"It was the best of times, it was the worst of times": Internet und Demokratie nach den Snowden-Leaks

Thiel, Thorsten

Postprint / Postprint
Sammelwerksbeitrag / collection article

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Hessische Stiftung Friedens- und Konfliktforschung (HSFK)

Empfohlene Zitierung / Suggested Citation:
Thiel, T. (2014). "It was the best of times, it was the worst of times": Internet und Demokratie nach den Snowden-Leaks. In I.-J. Werkner, J. Kursawe, M. Johannsen, B. Schoch, & M. v. Boemcken (Hrsg.), *Friedensgutachten 2014* (S. 252-263). Berlin: Lit-Verl. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54789-3

3.3. „It was the best of times, it was the worst of times". Internet und Demokratie nach den Snowden-Leaks

Thorsten Thiel

Nachdem das Internet lange mit Demokratie und freiheitlicher Politik identifiziert wurde, haben die durch Edward Snowden enthüllten Überwachungspraktiken der *National Security Agency* (NSA) und anderer Geheimdienste starke Zweifel an den Segnungen digitaler Kommunikation ausgelöst. Es liegen nur zwei Jahre zwischen der Ernennung des unbekannten Protestierenden zur Person des Jahres, in der sich der feste Glaube an die emanzipatorische Kraft einer anders kommunizierenden Gesellschaft manifestierte, und den ungezählten Leitartikeln, die das düstere Bild einer den Bürger vollständig entmündigenden Macht zeichnen. Die Vorstellung von der emanzipatorischen Kraft des Netzes hat sich in die Warnung vor dessen repressivem Potenzial verkehrt.

Dieser Beitrag soll nachzeichnen, was die emanzipatorische bzw. repressive Bewertung begründet. Meine These lautet, dass wir Gefahr laufen, das Kind mit dem Bade auszuschütten. Beide Positionen überschätzen den Grad der Determiniertheit dieser Entwicklung und ignorieren tendenziell deren soziale wie politische Faktoren. Die Hoffnung auf eine demokratische Dividende der informationstechnologischen Revolution muss auch nach der NSA-Affäre nicht einfach aufgegeben werden. Um sie aber realisieren zu können, wird es nötig sein, die Offenheit des Netzes in mehreren Dimensionen zu sichern: technisch, wirtschaftlich, politisch und rechtlich. Dabei ist der modischen Forderung nach der Rückbindung des Cyberspace in die Domäne nationalstaatlicher Souveränität ebenso entgegenzutreten wie dem libertären Appell, das Netz den Marktmechanismen zu überlassen. Eine eigenständige, dem Netzwerkcharakter digitaler Kommunikation angepasste und transnational erarbeitete Internetpolitik bietet am ehesten die Chance, das Potenzial der sich ändernden Kommunikationsbedingungen auszuschöpfen. Nur so lässt sich verhindern, dass das Internet sich in jenen gefahrvollen und fragmentierten Raum verwandelt, den die von Snowden enthüllte geheimdienstliche Aktivität zu bekämpfen vorgibt.

Die Versprechen digitaler Kommunikation

Der Einfluss digitaler Kommunikationsnetze auf das Zusammenleben moderner Gesellschaften ist enorm; die fortschreitende Vernetzung aller technischen Geräte ist so umfassend wie permanent. Moderne Informationstechnologie

strukturiert, was uns an Kommunikationen erreicht und definiert, wie wir auf diese reagieren können. Nur so bleibt es möglich, die exponentiell gestiegene Zahl von potenziell relevanten Kommunikationen zu bündeln und beherrschbar zu machen. Informationstechnologie hat somit tiefgreifende und weitgehend irreversible Folgen für menschliches Wirken und Handeln.[1]

Digitale Kommunikation hat charakteristische Eigenschaften, die sie von analogen Medien deutlich unterscheidet: Sie reduziert die Bedeutung räumlicher Faktoren, sie macht große, nicht festgelegte Gruppen erreichbar, ohne von *Gatekeepern* wie Zeitungsredaktionen abhängig zu sein, sie erlaubt die verlustfreie Speicherung und Vervielfältigung von Kommunikationsinhalten sowie die Übermittlung und Verarbeitung von sehr großen Mengen an Informationen in sehr kurzer Zeit.

Die Ausbreitung digitaler Kommunikation senkt zunächst quantitativ die Kommunikationskosten, doch kommt es in der Folge auch qualitativ zu gravierenden Veränderungen: Emails sind nicht einfach eine papierfreie Form des Briefes, Webseiten nicht sich schneller aktualisierende Zeitungen, Chaträume nicht die Kaffeehäuser des 21. Jahrhunderts. Vielmehr vollzieht sich in jeder dieser Instanzen – und mehr noch in genuin durch das Internet hervorgebrachten Formaten wie der Wikipedia – eine tiefgreifende Transformation sozialen Zusammenlebens.[2] Der neue „Strukturwandel der Öffentlichkeit" durch die Möglichkeiten der *many-to-many*-Kommunikation reduziert strukturelle Barrieren kollektiven Handelns und wirft dadurch insbesondere die Frage auf, wie sich die informations- und kommunikationstechnologische Revolution auf die normative Qualität sozialer und politischer Ordnungen auswirkt, sprich: inwiefern Digitalisierung Demokratisierung nach sich zieht.

Aus den genannten Strukturmerkmalen digitaler Kommunikation lässt sich unter Bezug auf gängige Demokratietheorien eine Position formulieren, die die Chancen des Medienwandels für die Demokratie betont und auf die öffentliche Imagination des Cyberspace zunächst großen Einfluss ausübte. So stellt für ein liberales Verständnis von Demokratie mehr Transparenz und dadurch verbesserte Kontrolle von Eliten potenziell eine enorme Aufwertung der Demokratiequalität dar. Ob mittels *Leaking*, *Open Government Data* oder *Bottom-Up*-Initiativen wie *abgeordnetenwatch.de* oder *fragdenstaat.de*: Digi-

1 Manuel Castells: The Rise of the Network Society, Cambridge, Mass. 2010.

2 Zentrale Studien zum politischen Potenzial dieser Veränderung sind: Yochai Benkler: The Wealth of Networks: How Social Production Transforms Markets and Freedom, New Haven 2006; Jennifer Earl/Katrina Kimport: Digitally Enabled Social Change, Boston 2011; Clay Shirky: Here Comes Everybody, London 2008; Lance W. Bennett/Alexandra Segerberg: The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics, Cambridge 2011.

tale Kommunikation wird als Chance begriffen, Meinungsvielfalt zu sichern und die Qualität öffentlicher Diskurse zu erhöhen. Anhänger eines partizipatorischen Demokratieverständnisses sehen in der Ausbreitung digitaler Kommunikationsformen gar die Möglichkeit, das klassische athenische Demokratieideal wieder aufleben zu lassen. So soll das Ohnmachtsgefühl gegenüber der Spezialisierung funktional differenzierter Politik zurückgehen und eine unmittelbare Beteiligung an Entscheidungen möglich werden. In einer dritten, kritischen Tradition demokratietheoretischen Argumentierens wird schließlich auf die neuen Möglichkeiten zivilgesellschaftlicher Selbstorganisation gegen die etablierten Autoritäten oder jenseits von ihnen verwiesen. So wird die rasche Ausbreitung politischer Protestbewegungen unter Rückgriff auf die gestiegenen Organisationsmöglichkeiten durch Vernetzung erklärt. Auch die Struktur dieser Protestbewegungen, die sich häufig transnational organisieren und statt konkreter Forderungen den Anspruch erheben, selbst eine demokratische Alternative zu schaffen, wird auf die Parallelität zu den viel genutzten digitalen Netzwerken zurückgeführt.[3]

Die Ansicht, dass Digitalisierung Demokratisierung vorantreibt, hat also theoretisch einiges für sich und lässt sich auch mit Beispielen unterfüttern. Im Zuge der Kommunikationsrevolution entstehen dezentralisierte und transnationale Organisationsformen, die die Erwartung steigender Autonomie und partizipatorischer Gleichheit schüren. Doch jedem der benannten Pfade liegt eine Vielzahl von Vorbedingungen zugrunde und es lassen sich auch gegenläufige Tendenzen beobachten: So kann etwa Transparenz Informalität befördern, technisch gleicher Zugang ist nicht gleichzusetzen mit gleichen Partizipationschancen und einfach zu realisierender digitaler Aktivismus kann Energie und Aufmerksamkeit anderen Protestformen entziehen (*slacktivism)*. Deshalb dürften es eher reformerische als revolutionäre Wirkungen sein, die in etablierten Demokratien von der Digitalisierung zu erwarten sind.[4]

Der behauptete Zusammenhang zwischen Digitalisierung und Demokratisierung tritt noch stärker hervor, wenn nicht liberale westliche Demokratien in den Blick rücken, sondern autoritäre Staaten. Man nimmt an, dass diese mit Meinungsvielfalt und Kritik nicht umgehen können. Die Ausbreitung digitaler Kommunikationsmöglichkeiten erscheint daher als probates Mittel, die Bürger umfassender über ihre Regime zu informieren. Digitale Kommunikation soll

3 Manuel Castells: Networks of Outrage and Hope: Social Movements in the Internet Age, London 2012, S. 9; Jeffrey S. Juris: Reflections on Occupy Everywhere: Social Media, Public Space, and Emerging Logics of Aggregation, in: American Ethnologist (2012): 2, S. 259-279.

4 Archon Fung/Hollie Russon Gilman/Jennifer Shkabatur: Six Models for the Internet + Politics, in: International Studies Review (2013): 1, S. 30-47.

grundsätzlich die Möglichkeit schaffen, Protest zu organisieren und öffentliche wie externe Unterstützung einzuwerben. Eine Hoffnung, die in der Rezeption des arabischen Frühlings als *Facebook*-Revolution exemplarisch zum Ausdruck kommt, und die sich in den außenpolitischen Doktrinen westlicher Staaten fest etabliert hat, die die Ausbreitung (unzensierter) digitaler Kommunikation generell als ein Mittel befürworten, um Demokratisierung voranzutreiben.[5]

Die dunkle Seite digitaler Kommunikation

Die Diskreditierung der bisher geschilderten positiven Sicht auf den Zusammenhang von Medienwandel und Demokratisierung erfolgte atemberaubend schnell: Zwar gab es schon lange Zweifel und Kritik an einer zu positiven Bewertung des Effekts der Digitalisierung auf die Demokratie, doch die von Edward Snowden enthüllten, sehr weitreichenden Bemühungen von Geheimdiensten westlicher Staaten, auf weite Teile digitaler Kommunikation zuzugreifen, veränderten den Diskurs grundlegend. Im Fokus steht seitdem die Frage, inwieweit digitale Kommunikation die Demokratie gefährdet.[6]

Es ist sinnvoll, auch hier von der Debatte um konkrete Ereignisse zu abstrahieren und sich zunächst die generellen Argumente vor Augen zu führen. Wurde in der Diskussion um die emanzipatorischen Potenziale des Netzes die von diesem erzeugte Konnektivität betont, so sind es nun zwei andere Aspekte digitaler Kommunikation, denen prägende Wirkung auf die Entwicklung demokratischen Zusammenlebens zugeschrieben wird: der nicht zu unterdrückende Datenschweif und dessen immer effizientere Nutzbarmachung. Digitale Kommunikation basiert permanent darauf, dass sämtliche Kommunikationsinhalte ein Format erhalten, das sich zwischenspeichern und verlustfrei vervielfältigen lässt und das mittels Metadaten eine hohe Identifizierbarkeit erlaubt. Diese Eigenschaften liegen in der technischen Struktur selbst begründet; und sie sind durch die Allgegenwart digitaler Infrastruktur, den Anstieg an Speichermöglichkeiten und Verarbeitungskapazitäten sowie die Kommerzialisierung und immer stärkere Personalisierung des Netzes exponentiell gewachsen. So stellt sich die Frage, wieso diese Entwicklung lange nicht als demokratierelevantes Problem identifiziert wurde.

5 Vgl. John D. McCarthy: Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet, in: Foreign Policy Analysis (2011): 1, S. 89-111.

6 Vielleicht am pointiertesten ausgedrückt bei Sascha Lobo: Abschied von der Utopie. Die digitale Kränkung des Menschen, in: Frankfurter Allgemeine Sonntagszeitung, 12.01.2014.

Hierauf gibt es zwei Antworten: Zum einen wurde lange angenommen, dass Internetkommunikation aufgrund des *end-to-end*-Prinzips[7] und der unüberblickbaren Gesamtmenge an Kommunikation schon technisch nicht überwachbar sei. Anonymität galt als Eigenschaft des Netzes, eine Überzeugung, die in der legendären, bereits 1993 im *New Yorker* publizierten Karikatur „On the Internet, nobody knows you're a dog" deutlich wird. Zum anderen herrschte die Ansicht, dass es nationalstaatlichen Institutionen an Reaktionsgeschwindigkeit und technischem *Know-How* fehle – ganz zu schweigen von der Annahme, dass es globaler Einigkeit bedürfe, um ein globales Netz zu regulieren. Die von Snowden enthüllten Fähigkeiten der NSA und weiterer westlicher Geheimdienste haben die technische wie die staatsskeptische Seite der Argumentation unwiderruflich widerlegt. Sie zeigen mehr als deutlich, dass staatliche Akteure über ein umfangreiches Repertoire an Handlungsoptionen verfügen. Und dies sowohl durch direkte Überwachung als auch durch das Ausüben von Druck auf privatwirtschaftliche Akteure, die die materiell-physische wie die virtuelle Infrastruktur der Netzwerke kreieren und pflegen.[8] Die Beschäftigung mit der Struktur und Auswirkung digitaler Kommunikation darf deshalb nicht die Augen davor verschließen, dass offene Standards der Datenübertragung ausgenutzt werden können – und sich ebenso wenig der Erkenntnis entziehen, dass diese Art von Eingriffen auch durch rechtsstaatliche Demokratien in großem Stil vorgenommen wird.

Worin genau besteht aber aus einer demokratietheoretischen Perspektive die Gefahr dieser Entwicklung? Schließlich lassen sich die wachsenden Kapazitäten zur Überwachung des Netzes durchaus mit dem Argument verteidi-

7 Das *end-to-end*-Prinzip besagt, dass die anwendungsspezifischen Aspekte digitaler Kommunikation nur bei Sender und Empfänger eine Rolle spielen sollen, die dazwischen liegende Übermittlung durch Intermediäre ohne Ansehen des Gegenstands zu erfolgen hat. Das Prinzip beschreibt allerdings nur eine praktische Konvention, es ist nicht als eine dem Internetprotokoll inhärente Eigenschaft zu verstehen. Technisch ist die Überwachung und Diskriminierung von Inhalten kein Problem und dank immer größerer Rechnerkraft auch bei großen Datenmengen möglich. Eine besonders relevante Entwicklung ist die *Deep-Paket-Inspection*, das in Echtzeit erfolgende Überwachen und Administrieren von IP-Paketen. Eine Technik, die umfassende Kontrolle von Inhalten erlaubt und das Potenzial hat, die frühen Verständnisse von Internetkommunikation als ‚dummer' Kommunikation ebenso zu beenden wie das zudem auch unter kommerziellen Druck geratene Prinzip der Netzneutralität. Vgl. Ralf Bendrath/Milton Mueller: The end of the net as we know it? Deep Packet Inspection and Internet Governance, in: New Media & Society (2011): 7, S. 1142-1160.

8 Bereits früh wird dies herausgestellt bei Jack Goldsmith/Tim Wu: Who Controls the Internet? Illusions of a Borderless World, Oxford 2006. Einen aktuellen Überblick über Kontrollmöglichkeiten gibt Roland J. Deibert: Black Code. Sureveillance, Privacy and the Dark Side of the Internet, Toronto 2013.

gen, dass dies im Interesse der Demokratie liege, ja, letztlich eine Notwendigkeit für deren Fortbestehen und Prosperität sei. Das Argument lautet, dass aufgrund der wachsenden gesellschaftlichen Abhängigkeit von digitaler Kommunikation der Staat in diese Sphäre hineinwachsen müsse. Nur so könne er den vielfältigen Feinden der offenen Gesellschaft (seien es Kriminelle, Terroristen oder feindliche Mächte) trotzen. Die Reduzierung der Kommunikationskosten macht es demnach notwendig, aber auch möglich, die politische Ordnung präventiv zu schützen. Das Sammeln von Daten gilt als Grundlage, um künftiges Handeln zu prognostizieren – und erscheint damit als adäquates Mittel, um die hohe Verletzlichkeit digital vernetzter Gesellschaften zu kontern. Hierdurch wird aber genau das geopfert, was das emanzipatorische Potenzial digitaler Kommunikation ausmacht: die Pluralität und chaotische Kreativität offener Kommunikation und die sich daraus ergebende Nivellierung des Unterschiedes zwischen der organisierten, machtvollen Politik und den dieser Unterworfenen. In (mindestens) drei Dimensionen lässt sich diese Gefahr illustrieren:

1. Zunächst bezeugen die langanhaltende Speicherung sowie das umfassende, nicht anlassbezogene *Screening* digitaler Kommunikation einen Generalverdacht gegenüber den Bürgerinnen und Bürgern. Diese können sich der Überwachung und der mit ihr einhergehenden permanenten Typologisierung in gefährlich/ungefährlich weder entziehen noch erwehren. Schon die als harmlos apostrophierte massenhafte Überwachung von Metadaten verletzt alle Regeln der Verhältnismäßigkeit und führt zu einem nachhaltigen Vertrauensverlust, der im Widerspruch zur angestrebten Sicherheit steht.[9]
2. Hiermit geht unmittelbar eine enorme Gefahr von Missbrauch und Manipulation einher – eine Diagnose, die zunächst von westlichen Staaten gestellt wurde, wenn sie die Netzpolitik autoritärer Staaten kritisierten. Denn diese üben die staatliche Kontrolle digitaler Kommunikation nicht nur in Form von Zensur und Überwachung aus, an ihnen lässt sich vielmehr auch studieren, wie mittels manipulativer Praktiken regimekritische Kräfte identifiziert und diskreditiert werden. Die Hoffnung, dass durch digita-

9 Im deutschen Raum wurde dies lange vor den Snowden-Enthüllungen umfassend und kritisch mit Blick auf die Vorratsdatenspeicherung erörtert. Dass deren Durchsetzung im aktuellen Koalitionsvertrag ungeachtet der Enthüllungen erneut angestrebt wird, zeigt, wie stark sich der Diskurs immer nur auf konkrete Missbrauchsfälle konzentriert und wie unzureichend das generelle Problem umfassender Datensammlung begriffen wird. Das am 08.04.2014 ergangene Urteil des EuGH zur Vorratsdatenspeicherung stellt die Unzulässigkeit der verdachtsunabhängigen Datensammlung klar heraus und bietet für die deutsche Politik eine erneute Chance, an dieser Stelle grundlegend umzusteuern.

le Selbstorganisation zivilgesellschaftliche Kräfte Gegenmacht ausbilden können, ist somit von der Gefahr überschattet, dass sich der Einsatz digitaler Kommunikationsmittel jederzeit gegen die Aktivisten kehren kann.[10] Die Snowden-*Leaks* zeigen, dass ein solcher Missbrauch auch in demokratischen Staaten nicht ausgeschlossen ist und sich selbst im Fall der Entdeckung nur schwerlich verfolgen lässt.[11]

3. Schließlich zeigt sich ganz grundsätzlich das repressive Potenzial darin, dass ein prinzipieller Gehalt von Demokratie, die autonome Selbstbestimmung der Individuen, *ad absurdum* geführt wird, wenn jegliche Handlung des gläsern gewordenen Bürgers unter Beobachtung steht. Der enorme Konformitätsdruck in sicherheitsrelevanten Räumen wie z.B. Flughäfen ist hierfür eine gute Analogie: In einem solchen Setting wird das eigene Verhalten normiert, die Stimme gesenkt und falsch einzuschätzende Bewegungen werden, wenn möglich, vermieden. Eine solche Anpassung unterminiert die Ausübung demokratischer Grundrechte und setzt die Demokratie insgesamt der Gefahr aus, die charakteristische Diversität und Kreativität ihrer selbstbewussten Bürger zu verlieren.

Der im emanzipatorischen Diskurs hergestellte positive Zusammenhang zwischen Digitalisierung und Demokratisierung ist seit den Snowden-*Leaks* also grundlegend und zu Recht in Frage gestellt. Die perspektivische Verschiebung von horizontalen Kommunikationschancen hin zu Überwachungsmöglichkeiten hat eine in der öffentlichen Diskussion zuvor weitgehend ignorierte Gefahr der technischen Entwicklung offenbart. Trotzdem will ich im Folgenden dafür plädieren, nicht einfach für falsch zu erklären, was man sich vorher vom Internet erhofft hat. Die beiden hier schematisch skizzierten Positionen liegen nämlich nur scheinbar auf derselben Ebene: Sie widersprechen sich zwar in ihrem Urteil, schließen einander aber nicht aus. Es ist einzig die Ontologisierung der Diskussion um die Wirkung *des* Internets auf *die* Demokratie, die bewirkt, dass eine Entscheidung zwischen dem utopischen und dem dystopischen Szenario zu treffen ist.

10 Evgeny Morozov: The Net Delusion, London 2011.

11 Zwei Details aus den Leaks machen dies besonders deutlich: Die gezielte Überwachung der Plattform WikiLeaks (Glenn Greenwald/Ryan Gallagher: Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters, 2014, https://firstlook.org/theintercept/article/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/) und das Training des britischen Geheimdienstes zur digitalen Diskreditierung von politischen Gegnern (Glenn Greenwald: How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations, 2014, https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/).

Gerade der sich in Superlativen überbietende öffentliche Diskurs in Deutschland transportiert häufig eine per se technikskeptische Haltung, in welcher unbestimmte Ängste vor einer Mensch-Maschine-Konfrontation und der unendlich gedachten Macht kommerzieller und staatlicher Datenkraken das Denken bestimmen.[12] Die Angst vor unkontrollierter geheimdienstlicher Macht vereint sich mit den Bedenken gegenüber dem als chaotisch empfundenen Wesen des Netzes, der Vorstellung der Vulnerabilität ganzer Gesellschaften durch Cyberangriffe und der ohnehin vorhandenen Skepsis ob der undurchsichtigen Praktiken kommerzieller Datennutzung. In einem solchen Klima des Misstrauens liegt selbst ein Risiko: Verstärkt sich das Ohnmachtsgefühl, so steht in einer paradoxen Volte am Ende häufig die Forderung nach einer souverän durchgesetzten Gewährleistung von Sicherheit und damit letzten Endes die Abkehr von der als unsicher empfundenen dezentralen Architektur digitaler Kommunikation. Gegen diese Form des Selbstmords aus Angst vor dem Tod möchte ich abschließend argumentieren.

Versuche der Restrukturierung digitaler Kommunikation und deren Risiken

Das Aufdecken der selbst in liberalen Demokratien gängigen Praktiken, offene Netzwerkstrukturen auszunutzen, macht es unumgänglich, Architektur und Politik des Netzes auf den Prüfstand zu stellen. Die Kosten für Datensammlung und -auswertung müssen in einem solchen Maß erhöht werden, dass ein vertrauensvoller Umgang mit digitalen Kommunikationsmitteln wieder möglich wird. Das erfordert, die politische wie die technische Dimension des Problems gleichermaßen und gleichzeitig anzugehen. Neben der Frage, wie dies am besten erreicht werden kann, ist zentral, welchem Typ von Akteur man die Aufgabe überträgt, die freiheitliche und freiheitsfördernde Wirkung des Netzes zu sichern.

In der Diskussion lassen sich grob zwei Typen von Vorschlägen unterscheiden: liberale Ansätze, für die der Staat das eigentliche Problem darstellt und die entweder im Markt oder im individuellen Selbstschutz den Ansatzpunkt sehen, auf die Enthüllungen zu reagieren, und zweitens Vorschläge, die die Regulierung des Internets selbst zu verändern suchen und häufig eine stärkere Rolle des Staates als Regulierungsinstanz fordern.

Die liberale Position problematisiert die gewachsene Bedeutung des Staates im Netz und sieht in dessen unstillbarem Machthunger die eigentliche

12 Evgeny Morozov: Mehr Politik, in: Frankfurter Allgemeine Zeitung, 15.01.2014.

Gefahr. Der Weg zurück in den weniger regulierten Zustand früherer Tage wird daher als Mittel gegen den Missbrauch digitaler Kommunikation gesehen. Zwei sehr unterschiedliche Ausgestaltungen dieses Arguments existieren: Zum einen lässt sich die Position libertär zuspitzen, wenn man allein auf Marktmechanismen als Regulierungsinstanz setzt;[13] zum anderen lässt sie sich technisch wenden, wenn man individuelle Initiative betont, die alleine die ursprüngliche Freiheit des Netzes wiederherstellen könne.

Die libertäre Position hat gleich mehrere Denkfehler: So übersieht sie, dass das Missbrauchspotenzial nicht erst durch staatliche Instanzen gegeben ist, sondern durch die zur Monopolbildung tendierende Informationstechnologie ohnehin existiert. Große Datensammlungen und die Möglichkeit ihrer automatisierten Auswertung (*Big Data*) bergen an sich ein ungeheures Beherrschungspotenzial. Und nicht zufällig erwiesen sich die großen Internetunternehmen in der NSA-Affäre als zumeist willfährige Gehilfen staatlicher Anfragen. Marktakteure werden immer für die Forderungen marktkonstituierender Akteure empfänglich sein. So beteiligen sich schon lange viele Unternehmen an den Zensurmaßnahmen autoritärer Staaten. Weiterhin hat die Kommerzialisierung des Netzes zwar zu dessen rasanter Verbreitung beigetragen, die Freiheit, was wir mit Technik machen können, nimmt durch die Konkurrenz von Unternehmen aber nicht notwendig zu: Kommerzielle Interessen fördern vielmehr nur unter ganz bestimmten Bedingungen die Offenheit von Standards und Kommunikation. Die Geschichte der Informationsmedien zeigt, dass Schließungsprozesse und Monopolbildung, wie sie sich derzeit zum Beispiel in der Tendenz zur *Verappisierung* oder in den geschlossenen Standards sozialer Netzwerke zeigen, mindestens ebenso zur Logik einer marktdominierten Entwicklung gehören.[14]

Die technokratisch-individualistische Position versucht die dezentrale Freiheit auf technischem Wege wiederherzustellen. Sie plädiert beispielsweise für Verschlüsselung und *Open-Source*-Lösungen oder unterstützt Angebote, die das Sammeln von Daten nicht zum Geschäftsmodell erheben, sondern zu minimieren suchen. Ein solcher individueller Weg bietet sicher eine Möglich-

13 Ein Beispiel hierfür ist der von den großen amerikanischen Internetunternehmen gemeinsam getragene Aufruf zu einer "Global Government Surveillance Reform", http://www.reformgovernmentsurveillance.com/. Die libertäre Position ist in Deutschland schon wegen der nur rudimentär entwickelten eigenen Internetindustrie selten.

14 Die Wiederkehr dieses Musters wird bei Tim Wu beschrieben (vgl. Tim Wu: The Master Switch. The Rise and Fall of Information Empires, New York 2010). Jonathan Zittrain erörtert die Abläufe und Risiken der gegenwärtigen Entwicklung und geht besonders darauf ein, wie geschlossene, spezialisierte Anwendungen (*Apps*) an die Stelle offener Systeme treten (vgl. Jonathan Zittrain: The Future of the Internet. And How to Stop It, London 2009).

keit, die Gefahr der Überwachung zu mindern, ohne das Potenzial digitaler Kommunikation aufzugeben. Es stellt sich allerdings die Frage, ob dieser auf Selbsthilfe setzende Ansatz nicht die politische Dimension des Problems unterschätzt und durch seine technische Natur vieles außen vor lässt. Eine solche Strategie kann nie mehr sein als ein Teil der Lösung. Sie muss durch die umfangreiche und breitenwirksame Förderung digitaler Kompetenz flankiert werden und sich bewusst bleiben, dass die extrem ungleichen Machtverhältnisse es stets riskant machen, auf Eigeninitiative zu setzen – wie das Bemühen der NSA zeigt, kryptographische Algorithmen aktiv zu brechen.

Nicht das Herausdrängen des Staates, sondern die Neugestaltung der Bedingungen und Regeln digitaler Kommunikation bildet das Zentrum einer zweiten Linie von Diskussionen. Erörtert wird hier, wie sich demokratische Kontrolle wiederherstellen lässt. Bezieht sich die Diskussion dabei auf die politischen und rechtlichen Rahmenbedingungen freiheitlicher Netzkommunikation, etwa, dem Anlass der Snowden-Enthüllungen angemessen, auf die Reform von Geheimdiensten oder die Anpassung, Erweiterung und Durchsetzung des Datenschutzrechts an das digitale Zeitalter, so sind diese Forderungen aus demokratietheoretischer Sicht absolut zu unterstützen. Solche Reformen werden nötig sein, ohne sie sind alle anderen Überlegungen zur Freiheit im Internet Makulatur. Die Herausforderung besteht darin, Strukturen zu schaffen, die dem überstaatlichen Wirken der Geheimdienste wie den transnational operierenden Internetunternehmen effektiv rechtliche wie politische Grenzen setzen können.

Wesentlich ambivalenter sind jene Vorschläge, die das Netz selbst, also dessen technische Regulierung und administrative Verfasstheit, zu verändern suchen. Im Namen demokratischer Kontrolle wird hier häufig versucht, die Logik staatlicher Souveränität für das Netz einzuführen. So soll dem Abhören digitaler Kommunikation durch fremde Geheimdienste mittels nationalstaatlichem *Routing*, der Verkehrslenkung des Netzes, begegnet werden (*Schengenrouting* oder das *Schlandnetz* sind Forderungen dieser Art). Die Etablierung (national-)staatlicher Netzhoheit verteuert aber gerade nicht die Überwachung. Durch sie ändert sich, wenn überhaupt, nur der Kreis derjenigen, die zu deren Missbrauch in der Lage sind. In Hinblick auf den Schutz der Bürger birgt ein solches Vorgehen daher mehr Risiken als Vorzüge: Es hat sich ja gerade erst gezeigt, wie schwierig sich die Überwachung der Überwacher gestaltet und wie wenig auf deren Selbstkontrolle zu geben ist. Die Schließung europäischer Netze und die Weiterentwicklung von Technologien zur Lenkung und Filterung von Datenströmen ziehen zudem unweigerlich parallele Entwicklun-

gen in autoritären Regimen nach sich und erhöhen die Legitimität repressiver Netzpolitiken.[15]

Je stärker also der Staat mit der Regulierung und Administration des Netzes betraut wird, umso weiter entfernen wir uns von dem dezentralen Ideal, welches Ausgangspunkt der emanzipatorischen Vision des Internets war. Obwohl das gewachsene System der Internetadministration mit seiner auf zivilgesellschaftliche Beteiligung und transnationale Kooperation setzenden Logik nicht verhindern konnte, dass die offenen Standards digitaler Kommunikation für die massenhafte Überwachung ausgenutzt wurden, muss dieses System doch noch nicht aufgegeben werden. Der Fehler im System sind nicht die offenen Standards, sondern die Möglichkeiten machtvoller Akteure, sich den Datenverkehr anzueignen und diese Standards auszunutzen. Bei aller notwendigen Kritik gilt es daher, das System der *Internet Governance* so zu reformieren – wie es beispielsweise im *Montevideo Statement on the Future of Internet Cooperation* gefordert und in der *NetMundial*-Konferenz im April 2014 in Brasilien angestrebt wird –, dass der dezentrale Charakter digitaler Kommunikation erhalten bleibt und einzelne politische Akteure nicht noch stärker als ohnehin in Entwicklung und Gestaltung des Netzes eingreifen können.[16]

Abschließend bleibt festzuhalten, dass die seit den Snowden-*Leaks* offen zutage liegende enorme Bedeutung von Machtstrukturen sowie die Anfälligkeit der offenen Strukturen digitaler Kommunikation für Missbrauch ein neues Abwägen nötig machen: Wie lassen sich jene Charakteristika von Netzwerkkommunikation stärken, die die ursprüngliche emanzipatorische Hoffnung befeuerten, und wie lässt sich zugleich verhindern, dass politische oder wirtschaftliche Akteure die entstehenden Überwachungs- und Manipulationsmöglichkeiten ausnutzen? Es hat sich gezeigt, dass dies ebenso sehr eine politische Aufgabe wie eine technologische Herausforderung ist. Machtfragen müssen

15 Schon lange und nicht zufällig ist die Forderung nach einer durch Staaten verantworteten Regulierung des Netzes auf der Agenda autoritärer Regime. Einschlägig ist etwa der Versuch von China, Russland, Saudi-Arabien und den Vereinigten Arabischen Emiraten, die *International Telecommunication Union* (ITU) umfassender in die Regulierung der Internetkommunikation einzubinden und damit ein staatenbasiertes Gremium an die Stelle der etablierten *multistake-holder*-Mechanismen zu setzen. Die Bemühungen auf der *World Conference on International Telecommunication* in Dubai im Dezember 2012 scheiterten aber noch am heftigen Widerstand der westlichen Staaten, die den Vertrag trotz Abschwächungen bis heute größtenteils nicht unterzeichnet haben.

16 Detaillierte und gut abgewogene Einschätzungen der Entwicklung des Verhältnisses von Staat und Netzwerken finden sich bei Milton Mueller: Networks and States: The Global Politics of Internet Governance, Cambridge 2010; Laura DeNardis: The Global War for Internet Governance, New Haven 2014; und Ian Brown/Christopher T. Marsden: Regulating Code. Good Governance and Better Regulation in the Information Age, Cambridge, MA 2013.

direkt adressiert und sollten nicht durch einen die Technologie dämonisierenden Diskurs verschleiert werden. Gerade der Ruf nach einer souveränen Instanz, die Schutz zu versprechen scheint, wird nur die Missbrauchsanfälligkeit erhöhen. Reformen müssen stattdessen zum Ziel haben, die Kosten für das Sammeln und massenhafte Auswerten von Daten zu erhöhen: Mit Blick auf die Technik heißt dies, dass die dezentrale Architektur des Internets erhalten oder gestärkt werden sollte, in rechtlicher Hinsicht müssen Datenschutz und Privatsphäre aktualisiert und durchsetzungsfähig gemacht werden, und politisch gilt es, die auch in anderen Politikfeldern vorhandenen Tendenzen zur Dominanz exekutiver Akteure und zum Verfolgen präventiver Sicherheitslogiken zu hinterfragen, da sie die Möglichkeit prozeduraler Kontrolle zu unterhöhlen drohen.