

Das Internet als regulative Herausforderung für staatliches Handeln

1. Einleitung

Das Internet, eines der bestimmenden Phänomene unserer Zeit, ist eine Herausforderung für klassische Staatlichkeit. Es kennt und respektiert keine nationalen Grenzen und ist in seiner globalen Ausrichtung ein mächtiges Symbol für die Einheit unserer Welt. Die gute Hälfte der auf diesem Globus lebenden Menschen – knapp 4 Milliarden von insgesamt 7,5 Milliarden – nutzen gegenwärtig nach Angaben der *International Telecommunication Union* das Internet; klänge es nicht etwas pathetisch, könnte man vom Internet als einer gemeinsamen Menschheitserfahrung sprechen.

Diese Tatsache ist eine erhebliche Herausforderung für den auf Nationalität und Grenzen bezogenen Staat. Denn er reklamiert als klassisches Definitionsmerkmal die oberste Autorität auf alles, was innerhalb seines Territoriums geschieht. Im Wesen des Internets liegt aber genau das Gegenteil, nämlich die Verbindung seiner Teilnehmer über alle Grenzen hinweg.

Das Internet ist binnen nur zweier Jahrzehnte von einem Instrument für Spezialisten zu einem (s.o.) *Jedermannsinstrument* mutiert, ohne das wirtschaftliche, politische, soziale und kulturelle Prozesse nicht mehr funktionieren würden und das aus unserem Alltag nicht mehr wegzudenken ist. Welche Herausforderungen das für die Staatsaufgaben bedeutet und wie der Staat damit umgeht, dazu möchte dieser Beitrag einige Überlegungen anstellen.

Dazu gehen wir in drei Schritten vor. Zunächst werfen wir einen Blick auf das Internet als Ort der Freiheit. Ohne seine Entstehungsgeschichte sind die emanzipatorisch-libertären Grundimpulse, die sich durch Fundamentalentscheidungen bei der technischen Konstruktion des Internets ausdrücken und es bis heute prägen, nicht zu verstehen. Doch der Optimismus, mit dem auch in der Politik die Ausbreitung der Internetnutzung mit der dadurch positiv beeinflussten Ausbreitung von Demokratie gleichgesetzt wurde, hat in den letzten Jahren einige Enttäuschungen hinnehmen müssen. Kommunikation über *soziale Medien* wird heute oft auch mit demokratieschädlichen Konsequenzen in Verbindung gebracht, und verschiedene Beispiele (s.u.) weisen auf die Manipulationsmöglichkeiten demokratischer Prozesse durch neue Kommunikationsformen hin.

In einem zweiten Schritt werden daher die regulativen Herausforderungen für den Staat in den Mittelpunkt gestellt, die sich durch die zentrale Wichtigkeit des Inter-

nets in drei Bereichen ergeben: im Bereich der Wirtschaft, in der Bekämpfung von Kriminalität sowie im Schutz des Prozesses der demokratischen Willensbildung. Im dritten Schritt steht dann die Frage nach der Empirie im Mittelpunkt und es wird konkretes staatliches Handeln in der Bundesrepublik anhand von zwei Gesetzen betrachtet, mit denen Regulierung im Internet umgesetzt wird und bei denen die speziellen Bedingungen und Schwierigkeiten in diesem Politikfeld deutlich werden. Ein kurzer Schluss diskutiert die Ergebnisse und wirft weitere Forschungsfragen auf.

2. Das Internet – der Ort der Freiheit?

Die oft etwas anarchisch erscheinende Natur des Internets kann nicht verstanden werden ohne ein Wissen um seine Ursprünge. Denn das heutige Internet wurde so nie geplant, es ist in gewissem Maße als Resultat nicht vorhergesehener Dynamiken und Interaktionen passiert. Weder die segensreiche unsichtbare Hand des Marktes noch kluges und vorausschauendes Handeln von staatlicher Seite haben es zustande gebracht. Wenn man es einer einzelnen Kraft zu verdanken hat, dann am ehesten dem Zufall.

Betrachtet man das Internet vor allem als Wissensspeicher und Instrument zum Austausch und zur Diskussion, so gehen diesbezügliche Wünsche lange zurück. Der britische Schriftsteller H.G. Wells etwa schrieb 1937 einen Beitrag über „The idea of a permanent world encyclopaedia“, ein neues Medium, das das gesamte menschliche Wissen speichern und überall verfügbar machen sollte.¹ Wells sah als Speichermedium den Mikrofilm vor und hoffte, gemeinsame Wissensbestände würden das Ende menschlicher Konflikte und kriegerischer Auseinandersetzungen bringen.

Es liegt angesichts dieses Wunsches eine gewisse Ironie in der Tatsache, dass die Entwicklung von Vorläufern des Internets (als Verwirklichung der Vision vom Speicher allen menschlichen Wissens) weitgehend ausgerechnet von US-Militärs in der Situation des Kalten Krieges vorangetrieben wurde.² Um die im ganzen Land verstreuten und mit unterschiedlichen technischen Spezifikationen entwickelten Computerprojekte miteinander zu verbinden, wurde in der ersten Hälfte der 1960er Jahre ein Netzwerk konzipiert. Gleichzeitig begann man an der Nutzbarkeit der existierenden Computer für mehrere Nutzer im *interaktiven* Modus (anstelle des *batch processing*) zu arbeiten. Über Versuche, den Computer vor allem als Erweiterung des menschlichen Geistes zu verstehen, entstand eine Verbindung zwischen Computer-

1 Der Aufsatz, ursprünglich verfasst für die *Encyclopédie Française*, ist auch abgedruckt in Wells 1938.

2 Hafner/Lyon 2000; Cortada 2012.

technik und *counter culture* mit zahllosen grundlegenden Innovationen und einer libertär ausgerichteten „Hackerkultur“.³

Bis heute prägen die Ursprünge in dieser Zeit das Internet, etwa durch technische Grundentscheidungen wie die Offenheit für alle Inhalte (das Netz machte keine Vorschriften hinsichtlich der Art der zu transportierenden Inhalte) oder die Abwesenheit von Sicherheitsmechanismen beim TCP/IP-Protokoll (die kleine Gemeinschaft der Nutzer vertraute einander). Vermeintlich technische Entscheidungen erwiesen sich somit später als mit politischen und gesellschaftlichen Folgen behaftet.⁴

Auch der emanzipative und optimistische Grundimpuls, der dem Internet innewohnt („All information should be free“, heißt es in der von Steven Levy beschriebenen „Hacker Ethic“), entstammt dieser Kultur.⁵ Dass ein Informationssystem wie das Internet eine grundsätzlich positive Auswirkung auch auf den politischen Prozess haben könnte, postulierte der Demokratietheoretiker Robert Dahl schon zu einer Zeit, als diese Technologie noch weitgehend in den Kinderschuhen steckte. Er sah darin das Potential, politische Partizipation auszuweiten, da Bürger mit ihrer Hilfe den Informationsvorsprung von Eliten und Bürokratie reduzieren und sich so effektiver einmischen könnten.⁶ Diese Vorstellung war verbreitet – das Internet sollte den Weg „Von der Zuschauer- zur Beteiligungsdemokratie“ ebnen helfen, seine Verbreitung und steigende Nutzung konnte nur Gutes für die Demokratie bedeuten.⁷

Das Aufkommen von *social media* bot noch einmal Grund, den Optimismus auszuweiten. Die Proteste im Iran 2009 sowie der (vorschnell so getaufte) „Arabische Frühling“ der Jahre 2010 und 2011 schienen die Optimisten zu bestätigen. Oppositionelle konnten dank Twitter ohne zentrale Organisation ihre Proteste koordinieren und die Kommunikationssperren autoritärer Regime umgehen. Die neuen Technologien schienen fundamentale Veränderungen im Prozess demokratischer Willensbildung zu ermöglichen, die *public sphere* vor einem grundsätzlichen Umbruch zu stehen.⁸

Durch Förderung dieser Technologien war gleichzeitig die Verbreitung von Demokratie direkt und relativ unproblematisch zu fördern, so die Einstellung der seinerzeitigen US-Regierung unter Präsident Obama. US-Außenministerin Hillary Clinton hielt im Januar 2010 eine große programmatische Rede unter dem Titel „Remarks on Internet Freedom“.⁹ Freie Information sei nicht nur das Vehikel zur Ausbreitung von wirtschaftlichem Wohlstand, sondern diene auch der Verbreitung de-

3 Levy 2010 [1984]; Markoff 2006.

4 DeNardis 2009.

5 Der Aufsatz, ursprünglich verfasst für die *Encyclopédie Française*, ist auch abgedruckt in Wells 1938.

6 Dahl 1989, S. 338ff.

7 Leggewie/Maar 1998.

8 Shirky 2011.

9 Clinton 2010.



mokratischer Werte und Gesellschaften. Daher sei es die Pflicht der USA (als Heimat vieler dieser Technologien), zu deren positiver Nutzung beizutragen. Die Außenministerin kündigte deshalb finanzielle und technologische Unterstützung für Gruppen in autoritär regierten Ländern an, damit diesen der freie Zugang zum Internet und das Umgehen politisch motivierter Zensur ermöglicht werde. Akademische Programme wie das zur „Liberation Technology“ der Stanford University unterstützten diese Politik durch die Entwicklung von Technologien und die Ausbildung von Aktivisten. Der Demokratieforscher Larry Diamond (einer der Verantwortlichen für das Programm) nannte den Kampf um freien Zugang zum Internet „really just the timeless struggle for freedom by new means. It is not technology, but people, organizations, and governments that will determine who prevails.“¹⁰ Das US State Department taufte den neuen Ansatz „21st century statecraft“ und versprach, die interne *Global Internet Freedom Task Force* (eine im Jahr 2006 von der damaligen Außenministerin Condoleezza Rice etablierte Arbeitsgruppe) wiederzubeleben.

Es gab aber auch skeptische Stimmen zum Potential dieser Technologien. Der ursprünglich aus Weißrussland stammende Blogger und Journalist Evgeny Morozov, vielleicht der bekannteste Verfechter dieser Position, verwies auf das ihnen innewohnende Überwachungs- und Kontrollpotential, das gerade autoritäre Regime nutzen könnten.¹¹ Er warf der Haltung des US-Außenministeriums „Cyber-Utopismus“ vor sowie eine Technologiegläubigkeit, die die notwendigen organisatorischen Grundlagen politischen Handelns völlig vernachlässige.

Zum anderen sind die Vorstellungen, Zugang zum Internet beeinflusse politische Partizipation und demokratische Entwicklung in quasi automatischer Weise, heute als allzu optimistische Hoffnungen entlarvt. Empirische Studien haben dazu ebenso beigetragen wie jüngere politische Erfahrungen. Der amerikanische Politikwissenschaftler Matthew Hindman kann beispielsweise zeigen, dass die neuen Technologien in Form von politischen Websites und Blogs keinesfalls zu einer Verbreiterung des politischen Diskurses in den USA geführt haben, sondern im Gegenteil die Diversität der *blogosphere* gegenüber dem Print-Journalismus sogar noch geringer ausfalle;¹² sie stelle eine weitere Verstärkung der in klassischen Medien ohnehin erfolgreichen Positionen und Personen dar.¹³ Er kommt zu dem Schluss: „If we consider the ability of ordinary citizens to write things that other people will see, the Internet has fallen far short of the claims that continue to be made about it. It may be easy to speak in cyberspace, but it remains difficult to be heard.“¹⁴

Neben diesen gewissermaßen ausgebliebenen positiven Folgen der neuen Kommunikationstechnologien auf die innere politische Kommunikation von Demokrati-

10 *Diamond* 2010, S. 82.

11 *Morozov* 2009, 2011.

12 *Hindman* 2009.

13 Ebd., S. 128.

14 Ebd., S. 142.

en zeigen sich jedoch auch explizit negative Folgen in Form bewusster Nutzung zur Manipulation von Ergebnissen des Prozesses politischer Meinungsbildung. Der amerikanische Rechts- und Sozialwissenschaftler Cass Sunstein beschreibt die Paradoxie steigender Isolierung durch das alles verbindende Internet und die in ihm entstehenden Echokammern.¹⁵ Abnehmendes Verständnis füreinander befördere gesellschaftliche Polarisierung und soziale Fragmentierung und untergrabe so die Bindekräfte in der Gesellschaft. Sunsteins Befürchtung, so könne schließlich auch Freiheit in Gefahr geraten, wird in ihren Mechanismen illustriert durch die detaillierte Studie von Jamieson zum Einfluss russischer Hacker und Trolle auf die US-Präsidentenwahl 2016.¹⁶ Ihre abschließende Einschätzung ist es wert, wörtlich zitiert zu werden: „The conclusion that Russian trolls and hackers helped elect a US president draws support from decades of scholarly work probing the effects of agenda setting, framing, priming, message weighting, debates, negative information, contagion, peer influence, and the spiral of silence. As earlier chapters have argued, the Kremlin-tied interventions functioned in each of these areas in ways that in past elections have produced discernible effects, many of them larger than the one required to alter the 2016 outcome“.¹⁷ Auch die noch nicht vollständig aufgeklärten Versuche, über das Internet das britische Brexit-Referendum zum Austritt aus der Europäischen Union zu beeinflussen,¹⁸ oder wissenschaftliche Studien zum Einsatz von *social bots* (Computerprogrammen, die eine menschliche Identität im Online-Austausch vortäuschen und von interessierter Seite zur Förderung ihrer Interessen eingesetzt werden) zum Einfluss auf politische Diskurse und Wahlergebnisse machen deutlich, dass durch solche Verwendung der neuen Kommunikationstechniken Verzerrungen im politischen Prozess eintreten können, die aus der Perspektive liberaler Demokratie nicht hinnehmbar sind.¹⁹

3. Herausforderungen für den Staat

Das Internet und seine heutige Nutzung, das hat der erste Teil dieses Aufsatzes ergeben, weisen demnach eine ganze Reihe von Herausforderungen für den Staat auf, die (zumindest aus der Perspektive des Staates) nicht unerwidert bleiben können. Die Entwicklung ist somit deutlich anders verlaufen als sich seine Erfinder das in der Frühzeit des Internets vorgestellt und erhofft hatten.

Die libertär-avantgardistische Kultur der (kleinen und technisch hoch kompetenten) Gründergeneration des Internets hatte diese als einen Ort des freien Austauschs

¹⁵ Sunstein 2017.

¹⁶ Jamieson 2018.

¹⁷ Ebd., S. 212.

¹⁸ Siehe dazu etwa Cadwalladr 2017.

¹⁹ Siehe Neudert u. a. 2017 für das Beispiel der Wahl des deutschen Bundespräsidenten.

gesehen, frei nicht zuletzt von kommerziellen Interessen und Erwägungen. Und genau genommen auch physisch ortlos (eben im *cyberspace*) und daher nicht regulierbar. Die bekannteste Formulierung dieser utopischen Vision ist wohl die „Declaration of the Independence of Cyberspace“, verfasst von John Perry Barlow, einem frühen Netzaktivisten, Mitgründer der *Electronic Frontier Foundation* und ehemaligen Texter der kalifornischen Kultband *Grateful Dead*. In dieser Erklärung wird der Raum des Netzes als staatlicher Regulierung unzugänglich beschrieben:²⁰

„Governments of the Industrial World, you weary giants of flesh and steel,
I come from Cyberspace, the new home of Mind.
On behalf of the future, I ask you of the past to leave us alone.
You are not welcome among us. You have no sovereignty where we gather.
We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks.
I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us.
You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.“

Diese Erwartung hat sich als falsch herausgestellt – und nicht nur, weil konkrete IT-Infrastruktur immer irgendwo auf einem politischer Herrschaft unterworfenen Territorium stehen und daher den dort geltenden Regeln folgen muss.²¹ Vor allem hat der Erfolg des Internets und seine Zentralität für das heutige Leben es für den Staat unverzichtbar gemacht, seine Interessen und Aufgaben auch im Internet durchzusetzen, zumeist durch Regelsetzung.

Drei Bereiche stehen dabei im Vordergrund: Wirtschaft, Kriminalität und Sicherung des demokratischen Prozesses. Auf sie soll im Folgenden genauer eingegangen werden.

4. Wirtschaft

Das Internet, ursprünglich als Forschungs- und Militärintstrument entstanden, ist heute von zentraler wirtschaftlicher Wichtigkeit. Das spiegelt sich nicht nur durch innovative Geschäftsideen, aus denen große und in ihren Bereichen dominante Unternehmen wie Amazon, Google oder Facebook entstanden sind – Unternehmen, die heute nach Marktkapitalisierung in der weltweiten Spitzengruppe liegen.²² Es ist

²⁰ Barlow 1996.

²¹ Nur im Roman kann dieser Zwang umgangen werden, etwa in Neal Stephenson's „Cryptonomicon“ (Stephenson 1999).

²² Siehe dazu die Liste der „Global Top 100 Companies by market capitalisation“, erstellt von der Wirtschaftsprüfungsgesellschaft *PricewaterhouseCoopers*. Unter: <https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2017-final.pdf>, download 1.9.2018).

auch Reflex der seit langem wachsenden Rolle, die informationsbezogene Güter in den entwickelten Volkswirtschaften spielen: ihr Anteil am BIP ist in den G7-Ländern mittlerweile auf über 70 Prozent gestiegen, sie ersetzen in der Informationsökonomie in wachsendem Maße die Rohstoffe, die in der Industriegesellschaft noch von zentraler Wichtigkeit gewesen waren (Öl, Eisenerz, Kohle).²³ Daten werden deshalb auch häufig als das „Öl des Internet-Zeitalters und neue Währung der digitalen Welt“ beschrieben.²⁴

Angesichts dieser zentralen Wichtigkeit des Internets ist die Frage staatlicher Regulierung nicht mehr eine des *ob*, sondern eine des *wie* und *auf welche Weise* geworden. An Herausforderungen mangelt es dennoch nicht, sind die Aufgaben doch über ein breites Feld unterschiedlicher Politikbereiche (von der inneren Sicherheit über die Regelung von Arbeitsbedingungen bis zu Fragen des Datenschutzes) verteilt. Zudem erweist sich regulative Politik generell als sehr voraussetzungsreich, soll sie nicht negative Nebenfolgen mit sich bringen, die den Regulierungszweck untergraben. Deshalb ist hier auch ein relativ hohes Ausmaß an Konfliktrichtigkeit zu erwarten, ebenso wie große Schwierigkeiten bei der Kompromissfindung aufgrund der Komplexität der Sachlage.²⁵ Abstimmungen über mehrere Ebenen (z.B. in der Europäischen Union) erschweren die Aufgabe weiter.

Schließlich ist zu sagen, dass durch den Einsatz und die Nutzung des Internets in wirtschaftlicher Hinsicht generell Einsparungen durch Effizienzgewinne anfallen, denen jedoch eine tendenziell größere Abhängigkeit von kritischen Infrastrukturen gegenübersteht. Ein Ausfall der Stromversorgung hat in einer Wirtschaft, in der von der Logistik bis zur Produktion alles von Elektronik und Kommunikation abhängt, natürlich weitaus gravierendere Folgen als das in früheren Jahrzehnten der Fall war. Mit der Abhängigkeit steigt auch die Verwundbarkeit gegenüber Angriffen, die zudem nicht mehr in physischer Form, sondern eventuell über das Internet selbst ausgeführt werden können.²⁶ Fraglos besteht hier ein erhebliches Schadens- und Erpressungspotential für technisch kompetente Angreifer.

5. Kriminalität

Eine weitere Herausforderung für staatliches Handeln ist die Nutzung des Internets zur Begehung krimineller Tätigkeiten. Denn auch die Kriminalität hat natürlich die Potentiale des Internets entdeckt und bedient sich ihrer. Diese Tätigkeiten zu be-

²³ Floridi 2010, S. 5.

²⁴ *World Economic Forum* 2011.

²⁵ Busch 2012b, S. 38.

²⁶ Als Illustration kann hier der Angriff auf die Atomanlagen des Iran mittels des Virus *Stuxnet* dienen (Stöcker 2012). Entsprechend könnten auch Strom- oder Wasserversorgung oder andere Teile kritischer Infrastruktur ins Visier genommen werden.

kämpfen ist eine Herausforderung für den auf Einhaltung der geltenden rechtlichen Regeln bedachten Staat. Allerdings sieht dieser sich dabei mit erheblichen technischen Schwierigkeiten konfrontiert. Denn der wohl größte Teil von schwerer Kriminalität findet in einem Teil des Internets statt, der als sogenanntes „Dark Net“ für normale Nutzer weitgehend unsichtbar ist, da Inhalte und Verbindungen mit Hilfe von Verschlüsselungstechnologien verschleiert werden.²⁷ Diese Verschlüsselungstechnologien ermöglichen somit geschützte Kommunikation sowohl für politisch Verfolgte in autoritär regierten Staaten wie ein verdecktes Agieren für Kriminelle. Letzteres stellt ein politisches Problem für den Rechtsstaat dar, da in ihm Regeln universelle Geltung beanspruchen müssen, doch die technische Umsetzung dieses Anspruchs schwierig ist. Schon die Größe des *Dark Net* ist kaum seriös zu bestimmen; Abschätzungen der Größe der staatlichen Aufgabe fallen daher schwer. Von politischer Seite wird das Problem abstrakt ernst genommen, doch Konkretisierungen haben sich noch nicht durchgesetzt. Sogar im aktuellen Koalitionsvertrag von 2018, der dem Thema Sicherheit breiten Raum einräumt, wird das *Dark Net* erwähnt – im Zusammenhang mit Strafbarkeitslücken. So soll eine „Strafbarkeit für das Betreiben krimineller Infrastrukturen [eingeführt werden], um speziell im Internet eine Ahndung von Delikten wie z. B. das Betreiben eines Darknet-Handelsplatzes für kriminelle Waren und Dienstleistungen“ zu ermöglichen.²⁸ Inwieweit dieses Vorhaben in konkrete gesetzliche bzw. behördliche Maßnahmen umgesetzt wird, wird man erst zum Ende der Legislaturperiode bewerten können.

Neben der Bekämpfung von konventioneller Kriminalität, die sich aus verschiedenen Gründen ins Internet verlagert hat, gibt es auch neue Tatbestände, die erst durch das Internet entstanden sind bzw. an Relevanz gewonnen haben. Insbesondere sind hier zu nennen die Themen *hate speech* und *Verletzung von copyright*.

Hate speech bezeichnet ein im Zusammenhang mit der Kommunikation über das Internet zunehmend zu konstatierendes Phänomen herabsetzender bzw. offen feindlicher Rede. Objekt der Herabsetzung sind dabei Individuen bzw. ganze Gruppen auf der Basis von Merkmalen wie ethnische Herkunft, religiöse Zugehörigkeit, Staatsangehörigkeit oder sexuelle Orientierung. Die Möglichkeit zur anonymen Äußerung im Internet hat das Volumen von *hate speech* sichtbar gemacht bzw. zu seinem Anstieg beigetragen und die Frage nach strafrechtlichen Reaktionen aufgeworfen. Da Staaten auf unterschiedliche Weise mit dem Thema Redefreiheit umgehen – in den USA etwa ist auch *hate speech* unter dem Prinzip der Redefreiheit nach dem *First Amendment* zur Verfassung geschützt, während in der Bundesrepublik beispielsweise

27 Siehe zum Phänomen des „Dark Net“ die Themenausgabe von *Aus Politik und Zeitgeschichte* 46–47/2017, die Aufsätze sowohl zur technologischen Konstruktion des Dark Net enthält, aber auch dessen Ambiguität aufgrund seiner Wichtigkeit für geschützte Kommunikation unter Dissidenten in autoritär regierten Staaten hervorhebt. Zum Thema Sicherheit im Internet siehe den zusammenfassenden Aufsatz von Rohs 2019.

28 Christlich-Demokratische Union Deutschlands u. a. 2018, S. 126.

se die Leugnung des Holocaust unter Strafandrohung gestellt ist –, sind Debatten um die Definition und Bewertung von *hate speech* sowie das Verhältnis zur Redefreiheit notwendig – in der Bundesrepublik gibt es zwar ein Grundrecht auf freie Meinungsäußerung (Art. 5 GG), doch existieren auch Einschränkungen, etwa im Fall von Beleidigung, Verleumdung und Volksverhetzung.²⁹

In ähnlicher Weise ist mit der Frage der Verletzung von *copyright* ein weiteres, lange existierendes Thema durch das Internet zu neuer Relevanz gekommen. Die durch Digitalisierung ermöglichte verlustfreie Kopie von Werken bedroht etablierte Systeme von Autoren- und Urheberrechten und hat Fragen nach dem Besitz an geistigem Eigentum neu auf die Agenda gebracht, weil in der Wissens- und Informationsgesellschaft solche Besitzrechte von zentraler wirtschaftlicher und kultureller Bedeutung sind.³⁰ Die Kombination von Konflikten über materielle Gewinne und Verluste mit solchen struktureller Änderungen in vielen *content*-Industrien (wie Musik-, Verlags- und Filmindustrie) und Fragen der Obsoleszenz nationaler Grenzen bei der Verbreitung über das Internet haben zu langwierigen politischen Auseinandersetzungen geführt, die noch der Lösung bedürfen.³¹

6. Schutz des Prozesses der politischen Willensbildung

Dem Internet wohnt ein emanzipativer und optimistischer Grundimpuls inne, der – wie oben geschildert – aus seiner (stark durch Zufälle geprägten) Entstehungsgeschichte stammt. „All information should be free“ ist einer der Grundsätze der Hackerkultur, die Steven Levy so gut beschrieben hat. Bereits weiter oben wurde auf Robert Dahl und seine Vorstellung von der den politischen Prozess positiv beeinflussenden Wirkung eines Informationssystems wie des Internets Bezug genommen. Dahl sah das Potential, politische Partizipation auszuweiten, den Informationsvorsprung von Eliten und Bürokratie zu reduzieren und sich so effektiver einmischen zu können.³² Diese Vorstellung war verbreitet – und sie erhielt weiteren Auftrieb durch das Aufkommen von *social media* und deren Nutzung bei Protesten im Iran sowie im „Arabischen Frühling“ von 2010 und 2011.

Heute, nur wenige Jahre später, ist auch das negative und manipulative Potential dieser Technologien offenkundig geworden. Im US-Wahlkampf 2016 etwa haben Firmen wie *Cambridge Analytica* personenbezogene Daten zur verdeckten Einflussnahme auf ausgewählte Wählergruppen eingesetzt. Wir wissen um Versuche, demo-

29 Zum Versuch der Problemlösung in diesem Bereich durch das Netzwerkdurchsetzungsgesetz siehe weiter unten im Text.

30 Siehe für die Schilderung der historischen Entwicklung von „geistigem Eigentum“ und Urheberrecht z.B. den Aufsatz von Siegrist 2006.

31 Lindow 2019.

32 Dahl 1989, S. 337–340.

kratische Prozesse durch Einsatz digitaler Medien zu untergraben, von innen wie von außen. Und wir sehen, dass ihr Einsatz den demokratischen Diskurs in liberalen Demokratien beschädigt. Wolfgang Merkel spricht von einer „digital geförderten Teilvernichtung einer demokratisch-toleranten Öffentlichkeit“ durch *shitstorms*, Beleidigungen, Hasstiraden und unverhohlene Drohungen sowie von einer massenhaften „Senkung der Scham-, Hemm- und Hassschwelle“.³³ Diese Entwicklungen bedrohen den demokratischen Prozess der politischen Willensbildung.

Vom vielversprechenden Positivum hat sich die Internettechnologie zum bedrohlichen Negativum gewandelt – so kann die hier sehr holzschnittartige Darstellung knapp zusammengefasst werden. Dem demokratischen Staat stellt sich dadurch eine weitere Herausforderung, nämlich die des Schutzes für den Prozess der demokratischen Willensbildung.

7. Was tut der Staat?

Der Staat sieht sich durch das Internet – das wurde oben deutlich – in einer ganzen Reihe von Bereichen nicht nur herausgefordert, sondern auch in der Erfüllung seiner Aufgaben behindert. Wie er darauf reagiert, das soll – in notwendiger Kürze – im Folgenden betrachtet werden.

Aufgrund der Natur des Internets als den Globus umspannende Einrichtung sowie seiner (oben geschilderten) Entwicklungsgeschichte sehen sich Nationalstaaten schon auf der technischen Ebene erheblichen Herausforderungen ausgesetzt, wenn sie regulierend eingreifen wollen. Das wurde bereits zu einem relativ frühen Zeitpunkt deutlich anhand des Themas Datenschutz. Hier hatten Staaten wie Schweden und die Bundesrepublik Deutschland in den 1970er Jahren gesetzliche Regelungen erlassen und Datenschutzbeauftragte institutionalisiert. Damit waren Standards geschaffen worden in einer Zeit, in der Datenverarbeitung noch (zumeist mit großen „mainframe“-Computern) ausschließlich lokal stattfand, Datenaustausch durch den physischen Transport von Magnetbändern erfolgte und entsprechend kontrolliert und reguliert werden konnte. Die sich im Lauf der Zeit national ausbildenden Datenschutzregelungen variierten inhaltlich in vielerlei Hinsicht, was angesichts unterschiedlicher nationaler Präferenzen nicht weiter Anlass zur Verwunderung ist.³⁴ Am deutlichsten unterschieden sich die (im Zuge der Schaffung des EU-Binnenmarkts durch eine Richtlinie zum Datenschutz im Jahr 1995 harmonisierten) Regeln in der Europäischen Union einerseits und in den USA andererseits, was mit der Ausbreitung der Nutzung des Internets zu einem regulativen Problem wurde.³⁵ Die Suche

³³ Merkel 2015, S. 86.

³⁴ Newman/Bach 2004; Newman 2008.

³⁵ Busch 2006, 2012a.

nach gemeinsamen Regeln (nicht nur im Bereich Datenschutz) erwies sich als ausgesprochen schwierig³⁶, zumal unklar und umstritten war, „wer das Internet kontrolliert“.³⁷

Wollte man die mannigfachen wirtschaftlichen Vorteile des Internets nutzen, so musste man auf nationalstaatlicher Ebene bereit sein, kaum Kontrolle über die Datenübertragung zu haben. Doch dazu waren autoritär oder diktatorisch regierte Staaten nicht bereit, die das emanzipatorische Potential freier Kommunikation fürchteten und daher den Zugang zum Internet nur sehr beschränkt gewährten bzw. ihn hinsichtlich der Inhalte (etwa durch technisch aufwendige Filter wie die „Great Firewall“ in China) kontrollierten.

Solche Einschränkungen beim Zugang zu Information sind für liberale, demokratische Rechtsstaaten ein Verstoß gegen normative Grundlagen, zu denen zentral das Recht zur freien Meinungsäußerung und der Zugang zu Informationen gehören. Andererseits können gerade die Durchsetzung geltenden Rechts und der entsprechende demokratische Wille auch Gründe liefern, dass Staaten inhaltliche Kontrolle über das Internet auf ihrem Territorium ausüben wollen. Dies gilt insbesondere für Themen, die hochrangig auf der politischen Agenda stehen, wie im Folgenden deutlich werden wird.

Kontrolle darüber, welche Inhalte zugänglich sind, ist im Internet territorial gebunden leichter zu erlangen als Kontrolle über die Übertragung von Daten. Diesen Umstand haben sich autoritäre Staaten schon früh zu Nutze gemacht. Wie die in der *Open Net Initiative* (ONI) zusammengeschlossenen Forscher bereits zu Beginn der 2000er Jahre durch systematische empirische Tests belegen konnten, verhinderten diese Staaten durch zum Teil ausgefeilte Techniken der Filterung den freien Zugriff auf bestimmte Teile des Internets, also auf Websites mit unerwünschten Inhalten.³⁸

Doch ist, wie neuere Untersuchungen zeigen, das Thema Regulierung von Internetinhalten mittlerweile nicht mehr auf autoritäre Staaten beschränkt, sondern auch in liberalen Demokratien weitgehend etabliert.³⁹ Den politischen Bedenken, solche Regulierung führe zu Spannungen mit Grundlagen der liberalen Demokratie, wird im innenpolitischen Diskurs oft entgegengehalten, das Internet dürfe „kein rechtsfreier Raum“ sein. Hinzuzufügen ist, dass es auch aus demokratietheoretischer Perspektive grundsätzlich positiv zu bewerten ist, wenn verbreitete Wünsche nach Regulierung nicht aus technokratischen Gründen abgelehnt oder ihre Umsetzung für technisch unmöglich erklärt wird. Gerade das Thema der sogenannten „Kinderpor-

36 Bendorath u. a. 2008.

37 So der Titel von Goldsmith/Wu 2006.

38 Deibert u. a. 2008, 2010.

39 Busch 2017; Küllmer 2018.

nografie“⁴⁰ – ein von allen politischen Seiten vehement abgelehnter Tatbestand, dessen strafbewehrte Verfolgungswürdigkeit praktisch von niemandem in Frage gestellt wird – hat zur Zunahme von Maßnahmen und Infrastruktur zur Ermöglichung von Inhaltsregulierung im Internet auch in etablierten liberalen Demokratien geführt, wie eine Untersuchung über 21 Länder und den Zeitraum zwischen 2004 und 2012 zeigen konnte.⁴¹ Dass dabei in den verschiedenen Ländern unterschiedlich vorgegangen ist und politische Variablen diese Varianz zumindest teilweise erklären können, ist ein weiterer interessanter Befund.

Dennoch sind solche regulativen Eingriffe auch mit Problemen verbunden, wie eine genauere Betrachtung der beiden bisher in der Bundesrepublik unternommenen Versuche staatlicher Regulierung – das „Zugangerschwerungsgesetz“ (ZugEr-schwG) von 2010 und das „Netzwerkdurchsetzungsgesetz“ (NetzDG) von 2017 – zeigt. Ersteres wurde im Jahr 2009 (kurz vor der bevorstehenden Bundestagswahl) von der damaligen Bundesfamilienministerin Ursula von der Leyen mit dem expliziten Ziel der Bekämpfung von Kinderpornografie initiiert. Als technische Umsetzung war eine zentrale Erfassung von Webseiten mit entsprechenden Inhalten durch das Bundeskriminalamt vorgesehen. Auf Basis einer solchen Datenbank sollten dann alle Internetprovider Versuche des Zugriffs auf diese Seiten auf eine Stoppmeldung umleiten und die IP-Adressen der Nutzer speichern, um eine Strafverfolgung zu ermöglichen.⁴² Auf Probleme mit diesem Ansatz wiesen die skeptische Rezeption des Vorhabens in der rechtswissenschaftlichen Debatte ebenso hin,⁴³ wie die ursprüngliche Weigerung von Bundespräsident Köhler, das Gesetz ohne Vorlage zusätzlicher Informationen zu unterzeichnen.⁴⁴ Der im Gesetz vorgesehene Auf- und Ausbau einer Infrastruktur zur Sperrung von Internetinhalten durch das BKA sowie die notwendige Kooperation mit den Internet Providern erwiesen sich als administrativ heikel und als politisch hoch kontrovers. Eine Mobilisierung der Öffentlichkeit durch Aktivisten, die mit dem Slogan „Löschen statt Sperren“ eine von vielen Beobachtern als dem Gesetz überlegene Lösung vorschlugen, führte – gemeinsam mit einem Koalitionswechsel als Folge der Bundestagswahl, die die dem Gesetz ablehnend gegenüberstehende FDP zum neuen Koalitionspartner der CDU/CSU machte – zunächst zu einer abgestimmten Nichtanwendung des Gesetzes und schließlich zu seiner Aufhebung im Dezember 2011.⁴⁵

40 Dieser Begriff wird hier verwendet, da er weit verbreitet und leicht verständlich ist. Allerdings soll auch darauf hingewiesen werden, dass er den Sachverhalt nicht korrekt beschreibt, da man eigentlich von organisiertem und medial festgehaltenem Kindesmissbrauch sprechen muss.

41 *Busch* 2017, S. 339–342.

42 Siehe den Gesetzentwurf vom 5.5.2009 (BT-Drs. 16/12850).

43 z.B. *Frey/Rudolph* 2009.

44 Bundespräsident Köhler unterzeichnete das Gesetz im Februar 2010 schließlich doch. Vgl. für Details *Busch* 2010, S. 420ff.

45 Siehe den Gesetzentwurf vom 20.7.2011 (BT-Drs. 17/6644).

Beim nächsten regulativen Eingriffsversuch der Bundesregierung in das Internet, dem „Netzwerkdurchsetzungsgesetz“ im Jahr 2017, hatten sich Problemgebiet und Ansatz verschoben. Als Problem wurde die – aufgrund der zwischenzeitlich deutlich gestiegenen Verbreitung von „Sozialen Netzwerken“ (wie Facebook oder Twitter) – vermehrte Inzidenz von Diffamierung durch „Hasskriminalität und andere strafbare Inhalte“ angesehen, die „eine große Gefahr für das friedliche Zusammenleben einer freien, offenen und demokratischen Gesellschaft“ bildeten.⁴⁶ Bessere Rechtsdurchsetzung in sozialen Netzwerken solle erreicht werden durch an deren Betreiberfirmen gerichtete Berichtspflichten sowie die Androhung von empfindlichen Strafen (bis zu 50 Mio. Euro, vgl. § 4 Abs. 2 NetzDG), falls „offensichtlich rechtswidrige Inhalte“ nicht innerhalb knapp bemessener Fristen gelöscht oder für den Zugang gesperrt werden. Auch bei diesem Gesetz überwog aber in der Rezeption deutlich die Kritik. Bürgerrechtsorganisationen, Verbände und Pressekommentare äußerten sich einhellig sehr skeptisch hinsichtlich der gewählten Instrumente, wie der Durchsetzungschancen. Grundsätzlich wurde kritisiert, die Höhe der Strafen werde zu voreilem Löschen auch von bei genauerer Betrachtung nicht strafbarem Material führen und somit die verfassungsmäßig garantierte Meinungsfreiheit beeinträchtigen. Die Entscheidung über Rechtswidrigkeit und Strafbarkeit sei eine Aufgabe der Justiz, die nicht an private Akteure (wie die Internetprovider) übertragen werden dürfe.⁴⁷ Wie schon im Fall des 

ZugErschwG formierte sich also auch in diesem Fall ein gesellschaftlich breit aufgestellter Protest, der nicht die *Zielsetzung* des geplanten regulativen Eingriffs in Frage stellte (der diesbezügliche Handlungsbedarf wurde jeweils explizit von den Kritikern anerkannt), jedoch die gewählten *Instrumente und Methoden* scharf kritisierte. Inwieweit die von den Netzbetreibern regelmäßig verlangten „Transparenzberichte“ zu einer Anpassung des Regulierungsansatzes führen werden, muss derzeit (Februar 2019) noch offenbleiben. Im Parlament sitzen jedenfalls kritische Beobachter des Gesetzes und verlangen diesbezüglich Auskunft von der Regierung.⁴⁸

Zusammenfassend kann man festhalten, dass beide bisher unternommenen Regulierungsversuche im Bereich des Internets erhebliche Probleme aufweisen. Während ihre grundsätzliche Zielsetzung nicht in Frage gestellt wird und ihren Absichten abstrakte Zustimmung zuwächst, erweisen sie sich zum einen als technisch schwierig umsetzbar; zum anderen zeigt sich in den Konkretisierungen der Umsetzung viel Po-

⁴⁶ Siehe den Gesetzentwurf vom 16.5.2017 (BT-Drs. 18/12356).

⁴⁷ Vgl. die „Deklaration für die Meinungsfreiheit“, unter: <http://deklaration-fuer-meinungsfreiheit.de>, download am 4.2.2019, die von zahlreichen Industrie- und Journalistenverbänden, Bürgerrechtsorganisationen sowie einzelnen Akademikern und Politikern unterzeichnet ist.

⁴⁸ Siehe beispielsweise die Kleine Anfrage der Abgeordneten Manual Höferlin, Frank Sitta, Grigorios Aggelidis und der Fraktion der FDP vom 18.12.2018 (BT Drs. 19/6739) sowie die Antwort der Bundesregierung vom 15.1.2019 (BT Drs. 19/7023).

tential für politisch kontroverse Debatten, die Spannungen mit zentralen Fundamenten der liberalen Demokratie verdeutlichen.

8. Schluss

Das Internet als globale, jedenfalls aber transnational angelegte Struktur ohne zentrale Steuerung und mit höchster ökonomischer und sozialer Relevanz für das Leben der Gegenwart stellt den modernen Staat vor große Herausforderungen. Seine regulativen Fähigkeiten sind in diesem Bereich eingeschränkt, während gleichzeitig die Erwartungen der Bürger auf erfolgreiche Erfüllung der ihm gestellten Aufgaben wachsen und eine Bedrohung seiner demokratischen Substanz die Verteidigung der Grundlagen des Staates immer wichtiger erscheinen lässt.

Doch zeigen die angeführten Beispiele aus der bundesdeutschen Gesetzgebung, dass erfolgreiche Regulierung nicht nur hoch komplex und (wie regulative Politik generell) „höchst voraussetzungsvoll“ ist, sondern dass Versuche in diese Richtung, die vorschnell (etwa unter dem Imperativ gewünschter Vorteile in bevorstehenden Wahlkampfauseinandersetzungen) und mit mangelhafter Vorbereitung und Durchdringung des Sachverhalts erfolgen, größere schädliche Nebenwirkungen als Nutzen stiften können.

Notwendig ist daher eine Zurückhaltung bei Versprechungen hinsichtlich dessen, was der Staat in diesem Bereich leisten kann. Unerfüllte Erwartungen können die Legitimität staatlichen Handelns nämlich in Frage stellen und nachhaltig beschädigen. Zum anderen ist die Aufgabenzuweisung zwischen Staat und Gesellschaft in diesem Bereich zu überdenken. Nicht alles muss von staatlicher Stelle bearbeitet werden, auch wenn etwa die oben angeführten Themen wohl am besten in die Obhut des Staates gehören. Jedoch ist zum Beispiel im (hohe Flexibilität und sofortige Reaktion erfordernden) Themenbereich *fake news* eventuell gesellschaftlichen Bearbeitungsmechanismen (durch Kompetenzteams bei den Medien oder Spezialisten wie das *Digital Forensic Research Lab* des *Atlantic Council*) gegenüber denjenigen staatlicher Gesetzes- und Behördenmechanismen der Vorzug zu geben. Denn der Staat muss sich nicht selbst um alles kümmern, sondern kann sich durch Arbeitsteilungen mit gesellschaftlichen Akteuren zum einen selbst entlasten, zum anderen eventuell sogar bessere Bearbeitungsergebnisse erreichen. Gerade dem an solches Staatshandeln *at arm's length* gewohnten „semi-souveränen“ Staat der Bundesrepublik sollte eine solche produktive Selbstbescheidung eher leichtfallen.⁵⁰ Dass diese jedoch wieder ganz eigene Probleme aufwerfen kann, hat sich am Fall des *Netzwerkdurchsetzungsgesetzes* gezeigt. Wenn daraus ein Schluss gezogen werden

49 Czada/Lütz 2003, S. 13.

50 Katzenstein 1987; Green/Paterson 2005; Busch 2005.

kann, dann wohl am ehesten der, dass in den nächsten Jahren das praktische Experimentieren mit verschiedenen Konfigurationen von staatlich-hoheitlicher und gesellschaftlich-privater Involvierung sich in diesem Bereich als der beste Weg herausstellen mag.

Literatur

- Barlow, John Perry, 1996: A Declaration of the Independence of Cyberspace. Unter: <https://projects.eff.org/%7Ebarlow/Declaration-Final.html>, download am 11.9.2015.
- Bendrath, Ralf/Hofmann, Jeanette/Leib, Peter/Mayer, Peter/Zürn, Michael, 2008: Namensräume, Datenschutz und elektronischer Handel. Die Suche nach Regeln für das Internet. In: Hurrelmann, Achim/Leibfried, Stephan/Martens, Kerstin/Mayer, Peter (Hrsg.), 2008: Zersplitterung der Nationalstaat? Die Internationalisierung politischer Verantwortung, Frankfurt am Main, S. 209–239.
- Busch, Andreas, 2005: Shock absorbers under stress: parapublic institutions and the double challenges of German unification and European integration. In: Green, Simon/Paterson, William E. (Hrsg.), 2005: Governance in contemporary Germany. The semisovereign state revisited, Cambridge, S. 94–114.
- Busch, Andreas, 2006: From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic. In: SCRIPT-ed. A Journal of Law and Technology 3, S. 304–321. Unter: <http://www.law.ed.ac.uk/ahrc/script%2Ded/vol3-4/busch.asp>, download am 7.2.2019.
- Busch, Andreas, 2010: Kontinuität statt Wandel. Die Innen- und Rechtspolitik der Großen Koalition. In: Egle, Christoph/Zohlnhöfer, Reimut (Hrsg.), 2010: Die zweite Große Koalition. Eine Bilanz der Regierung Merkel 2005–2009, Wiesbaden, S. 401–430.
- Busch, Andreas, 2012a: Die Regulierung transatlantischer Datenströme: zwischen Diktat und Blockade? In: Busch, Andreas/Hofmann, Jeanette (Hrsg.), 2012a: Politik und die Regulierung von Information. [= Sonderheft Nr. 46 of Politische Vierteljahresschrift], Baden-Baden, S. 408–440.
- Busch, Andreas, 2012b: Politische Regulierung von Information – eine Einführung. In: Busch, Andreas/Hofmann, Jeanette (Hrsg.), 2012b: Politik und die Regulierung von Information. [= Sonderheft Nr. 46 of Politische Vierteljahresschrift], Baden-Baden, S. 24–47.
- Busch, Andreas, 2017: Netzzensur in liberalen Demokratien. In: Croissant, Aurel/Kneip, Sascha/Petring, Alexander (Hrsg.), 2017: Demokratie, Diktatur, Gerechtigkeit. Festschrift für Wolfgang Merkel, Wiesbaden, S. 331–352.
- Cadwalladr, Carole, 2017: The great British Brexit robbery: how our democracy was hijacked. Unter: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy>, download am 7.2.2019.
- Christlich-Demokratische Union Deutschlands/Christlich-Soziale Union in Bayern/Sozialdemokratische Partei Deutschlands, 2018: Ein neuer Aufbruch für Europa – Eine neue Dynamik für Deutschland – Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode, Unter: <https://goo.gl/oJi7bH>, download am 7.2.2019.

- Clinton*, Hilary, 2010: Remarks on Internet Freedom. Unter: <http://www.state.gov/secretary/rm/2010/01/135519.htm>, download am 7.2.2019.
- Coleman*, E. Gabriella, 2013: Coding freedom. The ethics and aesthetics of hacking. Princeton.
- Cortada*, James W., 2012: The digital flood. The diffusion of information technology across the U.S., Europe, and Asia. Oxford.
- Czada*, Roland/Lütz, Susanne, 2003: Einleitung – Probleme, Institutionen und Relevanz regulativer Politik. In: Czada, Roland/Lütz, Susanne (Hrsg.), 2003: Regulative Politik. Zählungen von Markt und Technik, Opladen, S. 13–32.
- Dahl*, Robert A., 1989: Democracy and its critics. New Haven.
- Deibert*, Ronald/*Palfrey*, John/*Rohozinski*, Rafal/*Zittrain*, Jonathan (Hrsg.), 2008: Access denied. The practice and policy of global Internet filtering. Cambridge; Mass.
- Deibert*, Ronald/*Palfrey*, John/*Rohozinski*, Rafal/*Zittrain*, Jonathan (Hrsg.), 2010: Access controlled. The shaping of power, rights, and rule in cyberspace. Cambridge; Mass.
- DeNardis*, Laura, 2009: Protocol politics. The globalization of Internet governance. Cambridge; Mass.
- Diamond*, Larry, 2010: Liberation Technology. In: Journal of Democracy 21, S. 69–83.
- Floridi*, Luciano, 2010: Information. A very short introduction. Oxford.
- Frey*, Dieter/*Rudolph*, Matthias, 2009: Zugangserschwerungsgesetz: Schnellschuss mit Risiken und Nebenwirkungen. In: Computer und Recht: Zeitschrift für die Praxis des Rechts der Informationstechnologien 25, S. 644–650.
- Goldsmith*, Jack L./*Wu*, Tim, 2006: Who controls the Internet? Illusions of a borderless world. Oxford.
- Green*, Simon/*Paterson*, William E. (Hrsg.), 2005: Governance in contemporary Germany. The semisovereign state revisited. Cambridge.
- Hafner*, Katie/*Lyon*, Matthew, 2000: ARPA Kadabra oder die Geschichte des Internet 2., korr. Aufl.. Heidelberg.
- Hindman*, Matthew, 2009: The myth of digital democracy. Princeton.
- Jamieson*, Kathleen Hall, 2018: Cyberwar. How Russian hackers and trolls helped elect a president; what we don't, can't, and do know. New York.
- Katzenstein*, Peter J., 1987: Policy and politics in West Germany. The growth of a semisovereign state. Philadelphia.
- Küllmer*, Björn, 2018: Die Regulierung von Internetinhalten in demokratischen Systemen. Deutschland, Großbritannien, USA. Dissertation. Göttingen: Georg-August-Universität Göttingen.
- Leggewie*, Claus/*Maar*, Christa (Hrsg.), 1998: Internet & Politik. Von der Zuschauer- zur Beteiligungsdemokratie? Köln.
- Levy*, Steven, 2010 [1984]: Hackers. Heroes of the computer revolution. Sebastopol. California.
- Lindow*, Stefan, 2019: Magna Carta, magna controversia. Ideen, Interessen und Konflikte im Urheberrecht. In: Busch, Andreas/Breindl, Yana/Jakobi, Tobias (Hrsg.), 2019: Netzpolitik. Ein einführender Überblick, Wiesbaden, S. 225–261.

- Markoff*, John, 2006: What the dormouse said. How the sixties counterculture shaped the personal computer industry. New York.
- Merkel*, Wolfgang, 2015: Nur schöner Schein? Demokratische Innovationen in Theorie und Praxis. Eine Studie der Otto Brenner Stiftung. Frankfurt (Main).
- Morozov*, Evgeny, 2009: How dictators watch us on the web. Unter: <http://www.prospectmagazine.co.uk/2009/11/how-dictators-watch-us-on-the-web/>, download am 7.5.2019.
- Morozov*, Evgeny, 2011: The net delusion. The dark side of internet freedom. New York.
- Neudert*, Lisa-Maria/*Kollanyi*, Bence/*Howard*, Philip N., 2017: Junk News and Bots during the German Federal Presidency Election. What Were German Voters Sharing Over Twitter? COMPROP DATA MEMO 2017.2 / 27 March 2017. Unter: <http://politicalbots.org/wp-content/uploads/2017/03/What-Were-German-Voters-Sharing-Over-Twitter-v4.pdf>, download am 15.5.2017.
- Newman*, Abraham L., 2008: Protectors of privacy. Regulating personal data in the global economy. Ithaca u. a..
- Newman*, Abraham L./*Bach*, David, 2004: Self-Regulatory Trajectories in the Shadow of Public Power. Resolving Digital Dilemmas in Europe and the United States. In: *Governance* 17, S. 387–413.
- Rohs*, Bastian, 2019: Sicherheit im Internet: Cybercrime, Cyberterror und Cyberwar. In: Busch, Andreas/Breindl, Yana/Jakobi, Tobias (Hrsg.), 2019: Netzpolitik. Ein einführender Überblick, Wiesbaden, S. 303–332.
- Shirky*, Clay, 2011: The Political Power of Social Media. Technology, the Public Sphere, and Political Change. In: *Foreign Affairs* 90, S. 28–41.
- Siegrist*, Hannes, 2006: Geschichte des geistigen Eigentums und der Urheberrechte. Kulturelle Handlungsrechte in der Moderne. In: Hofmann, Jeanette (Hrsg.), 2006: Wissen und Eigentum. Geschichte, Recht und Ökonomie stoffloser Güter, Bonn, S. 64–80.
- Stephenson*, Neal, 1999: Cryptonomicon. New York.
- Stöcker*, Christian, 2012: Enthüllung über Stuxnet-Virus: Obamas Cyber-Angriff auf Irans Atomanlagen. Unter: <http://www.spiegel.de/netzwelt/netzpolitik/usa-und-israel-sollen-stuxnet-virus-gegen-iran-entwickelt-haben-a-836401.html>, download am 7.2.2019.
- Sunstein*, Cass R., 2017: #Republic. Divided Democracy in the Age of Social Media. Princeton.
- Wells*, Herbert George, 1938: World brain, London.
- World Economic Forum*, 2011: Personal Data: The Emergence of a New Asset Class. Unter: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf, download am 7.2.2019.