ihre eigene Digitalstrategie, die darauf abzielt, eine datengetriebene Wirtschaft zu fördern.[22] Handelt es sich aber um politische Kommunikation so ist die Nutzung von Profiling und zielgerichteter, personalisierter Information in den letzten Jahren ganz

[21] https://www.spektrum.de/kolumne/boersenhandel-in-lichtgeschwindigkeit/1331927. Vgl. dazu auch den weltweiten Börsencrash, der durch die falsche Nachricht auf Twitter von einer Attacke auf das Weisse Haus ausgelöst wurde.

[22] Vgl. dazu z.B. die «Single Digital Market»-Initiative der EU.

offensichtlich zu einem grossen Problem geworden. Die Rede ist von Manipulation und «Nudging», dem sanften Schubsen Richtung Verhaltensänderung. Auch wenn es praktisch keine wissenschaftlichen Beweise für die Wirksamkeit von Manipulation durch personalisierte politische Kommunikation gibt, so treiben Angst und Ressentiments insbesondere seitens der politisch Unterlegenen zum Ruf nach mehr Regulierung. In diesem Zusammenhang wird Privatheit oft als geeignetes Mittel zur Verhinderung von Profiling ins Feld geführt.

So genannte Netzwerkeffekte führen trotz der nicht-hierarchischen Struktur des Internets schliesslich dazu, dass eine gewisse Zentralisierung oder Monopolbildung stattfindet. Als Netzwerkeffekt bezeichnet man die zunehmende Wertsteigerung eines Produktes oder Dienstleistung je mehr Personen diese nutzen. Facebook wird oft als Beispiel zitiert. Je mehr Menschen Facebook nutzen, umso mehr Wert hat die Nutzung von Facebook für die Teilnehmenden. Dies führt in bestimmten Fällen zu einer Art Zentralisierung oder Monopolstellung. Neue Marktteilnehmer oder Konkurrenzangebote haben fast keine Chancen, da die meisten Menschen bereits Facebook nutzen. Die Internetgiganten verfügen zudem aufgrund der enormen Datenmengen und des Kapitals, die sie besitzen, wirtschaftliche Vorteile, die marktverzehrend wirken. Es scheint also unvermeidlich, dass Netzwerkeffekte zur Etablierung grosser, ausser Konkurrenz stehender Internetfirmen wie Apple, Google, Facebook, Amazon, Microsoft oder Alibaba führen. Diese Tatsache wiederum führt angesichts der damit zusammenhängenden Abhängigkeiten zur Forderung nach Regulierung oder gar Zerschlagung durch die konsequente Anwendung von Anti-Kartell- und Anti-Monopol-Gesetzen. Immer mehr Kritiker schlagen auch vor, dass solche Firmen als Infrastruktur angesehen und entsprechend durch die Staaten geregelt werden sollen.[23] Da das Businessmodell vieler dieser Unternehmen auf das Sammeln und Auswerten von Kundendaten basiert, wird Privatheit und Datenschutz auch in diesem Fall oft als Massnahme gegen das ungebremste Wachstum dieser Firmen betrachtet.

Vor dem Hintergrund dieser oben geschilderten unterschiedlichen Problemfelder einer digitalisierten Gesellschaft werden Privatheit und Datenschutz häufig als dringend notwendige Lösung betrachtet. Der Rekurs auf Privatheitsrechte und die Forderung der Verstärkung von Datenschutzregulierungen sollen dem Schaden entgegenwirken, der aus Phänomenen wie Filterblasen, Echokammern, unkontrollierte Amplifikation, ungebremster Geschwindigkeit, opportunistische Monetarisierung, Ausbeutung von Daten und Information oder aus monopolisierenden Netzwerkeffekten resultieren.

So sehr man auch Hoffnungen in Privatheitsrechte und Datenschutzregulierungen setzt, so ist doch die Frage berechtigt, ob Privatheit und Datenschutz, die ihrerseits tief in den Werten, Haltungen und Erwartungen der Industriegesellschaft wurzeln, die richtigen Instrumente sind, um Ordnung in die scheinbar unkontrollierte und gefährliche digitale Welt zubringen.

Ist Privatheit die Lösung?

Da gegenwärtig so viele Hoffnungen in strengere Privatheitsrechte gesetzt werden, ist es vielleicht hilfreich, der Frage nachzugehen, welche Art von Recht denn das Recht auf Privatheit überhaupt ist. Was ist Privatheit? Welches Sicherheitskonzept steht hinter der Idee von Datenschutz? Was bedeutet es, Daten zu «schützen»? Handelt es sich beim Datenschutz um ein Sicherheitskonzept, das für das digitale Zeitalter überhaupt geeignet ist? Oder versuchen wir vielleicht, mit Vorstellungen, Werten

[23] https://www.youtube.com/watch?v=QogxTW49QZ0 Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities, Georgetown Law Technology Review, 2018. Vgl. auch die gegenwärtigen Diskussionen über die Verantwortung von Facebook und ähnlichen Plattformen für Probleme wie Hassreden und «Fake News».

und Gesetzen, die aus dem Industriezeitalter stammen, Probleme zu lösen, die völlig anderer Natur sind und die möglicherweise nur auf Basis neuer Werte, eines neuen Menschenverständnis und neuen Formen der Regulierung adäquat angegangen werden können? Angesichts der Möglichkeit, dass wir allem Anschein nach tatsächlich keine Privatheit mehr haben, entsteht leicht der Eindruck, dass die gegenwärtige Aufregung rund um das Thema Privatheit nicht nur zu spät kommt, sondern auch auf ziemlich wackligen Beinen steht. Natürlich ist es nicht trivial, möglichen Problemen, die auf dem Hintergrund neuer Technologien entstehen, präventiv entgegenzuwirken. Wir stehen am Anfang der gesellschaftlichen Durchdringung von Technologien wie künstliche Intelligenz, Internet der Dinge oder Big Data. Angesichts der disruptiven Kraft solcher exponentiellen Technologien hinkt das Problembewusstsein der tatsächlichen Problematik vermutlich immer etwas hinter her. Doch auch wenn es kaum möglich sein wird, Probleme, die neue Technologien verursachen, schon im Voraus zu erkennen und mittels bestehender Instrumente entgegenzuwirken, so können wir vielleicht doch bestehende Methoden, Verfahren und Formen zur Problemlösung, die uns zur Verfügung stehen, genauer unter die Lupe nehmen und die Frage stellen, ob sie überhaupt zukunftstauglich sind. Es dauerte lange, bis die Idee des autonomen, rationalen Subjektes der europäischen Aufklärung zur Basis eines Rechtes auf Privatheit wurde. Es könnte also durchaus sein, dass das Thema der Privatheit derart problematisch geworden ist, weil die Idee von Privatheit und Datenschutz im Kontext einer digitalisierten Welt neu konzipiert werden muss und dass dies ebenso seine Zeit braucht.

Es ist zudem tatsächlich so, dass es keine allgemein akzeptierte Definition von Privatheit gibt.[24] Auch wenn die philosophischen oder kulturellen Grundlagen des Rechtes auf Privatheit nicht eindeutig sind, so erlauben geltende Gesetze und die Rechtsprechung Rückschlüsse auf das, was Privatheit bedeutet. Es gibt zwei grundsätzliche Auffassungen über Privatheit als Recht. Für die eine Sichtweise ist Privatheit eher ein instrumentelles Recht, dessen Sinn und Zweck darin liegt, anderes Recht zu stärken, z.B. das Recht auf Eigentum, Freiheit oder Sicherheit.[25] Die andere Sichtweise betrachtet Privatheit als ein fundamentales Recht, das nicht gegen andere Rechte ausgetauscht oder relativiert werden kann. Dieser Auffassung zufolge gibt es keine Berechtigung auf Privatheit zu verzichten. Privatheit ist ein Menschen- oder Grundrecht, das unter keinen Umständen kompromittiert werden darf.[26] Privatheit als instrumentelles Recht ist typisch für die USA, Privatheit als unverzichtbares Menschenrecht ist typisch für Europa. So gibt es zum Beispiel keine Verankerung eines Rechtes auf Privatheit in der amerikanischen Verfassung, so wie dies in den Verfassungen vieler europäischer Länder und der EU der Fall ist. Aus der Sicht von Privatheit als instrumentelles Recht werden als Legitimation für Regulierungen der Privatheit jene Schäden betrachtet, die durch den Verlust von Privatheit entstehen könnten. Wird Privatheit als ein fundamentales Recht verstanden, dann ist der Verlust von Privatheit an sich ein Schaden.

Die Auffassung von Privatheit als instrumentelles Recht geht zurück auf den berühmten Aufsatz von Warren und Brandeis 1890.[27] Die beiden Rechtsgelehrten definierten Privatheit als das Recht «allein gelassen» zu werden und begründeten es folgendermassen:

> The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent,

[24] Vgl. dazu die umfassende Kritik des Privacybegriffs in Macleod (2018).
[25] Vgl. Waldo/Lin/Millett (1997).
[26] Vgl. Floridi (2014).
[27] Vgl. dazu https://en.wikipedia.org/wiki/The_Right_to_Privacy_(article)

> column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.

Das Aufkommen von Boulevardpresse und Fotografie veranlasste die Einführung eines in den USA bis dahin unbekannten Rechts auf Privatheit. Das, was auf dem eigenen Grundstuck oder in den eigenen vier Wänden geschah, sollte nicht öffentlich bekannt gemacht werden, dies um der Befriedigung der Sensationsgier der niederen Klassen und der Rufschädigung der Betroffenen entgegenzuwirken. Ausschlaggebend für den Anspruch auf Privatheit ist das «overstepping», das Übertreten einer Grenze und das Eindringen in den häuslichen Bereich. Hier liegen auch Eigentums- und Sicherheitsrechte zur Grunde. Das unbefugte Eindringen in das Haus einer Person ist offensichtlich eine strafbare Handlung, die durch Diebstahl von Information, die im Haus aufbewahrt wird, noch verschlimmert wird. Privatheit wird damit «territorial» und als eine Form von Grenzerhaltung, Grenzpflege oder Grenzmanagement verstanden. Dies wird in der berühmten Definition von Privatheit, die von A. Westin stammt, klar zum Ausdruck gebracht:

> Privacy is "the claim of an individual to determine what information about himself or herself should be known to others." (Westin 1967)

Das Individuum hat das Recht, darüber zu bestimmen, welche Information über es bekannt wird. Privatheit ist also ein Recht auf die Entscheidung, ob irgendeine Information entäussert werden kann. Es handelt sich dabei zwar nicht ausdrücklich um ein Eigentumsrecht, aber in der Praxis kommt es dem sehr nahe.[28] Denn etwas zu besitzen bedeutet, dass man souverän darüber entscheiden kann, ob die Sache (*res*) entäussert wird. Deshalb ist, weil man das eigene Heim vermutlich besitzt, das Eindringen in dieses Heim an sich ein Übergriff auf Eigentum.

Die europäische Auffassung von Privatheit als fundamentales Recht hingegen geht zurück auf die Allgemeine Erklärung der Menschenrechte (1948), wo in Art. 12 ausdrücklich erklärt wird:

> Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

Privatheit wird unabhängig irgendwelcher zu erwartenden Schäden als Menschenrecht definiert. Diese Auffassung wurde in der Europäischen Menschenrechtskonvention (1950/53) wiederholt, worin es nach Art. 6 Abs. 1 heisst:

> Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

In der Charta der Grundrechte der Europäischen Union (2012) wurde in Art. 8. Abs. 1 dieses Recht ausdrücklich zum ersten Mal auf Information und Daten ausgeweitet:

> Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Schliesslich wurde diese Auffassung von Privatheit als Grundrecht in der neuen Datenschutzgrundverordnung (DSVGO) (2018) der EU in Art. 1, Abs 2 aufgenommen:

> Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

[28] Vgl. z.B. die Diskussion in Thouvenin (2017).

Die Verwendung des Begriffs «Grundfreiheiten» mit Blick auf personenbezogene Daten ist für die Sprache der Menschenrechte ungewöhnlich, denn Freiheit wird ausdrücklich als Grundrecht unabhängig von Privatheit genannt. Die Art und Weise wie die DSVGO «Grundfreiheiten» schützen will, lässt sich aus den Rechten, die sie den Datensubjekten verleiht, erkennen. Diese können folgenderweise zusammengefasst werden:

1. Rechtmässigkeit: es muss eine eindeutige Einwilligung auf Basis von Transparenz (d.h. in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache) über Zweck, Empfänger und Verantwortliche der Datenverarbeitung, Dauer der Datenspeicherung, Recht auf Berichtigung, Sperren und Löschen und Verwendung der Daten zu Profiling-Zwecken gegeben werden. Wenn sich der Zweck ändert, ist die betroffene Person aktiv zu informieren.
2. Recht auf Einsicht
3. Zweckbindung
4. Datenminimierung
5. Richtigkeit (löschen/berichtigen/sperren)
6. Recht auf Vergessenwerden (löschen aller Daten, wenn Gründe nicht mehr gegeben sind)
7. Speicherbegrenzung (Zeitbegrenzung)
8. Integrität und Vertraulichkeit (Sicherheit)

Auch wenn die philosophischen Grundlagen und die historische Entwicklung der amerikanischen und der europäischen Auffassungen zur Privatheit verschieden sind, so scheint Privatheit in der Praxis auf einer dem Eigentumsrecht ähnlichen Entscheidungsbefugnis über die Ausgabe und Nutzung persönlicher Information zu basieren. Sowohl für die DSVGO, als auch für das amerikanische Recht ist die einzige Rechtsgrundlage für die Sammlung und Nutzung personenbezogener Daten die Einwilligung auf Basis von Transparenz oder dessen, was in den USA als «informed consent» (informierte Einwilligung) bezeichnet wird.[29] Diese Haltung kommt auch im Begriff der «informationellen Selbstbestimmung», die vom Deutschen Bundesverfassungsgericht 1983 als Grundrecht anerkannt wurde, zum Ausdruck.[30]

Die Betonung der Entscheidungsfreiheit bei der Definition von Privatheitsrechten erklärt sich aus der Nähe der beiden Themen Privatheit und Eigentumsrecht. Auch wenn Daten juristisch nicht als Eigentum definiert sind, so scheint beiden Begriffen das gleiche grundlegende Sicherheitskonzept zugrunde zu liegen. Es wird dabei explizit oder implizit davon aus gegangen, dass es so etwas wie eine territorial gedachte «Sphäre» gibt, in der das Recht auf Privatheit gilt und in der Wertsachen in Form von Daten und Informationen aufbewahrt und geschützt werden. Die Grenze dieser «Privatsphäre» gilt es aufgrund von Rechten und Regulierungen, die vom Staat eingesetzt und sanktioniert werden, persönlich zu managen. Nennen wir dieses Sicherheitskonzept das «Schlosskonzept». Die Grundidee ist ein Schloss umgeben von einer dicken Schlossmauer mit wenigen, gut kontrollierbaren Ein- und Ausgängen. Im Schloss wird der Schatz – in diesem Fall personenbezogene Daten – sicher gegen feindliche Angriffen und unkontrollierte Nutzung aufbewahrt. Dieses Sicherheitskonzept ist uralt. Die Errichtung von Mauern, um etwas Wertvolles zu schützen, kennt man seit Menschengedenken und kommt als Sicherheitskonzept bis heute zur

[29] Natürlich gibt es viele Ausnahmen wie jene für die nationale Sicherheit, Steuern, Militärdienst, Justiz, legitime Interessen der Datenkontroller.

[30] «Das Recht auf informationelle Selbstbestimmung ist im Recht Deutschlands das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Es ist nach der Rechtsprechung des Bundesverfassungsgerichts ein Datenschutz-Grundrecht, das im Grundgesetz für die Bundesrepublik Deutschland nicht ausdrücklich erwähnt wird.» https://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung.

Anwendung, etwa wenn der US-amerikanische Präsident beabsichtigt eine Mauer zum Schutz der USA zu errichten. Jedes gegenwärtige IT-Sicherheitskonzept ist letzten Endes auf diesem uralten Schlosskonzept begründet. Das Deutsche Bundesdatenschutz-Gesetz z.B. versteht Datensicherheit als Grenzkontrolle. Das Gesetz schreibt vor, dass Datensicherheit darin besteht, dass die Zutrittskontrolle zu Serverräumen, die Zugangskontrolle zu Systemen, die Zugriffskontrolle zu Information, die Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle in Bezug auf Infrastruktur garantiert sein müssen.[31] Dabei geht es im Kern überall um dasselbe, nämlich, dass Sicherheit darin besteht, Daten in schlossartigen Silos aufbewahrt werden, deren Grenzen strengstens kontrolliert werden. Datenschutz ist zwar nicht das gleiche wie Privatheit, aber die Entscheidungsmacht über die Ausgabe von Daten und Information, die etwa die DSVGO etabliert, basiert auf einem bestimmten Konzept von Datensicherheit. Es kommt nicht von ungefähr, dass Privatheit oft mit Datenschutz und -sicherheit gleichgesetzt wird. Privatheit und Datensicherheit sind eng miteinander verbunden. Gäbe es keine Datensicherheit, so bestünde auch keine Möglichkeit Entscheidungsmacht, was Privatheit zumindest in der Praxis ausmacht, auszuüben. Datenschutz errichtet quasi die Schlossmauer und gibt dem Individuum den Schlüssel in die Hand, der für das Management der Zugänge nötig ist. Privatheit als Entscheidungsmacht über Zugang und Nutzung personenbezogener Daten wird durch das Schlosskonzept verständlich und praktikabel gemacht. Wann immer es um Datensicherheit geht, geht es um Mauern, reale oder virtuelle, die Daten umschliessen. Und wenn es um Privatheit geht, geht es um die Entscheidungsmacht aus freier und souveräner Entscheidung heraus die Zugänge zu kontrollieren.

Das Schlosskonzept von Sicherheit und die souveräne Entscheidungsmacht, die damit dem Schlossherrn gegeben wird, hängen davon ab, dass der sich im Schloss befindliche Schatz bestimmte Eigenschaften hat, die es erlauben, ihn durch Mauern und Grenzkontrollen sicher aufzubewahren und zu kontrollieren. Angesichts des omnipräsenten Hacking, von kommerziellem Profiling und der unvermeidlichen Preisgabe persönlicher Information in fast jeder sozialen Interaktion könnte man aber berechtigterweise die Frage stellen, ob das Schlosskonzept für den Schutz von Daten und Information geeignet ist. Worin besteht der Schatz, den wir im Schloss sicher aufbewahren wollen? Es handelt sich um «personenbezogene Daten». Gemäss DSVGO (Art. 4) sind personenbezogene Daten:

> … alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden 'betroffene Person') beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann…

Wichtig an dieser Definition ist ihre Breite und Reichweite. Es geht also um «alle» Information, die auf eine Person bezogen werden «kann». Wenn man nun die Praktiken und Ressourcen von Datenbrokern wie Acxion oder Oracle in Betracht zieht und die Möglichkeiten von Big Data-Analysen mitdenkt, dann umfasst diese Definition jede Information überhaupt, denn welche Information gibt es noch, die nicht durch Kombination mit anderen Informationen zur Identifizierung einer Person führen könnte? Die Katze scheint längst aus dem Sack und lässt sich nicht mehr einfangen. Der Tenor

[31] Vgl. Bundesdatenschutz-Gesetz §64 https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1533716580546. Vgl. dazu auch die vergleichbaren Massnahmen unter den Richtlinien für die Zugriffs- bzw. Zugangskontrolle von ISO 27001, International Standard für das Management der Informationssicherheit.

der gegenwärtigen Diskussion und der aktuellen Regulierungen um Datensicherheit und Privatheit scheint aber eher dahin zu gehen, dass man die Katze wieder einfangen kann. Wenn es dabei tatsächlich um eine Katze ginge, wäre dies durchaus möglich. Aber vielleicht liegt das Problem eben gerade darin, dass Daten und Information eine besondere Art von Dingen sind, oder besser gesagt gar keine Dinge sind und damit auch nicht wie Dinge behandelt werden können. Dies führt uns zur Frage: Was ist eigentlich Information?

Trotz der Nähe von Eigentumsrecht und Datenschutz sind sich alle Experten einig, dass Daten keine Dinge (*res*) sind und daher nicht wie Eigentum behandelt werden können. Daten sind z.B. nicht rivalisierend, d.h. die Datennutzung durch eine Person bedeutet nicht, dass andere Personen die gleichen Daten nicht auch nutzen könnten. Daten und Informationen sind nicht ausschliessbar, d.h. wenn eine Person Daten nutzt, heisst dies nicht, dass die Daten nicht mehr vorhanden sind, ganz im Gegensatz etwa zu Äpfeln, die einmal verkauft nicht mehr im Supermarkt vorhanden sind. Diese Eigenschaften von Daten und Information sind letztlich darin begründet, dass Information in Netzwerken entsteht und eigentlich den Netzwerken, in denen sie zustande gekommen sind, gehören.[32] Da ein Netzwerk aus verschiedenen Akteuren besteht, kann kein einzelne Akteur behaupten, dass die Daten, die im Netzwerk entstanden sind, ihm alleine gehören und seiner souveränen Entscheidungsmacht unterliegen. Kurz, mein Facebook-Profil gehört nicht mir alleine, sondern ist ein Produkt der Vernetzung von Software, Hardware, Infrastruktur und Protokollen, bestimmten Geschäftsmodellen, Investitionen, organisationalen Strukturen, anderen Teilnehmenden etc., die ich alleine nicht kreiert habe und über die ich keine souveräne Kontrolle habe. In der Tat ist es so, dass die meisten Akteure in Netzwerken für sich in Anspruch nehmen, gewisse Rechte an den Daten, die im Netzwerk entstehen, zu haben. Bei näherer Betrachtung stellt sich heraus, dass Daten und Information viel eher Gemeingut denn Privateigentum sind. Gemeingüter sind zum Beispiel Luft, Wasser, Land etc., die nicht privat angeeignet werden können oder sollten und die durch das kooperative Handeln einer Gemeinschaft genutzt und verwaltet werden. Wir kommen später darauf zurück. Im Moment fragen wir uns, angesichts der Tatsache, dass Daten und Information nicht Dinge sind, die wie Eigentum behandelt werden können, welches Sicherheitskonzept der besonderen Natur von Daten und Information gerecht werden könnte.

Dieses Problem hat Paul Baran bereits 1960 im Auftrag der RAND Corporation durch das Konzept der «distributed networks» (verteilte Netzwerke) gelöst. Baran musste damals im kalten Krieg eine Lösung zum Problem der Aufrechterhaltung von Kommunikation im Falle einer nuklearen Attacke auf die USA finden. Wenn alle Information durch eine zentralisierte Kommandostelle fliessen musste, dann genügte eine gutplatzierte Atombombe, um die Kommunikation im ganzen Land zum Erliegen zu bringen. Wenn aber Information frei im Netzwerk fliessen kann und es keinen territorial zentralisierten Netzwerkknoten («node») gibt, dann kann das Netzwerk weiter funktionieren, auch wenn einige Knoten getroffen werden. Es wird oft vergessen und in der Literatur zum Thema Privatheit und Datenschutz nicht erwähnt, dass das Konzept der verteilten Netzwerke, das zur Grundlage des Internets wurde, ursprünglich ein Sicherheitskonzept war. Sichergestellt werden sollten aber nicht Dinge, wie im Schlosskonzept, sondern Konnektivität und das freie Fliessen («flow») von Information. Dass die digitale Welt als verteiltes Netzwerk zu verstehen ist und auch so funktioniert, erklärt zugleich, warum wir keine Privatheit haben und warum das Schlosskonzept von Sicherheit nicht funktionieren kann. Information kann nicht dadurch gesichert werden, dass man versucht sie in irgendwelche realen oder virtuellen Schlösser einzumauern, sondern im Gegenteil, dass man Information den Netzwerken übergibt, in denen sie entstanden sind. Dies scheint aber konzeptionell gerade das Gegenteil von Privatheit und Datenschutz zu sein. Denn diesem Konzept zufolge wird alles freigegeben und es gibt keine Grenzen und Mauern. Datenschutz und Privatheit

[32] Vgl. Belliger/Krieger (2018).

sind nicht mehr gewährleistet. Ohne Schutz der Privatsphäre sind wir aber all jenen Gefahren und Missbräuchen ausgeliefert, vor denen uns Privatheitsrechte und Datenschutzregulierungen bewahren sollen. Was können wir also tun, um dem Schaden, der durch den Verlust von Privatheit verursacht wird, entgegenzuwirken?

Sehen wir zunächst davon ab, Privatheit als ein fundamentales Menschenrecht zu betrachten, denn dieser Auffassung zufolge muss jede Preisgabe persönlicher Information als eine Art Übertretung des Rechts auf Privatheit betrachtet werden. Die Auffassung von Privatheit als fundamentalem Menschenrecht analog etwa zur Freiheit führt dazu, dass das Individuum mit seinen persönlichen Daten identifiziert wird und – wie Floridi dies interpretiert – der Verlust der Privatheit eher als eine Art «Entführung» der Person betrachtet werden müsste, was in keinem Fall rechtens wäre. In der Praxis geht die DSVGO nicht so weit und begnügt sich mit einer Auffassung von Privatheit als Entscheidungsmacht. Analog zur amerikanischen Auffassung von Privatheit als instrumentellem Recht sind personenbezogene Daten etwas, das wir «haben» und worüber wir entscheiden können, aber nicht etwas, das wir «sind». Privatheit stellt, wenn auch nicht in der Theorie so doch in der europäischen Praxis, kein fundamentales Recht wie z.B. die Freiheit dar. Wir können unsere Freiheit nicht entäussern oder uns in die Sklaverei verkaufen. Wir können aber sehr wohl unsere Daten preisgeben und tun dies ja auch ausgiebig. Die konkreten Freiheiten der DSVGO erlauben es, dass das Datensubjekt selber entscheidet, ob er oder sie persönliche Information entäussern und damit de facto Privatheit gegen etwas anderes eintauschen möchte.[33] Dies bedeutet, dass es sehr wohl andere Werte wie z.B. Geld, gewisse Produkte oder Dienstleistungen gibt, gegen die man persönliche Information tauschen kann.[34] Schauen wir uns also die Auffassung an, wonach Privatheit eher ein instrumentelles Recht darstellt und nur dann zur Geltung kommt, wenn Information missbraucht wird und konkrete Schäden entstehen. Nicht die blosse Kenntnis personenbezogener Information macht den Verlust von Privatheit aus, sondern der Missbrauch dieser Information, auch dann, wenn diese Information freiwillig und rechtens weitergegeben wurde. Vor welchem Schaden sollen uns aber die Privatheitsrechte schutzen?

Die Literatur zum Thema Privatheit erwähnt mindestens sechs verschiedene Schäden, die durch den Verlust von Privatheit entstehen:[35]

1. Missbrauch von persönlichen Informationen, z.B. Identitätsdiebstahl, Rufschädigung, Erpressung, Stalking
2. Verlust von Autonomie bzw. Konformismus oder “chilling effect” (abschreckende Wirkung) durch Überwachung
3. Repression durch Machtinstanzen, z.B. um Abstimmungen zu beeinflussen

[33] Diese Behauptung widerlegt den Versuch von Floridi, der DSVGO eine philosophische Grundlage zu geben, indem er argumentiert, dass der Mensch seine Daten *ist*, was bedeutet, dass diese Information einen Menschen *konstituieren* und somit niemals und unter keinen Umständen entäussert werden dürfen. Die Preisgabe persönlicher Information wäre, so Floridi, wie ein Kidnapping oder eine Entführung, da der Mensch aus seiner Information besteht. Das Problem dabei ist eigentlich nicht, dass der Mensch nicht Information ist, sondern, dass die Informationen, die er ist, nicht seine sind, sondern dem Netzwerk gehören. Das Netzwerk ist der Akteur.

[34] Natürlich werden personenbezogene Daten ganz legal für viele Zwecke erhoben und genutzt. Fast jede Interaktion mit Ämtern, der Justiz, der Steuerverwaltung, der Schule, mit Versicherungen und Banken etc. verlangt die Preisgabe personenbezogener Daten.

[35] Wir beschränken uns auf informationelle Privatheit und nicht auf den Schutz «against unreasonable searches and seizures» (gegen unangemessene Durchsuchungen und Beschlagnahmungen), die im 4. Zusatzartikel zur US-amerikanischen Verfassung eine grosse Rolle in der Rechtsprechung zum Thema Privatheit gespielt hat oder den Schutz vor «willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung», wie es in der Erklärung der Menschenrechte heisst.

4. Diskriminierung, wenn sensible Informationen, z.B. über Gesundheit, Ethnie, Religion, Sexualität die Gleichbehandlung verhindern
5. Kommerzielle Zielgruppenansprache («targeting») aufgrund von Profiling
6. Beeinflussung, Nudging oder Manipulation vor allem in politischer Kommunikation auf Basis von Profiling

Bei all diesen Schadenstypen, so könnte man sagen, entsteht der Schaden durch den Missbrauch von Information und nicht durch das blosse Wissen um diese Informationen. Wenn jemand meine persönlichen Daten nutzt, um illegale Einkäufe im Internet zu tätigen, dann ist dies Diebstahl und sollte entsprechend geahndet werden. Oder wenn ich erpresst werde, weil intime Bilder von mir gehackt werden, ist dies ebenso eine kriminelle Tat. Es entsteht aber kein Schaden, bloss weil die Information bekannt ist. Um aus dem Bekanntsein von Information ein Verbrechen zu machen, muss eine Verletzung meines Rechtes auf Privatheit hinzukommen.[36] In fast allen Fällen von Informationsmissbrauch sind andere Rechte als jenes auf Privatheit betroffen und diese Rechte sind durch entsprechende Gesetze geschützt.

Der zweite Schaden, der sich aus dem Verlust von Privatheit ergeben kann, ist der vermeintliche Verlust von Autonomie durch abschreckende Wirkung, den so genannten «chilling effect», der dadurch entstehen soll, dass man überwacht wird. Ob es diesen «chilling effect» wirklich gibt, ist fragwürdig. Niemals zuvor in der Geschichte der Menschheit wurde gleichzeitig so viel überwacht und so viel Diversität zur Schau gestellt und gefeiert. Überwachung ist zudem ein vielschichtiges Phänomen und funktioniert in alle Richtungen, nicht nur *top-down*, sondern ebenso gut auch *bottom-up,* wenn Bürger zum Beispiel die Handlungen der Polizei mit Smartphones aufzeichnen und auf Twitter posten. Daneben gibt es auch Co-veillance (Co-Überwachung), wie z.B. auf Facebook, wo alle einander überwachen.[37] Möglicherweise ist Facebook sogar das neue Panoptikum - nur eben mit umgekehrter Wirkung, indem alle ihre Nonkonformität zur Schau stellen. Dass man Privatheit braucht um anders zu sein, um «experiments with life» zu machen, wie John Stewart Mill es in seinem berühmten Aufsatz «On Freedom» behauptete, und um Freiheit und Autonomie zu garantieren, ist eine fragwürdige Annahme, die eher subjektive Befindlichkeiten als Tatsachen zum Ausdruck bringt und kaum als Rechtsbegründung herhalten kann.

Privatheit wird auch im Fall geheimer Abstimmungen ins Feld geführt. Das Problem der Repression von Bürgern, die nicht so wählen, wie die Machthaber es möchten, wurde durch das geheime Abstimmen gelöst. Wie man abstimmt, sollte niemand wissen, damit der Chef oder der Machthaber nicht Druck aufsetzen oder Vergeltung üben kann. Privatheit wird damit zur Voraussetzung für Demokratie.[38] Diese Lösung hat allerdings ihren Preis. Denn dieses Argument vergisst, dass demokratische Prozesse nicht alleine aus Abstimmungen und Wahlen bestehen. Vor der Abstimmung müssen öffentliche Diskurse, Debatten und Stellungnahmen geführt werden. Bürger müssen aufstehen und laut und klar sagen, wie sie wählen werden und warum. Wenn niemand öffentlich erklärt, wofür er oder sie zu politischen Themen steht, dann kollabiert die Demokratie. Wenn Martin Luther King und mit ihm viele andere nicht entschieden hätten, ihr Recht auf Privatheit beiseite zu lassen und aus dem Schatten zu treten, gäbe es keine Bürgerrechtsbewegung in den USA und keine

[36] Um doch ein Recht auf Privatheit zu begründen wird in solchen Fällen ein «psychischer» Schaden hinzugedacht, da anzunehmen ist, dass Personen - auch wenn tatsächlich noch nicht eingetreten - den Missbrauch fürchten und erwarten. Angesichts der Realität von Hacking, kommerziellem Profiling und Selbstpreisgabe von Information können wohl nur jene solche Angst- und Unsicherheitsgefühle vermeiden, die massive Selbsttäuschung ausüben.

[37] Vgl. z.B. Mann (2016).

[38] Wie umstritten diese Annahme tatsächlich ist und wie unterschiedlich Privatheit in politischem Handeln gehandhabt wird, lässt sich aus den historischen und theoretischen Studien in Elster (2018) belegen.

Gesetze gegen Rassismus und Diskriminierung. Die konsequente Geheimhaltung politischer Entscheidungen wirkt gegen die Demokratie, nicht nur weil sie Menschen daran hindert, politisch aktiv zu werden, sondern weil sie Missstände nicht offen bekämpft und somit den Missbrauch von Macht als unveränderbare Tatsache widerstandslos hinnimmt. Das wahre Paradoxon der Privatheit besteht nicht darin, dass Menschen Privatheit zwar explizit schätzen, trotzdem aber freiwillig ihre Daten preisgeben, sondern darin, dass Privatheit eigentlich das zementiert, wogegen sie kämpft, nämlich Diskriminierung und soziale Ungerechtigkeit.

Dies ist auch der Grund, warum das Argument von Privatheit als Schutz vor Diskriminierung nicht überzeugt. Information über Ethnizität, Rasse, Religion, sexuelle Präferenzen, politische Ansichten, Gesundheitszustand etc. wird als «sensibel» und besonders schützenswert betrachtet, weil sie als Grund für Diskriminierung missbraucht werden kann. Deswegen wird z.B. im Namen von Privatheit das Lügen über den eigenen Gesundheitszustand bei der Anmeldung für eine Krankenversicherung erlaubt. Oder bei Anstellungsbewerbungen werden Informationen über Rasse, ethnische oder religiöse Zugehörigkeit etc. ausgeklammert. Auch hier ist die Frage berechtigt, ob das Recht auf Privatheit nicht mehr bedeuten müsste, als das Recht darauf, Lücken zu finden und zu nutzen, um in einem an sich ungerechten System durch das Zurückhalten von Information möglichst viele Vorteile für sich heraus zu hohlen. Anstatt opportunistische Geschäftsmodelle im Gesundheitssystem anzuprangern und noch wirksamere Gesetze gegen Diskriminierung zu schaffen, wird Privatheit als Waffe der Schwachen eingesetzt, um ein bisschen mehr Gerechtigkeit aus dem nicht mehr zu ändernden und hoffnungslos ungerechten System herauszuholen.[39]

Privatheit wird schliesslich oft als Schutz gegen kommerzielles oder politisches *Targeting* eingesetzt. *Targeting* bedeutet, dass persönliche Informationen genutzt werden, um Werbung oder Botschaften gezielt z.B. auf die Interessen, die Kaufkraft, das Konsumverhalten, die Ansichten, das Alter einer Person abzustimmen. Dies wird oft auch als «Nudging» bezeichnet.[40] Beim *Nudging* (Stups oder Schubs) handelt es sich um eine Methode, das Verhalten einer Person durch gezielt angepasste Botschaften zu beeinflussen. Fitnesstrackers beispielsweise machen darauf aufmerksam, dass man nach einer bestimmten Zeit der Inaktivität aufstehen und sich bewegen sollte. Werbebotschaften sind in einer bestimmten Sprache und in bestimmten Medien platziert, um bestimmte psychologische Typen anzusprechen. In Prinzip gehört es zum *Nudging, dass es* transparent ist, d.h. ich weiss, dass mein Fitnesstracker weiss, dass ich schon zwei Stunden am Pult sitze und er mir deshalb die Ermahnung sendet, mich zu bewegen. Wenn *Nudging* nicht transparent ist, kann es als Manipulation bezeichnet werden.[41] Seit dem Einsatz personalisierter Kommunikation auf Basis von Profiling 2016 anlässlich der Präsidentschaftswahlen in den USA und des Brexits sind die Gefahren von Manipulation ins Zentrum der Diskussionen um Privatheit gerückt. Um personalisierter Werbung und politisch motivierter Manipulation entgegenzuwirken, wird auf Privatheit zurückgegriffen und zwar mit der Vorstellung, man könne das Problem durch das Zurückhalten persönlicher Informationen lösen. Profiling soll – sofern Transparenz fehlt oder das Profiling nicht gewollt ist – illegal sein. Wenn ich aber weiss, wozu meine Daten genutzt werden und ich stimme dieser Nutzung zu, dann ist alles in Ordnung. Ich kann also meine Privatheit gegen personalisierte Produkt- und Dienstleistungsangebote tauschen. Dies macht in vielen Fällen auch durchaus Sinn, denn wer will schon Spam, wenn man Werbung und politische Botschaften erhalten kann, die die tatsächlichen Interessen reflektieren und diesen entsprechen? Personalisierte Produkte, Dienstleistungen, aber

[39] Für Posner (1978: 26) ist Privatheit nichts anders als das «right to conceal discreditable facts" über sich, d.h. das Recht, diskreditierende Tatsachen zu verbergen.
[40] Vgl. Taler/Sunstein (2008).
[41] Vgl. dazu die differenzierte Analyse der Bedeutung und Methoden der Manipulation im entsprechenden Beitrag der Stanford Encyclopedia of Philosophy https://plato.stanford.edu/entries/ethics-manipulation/.

auch Informationen können als «smart» bezeichnet werden, wenn sie auf die tatsächlichen Interessen und Bedürfnisse von Individuen abgestimmt sind. Alles was «smart» ist, bietet einen Mehrwert für den Konsumenten oder den Bürger, auch wenn dies wirtschaftliche Konkurrenten oder politische Gegner so nicht anerkennen möchten.

In diesem Punkt erweist die DSVGO der Gesellschaft tatsächlich einen Dienst, denn sie zwingt Organisationen dazu, endlich Transparenz über die Sammlung und Nutzung personenbezogener Daten zu schaffen. Der Endeffekt von Transparenz ist jedoch, nicht wie die Befürworter der neuen Regulierung erwarten, Privatheit, sondern das Gegenteil, dass nämlich die meisten Menschen *smarte* Dienstleistungen wollen und Profiling akzeptieren oder sogar willentlich fördern, indem sie explizit noch mehr Information über sich preisgeben, um noch *smartere* Produkte und Dienstleistungen zu erhalten. Es ist ziemlich einfach für die Medien dauernd Skandale um das Thema «Privatheit» zu generieren wie wie vor einiger Zeit bei der Politberatungsfirma Cambridge Analytica.[42] Trotz Appellen prominenter Kritiker die Facebook-Kontos wegen dieses angeblichen Skandals zu löschen, waren die im April 2018 gemeldeten Quartalseinnahmen von Facebook die höchsten überhaupt.[43] Das Phänomen, dass Menschen einerseits sagen, sie hätten Angst vor dem Verlust der Privatheit, sie aber im eignen Handeln persönliche Information freiwillig und sorglos preisgeben, ist als «Privatheitsparadoxon» gut dokumentiert. Offensichtlich ist Privatheit zugleich etwas Wichtiges und doch etwas, das nicht besonders schützenswert ist, denn fast keiner der oben erwähnten und viel diskutierten Schäden, die aus dem Verlust von Privatheit entstehen, sind wirksam oder langfristig durch Privatheit zu verhindern. Im Gegenteil, man hat den Eindruck, dass das eigentliche Privatheitsparadoxon darin besteht, dass Privatheit zur Aufrechterhaltung der sozialen Missstände beiträgt, die es bekämpfen sollte. Das Privatheitsparadoxon könnte als wichtiger Hinweis verstanden werden, Privatheit als zutiefst problematischen Begriff zu betrachten, ein Begriff, der von Grund auf und im Rahmen des digitalen Zeitalters neu konzipiert werden muss.[44] Auf jeden Fall ergibt sich aus der Diskussion über die angeblichen Schäden, die aus dem Verlust von Privatheit entstehen, dass es durchaus Sinn machen könnte, Paul Barans Idee der *distributed networks,* der verteilten Netzwerke, als Sicherheitskonzept für die digitale Welt ernst zu nehmen.

«Get over it» - Auf dem Weg zur Network Publicy Governance

Diese Überlegungen führen unweigerlich zur Frage, was denn nun dieses «get over it» von McNealy in Bezug auf den Verlust der Privatheit bedeuten könnte. Stowe Boyd schlägt vor, von der Idee wegzukommen, der Mensch sei primär ein privates, eingegrenztes Individuum, das sekundär auf verschiedene Art und Weise über die Grenze dieser Privatheit hinaus geht, um sich in soziale Beziehungen zu begeben. Wir müssen von der Idee wegkommen, dass die Gesellschaft auf der einen Seite aus individuellen Menschen und auf der anderen Seite aus dem zentralistischen Staat, dem Leviathan, wie Hobbes sagt, besteht. Die Standardeinstellung des Menschen im digitalen Zeitalter ist nicht Privatheit, sondern, wie Boyd sagt, *Publicy*.

> There is a countervailing trend away from privacy and secrecy and toward openness and transparency, both in the corporate and government sectors. And on the web, we have had several major steps forward in social tools that suggest at least the outlines of a complement,

[42] Vgl. Wikipedia: https://de.wikipedia.org/wiki/Cambridge_Analytica.
[43] Vgl. Wikipedia: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.
[44] Es scheint, dass Privatheit zum «obligatory passage point» (obligatorischer Durchgangspunkt) geworden ist, um in die digitale Welt zu kommen. Vgl. Wikipedia https://en.wikipedia.org/wiki/Obligatory_passage_point: «An OPP can be thought of as the narrow end of a funnel, that forces the actors to converge on a certain topic, purpose or question."

> or opposite, to privacy and secrecy: publicy. The idea of publicy is no more than this: rather than concealing things, and limiting access to those explicitly invited, tools based on publicy default to things being open and with open access.[45]

Falls Boyds Vermutung stimmt, dass der Mensch gar nicht ein Privat-Individuum , sondern von Natur aus in Informationsnetzwerken beheimatet ist, dann verschwindet die philosophische Grundlage der Idee von Privatheit.[46] Das autonome, rationale Subjekt der europäischen Aufklärung, das isolierte Individuum der modernen politischen Theorie, das individualistisch gedachte Subjekt der Menschenrechte löst sich auf in das, was als «informationelles Selbst» bezeichnet werden könnte. Floridi (2014) spricht vom «Inforg» statt Cyborg, der in einer Welt von Information, einer «Infosphere» existiert. Da Information in Netzwerken entsteht und Netzwerken gehört, ist der Grundzustand des informationellen Selbst die Publicy und nicht die Privatheit.

In diesem Zusammenhang ist es wichtig, sich daran zu erinnern, dass Privatheit nicht das einzige Recht ist, das mit Information zu tun hat. Es gibt auch das Recht auf freie Meinungsäusserung. Die Debatte, um nicht zusagen der Konflikt zwischen dem Recht auf Privatheit einerseits und dem Recht auf freie Meinungsäusserung andererseits ist bekannt, komplex und wird sowohl im akademischen Diskurs wie in der Rechtsprechung viel diskutiert und unterschiedlich beurteilt worden. [47] Die digitale Transformation ändert das Terrain für die Diskussion sowohl für das Thema Privatheit, als auch das Thema Recht auf freie Meinungsäusserung. Die Digitalisierung macht es notwendig, dass die ziemlich festgefahrenen Positionen der alten Debatten grundsätzlich revidiert werden. Der neue Grundzustand *d*es Menschen in Form von *Publicy* anstelle von Privatheit führt zu einer partizipativen Kultur, die die Bedeutung des Rechtes auf freie Meinungsäusserung ebenso wie die Bedeutung des «öffentlichen» Raumes erweitert. Das informationelle Selbst ist von sich aus auf Informationsproduktion und Kommunikation ausgelegt. Wo sich früher das Recht auf freie Meinungsäusserung eher auf die politische Debatte im Rahmen einer für die Politik reservierten «Öffentlichkeit» beschränkte, wird heute angesichts der durch die Digitalisierung entstandenen Kultur der Partizipation von einer Erweiterung des Rechts auf freie Meinungsäusserung auf alle kulturellen Schöpfungen und alle Formen der Informationsnutzung gesprochen. Egal ob das Thema Politik ist oder nicht, das Recht auf Zugang zu Information und das Recht, Information kreativ zu gestalten und zu verbreiten, trägt wesentlich zur «demokratischen Kultur» des digitalen Zeitalters bei. Die traditionelle, eher eingeschränkte Idee der politischen «Öffentlichkeit» wird durch eine globale und prinzipiell unbegrenzte «Sozio-Sphäre» ersetzt.[48]

Die «Affordances» (Einflüsse) der digitalen Technologien und das sozio-technische Ensemble von Netzwerkformen der Kommunikation und Kooperation haben nach Castells (2017) zu einer globalen Netzwerkgesellschaft geführt. Clay Shirky (2008) hat darauf hingewiesen, dass die neuen Medien nicht die Mittel der Informationsproduktion und -verteilung, sondern auch viele neuen Formen der sozialen und wirtschaftlichen Partizipation in die Hände aller gegeben haben. Jenkins et. al. (2005) sprechen von einer «participatory culture» (partizipative Kultur), die auf tiefe Hürden für kreative Informationsgestaltung und soziales Engagement, starke Unterstützung für das Teilen und Mitteilen von Information und die Überzeugung, dass Teilnahme und Mitgestaltung wichtig sind, baut. Der Verfassungsrechtler Jack M. Balkin (2016) spricht davon, dass die digitale Revolution in Bezug auf das

[45] Blogpost 2009: https://medium.com/@stoweboyd/secrecy-privacy-publicy-5bc7a5b67daa.
[46] Was nicht bedeutet, dass es nur noch den Staat gibt, dessen totalitärer Macht die Menschen nunmehr ohne den Schutz von Privacy wehrlos ausgeliefert sind. Mit dem Verschwinden der freien und im Naturzustand lebenden Individuen verschwindet auch der «Leviathan», der sie bändigen soll.
[47] Vgl. z.B. die vielen Beitrage zum Projekt «Free Speech Debate» http://freespeechdebate.com/de/discussions/
[48] Für eine Diskussion der Sozio-Sphäre vgl. Krieger/Belliger (2014).

Recht zu freier Meinungsäusserung eine neue Situation für die Demokratie geschaffen hat. Demokratische Kultur basiert für Balkin darauf, dass alle das Recht haben, kreativ und gestalterisch an Kultur im breitesten Sinn teilzuhaben, d.h. sich kulturelle Schöpfungen auf individuelle Art und Weise anzueignen, neu zu gestalten und zu verwenden. Für Balkin ebenso wie für Boyd stellt die «Demokratisierung» der Mittel der Informationsproduktion und -verteilung nicht nur Privatheit in Frage, sondern ebenso traditionelle Auffassungen des Immaterialgüterrechts, von Copyright und geistigem Eigentum. Im Gegensatz zu Privatheit und Datenschutz ist das Recht auf freie Meinungsäusserung gemeinsam mit der Versammlungsfreiheit auf dem Prinzip der Publicy begründet, d.h. auf Kommunikation, Partizipation und Transparenz. Wo der Diskurs zum Thema Privatheit Freiheit und Autonomie im Rückzug aus der Öffentlichkeit, in Gemeinhaltung oder im Zurückhalten von Information sieht, impliziert Publicy, dass Freiheit im Gegenteil darin besteht, an einer demokratischen Kultur der Partizipation teilzunehmen.
Balkin beschreibt dies folgendermassen:

> Freedom is participation. Freedom is distribution. Freedom is interaction. Freedom is the ability to influence and be influenced in turn. Freedom is the ability to change others and to be changed as well. […] Freedom is appropriation, transformation, promulgation, subversion, the creation of the new out of the old. Freedom is mixing, fusing, separating, conflating, and uniting. Freedom is the discovery of synergies, the reshuffling of associations and connections, the combination of influences and materials. Freedom is bricolage. (Balkin 2004: 44)

Wo Privatheit und Datenschutz ein fundamentales Recht auf die Entscheidungsbefugnis sieht, Information zurück- oder geheim zu halten, sehen Boyd, Balkin und andere die Verwirklichung der Freiheit und der Autonomie in der aktiven Partizipation an einer demokratischen Kultur. Kommunikation, Partizipation und Transparenz machen frei und eben nicht Geheimhaltung. Der Schutz der Freiheit liegt demnach nicht in der Privatheit, sondern in einer regulierten Publicy. Wie alles andere muss Publicy auch reguliert sein, um den oben erwähnten Missbräuchen der neuen Medien wie Filterblasen, Echokammern, Manipulation, schädlicher Amplifikation, Geschwindigkeitsexzessen oder Netzwerkeffekten entgegenzuwirken. Die Frage lautet also nicht, wie durch den Staat noch restriktivere Massnahmen zum Schutz von Privatheit und Datenschutz implementiert werden können, sondern wie Publicy reguliert werden kann. Diese Frage ist auch relevant für das Problem der Legitimation von Entscheidungsinstanzen und die Identifizierung von Verantwortungsträgern in einer globalen Netzwerkgesellschaft, in der sich traditionelle, zentralisierte Regulierung in verteilte Netzwerke aufgelöst hat.

Unter dem Stichwort «Governance statt Government»[49] werden neue Formen der Regulierung diskutiert, die anstelle traditioneller Hierarchien und top down Kommunikation verteilte und partizipative Regulierungspraktiken beschreiben. Governance ist besonders geeignet für die Regulierung von Netzwerkorganisationen, denn Netzwerke kennen keine zentrale

[49] Für eine grundlegende Diskussion vgl. Chhotray/Stoker (2009); Benz/Dose (2010) und als Beispiel http://www.partizipation.at/governance.html: «Governance bezeichnet allgemein das Steuerungs- bzw. Regelungssystem in einer Gesellschaft. Verschiedene Interessen von privaten und öffentlichen AkteurInnen (Bevölkerungsgruppen, Unternehmen, Politik und Verwaltung) werden über dieses System ausverhandelt und umgesetzt. Der Begriff Governance ist relativ jung und leitet sich vom englischen Government (Regierung) ab. Es gibt keine passende deutsche Übersetzung. Government steht für das traditionelle Lenken einer Gesellschaft über eine ‚top down' funktionierende Regierung. Governance soll ausdrücken, dass an der Steuerung und Regelung nicht nur der Staat, sondern auch die Privatwirtschaft und die Öffentlichkeit (Vereine, Interessensvertretungen, BürgerInneninitiativen, Medien, …) beteiligt sind, die über formelle und informelle Netzwerke zusammenwirken. Die Rolle des Staates soll nicht untergraben, sondern neu definiert werden. Partizipation spielt dabei eine grosse Rolle.»

Entscheidungsinstanz oder hierarchische Entscheidungssouveränität. In Bezug auf Privatheit bedeutet Governance, dass den Netzwerkeigenschaften von Information Rechnung getragen wird. In Netzwerken ist das Individuum nicht alleine ermächtigt, souverän über die Datennutzung zu entscheiden. Zwar hat jede Anspruchsgruppe ein Mitentscheidungsrecht, eine Stimme, aber nicht das alleinige Entscheidungsrecht, wie dies gemäss Datenschutz- und Privatheitsregulation vorgesehen ist. Im Privatheitsrecht werden Daten und Information ähnlich wie Privateigentum behandelt. Wenn Information, auch personenbezogene Information, aber nicht als Eigentum verstanden werden kann, als was dann? Um diese Frage zu beantworten, könnte man auf die Idee des Gemeinguts («Commons») zurückgreifen.[50] Auch wenn Information nicht ohne weiteres mit natürlichen Ressourcen wie Wasser, Land, Wälder und Wiesen gleichzusetzen ist, kann Wissen, Code und Information als eine Art Gemeingut verstanden werden, denn Information gehört dem Netzwerk, d.h. einer Gemeinschaft und kann dementsprechend von allen Anspruchsgruppen im Netzwerk genutzt und verwaltet werden. Trotz anfänglicher Skepsis[51] hat Elinor Ostrom darauf hingewiesen, dass es viele erfolgreiche Beispiele für die Governance von «Common Pool Resources» gibt.[52] Was alle erfolgreichen Beispiele von Commons-Governance gemeinsam haben, sind Praktiken und Prinzipien, die eine Art Governance-Framework bilden. Diese sind:

- Die Identität der Gemeinschaft und der betroffenen Ressourcen sind klar definiert.
- Kosten und Nutzen sind proportional.
- Anspruchsgruppen verhandeln über Beiträge und Erträge.
- Die Mitglieder der Gemeinschaft müssen ihre eigenen Regeln implementieren und eigene Entscheidungen aufgrund von Konsens machen können.
- Kontrollmechanismen müssen vorhanden sein.
- Differenzierte und gestufte Sanktionen müssen getätigt werden können.
- Konfliktlösungsmechanismen sind eingerichtet.
- Das Recht, sich selber zu organisieren, ist anerkannt.
- Selbstverwaltung ist anerkannt.
- Verbindungen zu umgebenden sozialen Systemen und Koordination mit ihnen müssen vorhanden sein. (Wilson/Ostrom/Cox 2013: 2)

Will man diese Governance-Prinzipien spezifisch für Informationsnetzwerke, in denen das informationelle Selbst im Zustand der Publicy lebt, anwenden, dann müssen die Affordances digitaler Technologien und deren Einfluss auf die Ordnung des Wissens, auf soziales Handeln und auf das Selbstverständnis des Menschen berücksichtigt werden. Die Affordances digitaler Medien können als «Netzwerknormen» verstanden werden, d.h. als institutionelle und normative Handlungstendenzen. Diese sind, wie schon erwähnt, Kommunikation, Partizipation und Transparenz, hinzu kommen Konnektivität, Flow von Information, Authentizität und Flexibilität.[53] Anstelle des Managements der persönlichen Privatheit (Personal Privacy Management) tritt *Network Publicy Governance*.[54] Anstelle der reaktiven Tendenz nach immer restriktiveren Privatheits- und Datenschutzregulierungen könnten Missbräuche dadurch gekämpft werden, dass im Sinne von Paul Baron's *distributed networks* Konnektivität, Flow von Information, Kommunikation, Partizipation, Transparenz, Authentizität und Flexibilität durch geeignete Governance-Frameworks unterstützt werden. Die Rolle von Regierungen und Verwaltungen würde sich dementsprechend darauf beschränken, Massnahmen und Garantien

[50] Für eine Orientierung zu diesem Thema vgl. den Wikipedia-Artikel https://de.wikipedia.org/wiki/Commons.
[51] Vgl. dazu die «Tragedy of the Commons» (Allmendeproblematik) und viele der heute diskutierten Missbräuche des Internets.
[52] Vgl. dazu Ostrom (1990).
[53] Für eine ausführliche Diskussion und Begründung der Netzwerknormen vgl. Krieger/Belliger (2014).
[54] Vgl. Belliger/Krieger (2018).

zu etablieren, die garantieren, dass alle Anspruchsgruppen eine Stimme haben und Transparenz gewährleistet ist. Das Recht auf Privatheit wird ersetzt durch das Recht auf Publicy, d.h. auf Partizipation in Informationsnetzwerken. Das informationelle Selbst, dessen Grundzustand Publicy ist, würde Freiheit, Autonomie und Würde nicht durch Geheimhaltung, das Blockieren von Informationsflüssen oder durch das sich Abgrenzen von sozialen Beziehungen, sondern in der partizipativen Gestaltung und Verbreitung von Information erleben. Wenn es so ist, wie McNealy sagt, dass wir sowieso keine Privatheit haben, dann hängt vieles davon ab, ob und wie wir Privatheit «hinter uns lassen». *Network Publicy Governance* könnte den Weg in die digitale Zukunft bahnen und gegenwärtige Hindernisse in der Verwirklichung einer datengetriebenen Gesellschaft überwinden, ohne dabei Freiheit, Autonomie und Würde zu untergraben. Dies verlangt aber nach einem neuen Denken und der Bereitschaft traditionelle Werte und tief verankerte Annahmen zu hinterfragen.

Literatur

Balkin, J. M. (2004): "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society," in: New York University Law Review, Vol. 79, No. 1, 2004. Available at SSRN: https:// papers.ssrn.com/sol3/papers.cfm?abstract_id=470842

Balkin, J. M. (2008): "The Future of Free Expression in a Digital Age," in: Pepperdine Law Review, Vol. 36, pp. 101-118.

Balkin, J. M. (2016): "Cultural Democracy and the First Amendment." In: Northwestern University Law Review, Vol. 109, 2016. Available at SSRN: https://ssrn.com/abstract=2676027.

Barnes, S. B. (2006): A Privatheit Paradox: Social Networking in the United States. First Monday, 11(9). http://firstmonday.org/article/view/1394/1312_2.

Belliger, A., Krieger, D. J. (2016): Organizing Networks. An Actor-Network Theory of Organizations. Bielefeld: transcript.

Belliger, A., Krieger, D. J. (2018): Network Publicy Governance. On Privatheit and the Informational Self. Bilefeld: transcript.

Benz, A., Dose, N. (Hrsg.) (2010): Governance – Regieren in komplexen Regelsystemen. Eine Einführung. 2., aktualisierte und veränderte Auflage. VS Verlag, Wiesbaden.

Brandimarte, L., Acuisti, A., Lowenstein, G. (2012): Misplaced Confidences: Privatheit and the Control Paradox, in: Social Psychologal and Personality Science 4(3) 340-347. Sage.

Castells, M. (2017): Der Aufstieg der Netzwerkgesellschaft. Das Informationszeitalter – Wirtschaft , Gesellschaft, Kultur. Band 1. 2. Auflage. Springer VS: Wiesbaden.

Chhotray, V., Stoker, G. (2009): Governance Theory and Practice. A Cross-Disciplinary Approach. UK: Palgrave Macmillan.

Elster, J. (Hrsg.) (2018): Secrecy and Publicitiy in Votes and Debates. Cambridge University Press: UK.

Floridi, L. (2014): The Fourth Revolution: How the Infosphere Is Reshaping Human Reality. New York: Oxford University Press.

Gerber P., Volkamer M., Gerber N. (2017) Das Privatheit-Paradoxon – Ein Erklärungsversuch und Handlungsempfehlungen. In: DDV Deutscher Dialogmarketing Verband e.V. (eds) Dialogmarketing Perspektiven 2016/2017. Springer Gabler: Wiesbaden.

Gillespie, T. (2018): Custodians of the Internet Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media. New Haven & London: Yale University Press.

Habermas, J. (1997): Theorie des kommunikativen Handelns. (2 Bände), Neuauflage. Suhrkamp: Frankfurt a.M.

Jenkins, H. et al. (2005): Confronting the Challenges of Participatory Culture: Media Education for the 21st Century, http://www.newmedialiteracies.org/ wp-content/uploads/pdfs/NMLWhitePaper.pdf.

Krieger, D. J./Belliger, A. (2014): Interpreting Networks: Hermeneutics, Actor-Network Theory, and New Media. Bielefeld: Transcript.

Latour. B. (2017): Kampf um Gaia. Acht Vorträge über das neue Klimaregime. Suhrkamp: Frankfurt a.M.

Macleod, A. M. (2018): Privatheit: Concept, Value, Right?, in: Cudd, A. E., Navin, M. C. (eds.) (2018): Core Concepts and Contemporary Issues in Privatheit. Springer, 31-45.

Mann, S. (2016): "Surveillance (oversight), Sousveillance (undersight), and Metaveillance (seeing sight itself)." In: The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops. Available at: http://www.cvfoundation.org//openaccess/content_cvpr_2016_workshops/w29/papers/Mann_Surveillance_Oversight_Sousveillance_CVPR_2016_paper.pdf

Nissenbaum, H. (2004): "Privatheit as Contextual Integrity," in: Washington Law Review 79 (2004), pp. 101-139.

Norberg, P. A., Horne, D. R., Horne, D. A., (2007): "The Privatheit Paradox: Personal Information Disclosure Intentions versus Behaviors." In: Journal of Consumer Affairs 41(1), pp. 100-126.

Ostrom, E. (1990): Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge, UK: Cambridge University Press.

Posner, R. A., (1978): "An Economic Theory of Privatheit." in: Regulation 2, pp. 19–26.

Shirky, C. (2008): Here Comes Everybody. How Change Happens When People Come Together. New York: Penguin Press.

Taler, R., Sunstein, C. (2008). Nudging- Wie man kluge Entscheidungen anstösst. 5. Auflage. Econ: Berlin.

Thouvenin, F. (2017): Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs., In: Zinder, F. G., Schmid, H., Pichonnaz, P. (Hrsgs.) SJZ 113/2017 21-32.

Waldo, J., Lin, H. S., Millett, L. (eds.) (2007): Engaging Privatheit and Information Technology in a Digital Age. National Research Council. Committee on Privatheit in the Information Age. Washington DC: National Academy of Sciences.

Wilson, D.S., Ostram, E., Cox, M. E. (2013): "Generalizing the Core Design Principles for the Efficacy of Groups," in: Journal of Economic Behavior & Organization 90s (2013), pp. 21-32.