WBGU

Wissenschaftlicher Beirat der Bundesregierung
Globale Umweltveränderungen

Materialien

Prof. Dr. Jeanette Hofmann

Internet Governance

Expertise für das WBGU-Hauptgutachten
„Unsere gemeinsame digitale Zukunft“

Berlin 2017

Expertise zum Thema Internet Governance

Im Auftrag des
Wissenschaftlichen Beirats der Bundesregierung
Globale Umweltveränderungen

Berlin, 19.12.2017

Prof. Dr. Jeanette Hofmann
Reichpietschufer 50
10785 Berlin, Germany
+49 30 25491-0
jeanette@wzb.eu

Inhalt

Abbildungen iii

1. Internet Governance als analytisches Konzept 1

1.1. Der Begriff Internet Governance 1

1.2. Der Begriff Governance 2

2. Kritischen Infrastrukturen und Standards 4

2.1. Der Begriff kritische Infrastrukturen 4

2.2 Critical Internet Resources und Internet Standards 4

3. Besonders wichtige Infrastrukturen und Standards 6

4. Definition regulatorischer Lücken in Internet Governance 8

5. Privat organisierte Erbringung von Verwaltung und Dienstleistungen 10

5.1 Übergang vom Adressierungsstandard IPv4 zu IPv6 10

5.2 Interkonnektivität (Peering) 11

5.3 IoT Sicherheitsrisiken 13

6. Regulierung von Global Playern der Internetwirtschaft 15

6.1 Daten als Währung 16

6.2. Regulierung von Inhalten 18

6.3 Marktkonzentration 20

7. Aktueller Diskussionsstand über Multi-Stakeholder-Verfahren 22

8. Unabhängigkeit von ICANN und Ansätze der Selbstregulierung: Reconsideration (Art. 4 ICANN Bylaws), Ombudsman, Independent Review Process, Document Transparency 25

8.1 Request for reconsideration process (section 4.2.) 26

8.2 Independent review process (IRP) 27

8.3 ICANN Ombuds Office (IOO) 27

8.4 Documentary Information Disclosure Policy (DIDP) 28

9. Regulierung bzw. transparente Gestaltung von Standardisierungsprozessen neuer Technologien 29

10. Themen, Prozesse oder Weichenstellungen mit besonderer Relevanz für den globalen Umwelt- und Nachhaltigkeitsdiskurs 32

Literatur 33

Abbildungen

Abb. 1: Schematische Darstellung der DNS-Hierarchie ……6
Abb. 2: Internet Governance ……..9
Abb. 3: Schema interkonnektierender autonomer Systeme ……12
Abb. 4: Problembereiche bei der Regulierung von Informationsintermediären ……..16

1. Internet Governance als analytisches Konzept

1.1. Der Begriff Internet Governance

Der Begriff *Internet Governance* findet in der wissenschaftlichen Literatur erstmals 1997 Erwähnung (Kahin und Keller 1997). Er verbindet das Governance-Konzept erstmals mit einem spezifischen Feld politischer Intervention und Expertise. Die zentrale Frage der frühen Forschung zu Internet Governance zielte auf die "governability", die Regierbarkeit des Internets. Angesichts der grenzüberschreitenden Architektur des Kommunikationsnetzes problematisierten die Governance-Forscher nicht nur die Möglichkeit einer politischen Steuerung durch territorialstaatlich verfasste Regierungen, sondern auch die Erfolgschancen und die Legitimität hierarchischer Autorität im virtuellen Raum generell. Maximen wie "
"The Internet interprets censorship as damage and routes around it“ (John Gilmore zitiert in Lewis 1996) spiegeln den Zeitgeist der frühen Internet Governance Literatur wider.

Eine erste, bis heute vielfach zitierte Definition von Internet Governance wurde im Rahmen des UN World Summit on the Information Society (WSIS 2005) vorgelegt: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet” (WGIG 2005). Diese an die Definition internationaler Regime des US-amerikanischen Politikwissenschaftlers Stephen Krasner (1982, 186) angelehnte Formulierung akzentuiert eine Multi-Akteursperspektive ("Multi-Stakeholder-Ansatz").

Aus heutiger Sicht erscheint diese Definition von Internet Governance jedoch problematisch. Zunächst übersieht der Fokus auf "shared principles, norms, rules and decision-making procedures" die Konflikthaftigkeit der Aushandlungsprozesse, die sich sowohl zwischen als auch innerhalb der Stakeholder-Gruppen zeigen. Vor allem Regierungen und zivilgesellschaftliche Gruppen weisen ein breites Spektrum von normativen Positionen auf, das eine konsensuale Politikformulierung, wie auch ein einheitliche Repräsentation gemäß des Multi-Stakeholder Konzepts, schwer oder zuweilen unmöglich macht (Jeanette Hofmann 2016). Zudem vernachlässigt diese Definition Quellen der Ordnungsbildung, die im Bereich von Internet Governance eine zunehmend wichtige Rolle spielen: nationale Gesetze und vertragsförmige Regulierungsmaßnahmen (vgl. Bygrave 2015). Fragen der Machtverteilung, verstanden im Weberschen Sinne als asymmetrische Chancen zur Durchsetzung der eigenen Interessen, die sich auf die Entwicklung des Internets auswirken, bleiben unerwähnt. Und schließlich konzentriert sich die Definition vorrangig auf intentionale Formen von Governance und übersieht somit eine Vielzahl von Handlungen oder Prozessen, die gewissermaßen als Nebeneffekt auf die Netzinfrastruktur einwirken. DeNardis (2012) und Braman (2012) erwähnen in diesem Zusammenhang beispielhaft technische Standards, die die Rahmenbedingungen für die weitere Entwicklung von Datennetzen prägen, wenngleich sie zumeist sehr viel enger gesteckte Ziele anstreben.
Die heterogenen Quellen der Ordnungsbildung, die den Wandel des Internet vorantreiben und zugleich strukturieren, werden in der wissenschaftlichen Literatur als "patchworks of partly

complementary, partly competing regulatory elements in the form of legal rules and ordinances, mandatory and voluntary technical standards and protocols, international and national contracts and agreements, and informal codes of conduct and 'netiquette'" beschrieben (Jürgen Feick und Werle 2010, 525). Statt einer abgestimmten Institutionenstruktur ließe sich die Praxis von Internet Governance eher als eine Vielzahl sich wechselseitig überlagernder dialogförmiger Koordinationsvorgänge verstehen, die auf wechselseitige Anerkennung und (häufig projektbasierte) Koordination zielen (Brousseau, Marzouki, und Méadel 2012, 16f.). Bezogen auf die Definition von Internet Governance lässt sich aus diesen empirischen Beobachtungen der Schluss ziehen, dass es sich bei Internet Governance eher um ein transnationales Netzwerk eigenständiger Akteure als um einen abgestimmten Regulierungsprozess handelt. Unbeschadet der Frage, ob diese Diagnose auf andere transnationale Politikfelder ebenso zutrifft, lassen sich aus diesem Befund Überlegungen über die Definition des Begriffs Governance ableiten.

1.2. Der Begriff Governance

In den Sozialwissenschaften steht der Begriff *Governance* für eine Entkopplung zwischen dem Vorgang des Regierens und seinen Akteuren bzw. Organisationsformen.[1] Governance kann durch, unter der Mitwirkung von oder auch ohne Regierungen erfolgen. Der Begriff gewann diese Bedeutung mit dem von Rosenau und Czempiel im Jahr 1992 veröffentlichten Buch "Governance without Government", das die Ausdifferenzierung von Regulierungsprozessen beschrieb. Als wichtige Triebkräfte für die Ausdifferenzierung von Governance-Formen gelten die Transnationalisierung von Regelungsprozessen sowie die in den 1980er Jahren einsetzende Deregulierung. Letztere übertrug vormals hoheitliche Aufgaben nicht-staatlichen Einrichtungen, die dann ihrerseits einen Bedarf nach speziellen Rahmenreglungen, aber auch Aufsichtskompetenzen schufen. Mit der Zunahme von Akteuren aus dem privatwirtschaftlichen Sektor, aber auch der Zivilgesellschaft, haben sich die Instrumente und Ressourcen des Regierens erweitert. Unter dem Begriff "soft law" bzw. "soft regulation" (vgl. Mörth 2004) werden eine Vielzahl von Regelungsformen gefasst, darunter freiwillige Formen der Selbstverpflichtung (wie Verhaltenskodizes), technische Normen, Transparenzberichte und Algorithmen, aber auch prozedurale und dialogartige Formen wie etwa Multi-Stakeholder-Prozesse, die auf Transparenz, Integration von Interessengruppen oder Konsens zielen.

Der Governance-Begriff erfasst somit eine Vielzahl von Formen der nationalen und transnationalen Ordnungsbildung, die sich dem Begriff des Regierens teilweise entziehen, weil dieser traditionell für staatliche bzw. öffentliche Handlungskompetenzen reserviert ist. Die Erfassung eines weiten Spektrums von Ordnungsleistungen erkauft sich der Governance-Begriff mit einer viel beklagten analytischen Unschärfe (vgl. Grande 2012; Offe 2008): Wenn alle gesellschaftlichen und wirtschaftlichen Regelungsprozesse unter dem Governance-Konzept rubriziert werden können, was ist dann nicht Governance?

[1] Der in der Wirtschaftswissenschaft gebräuchliche Begriff "Corporate Governance" wird hier nicht behandelt.

Vor allem im europäischen Raum sind als Reaktion auf den Band von Rosenau und Czempiel viele Versuche einer definitorischen Eingrenzung verzeichnen (für einen Überblick s. Mayntz 2009). Bis heute hat keiner dieser Beiträge zu einem einheitlichen Verständnis und Gebrauch des Governance-Konzepts geführt mit der Folge, dass der Begriff in unterschiedlicher und teils widersprüchlicher Weise verwendet wird. Eine verbreitete Definition setzt diese mit Regulierung gleich (Feick und Werle 2010; Grande 2012; Rosenau 1992). Die Regulierungsforschung versteht unter Regulierung den gezielten Versuch, das Verhalten von Dritten gemäß explizierter Zwecke und Zielsetzungen zu beeinflussen (Black 2002, 170). Im Kern beschreibt der Regulierungsbegriff somit intentionale, zielorientierte Interventionen in einen Politikbereich (Jeanette Hofmann, Katzenbach, und Gollatz 2016). Als Regulierung interpretiert, gewinnt das Governance-Konzept zwar die gewünschte Eingrenzung, allerdings auf Kosten seiner Erklärungskraft. Die Regulierungsforschung vermag nur solche Ordnungsprozesse zu erklären, die im Rahmen intentionalen Handelns bzw. in Form von explizit formulierten Policy-Zielen entstehen. Nicht erfasst werden dagegen jene Regelungen und Institutionen, die als Nebeneffekt anderer Ziele oder aus dem kontextspezifischen Zusammenwirken verschiedener Akteure und Ereignisse hervorgehen.

Die historische Rekonstruktion vieler Regelungen, Regulierungskompetenzen und Organisationen weist für gewöhnlich einen hohen Anteil nichtintendierter Entwicklungen auf. So ist für das Feld von Internet Governance beobachtet worden, dass ein hoher Anteil strukturbildender Maßnahmen als Nebeneffekt anderer Handlungsziele erfolgt (Van Eeten und Mueller 2013). Ein weiteres Problem der Gleichsetzung von Governance und Regulierung besteht in der verbreiteten Grundannahme, dass Regulierungsmaßnahmen funktionale Lösungen für vorliegende Probleme darstellen. Vor allem umfangreichen, historisch gewachsenen Regelungssystemen wie Internet Governance liegen jedoch komplexe Abstimmungsprozesse zugrunde, die der Annahme einer einheitlichen zielbasierten Regulierung widersprechen.

Statt Governance also als Regulierung zu interpretieren, schlagen Hofmann et al. (2016) vor, Governance als eine fortlaufende Form der Koordination zu verstehen. Die Autoren unterscheiden hierfür zwischen einfachen und reflexiven Formen der Koordination. Während der erste Koordinationstyp alltägliche Routinehandlungen umfasst, beziehen sich reflexive Koordinationsprozesse auf "kritische Momente" (Boltanski und Thévenot 2006, Übersetzung JH). Diese treten dann auf, wenn Routinehandlungen problematisch oder gar unmöglich werden, weil zugrunde gelegte Normen, Erwartungen und Annahmen nicht länger anwendbar sind und möglicherweise Gegenstand einer Neuverhandlung werden. Einfache Koordination schlägt in reflexive Koordination um, wenn Regeln problematisiert werden, also eine Koordination von Koordinierungsprozessen erforderlich wird. Dies kann einen Disput über die Auslegung, Anwendbarkeit oder Geltungsreichweite einer Regel betreffen, aber auch die Frage, ob ein Gesetz zeitgemäß ist. Gemäß dieser Definition haben Governance-Prozesse folglich keinen klare Zielsetzung; man kann sich diese eher als kontinuierlichen Verhandlungsvorgang vorstellen, in dessen Zuge politische Ziele, Normen und Bewertungsmaßstäbe gelegentlich hinterfragt werden. Beispiele für solche institutionalisierten Governance-Prozesse stellen die Internet Corporation for Assigned Names und Numbers

(ICANN) und das Internet Governance Forum (IGF) dar. Beide Organisationen zeichnen sich dadurch aus, dass einfache und reflexive Koordinationsprozesse kontinuierlich ineinandergreifen.

2. Kritischen Infrastrukturen und Standards

2.1. Der Begriff kritische Infrastrukturen

Im Bereich der *kritischen Infrastrukturen* wird sachlich zwischen der nationalen und der internationalen Ebene unterschieden. Wie die Definition der EU Richtlinie zu kritischen Infrastrukturen zeigt, bezieht sich der Begriff der kritischen Infrastrukturen vorwiegend auf nationalstaatliche Ressourcen und Organisationen: "die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten" (Art. 2a EU Council Directive 2008/114/EC).[2] Die Bezugnahme auf den Nationalstaat impliziert, dass die Kritikalität wie auch die entsprechenden Sektoren und Einrichtungen national variieren (für einen Überblick s. Mattioli und Levy-Bencheton 2014, 5).

Die Definition des Bundesinnenministeriums des Inneren (BMI) lehnt sich an dieses Verständnis an. Im Mittepunkt stehen Organisationen und Einrichtungen mit hoher Bedeutung für das staatliche Gemeinwesen und die öffentliche Sicherheit. Ihre *Kritikalität* bemisst sich an den antizipierten Folgen eines Leistungsausfalls für "die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen" (BMI 2009, 5). Unterschieden wird zwischen technischen Basisinfrastrukturen, sozioökonomischen Dienstleistungsinfrastrukturen sowie den entsprechenden Gefahrenquellen. Informations- und Kommunikationstechnologien stellen neben Energieversorgung, Verkehr, Wasser- und Abwasserversorgung lediglich eine von mehreren kritischen Infrastrukturen dar. Wichtig ist der Hinweis des BMI, dass die betreffenden Infrastrukturen ganz überwiegend von privaten Akteuren betrieben werden, so dass auch die "Sicherheit, Zuverlässigkeit und Verfügbarkeit dieser Infrastrukturen zunehmend in private, zumindest aber geteilte Verantwortung" fällt (BMI 2009, 5ff.).

2.2 Critical Internet Resources und Internet Standards

Das Internet stellt zwar inzwischen zweifelsohne eine kritische Infrastruktur dar, wird aber üblicherweise nicht als solche klassifiziert, weil mit dem Begriff der kritischen Infrastruktur nationale regulatorische Zuständigkeiten, Kompetenzen und Verpflichtungen verbunden werden, denen das Internet aufgrund seiner transnationalen Architektur nicht unterliegt.

[2] Zuweilen wird auf nationaler und europäischer Ebene zudem zwischen kritischen Infrastrukturen (CI) und kritischen Informationsinfrastrukturen (CII) unterschieden. Letztere bezeichnen Informations- und Kommunikationssysteme mit infrastrukturellem Charakter bzw. einer solchen Bedeutung für andere Infrastrukturen.

Im Zuge des UN Weltgipfels zur Informationsgesellschaft (WSIS) setzte sich der Begriff *Critical Internet Resources* (CIR) für die Kontrolle und Verwaltung der Netzinfrastruktur durch. Darunter wurden folgende Elemente zusammengefasst: "administration of the domain name system and Internet protocol addresses, administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, as well as multilingualization" (Mueller 2010, 215). Nicht zuletzt aufgrund seines Entstehungskontextes hat der Begriff eine starke politische Konnotation. Wie Mueller feststellt, bildet CIR das "code word" für die politische Auseinandersetzung über die globale Regulierung des Internets; eine Auseinandersetzung, bei der sich die Anhänger des bestehenden Systems privater Selbstregulierung "im Schatten" der US Regierung und die Anhänger eines intergouvermentalen UN-basierten Systems gegenüberstanden. Auch wenn dieser Konflikt nie gelöst werden konnte, hat sich seine Intensität doch in den letzten Jahren zunehmend abgeschwächt. Der Begriff Critical Internet Resources hat ebenfalls an Bedeutung verloren und taucht in der akademischen Literatur nur noch selten auf. Die für das Internet zentralen Bausteine von CIR werden im Folgenden dargestellt.

Im Kern beruht das Internet auf einem Netz der Netze. Das heißt, seine Funktion besteht darin, untereinander autonome Kommunikationsnetze zu einer übergreifenden Kommunikationsinfrastruktur zu verbinden. Diese eigenständigen Netze werden als autonomous systems (AS) bezeicnet und mit einer eigenen Kennung versehen. Derzeit besteht das Internet aus knapp 60.000 AS (s. CIDR Report 2017). Die Verbindung der einzelnen Netze erfolgt vermittels technischer Standards, die im Bereich des Internet als Protokolle bezeichnet werden. Transmission Control Protocol/Internet Protocol (TCP/IP) sind die zentralen Standards, die die Interaktion zwischen den einzelnen Netzen normieren und auf diese Weise den globalen Datenverkehr ermöglichen. TCP/IP kann mit einer gemeinsamen Sprache verglichen werden, die die Kommunikation aller Netzknoten erst ermöglicht. IP definiert das Format für die Adressierung aller im Internet erreichbaren Netzknoten. TCP steuert den Datenfluss und zerlegt diesen in einzelne Pakete, die mit Zieladressen versehen von Router zu Router weitergeleitet werden, bis sie ihr Ziel erreichen. Ein wesentliches Merkmal der TCP/IP Protokollfamilie besteht darin, dass sie nicht für einzelne Anwendungen optimiert wurde (wie etwa das klassische Telefonnetz für den Sprachverkehr) und beliebige Kommunikationsdienste über TCP/IP betrieben werden können. Ein weiteres Charakteristikum besteht in der sogenannten "end-to-end communication", die die Kontrolle über die Datenströme an die Endpunkte des Netzes verlagert und auf diese Weise die technischen Voraussetzungen dafür schafft, was heute ein wenig euphemistisch als "permissionless innovation" bezeichnet wird: Es gibt keine technisch implementierte Kontroll- oder Vetoinstanz für neue Dienste. TCP unterstützt alle Typen von Datenflüssen bzw. Anwendungen.

Neben TCP/IP werden das Domainnamensystem einschließlich der Rootserver sowie das Routingsystem zum Kernbestand der Netzarchitektur gezählt. Das Domainnamensystem ist ein globaler hierarchisch angeordneter Verzeichnisdienst. Dieser konstituiert den sog. *Namensraum* des Internets, indem er Internetadressen (mithilfe von sog. Name Servern) in

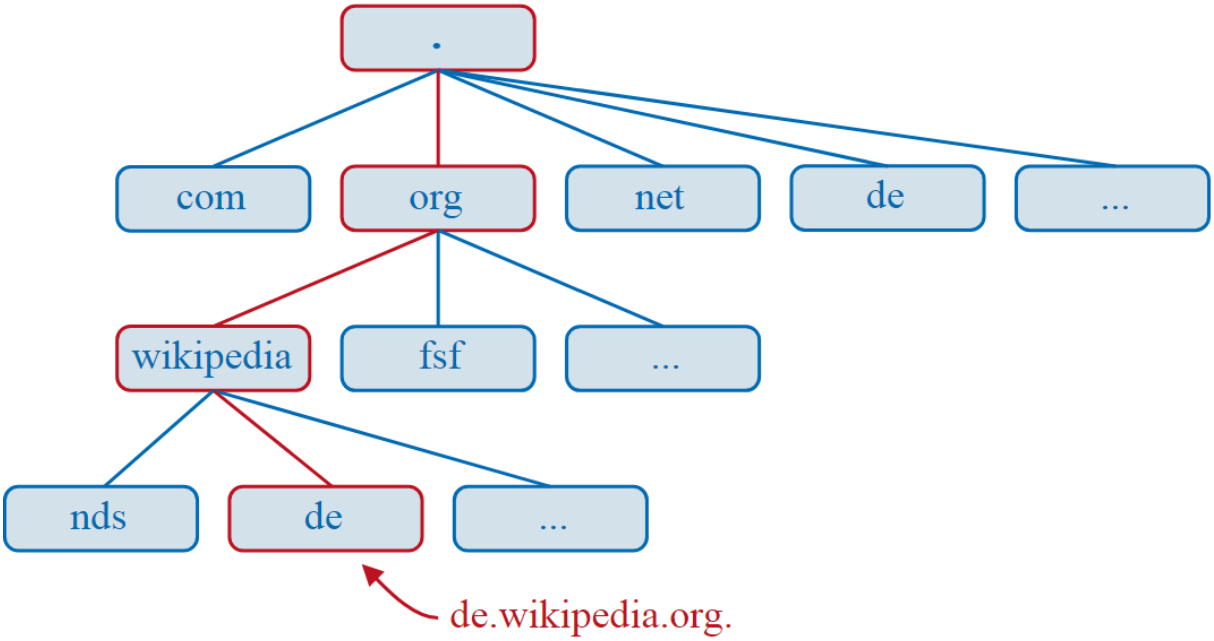

Abb. 1: Schematische Darstellung der DNS-Hierarchie. Quelle: (Wikimedia Commons 2006).

eineindeutige Domainnamen übersetzt und vice versa. Die Wurzel des verteilten Domainnamensystems (in der Abbildung als Punkt ausgedrückt) besteht aus 13 Rootservern, die die Adressen aller Top-Level-Domains vorhalten[3] Die ungleiche regionale Verteilung der Standorte der Root Server wie auch die Kontrolle der US-Regierung über den autoritativen Root Server hat auf der internationalen Ebene wiederholt zu Kritik geführt (Mueller 2010).

Die technischen Standards für die Wegeleitung der Datenströme (routing) sowie das dafür essentielle System der "Autonomous Systems" ermöglichen, dass der in Datenpakete unterteilte Datenstrom schritt- bzw. sprungweise zum Ziel geleitet wird (s. Abb. 1): Jedes lokale Netz verfügt über mindestens einen Router, die Informationen über weitere Netze (bzw. Autonomous Systems) in der topologischen Umgebung in Form von Routingtabellen vorhält. Anhand dieser Informationen entscheidet der Router, an welchen benachbarten Router Datenpakete weitergeleitet werden. Jeder Router kennt immer nur ein Teilsegment des Internets; alle Datenpakete bewegen sich von Router zu Router bzw. von Netz zu Netz zur Zieladresse. Die zugrundeliegenden Verfahren definiert das "Border Gateway Protocol".

3. Besonders wichtige Infrastrukturen und Standards

Nach dem mobilen Internet, das eine Vielzahl neuer digitaler Anwendungen und Nutzungsformen hervorgebracht hat, gilt das *Internet of Things* (IoT) als nächste bedeutsame technische Entwicklung, die im Verbund mit Cloud Computing und Big Data einen anhaltenden Innovationsschub auslösen und eine Vielzahl neuer Produkte und Dienste hervorbringen wird (Abdmeziem et al. 2016, 55; Vermesan et al. 2011, 18). Vermesan et al. (2011, 10) definieren IoT als dynamische globale Infrastruktur mit "self-configuring capabilities based on standard and interoperable communication protocols where physical and

[3] Für einen Überblick über die Standorte und Betreiber der Rootserver siehe www.root-servers.org (zuletzt abgerufen am 19.12.2017).

virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces". Das Institute of Electrical and Electronics Engineers (IEEE) definiert IoT als Netzwerk "that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the ‘Thing’ can be changed from anywhere, anytime, by anything“ (Minerva, Biru, und Rotondi 2015, 74). Mit anderen Worten wird eine wachsende Anzahl von Objekten mit Sensoren ausgestattet, so dass diese digital adressier- und steuerbar werden.

Wichtige Anwendungsfelder von IoT sind Industrie, Logistik, (Einzel-)Handel, Umwelt, Agrarsektor, Mobilität, sowie Infrastrukturen (smart water, smart grid smart city, smart home) (vgl. Maple 2017, 160f.). Erwartet wird, dass die IoT Infrastruktur das heutige Internet nicht ersetzt, sondern dieses erweitert. Mehr noch als das Internet selbst, wird das globale Netz der Dinge in hohem Maße dezentralisiert operieren, weshalb der Interoperabilität und Skalierbarkeit der künftigen Standards, Systeme und Anwendungen eine zentrale Bedeutung zukommt (Abdmeziem, Tandjaoui, und Romdhani 2016, 57). Während im Falle des Internets die zentralen Standards TCP/IP bereits vorlagen, als der kommerzielle Erfolg des Netzes begann, liegt bei IoT die umgekehrte Reihenfolge vor: kommerzielle IoT Anwendungen erobern den Markt und überholen den seit langem stagnierenden Standardisierungsprozess. Dafür verantwortlich gemacht wird ein Mangel an internationaler Koordination (Maple 2017, 175). Es gibt derzeit mehr als 50 IoT Standardisierungsinitiativen (IEC 2016, 87).[4] Ein Grund für diesen Mangel an Koordination ist eine Wettbewerbssituation, die verspricht, die erfolgreichen Anbieter bzw. Standardisierungskonsortien in Form von de facto Standards zu prämieren. In Abwesenheit eines allseits akzeptierten Koordinationsforums fungiert Marktmacht ersatzweise als Normsetzungsinstanz.[5]

Wünschenswert, wenn nicht erforderlich für die globale Interoperabilität von IoT sind offene Standards, wie Vermesan et al. (2011, 25) betonen: "Without global recognized standards (such as, the TCP/IP protocol suite or GSM/UMTS/LTE) the expansion of RFID and M2M solutions to the Internet of Things cannot reach a global scale". Erheblicher Regelungsbedarf wird zudem in den Bereichen Datenschutz, Sicherheit bzw. Zugangskontrolle, Dateneigentum und Haftung festgestellt (IEC 2016; Maple 2017). Eine Herausforderung im Hinblick auf den Datenschutz besteht in den (aus der Diskussion um Big Data bereits bekannten) verschwimmenden Grenzen zwischen personenbezogenen und nicht personenbezogenen Daten (s.Abschnitt 5.3). Die Frage des Dateneigentums gilt heute als rechtlich ungeregelt. Zwar sind Daten als solche nicht schutzfähig, aber die Investitionen, die der Erzeugung vorausgehen, ihre Speicherung und Analyse betreffen, womöglich schon. Die Europäische Kommission hat zu diesem Thema im Frühjahr 2017 eine öffentliche Konsultation durchgeführt (Europäische Kommission 2017). Im Herbst 2017 hat die Kommission einen

[4] In einigen Initiativen engagiert sich auch die Europäische Kommission. Beispiele sind das *European Research Cluster on the Internet of Things* (IERC: www.internet-of-things-research.eu) sowie das PICASSO Project *ICT Policy, Research and Innovation for a Smart Society: towards new avenues in EU-US ICT collaboration*, das speziell die Zusammenarbeit der EU mit den USA unterstützt (www.picasso-project.eu/project).

[5] Beispiele aus der jüngeren IT-Geschichte für einflussreiche de facto Standards sind Personal Computers von IBM, das dazugehörige Betriebssystem von Microsoft sowie Android als Betriebssystem für Smartphones.

Vorschlag für einen Verordnung des Europäischen Parlaments und des Rates „über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union“ vorgelegt (COM(2017) 495 final). Die verteilte und dynamische Struktur von IoT, die die Interaktion einer hohen Anzahl von Objekten, Diensteanbietern und Datenverarbeitern erfordert, stellt auch das Haftungsrecht im Falle von Schadensfällen vor große Herausforderungen (Vermesan et al. 2011, 26).

4. Definition regulatorischer Lücken in Internet Governance

Die Literatur über Internet Governance bietet keine formale Definition zu "regulatorische Lücken". Ebenso wenig finden sich allgemeine Überblicke über Regulierungsdefizite. Offensichtliche Gründe für diese auffälligen analytischen Leerstellen liegen zunächst darin, dass Internet Governance immer noch ein Randgebiet in der juristischen und sozialwissenschaftlichen Regulierungsforschung darstellt. Angesichts der Breite des Feldes würde ein verlässlicher Überblick über Regulierungsdefizite jedoch eine größere Anzahl von Einzelstudien voraussetzen. Als weiterer Grund für diese Leerstelle kann aber auch die fundamentale Uneinigkeit über Regulierungserfordernisse im Bereich Internet Governance gelten. Vor allem staatliche Formen der Regulierung des Internet sind Gegenstand politischer und hochgradig ideologischer Auseinandersetzungen sowohl zwischen Regierungen als auch Teilen der Zivilgesellschaft. Bereits in den späten 1990er Jahren ließen sich Konflikte über die Notwendigkeit, Formen und Grenzen einer Regulierung der Netzinfrastruktur beobachten. Einige der wenigen, von Seiten der internationalen Forschung und der Zivilgesellschaft allgemein akzeptierten staatlichen Eingriffe betrifft die Sicherstellung der sog. "Netzneutralität". Gerade in diesem Bereich aber können sich nur wenige Regierungen zu strikten Regulierungsmaßnahmen durchringen (Belli 2017; Marsden 2017).

Bezogen auf regulatorische Lücken kann im Bereich der inter- und transnationalen Regulierung grob zwischen dem Fehlen von Regeln, Kompetenzen (Zuständigkeiten, Expertise), Standards oder Verfahren einerseits und Schwächen in der Durchsetzung bzw. dem Vollzug andererseits unterschieden werden.[6]

Auffällig im Unterschied zu anderen internationalen Kommunikationsinfrastrukturen wie Post und Telekommunikation ist der Umstand, dass die Verwaltung der Infrastruktur des Internets ganz überwiegend durch nicht-staatliche Organisationen erbracht wird. Diese betrifft auch die CIR. Internationale Organisationen und Regierungen wirken eher indirekt in das Regelungsfeld hinein. Beispiele dafür sind die Beteiligung in Organisationen wie dem IGF oder ICANN sowie die Anwendbarkeit internationaler Abkommen auf die Netzinfrastruktur sowie den Datenverkehr. Beispiele für den Einfluss internationaler Abkommen auf die

[6] Eine Studie über das internationale Regime für die Artenvielfalt der Meere (IUCN 2008) unterscheidet zwischen "regulatory gaps" und "governance gaps“. Regulatorische Lücken beziehen sich auf das Fehlen substantieller Regeln im rechtlichen Rahmenwerk während governance gaps inkonsistente Mandate sowie das Fehlen von Institutionen oder Mechanismen bezeichnen.

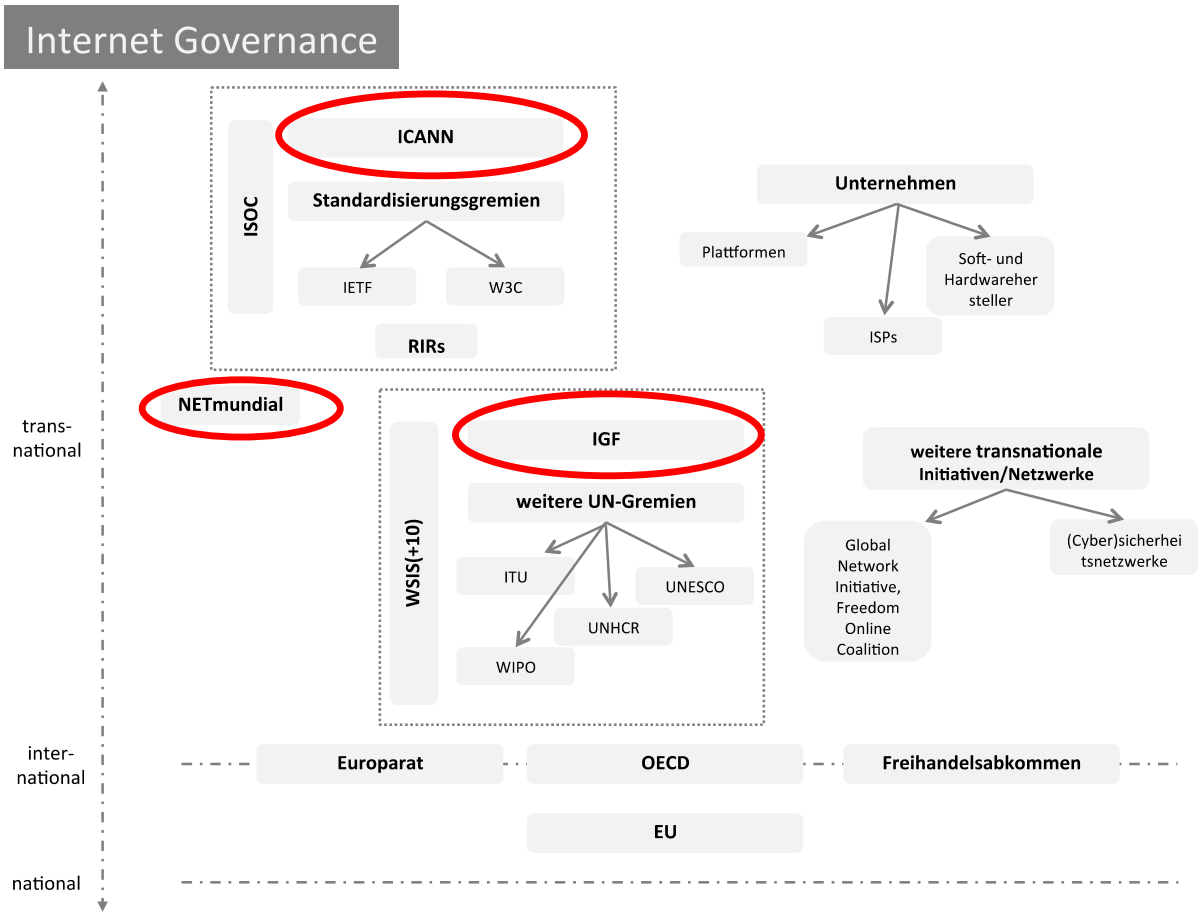

Abb. 2: Internet Governance. Quelle: Eigene Darstellung.

Datenflüsse des Internet sind die Regeln des Urheberrechts, die zumeist in automatisierter Form die Verbreitung von Inhalten reglementieren, aber auch das "Privacy Shield"-Abkommen, das den Datentransfer zwischen der EU und den USA regelt sowie die neu geschaffene EU Datenschutz-Grundverordnung (EU-DSGVO). Auf den Kernbereich der Netzinfrastruktur haben Regierungen nach der vollständigen Privatisierung von ICANN (s.Abschnitt 8) nur mehr als primus inter pares Einfluss.

Wie bereits eingangs festgestellt wurde, folgt die Organisationsstruktur von Internet Governance keiner umfassenden Systematik. Die ersten institutionalisierten Regelungskompetenzen entstanden im Bereich der technischen Normierung und der Zuteilung der hierdurch geschaffenen Ressourcen, darunter Internetadressen und Domainnamen, etc.: die Internet Engineering Task Force (IETF)[7] und ICANN. "If it ain't broke, don't fix it", gilt bis heute als das die institutionelle Entwicklung von Internet Governance bestimmende Prinzip. Die Sorge vor der Entstehung innovations- und wettbewerbsbehindernder regulatorischer Autorität ist zumindest im globalen Norden größer als das Interesse an einheitlichen internationalen Regeln.

[7] Die IETF ist das informelle, nicht-inkorporierte Äquivalent zu UN Organisationen wie der International Telecommunication Union (ITU).

5. Regulatorische Lücken in der Internetregulierung auf nationaler, supranationaler und internationaler Ebene?

Die überwiegend privat organisierte Erbringung von Verwaltung und Dienstleistungen im Bereich der Infrastruktur, des Netzzugangs und der Kommunikationsdienste erzeugt stellenweise suboptimale Prozesse und Ergebnisse. Dafür werden im Folgenden drei Beispiele angeführt: Die Einführung eines neuen Adressierungsstandards (5.1), die Schaffung von Internetkonnektivität (5.2) und die Sicherheitsrisiken von IoT (5.3).

5.1 Übergang vom Adressierungsstandard IPv4 zu IPv6

Bereits in den 1990er Jahren zeichnete sich ab, dass die Kapazität des IPv4-basierten Adressierungssystems in den kommenden Jahren erschöpft sein würde. Deshalb entwickelte die IETF den Nachfolgestandard IPv6. Seine Grundstruktur ist seit 1998 definiert; in den nachfolgenden Jahren wurde er zur Anwendungsreife gebracht. Die in die Entwicklung von IPv6 involvierten Mitglieder der IETF konzentrierten sich auf die Eigenschaften des Adressierungssystems. Dem Übergang von IPv4 zu IPv6 hielten sie für einen unproblematischen Vorgang, für den der Markt sorgen würde.

Im Unterschied zum Telefonnummernsystem, dessen Nummernblöcke der nationalstaatlichen Souveränität unterliegen, gilt der Adressraum des Internets als global verwaltetes *Allmendegut* („common pool resource“). Seit den frühen 1990er Jahren obliegt diese Aufgabe weltweit fünf nicht-kommerziellen *Regional Internet Registries* (RIRs). Die Hauptaufgabe der RIRS besteht in der Verwaltung von Internetadressen und in der Festlegung von Regeln für ihre Zuteilung an die *Internet Service Provider* (ISPs), die wiederum die wichtigsten Kunden der RIRs sind. Das Modell der Selbstregulierung im Bereich der Vergabe von Internetadressen stieß an seine Grenzen, als der Pool der IPv4 Adressen zur Neige ging und die Nachfrage nach IPv6 ausblieb. Die ISPs zögern den Übergang zu IPv6 bis heute hinaus, weil die Umstellung aus ihrer Sicht Kosten verursacht, denen keine Nachfrage und höhere Zahlungsbereitschaft auf Seiten der Endkunden gegenübersteht (Mueller, Kuerbis, und Asghari 2013; Jeanette Hofmann 2010). Obwohl der IPv4 Adresspool seit 2015 als erschöpft gilt, ist die Umstellung auf IPv6 bis heute nur partiell erfolgt.[8]

Die Umstellung auf den neuen Adressierungsstandard ist ein Beispiel für die nahezu unüberwindlichen Hürden, mit denen wünschenswerte "Updates" der globalen Infrastruktur konfrontiert sind. Obwohl die Netzinfrastruktur eigentlich ein "periodic updating of its core operations" erfordere, wie die Informatikerin Leslie Daigle (2015, 29) feststellt, zeige sich, dass "changes to the underlying transmission layer of the Internet are all but impossible". Die Gründe dafür, dass Updates der Netzinfrastruktur nicht möglich sind, liegen in der dezentralen Struktur seiner Verwaltung sowie der verteilten Architektur eines Netzes der Netze: Ohne eine alle Netze umfassende Koordinationsinstanz, die Updates hierarchisch anordnen und durchsetzen kann, führen Maßnahmen wie die Umstellung auf ein neues

[8] Für aktuelle Zahlen zur Diffusion von IPv6 in Deutschland siehe: http://ipv6-test.com/stats/country/DE (zuletzt abgerufen am 19.12.2017).

Adressierungssystem bestenfalls zu Parallelwelten (IPv4 und IPv6 werden gleichzeitig verwendet) und schlimmstenfalls zu einer Fragmentierung des Netzes.

Am Beispiel der schleppenden Umstellung auf IPv6 zeigen sich die Grenzen des Selbstregulierungsmodells ohne hierarchische Handlungsautorität im Bereich Internet Governance: Das hohe Gut der globalen Konnektivität wird zwar von allen relevanten Akteuren sehr geschätzt, aber wenn die Handlungskalküle individueller Netzbetreiber mit den Erfolgsbedingungen globaler Konnektivität nicht übereinstimmen, leidet letztere. Im Rahmen der bestehenden Struktur von Internet Governance lassen sich nur solche technischen Maßnahmen durchsetzen, die dezentral erfolgen können, ohne die Interoperabilität des Netzes der Netze zu gefährden. Die Alternative zu dem bestehenden Modell der freiwilligen Koordination liegt nicht auf der Hand. Für eine globale Regulierungsinstanz etwa unter dem Dach der International Telecommunication Union (ITU) fehlt aus vielen Gründen die politische Unterstützung. Der Gewinn an Koordination würde mit einem gravierenden Verlust an Legitimation und Durchsetzungschancen erkauft. Kurz gesagt: Es gibt keine Organisationsstruktur, die das globale Gut der Interkonnektivität verlässlich an erste Stelle setzen würde, ohne sich dem Verdacht auszusetzen, die hierfür erforderliche Autorität für andere politische Zwecke zu missbrauchen.

5.2 Interkonnektivität (Peering)

Das Internet bildet einen Zusammenschluss von autonomen Netzen. Die lokalen Netze sind untereinander durch Verbindungsarrangements oder sog. "peering agreements" verbunden. Diese Verbindungsarrangements legen fest, unter welchen Bedingungen kooperierende Netze den Datenverkehrt für die Kunden der jeweils anderen Netze weiterleiten. Generell wird zwischen zwei Typen von Vereinbarungen unterschieden: Im Rahmen von Peering-Vereinbarungen leiten zwei in etwa gleichgroße Netze die Datenströme des Partners entgeltfrei weiter; Transit-Vereinbarungen werden zwischen unterschiedlich großen Netzen geschlossen, wobei der kleinere Partner für den Transit seiner Daten Zahlungen leistet (s. Abb. 3).

Obwohl Verbindungsarrangements eine essentielle Bedingung für das Bestehen des Internets darstellen, erfolgen sie ganz überwiegend informell, intransparent und außerhalb regulatorischer Aufsicht: "There is no central feature of the internet that has been subject to as little formal regulation as internet interconnection." (Meier-Hahn 2016, 1). Studien aus den Jahren 2011 und 2016 (Woodcock und Frigino 2016) kommen zu dem Schluss, dass nahezu alle Peering-Vereinbarungen auf sogenannten "handshake agreements" beruhen. Förmliche Vertragsbeziehungen sind dagegen eher die Ausnahme. Die Kontinuität der informellen Verbindungsarrangements beruht auf der weiten Verbreitung und allgemeinen Anerkennung von grundlegenden Normen und "best practices" unter den Akteuren, die für Herstellung der Interkonnektivität zuständig sind (Meier-Hahn 2016).

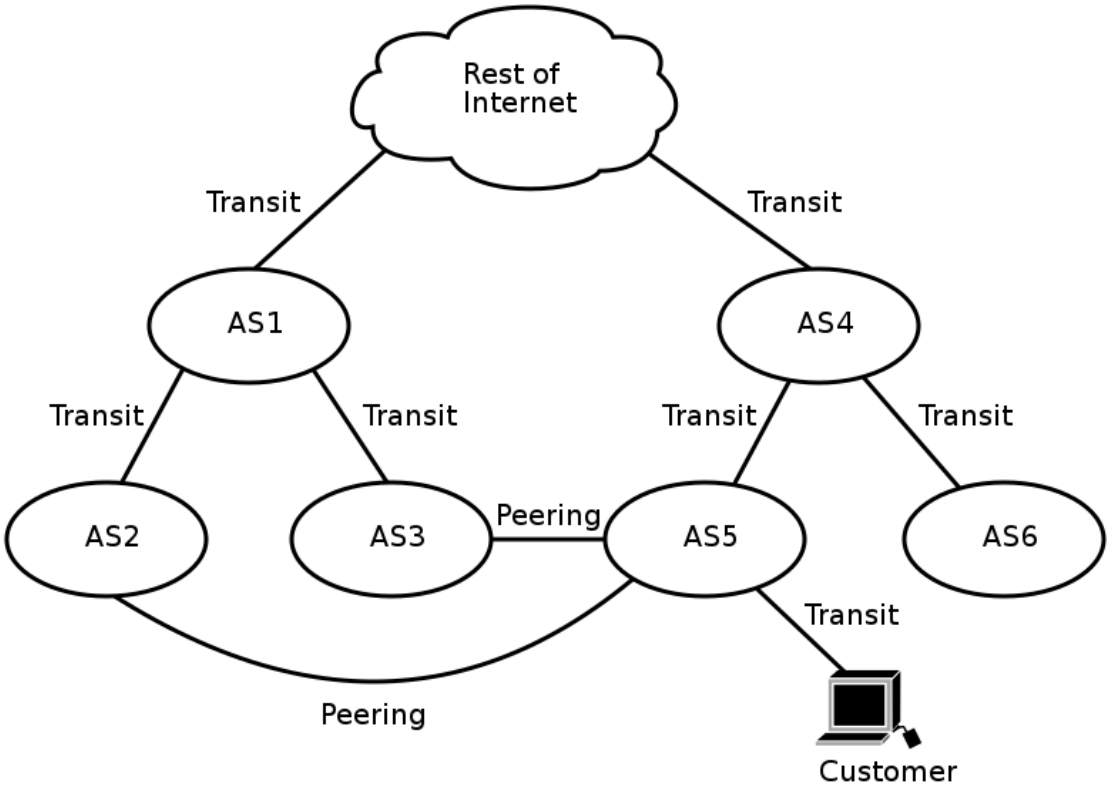

Abb. 3: Schema interkonnektierender autonomer Systeme. Quelle: (Wikimedia Commons 2017).

Allerdings hat sich der Markt für Interkonnektivität mit dem Aufkommen von breitbandintensiven Videoangeboten, die derzeit rund 70% des gesamten Datenverkehrs ausmachen (Cisco 2017, 10), verändert. Viele Content-Anbieter betreiben inzwischen ihre eigenen Auslieferungsnetze, um den Videostream möglichst störungsfrei bis zu den Kunden zu transportieren. Die Entstehung der Content Delivery Networks hat die Akteurskonstellation im Bereich der Interkonnektivität erweitert: Neben "Transit" und "Peering" etabliert sich ein neuer Markt zwischen ISPs und Content-Lieferanten, auf den die etablierten Normen für die Herstellung von Interkonnektivität nicht ohne weiteres anwendbar sind (Scott et al.2015, 81f.). Die veränderte Marktkonstellation birgt die Gefahr, dass auf Konsumenten spezialisierte große ISPs ihre Kontrolle über die letzte Meile dazu nutzen, um eine Art Wegzoll von den Content-Anbietern zu verlangen. Knappe bzw. verknappte Bandbreiten können dazu genutzt werden, Aufpreise für eine störungsfreie Durchleitung bandbreitenintensiver Dienste zum Endkunden zu verlangen: "If the prices for interconnection are unregulated, not transparent, and not related to the actual costs of carrying traffic, the incentive to gouge other service providers will be clear and lucrative. These kinds of policies could easily take on the political purpose of economic protectionism or content censorship" (Scott et al. 2015, 82). Die schrumpfenden Gewinnmargen für den Betrieb von Datennetzen könnten durch steigende Preise für den Datentransit kompensiert werden. Diese Entwicklung reduziert zugleich die ökonomischen Anreize für einen weiteren Ausbau der Netze.[9]

[9] Für einen Vergleich des Anteils von Glasfaseranschlüssen innerhalb der OECD siehe: de.statista.com/statistik/daten/studie/415799/umfrage/anteil-von-glasfaseranschluessen-an-allen-Breitbandanschluessen-in-oecd-staaten/ (zuletzt abgerufen am 18.12.2017).

Vor diesem Hintergrund hat sich die US amerikanische Regulierungsbehörde FCC im Rahmen ihrer Netzneutralitätsregulierung im Jahr 2015 das Recht eingeräumt, den Markt für Interkonnektivität zu regulieren, um auf einen potentiellen Missbrauch von Marktmacht zulasten der Konsumenten reagieren zu können (FCC 2015). [10] Die EU-Verordnung 2015/2120 über "Maßnahmen zum Zugang zum offenen Internet" verzichtet auf die Schaffung einer vergleichbaren Regulierungskompetenz. Der Art. 19 führt jedoch Berichtspflichten ein, die auch die Wettbewerbseffekte der Verbindungsarrangements umfassen. Die französische Regulierungsbehörde ARCEP geht einen Schritt darüber hinaus, indem sie den ISPs Informationspflichten über ihre Interkonnektivität- und Routingpraktiken auferlegt. Auf diese Weise wird die viel beklagte Intransparenz des Marktes für Interkonnektivität verringert (ARCEP 2017, 13; vgl. BEREC 2017, 14).

Die Internetwirtschaft steht regulatorischen Eingriffen in den Markt für Interkonnektivität überwiegend skeptisch gegenüber. Eine OECD Studie kommt zu dem Schluss, dass der Markt für Interkonnektivität bislang überwiegend bislang gut funktioniert und sehr innovativ ist (Dennis Weller und Bill Woodcock 2014).[11] Der Missbrauch lokaler Marktmacht durch große Provider ("incumbents") in Form von überhöhten Preisen für Transit oder der Verweigerung von Peering-Vereinbarungen, wird in der Branche als Ausnahme wahrgenommen.[12] Aus Sicht von Peering-Experten wie Bill Woodcock könnten geeignete Maßnahmen darin bestehen, eine größere Transparenz über die Interkonnektivitäts-Arrangements zwischen den ISPs herzustellen oder auch, verbindliche Regeln für die Interkonnektivität zu entwickeln.

5.3 IoT Sicherheitsrisiken

Das Internet der Dinge verspricht, in den kommenden Jahren eine schnell wachsende Anzahl von Objekten mit digitalen Schnittstellen auszustatten, so dass diese miteinander interagieren und über beliebige räumliche Distanzen gesteuert werden können. Dafür erforderlich ist das Zusammenspiel einer nahezu unüberschaubaren Vielfalt von Systemkomponenten, Diensten, Daten, Herstellern und Anwendungsbereichen in der Produktion, im Verkehrs- und Gesundheitsbereich wie auch in der eigenen Wohnung. Die Ausdehnung der technischen Kontrolle auf eine Vielzahl von Objekten schafft allerdings auch neue Formen von Verwundbarkeiten oder Gefährdungen, die sich faktisch auf alle Dimensionen des gesellschaftlichen Lebens erstrecken: "IoT compounds every security problem of the Internet.

[10] "While we have more than a decade's worth of experience with last-mile practices, we lack a similar depth of background in the Internet traffic exchange context. Thus, we find that the best approach is to watch, learn, and act as required, but not intervene now, especially not with prescriptive rules. This Order—for the first time—provides authority to consider claims involving interconnection, a process that is sure to bring greater understanding to the Commission" (FCC 2015). Die FCC hat diese Regelung im Dezember 2017 aufgehoben.

[11] Beispiele für Innovationen stellen die Entstehung von spezialisierten Content Delivery Networks (CDN) dar, die zeitkritische Inhalte von den Anbietern bis zur letzten Meile an ihre Kunden ausliefern sowie lokale Austauschpunkte für den Datenverkehr, die von ISPS unterhalten werden, um die Datenströme zwischen ihren Netzen möglichst kostengünstig weiterzuleiten. S. https://de.wikipedia.org/wiki/Internet-Knoten (zuletzt abgerufen am 12.12.2017).

[12] S. Zusammenfassung des IGF 2015 Workshops "Internet interconnection under regulatory pressure" unter: https://www.intgovforum.org/cms/wks2015/index.php/proposal/view_public/214 (zuletzt abgerufen am 12.12.2017).

Your toaster could be sending out spam" (ISOC 2017, 47). Angriffe auf unzureichend gesicherte Objekte und Netzwerke können hohe Schäden auch für Dritte erzeugen.

Die Literatur zur IoT betont, dass die digitale Vernetzung von Objekten neue Typen von Ausfall- und Angriffsrisiken hervorbringt. Vor allem Industrieanlagen und kritische Infrastrukturen, darunter Krankenhäuser, Transportsysteme oder die Energieproduktion, erweisen sich als anfällig für Angriffe, wie viele Beispiele aus den vergangenen Jahren zeigen (Simon 2017, 101). Auch Konsumgüter sind vielfach unzureichend gesichert. So belegten Tests in den vergangenen Jahren, dass sich vernetzten Geräte – von den Bremsen des PKWs über das Heizsystem bis hin zur Toilettenspülung – durch Unbefugte von außen kontrollieren ließen (Beuth 2013; vgl. Bugeja et al. 2016). Da für viele Konsumgüter im IoT Bereich keine Updates vorgesehen sind, können sich solche Befunde allenfalls auf künftige Gerätegenerationen auswirken. Ungenügend gesicherte Geräte lassen sich wiederum für global operierende "Bot-Netze" nutzen, die die Kontrolle über digitale Konsumgütergeräte übernehmen, um diese für Angriffe auf digitale Infrastrukturen zu nutzen (vgl. ISOC 2017, 46). Die Reichweite der Schäden, die Schwachstellen einzelner Geräte verursachen können, reicht somit weit über die eigentlichen Anwender hinaus: "A lack of agreement on IoT Security frameworks and best practices may jeopardise the safety of individuals around the globe" (ISOC 2017, 46).

Aus ökonomischer Sicht signalisiert die unzureichende Sicherung von IoT Systemen im Konsumgüterbereich ein Marktversagen. Die Hersteller von Heimgeräten sparen an Komponenten, die aus Wettbewerbssicht nicht essentiell erscheinen. Die Schäden, die die Sicherheitsrisiken ihrer Produkte potentiell erzeugen, stellen "Externalitäten" dar, die – typischerweise vertraglich abgesichert – von den Kunden und nicht den Hersteller getragen werden. Den Nachfragen wiederum fehlt die Kompetenz, um die Qualität der Sicherheitsvorrichtungen ihrer Geräte und Dienste sachgerecht beurteilen zu können (ISOC 2017, 18.).

Erschwert wird die Entwicklung von verbindlichen Qualitäts- und Sicherheitsstandards durch die wachsende Vielfalt und Komplexität, aber auch den schnellen Wandel und die Internationalität der Märkte von IoT Produkten (Maple 2017). Die Internet Society (2017) kommt zu dem Schluss, dass eine Verbesserung der Sicherheit von IoT basierten Produkten nur durch das Zusammenwirken vieler Akteure erreicht werden kann. So könnten beispielsweise Versicherungen den Versicherungsschutz von IoT Produkten an die Existenz von Sicherheitszertifikaten knüpfen. Fraglich ist jedoch, ob marktwirtschaftliche Lösungen die erforderliche Flächendeckung erreichen können oder ob in diesem Fall nicht eine international koordinierte Zusammenarbeit zwischen Regierungen, IT-Wirtschaft und Sicherheitsforschung empfehlenswert ist.

Die aufgezeigten Regulierungslücken demonstrieren exemplarisch, dass die Herstellung und Aufrechterhaltung der Netzinfrastruktur eine zunehmend anspruchsvolle Aufgabe darstellt, die aufgrund der überwiegend polyzentralen Architektur des Netzes große Koordinationsprobleme aufwirft. So verspricht IoT, das Internet in vielen Dimensionen zu

erweitern und damit zugleich die Anfälligkeit seiner Dienste erheblich zu vergrößern. Ein wahrscheinliches Szenario läuft auf eine wachsende Abschottung und Überwachung lokaler und funktional spezialisierter Netze heraus, die dann wiederum neue Risiken der Fragmentierung der Netzinfrastruktur nach sich ziehen.

6. Regulierung von Global Playern der Internetwirtschaft[13]

Mit der Entstehung von Suchmaschinen und sozialen Netzwerken ist ein neuer Typ von Intermediären entstanden, der sich durch seine "Vermittlungsleistung zwischen Inhalten oder Inhaltsangeboten und Nutzerinnen und Nutzern" (Schulz und Dankert 2016, 15) auszeichnet. Das Kennzeichen von Informationsintermediären besteht folglich darin, dass diese in aller Regel keine eigenen Inhalte produzieren, sondern diese auf verschiedene Weise "kuratieren", d.h. bezogen auf spezifische Nutzergruppen selektieren und aggregieren. Einen systematischen Überblick über die Regulierungsfragen, die sich im Kontext der deutschen Rechtsordnung stellen, haben Schulz und Dankert (2016, 31) vorgelegt (s. Abb. 4). Die Abbildung dient als Orientierungsrahmen für die Verortung der Problembereiche, die im Folgenden knapp skizziert und im Hinblick auf mögliche Regulierungsbedarfe betrachtet werden: 6.1 Daten als Währung (D2), 6.2 Regulierung von Inhalten (B, D1, E, F), 6.3 Monopolstellung von Intermediären (A).

[13] "Global Players" erscheint als Begriff zu umfassend und ungenau für eine Darstellung von Regulierungsherausforderungen. Ich werde mich daher auf ausgewählte Probleme in Bezug auf soziale Netzwerke bzw. Plattformen (hier als neuer Typ von "Intermediären" gefasst) beschränken.

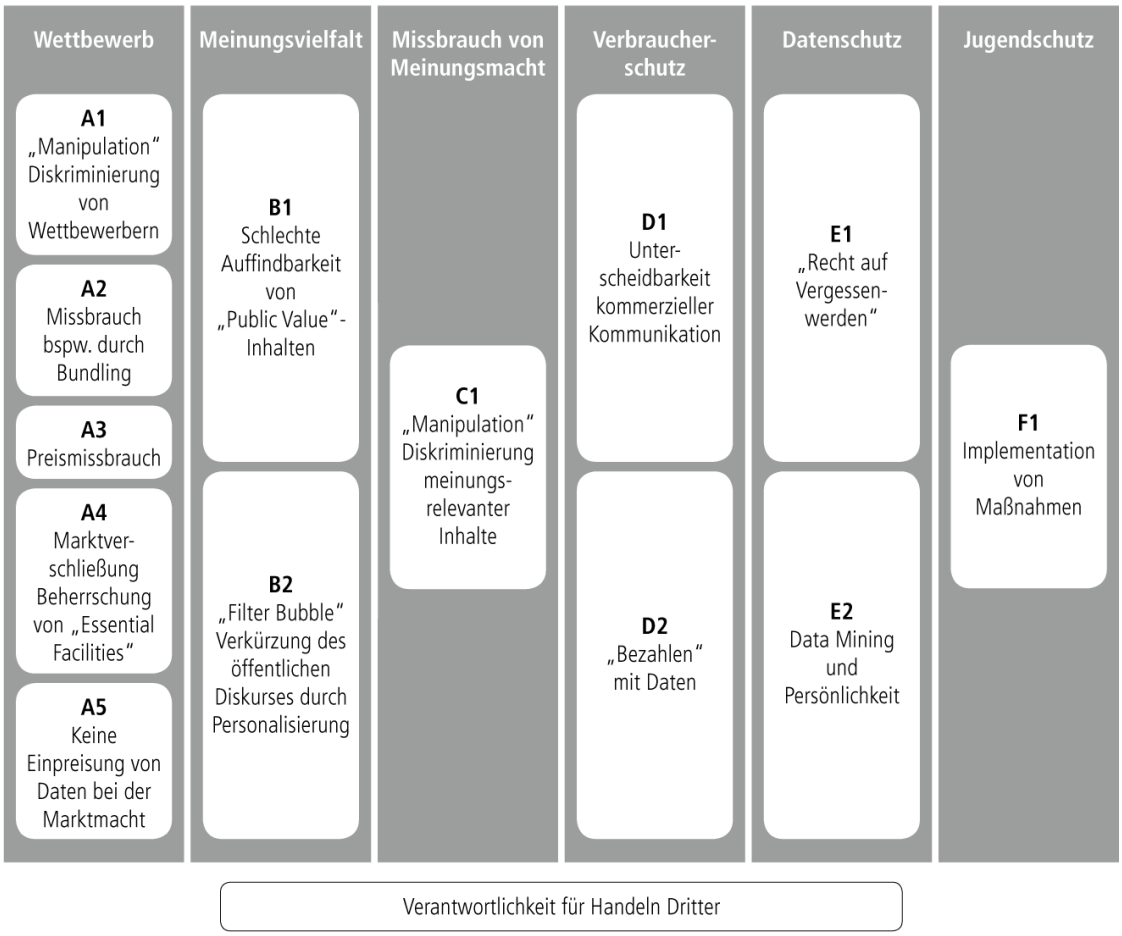

Abb. 4: Problembereiche bei der Regulierung von Informationsintermediären. Quelle: (Schulz und Dankert 2016, 29).

6.1 Daten als Währung

Die Nutzung der meisten kommerziellen digitalen Dienste, wie etwa Suchmaschinen, soziale Netzwerke oder Apps für das Smartphone, erfolgt heute im Tausch gegen die Einräumung von Verwertungsrechten personenbezogener Daten. Dabei handelt es sich in der Regel nicht nur um die eigenen Daten, sondern auch die (Kontakt-)Daten dritter, die sich im persönlichen Adressbuch oder der eigenen Fotogalerie befinden. Das auf "Daten als Währung" beruhende Geschäftsmodell verzeichnet auf der einen Seite beispiellose Integrationseffekte: Die persönlichen Daten der Nutzer gelten bislang als unterschiedslos wertvoll, so dass alle Bürger unbegrenzt von den Vorteilen digitaler Kommunikationsdienste profitieren können und keine Personengruppen systematisch ausgeschlossen werden. Auf der anderen Seite führt dieses Geschäftsmodell zu einer langfristigen und substantiellen Aushöhlung der Privatsphäre, deren Folgen für den Einzelnen, wie auch die Gesellschaft insgesamt, heute noch nicht hinreichend abschätzbar sind.

Seit mehreren Jahren mehren sich unter Datenschutzexperten die kritischen Stimmen, die behaupten, dass das heutige Datenschutzrecht seinen eigenen Zielsetzungen nur noch bedingt gerecht wird und daher einer grundlegenden Neukonzeption bedarf (Manske und Knobloch 2017). Zwei besonders kritische Aspekte im Kontext von Daten als Währung sollen

herausgegriffen werden: personenbezogene Daten als zentraler Schutzgegenstand sowie die "informierte Einwilligung" als zunehmend wichtiges Instrument des Datenschutzes.

Das Datenschutzrecht bezieht sich traditionell auf personenbezogene Daten; das gilt auch für die nächstes Jahr inkrafttretende EU-DSGVO. Aufgrund der voranschreitenenden Digitalisierung und den in der Folge entstehenden, großen Datenmengen, wie auch der steigenden Analysekapazitäten, wird es immer leichter, einzelne Personen durch die Kombination von nichtpersonenbezogenen Daten zu identifizieren. Hinzukommt, dass sich personen- und gruppenrelevante Bewertungen oder Entscheidungen auch durch die Analyse aggregierter Daten vornehmen lassen (Pohle 2016). Aufgrund seines Fokus auf personenbezogene Daten erfasst das Datenschutzrecht neue Analyseverfahren wie "predictive analytics", die große unspezifische Datensätze auswerten, um Wahrscheinlichkeitsaussagen über künftiges individuelles Verhalten zu treffen, nur unzureichend. Obwohl die Privatsphäre und Entfaltungsfreiheit der Bürger durch Phänomene wie Big Data, neue Techniken der Datenauswertung und Automatisierung, etwa im Bereich des maschinellen Lernens, unmittelbar betroffen sind, schützt sie das neue Datenschutzrecht nur sehr eingeschränkt. Die Ausbreitung von IoT wird die zunehmende Vermischung von personen- und nichtpersonenbezogenen Daten voraussichtlich noch steigern.

Das Datenschutzinstrument der "informierten Einwilligung" zielt darauf, den Bürgern Wahlfreiheit gegenüber Anbietern und Diensten zu ermöglichen. Auf der Grundlage der Informationen, die der Anbieter bereitstellt, sollen die Bürger informierte Entscheidungen über die Nutzung von Kommunikationsdiensten treffen. Sofern digitale Kommunikationsdienste wie Suchmaschinen oder Plattformen infrastrukturellen Charakter annehmen, deren Nutzung ein Bestandteil der gesellschaftlichen Teilhabe geworden ist und die Einwilligung die notwendige Voraussetzung für die Nutzung des betreffenden Dienstes bildet, kann von Wahlfreiheit jedoch nur noch eingeschränkt gesprochen werden (vgl. Buchner 2016; Jeanette Hofmann und Bergemann 2016). Faktisch schreibt die "informierte Einwilligung" dem Einzelnen zwar die Verantwortung für die Folgen seines Handelns zu, ohne diesen aber tatsächlich Wahlfreiheit zu ermöglichen. Die 2018 in krafttretende europäische Datenschutzgrundverordnung hält an der informierten Einwilligung trotz dieser bekannten Problematik fest und wertet sie sogar noch auf.

Zu fragen ist, ob der Datenschutz auch weiterhin die Handlungsfreiheit des Einzelnen ins Zentrum seines Instrumentariums stellen soll (vgl. Matzneret al. 2016; van der Sloot 2014) oder ob es angesichts der infrastrukturellen Qualität vieler neuer Technologien nicht sinnvoller wäre, bereichs- oder anwendungsspezifische Lösungen zu wählen. Wenn es künftig immer schwerer möglich ist, digitale Technologien nicht zu nutzen, dann erweist sich das Konzept der informierten Einwilligung als überholt. Mit der Einführung von "Datenschutz durch Technikgestaltung" und "datenschutzfreundlichen Voreinstellungen" (Art. 25 EU-DSGVO) sowie dem Anspruch auf Datenportabilität (Art. 20 EU-DSGVO) entstehen jedoch neue Möglichkeiten zur Ausgestaltung des Datenschutzes, die die individuelle Verantwortung der Bürger gerade in Handlungsbereichen, in denen ihre Wahlfreiheit stark begrenzt ist, partiell auf technische Lösungen verlagern könnte. Hilfreich wäre zudem eine stärkere

Verknüpfung von Daten- und Verbraucherschutz. Ein Beispiel für eine solche Verknüpfung wäre die systematische Überprüfung der Wirksamkeit von Allgemeinen Geschäftsbedingungen, die Bürger als Voraussetzung für die Nutzung von digitalen Kommunikationsdiensten akzeptieren, mit dem Ziel, die Bürger beim Verwalten der Berechtigungen einzelner Apps durch allgemeine Richtlinien zu unterstützen. Besonders der Zugriff auf die Daten Dritter, die ihre Einwilligung nicht gegeben haben, sollte geprüft und ggf. beschränkt werden.

6.2. Regulierung von Inhalten

Das Markenzeichen sozialer Netzwerke besteht in der Kuratierung nutzergenerierter Inhalte. Inzwischen nutzen jedoch auch professionelle Medien Informationsintermediäre, wie etwa Facebook, Twitter oder YouTube, für die Verbreitung ihrer journalistischen Inhalte, weil sich die sozialen Netzwerke zu wichtigen transnationalen Infrastrukturen für die gesellschaftliche Meinungsäußerung entwickelt haben (Napoli 2015). Mit dem Aufstieg der neuen Medien steigt auch der meinungsbildende Einfluss der Algorithmen, die etwa bei Facebook derzeit rund 500.000 Kommentare pro Minute kategorisieren, filtern und hierarchisieren. Dies geschieht nach Regeln, die nicht offengelegt werden, aber faktisch über die Sichtbarkeit im Kommunikationsfluss entscheiden (Jeanette Hofmann 2017). Im Rahmen des amerikanischen Wahlkampfs 2016 wurde deutlich, dass Facebook primär diejenigen Beiträge privilegiert, die die größten Aussichten auf eine Weiterverbreitung unter den Nutzern haben. Die Entkopplung von Qualität und Popularität politischer Nachrichten in algorithmisch kuratierten Öffentlichkeiten gilt als Erklärung dafür, warum Falschmeldungen eine so große Verbreitung in den sozialen Netzwerken genießen.

Im Unterschied zu Tageszeitungen, Rundfunk- und Fernsehsendern, die sich ebenfalls über Werbung finanzieren, steht im Internet die personenbezogene Ansprache im Vordergrund. "Persönliche Öffentlichkeiten" (Schmidt 2011) zeichnen sich dadurch aus, dass Informationen nicht nach ihrem journalistischen Nachrichtenwert sortiert werden, sondern nach ihrer errechneten individuellen Relevanz. Eine Folge individualisierter Nachrichtenströme ist die Bildung sogenannter Filterblasen, die überproportional häufig Nachrichten und Kommentare enthalten, die unsere politischen Orientierungen und Weltbilder bestätigen. Für die Nutzer sozialer Netzwerke ist die Logik und Wirkungsweise algorithmischer Kuratierung intransparent und nicht nachvollziehbar. Der Einsatz von Algorithmen zur Hierarchisierung und Sortierung von Inhalten wird daher als Gefahr für die öffentliche Meinungsbildung betrachtet (Just und Latzer 2016).

Die wachsende Meinungsmacht von Informationsintermediären im Kontext von Wahlen und nationalen Referenden sowie die empirisch begründete Sorge vor Versuchen einer systematischen Manipulation der öffentlichen Meinungsbildung haben den Ruf nach der Regulierung sozialer Netzwerke bzw. ihrer Einordnung in das bestehende System der Medienregulierung geweckt. Gegenstand der Kritik ist unter anderem die asymmetrische Regulierung von traditionellen Massenmedien und Informationsintermediären, weil letztere

keiner Regulierung unterliegen (Schulz und Dankert 2016; Napoli 2015).[14] Um die freie Meinungsbildung zu sichern, wird verschiedentlich auch die Offenlegung oder Zertifizierung von Algorithmen bzw. ihrer Sortierungskriterien gefordert (zur technischen Machbarkeit vgl. Kitchin 2017).

Informationsintermediäre, deren Geschäftsmodell in Vermittlungsleistungen und der Verwertung personenbezogener Daten besteht, stellen einen kategorial neuen Organisationstyp dar, der sich mit herkömmlichen Organisationsmodellen im Medienbereich bloß funktional überlappt. Entsprechend können nutzergenerierte Inhalte nicht analog zur journalistischen Nachrichtenproduktion reguliert werden, sofern letztere eine öffentliche Aufgabe erfüllt und darin Anforderungen wie der sachlichen Berichterstattung und Quellenprüfung unterliegt. Der öffentliche Austausch zwischen individuellen Nutzern im Internet genießt dagegen Grundrechtsschutz, von dem lediglich Beleidigungen, Verleumdungen u. ä. strafrechtlich relevante Handlungen ausgenommen sind. Wenn Informationsintermediäre folglich nicht umstandslos in das bestehende System der Medienregulierung eingeordnet werden können, wirft ihre wachsende Meinungsmacht doch die Frage auf, ob es eines spezifischen Regulierungsrahmens bedarf. Damit zusammenhängend wird auch die Frage diskutiert, ob Plattformbetreiber für die Äußerungen ihrer Mitglieder verantwortlich gemacht werden können und sollen.

Viele Experten argumentieren dafür, von spezifischen Regulierungsmaßnahmen für Informationsintermediäre abzusehen und stattdessen Regelungen im Rahmen der in Deutschland institutionalisierten regulierten Selbstregulierung zu entwickeln.[15] Die Kuratierung von Inhalten durch soziale Netzwerke an sich, so Schulz und Dankert (2016, 41), wirft keinen staatlichen Handlungsbedarf auf, denn "dass ein Informationsintermediär in Bezug auf die Selektion oder Sortierung eines Inhaltsanbieters Unterschiede macht, konstituiert noch keinen Missbrauch seiner Stellung im Kommunikationsprozess, vielmehr kann darin gerade seine Leistung liegen". Der Bias in der Informationsaufbereitung ist kein Spezifikum der sozialen Netzwerke, er kennzeichnet vielmehr jedes Informationsmedium. Hinzukommt, dass objektive Kriterien für einen "Missbrauch kommunikativer Macht durch Intermediäre" bislang nicht definiert worden sind: "Ebenso wie bei Tendenzbetrieben kann die 'Neutralität' von Informationsintermediären nicht der Maßstab für ihre Regulierung sein" (Schulz und Dankert 2016, 9).

Das 2017 verabschiedete *Netzwerkdurchsetzungsgesetz* (NetzDG) weicht von dieser Auffassung ab und geht gegen "Hassrede", "Hasskriminalität" und "fake news" vor, indem Informationsintermediäre dazu verpflichtet werden, rechtswidrige Inhalte innerhalb bestimmter Fristen zu entfernen und dafür zu sorgen, dass sie nicht erneut verbreitet werden. Das NetzDG hat von vielen Seiten Kritik auf sich gezogen. Ein grundlegender Kritikpunkt betrifft die Ausrichtung auf den technischen Zugang zu rechtswidrigen Inhalten anstatt auf

[14] Die Betreiber sozialer Netzwerke wie Facebook haben lange argumentiert, dass sie keine Medienanbieter, sondern Technologieunternehmen sind, weil sie Informationen nicht selbst produzieren, sondern lediglich zugänglich machen (vgl. Pasquale 2016; Rentz 2016).

[15] Schulz und Dankert ziehen etwa Monitoringverfahren (2016, 76) sowie eine Deklarationspflicht des Selbstverständnisses von Informationsintermediären in Betracht, die "auch gesetzlich vorgeprägte Bestandteile enthalten könnte" (2016, 74).

ihre Urheber: "Instead of punishing bad behavior, we strive to control the tool that was used by the bad actor(s)" (Mueller 2015, 807; vgl. Schulz und Dankert 2016; Breindl 2013). Eine weitere grundsätzliche Kritik bezieht sich auf die Verlagerung der Rechtsdurchsetzung hin zu privatwirtschaftlichen Intermediären, die aufgrund ihrer Rolle nicht über Fragen der Meinungsfreiheit und der Rechtsmäßigkeit von Inhalten entscheiden sollten (Allianz für Meinungsfreiheit 2017)[16].

Kritisiert wird ferner die Unbestimmtheit der im Gesetzestext verwendeten Begrifflichkeiten, die darüber hinwegtäuscht, wie komplex und interpretationsoffen sich die Grenzziehung zwischen strafbaren Inhalten und dem Recht auf Meinungsäußerung im Einzelfall darstellt (Schulz 2017; Allianz für Meinungsfreiheit 2017). Die engen zeitlichen Fristen in Kombination mit den vorgesehenen Strafzahlungen des NetzDG führen zur Gefahr eines "Overblockings", demzufolge Intermediäre im Zweifelsfall Inhalte eher entfernen als schützen: "According to Facebook, defamation and hate speech alone account for 100.000 take-downs per month in Germany. Given that figure it seems rational for a provider to take down any flagged content if in doubt, just to save costs" (Schulz 2017, 3). Zusammengenommen wird das NetzDG als unverhältnismäßige und rechtlich zweifelhafte Einschränkung der Meinungsfreiheit gewertet, die nicht hinreichend in Betracht zieht, dass das "Notice-and-Take-Down"-Verfahren der europäischen E-Commerce Richtlinie (Art. 14) bereits Möglichkeiten zur Entfernung rechtswidriger Inhalte bereitstellt.

6.3 Marktkonzentration

Die Märkte für digitale Kommunikationsdienste sind durch starke Konzentrationstendenzen geprägt, die es potentiellen Konkurrenten zunehmend schwer, wenn nicht unmöglich machen, alternative Angebote zu etablieren. Dafür lassen sich mehrere Gründe benennen. Die Qualität datenbasierter Kommunikationsdienste, wie etwa Suchmaschinen, Dating-Portalen oder Übersetzungsprogrammen, hängt wesentlich von der Datenmenge ab, die für das "Training" von Algorithmen zur Verfügung stehen. Je größer der Marktanteil eines Anbieters, je umfassender der Zugriff auf Nutzungs- und Nutzerdaten in seinem Marktsegment, je größer der Datenvorsprung, desto spezifischer kann er seine Angebote auf spezifische Kontexte zuschneiden und desto größer sein Wettbewerbsvorteil gegenüber der Konkurrenz. Eine geringe Anzahl von Unternehmen (etwa Google/Alphabet, Amazon, Facebook, booking.com) beherrschen ihre jeweiligen Märkte auch aufgrund ihrer exklusiven Verfügung über die Daten, die in ihrem Geschäftsfeld fortlaufend entstehen. Zugleich eröffnen diese bestehenden Datensätze Möglichkeiten für die Entwicklung neuer datengestützter Dienste, derzeit etwa im Bereich der automatisierten Bild- und Sprachverarbeitung, der Verkehrssteuerung, der Diagnose, etc.

Verstärkt wird die Marktkonzentration durch Netzwerk- und Lock-in Effekte. Der Wert eines Dienstes steigt überproportional mit der wachsenden Anzahl seiner Nutzer. So steigert zum Beispiel jedes weitere Mitglied eines Vermittlungsdienstes für Ferienwohnungen den Nutzen

[16] Die Autorin gehörte zu den Erstunterzeichnern der Stellungnahme der Allianz für Meinungsfreiheit zum Entwurf des NetzDG. Diese ist abrufbar unter: deklaration-fuer-meinungsfreiheit.de (zuletzt abgerufen am 12.12.2017).

für alle anderen Nutzer. Der Zugang zu Risikokapital und das schnelle Wachstum einer neuen Plattform spielen daher eine entscheidende Rolle in der Frage, wer den Wettbewerb um die größte Anzahl von Mitgliedern für sich entscheidet. An der Anzahl der Nutzer wiederum bemisst sich der Wert eines Unternehmens und mithin die Kosten/Hürden für den Zugang zum Kapitalmarkt. Lock-in-Effekte beruhen auf den Transaktionskosten, die Nutzern entstehen, wenn sie einen Kommunikationsdienst wechseln (BMWI 2017, 57). Digitale Plattformen gelten als "Winner-takes-it-all"-Märkte, bei denen ein Anbieter das betreffende Marktsegment so stark dominiert, dass es für Wettbewerber nicht mehr lohnend erscheint, in diesem Bereich zu investieren, weil die Mitgliederzahl des größten Netzwerkes exponentiell steigt. Die daraus resultierende globale Markt- und Meinungsmacht weniger Unternehmen wirft die Frage nach staatlichen Interventionsmöglichkeiten auf.

Das Bundeswirtschaftsministerium hat 2017 das Wettbewerbsrecht novelliert, um den "Besonderheiten der daten- und internetbasierten digitalen Wirtschaft" besser Rechnung tragen zu können (9. GWB Novelle). Zu den wichtigsten Änderungen gehört die Einbeziehung von Märkten in das Kartellrecht, in denen keine Geldflüsse zu verzeichnen sind: "bei Suchmaschinen, Vergleichsportalen, Informationsdiensten oder Unterhaltungsmedien" (BMWI 2017, 58; vgl. Bundeskartellamt 2016). Darüber hinaus sollen künftig die für digitale Märkte typischen Netzwerk- und Skaleneffekte bei der Bewertung der Marktkonzentration berücksichtigt werden. Für eine effektive Verhinderung von hoher Marktkonzentration erweist sich das Kartellrecht allerdings nur in wenigen Fällen als ein geeignetes Instrument. Eine dominante Marktposition als solche stellt schließlich keinen Verstoß gegen das Wettbewerbsrecht dar (Schulz und Dankert 2016, 50). Die Anforderungen an die Feststellung eines Missbrauchs von Marktmacht sind wiederum sehr hoch, wie das Bundeskartellamt im Zusammenhang mit Suchmaschinen 2015 feststellt hat. Missbrauch besteht demnach in Verhaltensweisen, "die sich überhaupt nicht mehr damit erklären lassen, dass die Suchmaschine ihre Produkte zu verbessern oder zu verbilligen sucht oder sich rechtmäßig zu verhalten sucht. Gemeint sind hier Eingriffe, die aus dem Korridor legitimer unternehmerischer Motive 'ausbrechen'" (Bundeskartellamt 2015, 73).

Ein anderer Weg zur Senkung der Zutrittschancen für Wettbewerber könnte in der Öffnung des Zugangs und der Nutzung von Big Data bestehen. Zu prüfen wäre, ob gesetzliche Regelungen zur Nutzung öffentlicher Daten ("Open Data" bzw. "Open Government Data") auch ein Vorbild für "Open Corporate Data" Regime darstellen könnten (vgl. BMWI o. J.). Die neuen Regelungen der EU-DSGV zur Datenportabilität (Art. 20) stellen einen Schritt in diese Richtung dar, indem sie Individuen unter bestimmten Umständen die Möglichkeit bieten, die sie betreffenden personenbezogenen Roh- und Metadaten zu erhalten und Dritten zu übermitteln. Denkbar wären auch Lizensierungsmodelle für große anonymisierte Datensätze, die die Grundlage für neue Geschäftsmodelle und Märkte bilden könnten. Lizensierungsmodelle spielen im Immaterialgüterrecht eine große Rolle; sie bilden die Basis für den Markt der on-Demand-Dienste im audiovisuellen Bereich (Spotify, Netflix, etc). Die Lizensierung von Zugangs- und Nutzungsrechten hätte allerdings konkurrierende Schutzgüter wie die Privatsphäre der Bürger und den Investitionsschutz der Intermediären zu

berücksichtigen. Eine Lösung für das Problem der Netzwerkeffekte im Bereich der Plattformökonomie können Lizensierungsmodelle allerdings nicht bieten.

7. Aktueller Diskussionsstand über Multi-Stakeholder-Verfahren

Multi-Stakeholder Arrangements haben eine lange Tradition sowohl auf der nationalen als auch der internationalen Ebene. Aufgrund des Wandels der verwendeten Begrifflichkeiten ist diese Geschichte mitsamt der Vielfalt der Vorläufer allerdings weitgehend verschüttet.[17] Daher wird Multi-Stakeholder-Verfahren häufig ein größerer Neuigkeitswert zugeschrieben als angemessen wäre.

Das Ziel von Multi-Akteurs Partnerschaften besteht darin, die Vielfalt relevanter Perspektiven und Interessen in einer kleinen repräsentativ zusammengesetzten Gruppe zu bündeln, die im Namen aller Betroffenen konsensfähige Ergebnisse auszuhandeln soll, die von diesen als legitim anerkannt werden können, unabhängig davon, ob sie am Verhandlungsprozess beteiligt waren oder nicht (Jeanette Hofmann 2017). Während sich Multi-Stakeholder-Arrangements traditionell um die Interessenkonflikte zwischen Arbeit und Kapital gruppierten, sind es heute vor allem die Gegensätze zwischen der Wirtschaft, zivilgesellschaftlichen Interessen und der öffentlichen Hand bzw. der Staatengemeinschaft. In einigen Fällen beteiligen sich staatliche Akteure an Multi-Stakeholder-Prozessen.[18] Viele der zugrundeliegenden Regelungskonflikte sind heute eher transnationaler als nationaler Natur.

Als internationale Wiege des Multi-Stakeholder-Konzepts gilt die Konferenz der Vereinten Nationen über Umwelt und Entwicklung (Rio-Konferenz) im Jahr 1992 sowie in deren Folgeprozess, die Kommission für Nachhaltige Entwicklung, die entscheidend zur Institutionalisierung neuer Kooperationsformen zwischen Regierungen und Nicht-Regierungsorganisationen beitrugen. Das 2005 gegründete Internet Governance Forum (IGF) war die erste Organisation im Bereich von Internet Governance, deren Aufgabenstellung ausdrücklich die Realisierung des Multi-Stakeholder-Ansatzes beinhaltete.

Die wissenschaftliche Literatur befasst sich mit den Gründen für die rasche Ausbreitung und den politischen Bedeutungsgewinn des Multi-Stakeholder Ansatzes, sie zieht aber auch eine Leistungsbilanz. Im Rahmen empirischer Fallstudien werden die Performanz und der Erfolg einzelner Initiativen kritisch geprüft. Die Befunde dieses doppelten Fokus könnten nicht widersprüchlicher sein.

Der Aufstieg des Multi-Stakeholder-Ansatzes auf der inter- bzw. transnationalen Ebene wird überwiegend funktional mit Verweis auf die bekannten Herausforderungen und Defizite internationaler Regulierungsstrukturen erklärt. Ein gewichtiger Grund besteht folglich in der

[17] Ein Beispiel auf der internationalen Ebene ist die tripartistische Zusammensetzung der International Labor Organisation (ILO), eine UN-Organisation, die 1919 gegründet wurde. Ein Beispiel auf der nationalen Ebene stellen neo-korporatistische Aushandlungsverfahren dar, die in Europa vor allem in den 1970er Jahren verbreitet waren. Diese zielen darauf, organisierte Interessensverbände, etwa Arbeitgeber und Gewerkschaften, in staatliche Entscheidungsprozesse einzubeziehen, um deren Legitimität und Zustimmungsfähigkeit zu erhöhen.

[18] Ein Beispiel dafür ist der Netmundial-Prozess 2014, dessen Abschlussdokument von der Internetwirtschaft, Teilen der Zivilgesellschaft und Regierungsvertretern unterstützt wurde. S. http://netmundial.br (zuletzt abgerufen am 12.12.2017).

Zunahme grenzüberschreitender Regulierungsaufgaben, die die Koordinationsfähigkeit wie auch die Zuständigkeiten internationaler Organisationen überschreiten. Die Integration des privaten Sektors, der Zivilgesellschaft, aber auch der Wissenschaft dient entsprechend dazu, die erforderliche Expertise zu mobilisieren sowie die Befolgung der Regeln (Compliance) sowie Unterstützung in der Implementationsphase sicherzustellen: Multi-stakeholder initiatives "increasingly serve a global governance function in regulating what governments leave effectively unregulated" (Baumann-Pauly u. a. 2017, 772; Pattberg und Widerberg 2015).

Die empirischen Befunde zeigen allerdings, dass die Mehrzahl der Multi-Stakeholder-Initiativen diesen Anforderungen nicht gerecht wird. Eine neuere Überblicksstudie von Padberg und Widerberg über tripartistische Partnerschaften im Bereich der nachhaltigen Entwicklung kommt zu dem Ergebnis, dass die meisten der untersuchten Projekte nicht in der Lage waren, globale regulatorische Normen zu entwickeln oder ihre Implementation zu verbessern (Pattberg und Widerberg 2016). Auch ein weiteres Ziel, die Integration marginalisierter gesellschaftlicher Gruppen, wurde überwiegend verfehlt. Bäckstrand kommt zu dem Schluss, dass der Versuch Legitimationsprobleme in der internationalen Regulierung durch Multi-Stakeholder-Prozesse zu beheben, häufig neue Legitimationsprobleme schaffen (Bäckstrand 2006). Hofmann (2016) zeigt am Beispiel von ICANN und dem IGF, dass der Multi-Stakeholder Ansatz im Bereich von Internet Governance zwar einen sehr hohen politischen Stellenwert besitzt, seine Realisierung in der Praxis aber erhebliche Probleme aufwirft. Ein Grund dafür besteht darin, dass die Beteiligung nicht-staatlicher Akteure das Ungleichgewicht zwischen dem globalen Norden und Süden eher verschärft als verringert.

Die Gründe für die enttäuschenden empirischen Befunde lassen sich in folgender Weise zusammenfassen:

1. Ressourcen- und Machtasymmetrien

Die Teilnehmer von Multi-Stakeholder Prozessen sind mit ungleich verteilten Ressourcen ausgestattet (Faysse 2006; Boström und Tamm Hallström 2013). Repräsentanten des Privatsektors und der öffentlichen Hand verfügen über eine bessere Mittelausstattung, höhere organisatorische und personelle Kapazitäten und häufig auch eine umfassendere Expertise als die zivilgesellschaftlichen Vertreter (Fransen und Kolk 2007). Vor allem NGOs aus dem globalen Süden sind häufig nicht zu einer regelmäßigen Teilnahme und Mitarbeit in der Lage, mit der Folge einer weiteren Marginalisierung der Anliegen des globalen Südens.

2. Legitimationsdefizite

Multi-Stakeholder-Prozesse erzeugen hohe Erwartungen: Im Vergleich zu anderen Regulierungsverfahren sollen sie inklusiver und repräsentativer zusammengesetzt sein; sie sollen transparenter und responsiver agieren, konfligierende Interessen ausbalancieren und qualitativ bessere Ergebnisse erzielen. Gleichzeitig stehen sie unter beständiger Beobachtung, weil, wie Boström und Hallström (2013, 100) es formulieren, "no one has voted for them. They are, in a sense, self-selected (…) Accordingly, standard setters need to devote much of their organizing efforts to gain broad support". Der hohe Legitimationsbedarf legt wiederum eine Formalisierung von Organisationssstrukturen nahe, die die Beteiligung außenstehender

Akteure langfristig eher erschwert als erleichtert und somit potentiell neue Legitimationsdefizite erzeugt (Jeanette Hofmann 2016).

3. Selektivität
Im Bereich von Internet Governance finden sich Multi-Stakeholder-Verfahren nur in ausgewählten Regulierungsfeldern. Von zivilgesellschaftlicher Beteiligung ausgenommen sind staatsnahe Bereiche wie Cyber-Sicherheit, Handels- und Telekommunikationspolitik (Regeln zur Netzneutralität), aber auch der Selbstregulierung unterliegende Aufgaben wie die Vergabe von Internetadressen. ICANN ist die einzige Organisation, deren Verfahren den Multi-Stakeholder-Prinzipen entsprechen und die bindende Regeln setzt.

4. Begrenzte Wirksamkeit
Soft-Law-Instrumente wie freiwillige Selbstverpflichtungen, Best-Practice-Modelle oder Eco-Label-Konzepte erlangen selten eine mit gesetzlichen bzw. multilateralen Maßnahmen vergleichbare Reichweite und Bindewirkung (Moog, Spicer, und Böhm 2014).

Zusammenfassend stellen sich Multi-Stakeholder-Verfahren als Resultat und Treiber einer schrittweisen, wenngleich sehr selektiven Öffnung intergouvernementaler Regulierungsprozesse im internationalen Bereich dar. Positiv zu vermerken sind der zunehmende Einfluss zivilgesellschaftlicher Anliegen auf das politische Agenda-Setting, die zunehmende Transparenz politische Verhandlungsprozesse sowie die allgemein sinkenden Beteiligungsschwellen. Allerdings beziehen sich die positiven Effekte des Multi-Stakeholder-Ansatzes ganz überwiegend auf die Verfahrensdimension. Im Bereich der substantiellen Politikentwicklung haben Multi-Stakeholder-Prozesse nur wenige Erfolge zu verbuchen. Insbesondere zeigt sich, dass auch Multi-Stakeholder-Prozesse scheitern, wo zuvor bereits intergouvernementale Verfahren ihre Ziele verfehlten.

Die wohl wichtigste Alternative zu Multi-Stakeholder-Prozessen besteht im traditionellen Lobbying. Dabei konzentrieren NGOs ihre Anstrengungen darauf, ihre Expertise in einflussreiche Organisationen einzubringen oder politische Allianzen zu bilden. Bekannte Beispiele dafür sind das langfristige Engagement von NGOs bei internationalen Organisationen wie der World Trade Organisation, der World Intellectual Property Organisation, der Europäischen Kommission, der OECD oder den UN Weltkonferenzen. Obwohl es viel anekdotische Evidenz für die Wirksamkeit zivilgesellschaftlichen Engagements gibt, liegen keine über Fallstudien hinausreichenden Studien vor, die eine umfassende positive Bilanz stützen würden.

8. Unabhängigkeit von ICANN und Ansätze der Selbstregulierung: Reconsideration (Art. 4 ICANN Bylaws), Ombudsman, Independent Review Process, Document Transparency

Die US Regierung hat ICANN 1998 mit der Absicht gegründet, die Non-Profit-Organisation innerhalb von zwei Jahren in die Unabhängigkeit zu entlassen. Aus vielen Gründen, die ICANN zu einem nicht unerheblichen Teil selbst zu verantworten hat, verzögerte sich der Prozess bis zum Frühjahr 2014, als die US-Regierung verkündete, ihre Aufsichtsfunktion über ICANN und die sogenannten IANA-Funktionen beenden zu wollen.

Die singuläre Position der US-Regierung in der Aufsicht über die globale Netzinfrastruktur war lange Zeit politisch umstritten und galt zeitweilig als Risiko für den globalen Zusammenhalt des Internets. Zur Diskussion standen zwei Lösungen für dieses Problem: eine Internationalisierung der Netzinfrastruktur unter der Aufsicht einer UN-Organisation, wie der ITU, oder eine Entstaatlichung im Rahmen eines Multi-Stakeholder basierten Selbstregulierungsmodells. In ihrer Ankündigung zur vollständigen Privatisierung der von ihr ausgeübten Aufsichtsfunktionen erklärte die US-Regierung, dass sie nur Vorschläge für eine nicht-staatliche Lösung akzeptieren würde. [19] Die in der Regulierung des Domainnamensystems engagierten Akteure wiederum haben – mit Unterstützung der US-Regierung – ihre Zustimmung zu einer Privatisierung von ICANN an die Bedingung einer substantiellen Verbesserung der Rechenschaftspflichtigkeit von ICANN im Hinblick auf ihre der Prozesse, Funktionen und Entscheidungsgremien geknüpft (vgl. Taylor 2015, 69). Ein Teil der geforderten Reformen wurde als Bestandteil des "IANA Stewardship Transition" Prozesses verhandelt und beschlossen; andere, weniger essentielle Reformen auf einen späteren Zeitpunkt verschoben.[20]

Im Zentrum der Stärkung der Rechenschaftspflichtigkeit von ICANN steht eine veränderte Machtverteilung zwischen dem ICANN-Direktorium und den für die Politikentwicklung zuständigen Organisationseinheiten (supporting organisations, advisory committees). Der wichtigste Baustein hierfür ist die Schaffung der "empowered community", eine Mitgliedschaftsstruktur, die darauf zielt, die weitgehenden Rechte, die das kalifornische Recht den Mitgliedern gemeinnütziger Gesellschaften einräumt (California Corporations Code, Title 1, Division 2) durch spezifische Regeln und Begrifflichkeiten zu substituieren (Sidley Austin LLP and Adler & Colvin 2015).[21] Die "empowered community" ist mit sieben "community powers" ausgestattet. Zu den wichtigsten dieser "powers" gehören das Recht, die Budget- und Arbeitsplanung des Direktoriums abzulehnen, die Zustimmungspflichtigkeit grundlegender Änderungen der ICANN Bylaws sowie das Recht, einzelne Mitglieder sowie das gesamte Direktorium abzuberufen (NTIA 2016, 8).

[19] "Consistent with the clear policy expressed in bipartisan resolutions of the U.S. Senate and House of Representatives (S.Con.Res.50 and H.Con.Res.127), which affirmed the United States support for the multistakeholder model of Internet governance, NTIA will not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution" (NTIA 2014).

[20] Vgl. Aufgabenstellung der working group: https://community.icann.org/display/WEIA/Charter (zuletzt abgerufen am 19.12.2017).

[21] Die Frage, ob die sog. "ICANN community" in Form einer Mitgliedschaft organisiert sein sollte, hat ICANN schon in seiner Gründungsphase Ende der 1990er beschäftigt. Die ICANN beratenden Anwaltskanzleien haben stets davon abgeraten.

Die Rechte der "empowered community" kommen im Rahmen eines formalisierten "escalation process" zum Tragen (NTIA 2016, 8). Demzufolge korrespondiert die Eingriffsintensität des Rechts mit den Konsensanforderungen an dessen Unterstützer: Je drastischer die Macht, die gegen die Entscheidungen des Direktoriums mobilisiert wird, desto breiter muss die Zustimmung innerhalb der "empowered community" sein. Da die Interessen und Zielsetzungen der Stakeholder-Gruppen innerhalb ICANNs sehr divers sind, wird beispielweise eine Abberufung des Direktoriums nur im Falle schwerer Vergehen eine konsensfähige Option darstellen.

Die Schaffung der "empowered community" wird durch eine Vielzahl von Maßnahmen ergänzt, die darauf zielen, die Responsivität und Transparenz des Direktoriums sowie erstmals auch jene der Mitarbeiter von ICANN zu erhöhen. Im Zusammenhang betrachtet sind diese Maßnahmen durchaus geeignet, das Kräfteverhältnis innerhalb der Organisation signifikant zu verschieben. Allerdings hängt ihre Wirksamkeit, wie immer im Falle umfangreicher Organisationsreformen, von der konkreten Umsetzung ab. Deshalb ist es zu früh, ihre Effektivität einer Bewertung zu unterziehen.

Die ICANN Statuten sehen drei Mechanismen für Beschwerdefälle (appeals mechanisms) vor: 1. request for reconsideration process, 2. independent review panel, 3. Ombudsman. Diese werden im Folgenden vorgestellt. [22]

8.1 Request for reconsideration process (section 4.2.)

Der bisherige "request for reconsideration process" galt als mangelhaft, weil faktisch alle Beschwerdeverfahren negativ beschieden wurden (ICANN 2013, 53f.; Taylor 2015, 9).[23] Hinzukommt, dass sowohl die Bedingungen als auch die spezifischen Anlässe für Beschwerdeverfahren sehr eng gefasst waren[24] und lediglich von einem Unter-Komitee des Direktoriums geprüft und auf Vorschlag einer externen Rechtsberatung beschieden wurden (vgl. detailliert ICANN (Internet Corporation for Assigned Names and Numbers) 2016). Die neue Regelung dehnt die möglichen Anlässe für Beschwerden erheblich über den bisherigen Fokus auf Verfahrensfehler aus und schließt nun auch potentielle Verletzungen von ICANNs "mission", "core values" und "policies" mit ein. Die erste Bewertung der Beschwerden wird künftig von der Ombudsperson vorgenommen. Die finale Entscheidung obliegt dem gesamten Direktorium, dessen Urteil von dem eigens für diesen Prozess neu geschaffenen "Board Accountability Mechanisms Committee" abweichen kann. Das Direktoriumskomittee legt einen jährlichen Bericht über die behandelten Fälle und Entscheidungen vor, der auch Empfehlungen für weitere Prozessverbesserungen enthalten kann. Auch die Dokumentationsanforderungen bezüglich der Beschwerdefälle wurden verbessert.

[22] Eine Übersicht über die Geschichte der Rechenschaftspflichtigkeits-Mechanismen von ICANN findet sich unter: community.icann.org/download/attachments/51414329/History%20-%20Accountability%20Mechanisms.doc?version=1% (zuletzt abgerufen am 19.12.2017).
[23] Vgl. www.icann.org/public-comments/atrt2-recommendations-2014-01-09-en (zuletzt abgerufen am 19.12.2017).
[24] So konnte eine Beschwerde abgelehnt werden, wenn der Beschwerdeführer es versäumt hatte, seine Kritik in Rahmen des Aushandlungsprozesses der betreffenden Regel oder Entscheidung zu äußern.

8.2 Independent review process (IRP)

Der allgemeine Zweck des Independent Review Process besteht darin sicherzustellen, dass sich ICANNs Entwicklung im Rahmen seiner Statuten und entsprechend seiner Aufgabenstellung ("mission") vollzieht und eine schleichende Ausweitung dieser ("mission creep") verhindert wird. Bislang hat ICANN das International Centre for Dispute Resolution (der internationale Arm der American Arbitration Association) mit der Durchführung des independent review Prozesses beauftragt. Die zentrale Kritik an diesem Verfahren bezog sich auf die hohen Kosten für Beschwerdeführer, die Langwierigkeit des Prozesses sowie die Unverbindlichkeit der Ergebnisse. Wie das Berkman Center in einer Befragung der ICANN-Stakeholder ermittelte, bestand der Eindruck, dass der Independent review process nur für wohlhabende Akteure erschwinglich ist, nicht aber für die Mehrzahl der bei ICANN engagierten (Gasser et al. 2010, 123). Kritisiert wurde zudem, dass die Entscheidungen des Dispute Resolution Prozesses nicht bindend sind. Die im Rahmen der "IANA Stewardship Transition" beschlossene Reform trägt dem vielfach geäußerten Vorschlag Rechnung, dass ICANN auf eigene Kosten ein ständiges siebenköpfiges Expertenkommittee ("standing panel") einrichtet. Die Entscheidungen des "standing panels" sind bindend. Die Kosten für das Verfahren werden von den Streitparteien getragen. Eine davon abweichende Regelung greift, wenn die ICANN "empowered community", einer ihrer Stakeholder oder eine gemeinnützige Organisation Beschwerdeführer ist (ICANN Bylaws 4.3 (y)). Mit dieser Neuregelung soll sichergestellt werden, dass betroffene Akteure unabhängig von ihren finanziellen Ressourcen Zugang zu diesem Instrument der Beschwerdeführung haben.

Bemerkenswert ist, dass einige materielle Zuständigkeitsbereiche von ICANN nicht unter die IRP Regelung fallen. Dabei handelt es sich um die (häufig konfliktförmige) (Re-)Delegation von country-code TLDs und das Adressierungssystem des Internet (vgl. ICANN Bylaws 4.3.(b)). Derzeit befindet sich das neue Verfahren im Aufbau. Die Mitglieder des neuen "standing panels" sind noch nicht berufen worden.

8.3 ICANN Ombuds Office (IOO)

Das IOO wurde 2004 eingerichtet, seine Aufgaben regeln die ICANN Bylaws. Parallel zur Überprüfung der Ombudsfunktion im Rahmen der IANA Stewardship Transition wurde das IOO auch einer externen Evaluierung unterzogen. [25] Die Empfehlungen des Evaluierungsberichts bilden die Grundlage für die gegenwärtige Reformierung des IOO. Der Evaluierungsbericht kam zu dem Schluss, dass das IOO seine Funktionen im Großen und Ganzen erfüllt, Verbesserungen aber möglich und sinnvoll sind. Kritisiert wurden insbesondere die schwache Position und die unzureichende Unabhängigkeit der Ombudsfunktion. Die Evaluatoren argumentieren gegen die Übertragung von Entscheidungsautorität auf das IOO, schlagen aber vor, den Einfluss der Stellungnahmen des IOO durch verschiedene Maßnahmen zu erhöhen (Cameron et al 2017, 5).

[25] Evaluierungsbericht: www.icann.org/en/system/files/files/annex-b-ioo-independent-assessment-31jul17-en.pdf (zuletzt abgerufen am 19.12.2017).

Das IOO von ICANN entspricht einer internen Ombudsfunktion, die durch informelle Prozesse und niedrigschwellige Interventionen gekennzeichnet ist. Interne Kritiker dieser Struktur plädieren demgegenüber dafür, die Unabhängigkeit des IOO zu stärken, indem es institutionell aus ICANN ausgegliedert, personell aufgestockt und die zeitliche Befristung der Amtszeit aufgehoben wird.[26] Bemängelt wird insbesondere die "Vergemeinschaftung" der Ombudsperson mit den ICANN Stakeholdern (Cameron et al 2017, 31). Die Evaluatoren schlagen stattdessen vor, an der internen Lösung festzuhalten und die Unabhängigkeit des IOO durch die Einrichtung eines mehrköpfigen "Ombuds Advisory Panel" zu stärken. Die Verantwortung des IOO wird zusätzlich gestärkt durch die neue Rolle, die das Ombuds Office im Rahmen der reformierten Reconsideration Processes (4.2 Bylaws) erhält. Die Evaluatioren merken in diesem Zusammenhang einen systemischen Zielkonflikt an: Die Aufwertung der Rolle des IOO durch die Übernahme von Aufgaben zur Stärkung der Rechenschaftspflichtigkeit von ICANN schwächt zugleich die Unabhängigkeit des Amtes, die den Kern seiner Autorität bildet (Cameron.Ralph.Khoury 2017, 33). In leicht modifizierter Form liegen die Empfehlungen der Evaluatoren derzeit zur öffentlichen Kommentierung aus.[27]

8.4 Documentary Information Disclosure Policy (DIDP)

Das allgemeine Ziel der Documentary Information Disclosure Policy besteht darin, Informationen über die operativen Tätigkeiten von ICANN der Allgemeinheit zugänglich zu machen, sofern kein zwingender Grund zur Geheimhaltung besteht.[28] Im Februar 2017 hat die hierfür zuständige Unterarbeitsgruppe einen Entwurf für Empfehlungen zu den Transparenzregelungen von ICANN vorgelegt.[29] Der vorangestellte Bericht äußert scharfe Kritik an den bisherigen Transparenzregelungen von ICANN. Kritisiert werden insbesondere die weit gefassten Ausnahmebestimmungen, der unbestimmte Zeithorizont, innerhalb dessen Informationen offengelegt werden müssen, die Beschränkung von Informationsanfragen auf Dokumente, die noch nicht veröffentlicht worden sind sowie auf als vernünftig erachtete Auskunftsanträge.

Die Empfehlungen für eine Reform der Informationsoffenlegungsregeln zielen darauf ab, die Rechte der Auskunftssuchenden zu stärken, indem bestehende Einschränkungen enger gefasst oder ganz aufgehoben werden. So wird vorgeschlagen, die Beschränkung der DIDP auf operative Aktivitäten fallenzulassen. Gleiches gilt für die Beschränkung auf machbare, vernünftige und nicht übermäßig aufwändige ("overly burdensome") Anfragen. Von der Offenlegung ausgeschlossen sein sollten nur Informationen, deren Veröffentlichung materiellen Schaden für die betroffene Organisation oder das Internet nach sich ziehen würde. Empfohlen werden ferner die Einführung einer Pflicht zur akkuraten Dokumentation und

[26] Auskunft durch Dr Farzaneh Badii, Chair of the Non-Commercial Users Constituency.
[27] S. https://www.icann.org/en/system/files/files/ccwg-acct-ws2-draft-recs-ioo-05oct17-en.pdf (zuletzt abgerufen am 19.12.2017).
[28] S. https://www.icann.org/resources/pages/didp (zuletzt abgerufen am 19.12.2017).
[29] S. https://www.icann.org/en/system/files/files/ccwg-accountability-ws2-draft-recs-improve-transparency-21feb17-en.pdf (zuletzt abgerufen am 19.12.2017). Aktuelle Version: https://community.icann.org/download/attachments/59643288/CCWG-Accountability-WS2-Transparency-Rev.pdf?version=1&modificationDate=1508365977000&api=v2 (zuletzt abgerufen am 19.12.2017).

Archivierung aller Vorgänge, die Formulierung von Richtlinien für die Bearbeitung von Anfragen und ein Zeitlimit von maximal 30 Tagen für ihre Beantwortung. Die Vorschläge zur Verbesserung der Transparenz von ICANN sind noch nicht beschlossen.[30] Sollten sie in der vorliegenden Form angenommen werden, würden sie die Transparenz der ICANN Verwaltung erheblich erhöhen und die Rechte der Stakeholder ihr gegenüber entscheidend stärken.[31]

Zusammengenommen ist es beeindruckend, wie viele Reformschritte ICANN im Kontext der IANA Stewardship Transition initiiert hat. Nachdem ICANN über viele Jahre für seine intransparente und inkohärente Unternehmensführung sowie für den großen Einfluss der Regierungen auf die Entscheidungen des Direktoriums kritisiert worden ist (vgl. Bygrave 2015; Gasser et al 2010), geben die vielen in Umsetzung befindlichen Neuregelungen Anlass zu der optimistischen Annahme, dass die Entscheidungsabläufe und Beteiligungsverfahren regelkonformer, berechenbarer und damit legitimer werden. Insofern hat die Privatisierung von ICANN einen unerwartet wichtigen Beitrag zur Stärkung von allgemeinen Unternehmensführungsprinzipien geführt. Allerdings müssen die Reformen ihre Wirksamkeit erst noch unter Beweis stellen. Kritisch festzuhalten ist jedoch, dass ICANNs Organisationsstrukturen und -verfahren im Zuge der periodischen Reformprozesse einen Komplexitätsgrad erreicht haben, der sich als Barriere für sowohl für das Verständnis als auch für die Beteiligung potentiell Interessierter darstellen.

9. Regulierung bzw. transparente Gestaltung von Standardisierungsprozessen neuer Technologien

Die internationale und nationale Standardisierung von Kommunikationstechnologien galt bis zur Privatisierung der Telefonnetze ab den 1980er Jahren als staatliche Aufgabe. In der ITU war die Standardsetzung nach dem „one nation, one vote“-Prinzip organisiert. Auf der nationalen Ebene erfolgte sie in Zusammenarbeit zwischen Behörden und Lieferanten. Mit der Einführung von Wettbewerb im Bereich der Telefondienste und der zunehmenden wechselseitigen Durchdringung von Telekommunikation und Datenverarbeitung begannen sich die Kompetenzbereiche bestehender Standardisierungsorganisationen zu überlappen und zugleich neue Standardisierungskonsortien herauszubilden (Genschel 1995). Im Bereich der digitalen Technologien und Netzarchitekturen dominieren heute private Standardisierungsorganisationen wie die Internet Engineering Task Force (IETF) und das World Wide Web Consortium (W3C). Unabhängig davon, ob Standards von zwischenstaatlichen oder privaten Normsetzungsorganisationen entwickelt werden, ist festzuhalten, dass diese immer freiwilligen Charakter haben. Im Bereich des Internet gilt, dass der Markt entscheidet, ob sich ein Standard durchsetzt.

[30] S. zum aktuellen Stand: https://community.icann.org/display/WEIA/WS2+Dashboard?preview=/63151029/71606032/WS2%20Dashboard%20OCT-%2001Nov17-rev.pdf (zuletzt abgerufen am 19.12.2017).

[31] Erwähnenswert ist auch die Unterarbeitsgruppe zur Verbesserung der Rechenschaftspflichtigkeit des ICANN Management. Hierbei handelt es sich um einen neuen Reformbereich, der nach informellen Aussagen auf größeren Widerstand unter den Beschäftigten bei ICANN wie auch im Direktorium stößt. S. https://www.icann.org/public-comments/accountability-recs-2017-11-13-en (zuletzt abgerufen am 19.12.2017).

Es hat in den letzten Jahren verschiedentlich Vorstöße, vor allem von Ländern aus dem globalen Süden, gegeben, die weitere Entwicklung der Netzarchitektur und die Aufsicht über die kritischen Internetressourcen wieder stärker staatlich bzw. auf zwischenstaatlicher Ebene zu steuern.[32] Eine politische Mehrheit für eine staatliche Verwaltung des Internet ist derzeit jedoch nicht zu erwarten. Zum einen besteht die Sorge, dass eine stärkere staatliche Verantwortung eine Renationalisierung der transnationalen Infrastruktur zur Folge hätte (Mueller 2017). Zum anderen legen die jüngeren Entwicklungen im Bereich von Verschlüsselungsstandards nahe, dass ein staatliches Engagement in der Standardentwicklung nicht notwendigerweise zu einer Steigerung des Gemeinwohls und dem Schutz der individuellen Grundrechte führt.[33] Vielmehr ist im Bereich von Internet Governance eine Gemengelage von Interessen zu beobachten, die sich häufig quer zur traditionellen Grenzziehung zwischen staatlichen und privaten Akteuren formiert. Wenn staatliche Sicherheitsinteressen und der Schutz von Bürgerrechten, wie im Falle von Verschlüsselungsstandards, in Konkurrenz zueinander treten, wird es zur offenen Frage, welche Instanz die Interessen der Bürger besser schützt: private Normsetzungsorganisationen oder staatliche Akteure. Erwähnenswert ist auch, dass die zwischenstaatliche Normsetzungsorganisation ITU deutlich weniger transparent und beteiligungsoffen ist andere Standardisierungsorganisationen.

Standardisierungsorganisationen unterscheiden sich voneinander auch durch unterschiedlich hohe Zugangshürden und Beteiligungsregeln. Diese sind unmittelbar relevant für die Transparenz der Standardentwicklung. Eine, wenn nicht die offenste Standardisierungsorganisation, ist die IETF, die auf eine formale Inkorporierung wie auch Mitgliedschaftsregeln verzichtet. [34] Ihre wesentliche Beteiligungsschranke besteht in fachlicher Expertise. Ein Großteil der Arbeit an den Standards erfolgt über öffentlich archivierte Mailinglisten, die für alle Interessierten zur Subskription offenstehen. Auf diese Weise können auch Experten an der Standardentwicklung mitwirken oder diese nachvollziehen, die die steigenden Teilnahmegebühren für die Tagungen der IETF nicht aufbringen können.

Die meisten für das Internet relevanten Normsetzungsorganisationen erheben Mitgliedschaftsgebühren, die wiederum nach Beteiligungsrechten (ISO), der wirtschaftlichen Stärke (W3C), dem Ursprungsland oder Organisationstyp (ITU) gestaffelt sind. Auch die Standards selbst sind häufig nur gegen Gebühr zugänglich. Intergouvernementale Organisationen wie die ITU diskutieren seit vielen Jahren die Öffnung ihrer Arbeit über den Privatsektor hinaus für wissenschaftliche und zivilgesellschaftliche Organisationen. Ein

[32] Die letzte größere politische Kontroverse dazu entstand 2012 während der World Conference on International Communications (WCIT) (Kleinwächter 2012).

[33] So hat die International Standard Organisation (ISO) nach einem mehrjährigen Disput die Standardisierung von zwei Verschlüsselungstechniken der US-amerikanischen National Security Agency im Jahr 2017 abgelehnt, weil die Befürchtung bestand, dass "Simon" und "Speck" Hintertüren enthalten, die die Sicherheit der Standards unterlaufen (vgl. Reuters 2017).Hintertüren, die Regierungen den Zugriff auf verschlüsselte Dokumente erlauben, können auch von Dritten genutzt werden.

[34] Die IETF beschreibt sich selbst folgendermaßen: "The IETF is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications. The IETF is unusual in that it exists as a collection of happenings, but is not a corporation and has no board of directors, no members, and no dues" (TAO of the IETF 2012).

Hinderungsgrund scheint darin zu bestehen, dass der globale Norden über eine sehr viel stärker entwickelte wissenschaftliche und zivilgesellschaftliche Expertise verfügt, weshalb eine Integration entsprechender Organisationen das Ungleichgewicht zwischen globalem Norden und Süden noch vergrößern könnte. Inzwischen gibt es jedoch eine spezifische Mitgliedschaftskategorie für wissenschaftliche Einrichtungen.[35] Festzuhalten ist, dass die Transparenz und Zugänglichkeit von Standardisierungsprozessen stark variiert und die größte Transparenz bei einer Organisation mit einer historisch begründeten Verwurzelung im wissenschaftlich-akademischen Milieu zu beobachten ist.

Auch wenn die IETF eine traditionell technisch und meritokratisch ausgerichtete Kultur pflegt, die Vorschläge und Einwände nur von Personen mit anerkannter Expertise in ihrem Arbeitsbereich gelten lässt, haben sich die vormals äußerst strikten Grenzen zwischen Internettechnik und ihren gesellschaftlichen Implikationen in den letzten Jahren gelockert. So widmet die IETF seit den 2000er Jahren dem Thema Datenschutz zunehmend Aufmerksamkeit. Dies kommt auch in den 2013 verabschiedeten "Privacy Considerations for Internet Protocols" zum Ausdruck (RFC 6973). Hierbei handelt es sich um Richtlinien, die für eine Sensibilisierung unter Entwicklern, Anwendern und Nutzern technischer Standards für die potentiellen Implikationen für die Privatsphäre sorgen sollen. Der Einigung auf diese Richtlinien gingen eine mehrjährige Diskussion sowie ein Workshop mit anderen internetnahen (Standardisierungs-) Organisationen voraus, der darauf schließen lässt, dass die Bedrohung der Privatsphäre im Internet zum Thema für viele technisch ausgerichtete Organisationen geworden ist. Ausgehend von den "Privacy Considerations" hat die eine IETF im Jahr 2015 eine Forschungsgruppe eingerichtet, um die Beziehungen zwischen Internetstandards und Menschenrechten mit einem besonderen Fokus auf Meinungs- und Versammlungsfreiheit zu untersuchen. Das Ziel besteht in der Ergänzung der Richtlinien zur Privatsphäre um weitere Menschenrechte (Varon und Ten Oever 2015).

Die Integration von Menschenrechten als Designkriterium in die Entwicklung der Internetarchitektur und die aktive Mitwirkung von "Article 19", einer britischen NGO, an der Formulierung der Richtlinie deuten auf eine allmähliche gesellschaftliche Öffnung zumindest in Teilen der Standardentwicklung hin. Technische Standards werden nicht mehr allein unter operativen und funktionalen Gesichtspunkten bewertet, sondern auch im Hinblick auf ihre Konformität mit dem Prinzip des offenen Internet[36] sowie grundlegenden internationalen Werten und Prinzipien. Im Sinne einer Stärkung der Menschenrechte wäre es erstrebenswert, dass sich weitere Standardisierungsorganisationen diese Initiative zu Eigen machen. Voraussetzung dafür ist die Pflege langfristiger Kooperationsbeziehungen zwischen Experten für Menschenrechte und Experten für digitale Netztechnologien. Angesichts der Vielzahl von Standardisierungsorganisationen in diesem Bereich scheint eine umfassende staatliche Regulierung weder notwendig, noch wünschenswert oder machbar. Allerdings gibt es Ausnahmen, wie die Beispiele zu Regulierungslücken unter 5 zeigen. Im Bereich IoT spricht viel dafür, dass Regierungen die bekannten Sicherheitsrisiken zum Anlass nehmen, um in

[35] S. https://www.itu.int/en/join/Pages/Fees.aspx (zuletzt abgerufen am 19.12.2017).
[36] Vgl. den anhaltenden Streit innerhalb des W3C um die Integration von Kopierschutzverfahren in die Standards für Internetbrowser (Diedrich 2017).

koordinierender Weise die Festlegung von Standards zu befördern und ggf. Mindestanforderungen für den Verkauf bzw. Betrieb entsprechender Systeme festzulegen.

10. Themen, Prozesse oder Weichenstellungen mit besonderer Relevanz für den globalen Umwelt- und Nachhaltigkeitsdiskurs

Mir sind keine vergleichenden Arbeiten zwischen Umwelt- und Internet Governance bekannt, die es erlauben würden, Aussagen zur Übertrag- oder Vergleichbarkeit von Themen, Prozessen oder Weichenstellungen zwischen diesen Feldern zu treffen. Meine persönliche Vermutung wäre, dass Lernprozesse eher von der Umweltpolitik in Richtung Internet Governance erfolgen sollten als umgekehrt. Die globale Umweltpolitik ist sowohl auf der nationalen und internationalen Ebene in viel höherem Maße institutionalisiert, sie verfügt über eine breite akademische Forschungslandschaft und genießt große öffentliche Aufmerksamkeit. Internet Governance ist demgegenüber eher das kleine Geschwisterchen.

Literatur

Abdmeziem, Mohammed Riyadh, Djamel Tandjaoui, und Imed Romdhani. 2016. „Architecting the Internet of Things: State of the Art“. In *Robots and Sensor Clouds*, herausgegeben von Anis Koubaa und Elhadi Shakshuki, 55–57. Studies in Systems, Decision and Control 36. Springer International Publishing.

Allianz für Meinungsfreiheit. 2017. „Deklaration für die Meinungsfreiheit“. http://deklaration-fuer-meinungsfreiheit.de/.

ARCEP (Autorité de Régulation des Communications Électroniques et des Postes). 2017. „The state of the Internet in France“. https://www.arcep.fr/uploads/tx_gspublication/State-Of-Internet-in-France-2017_may2017.pdf.

Bäckstrand, Karin. 2006. „Multi-Stakeholder Partnerships for Sustainable Development: Rethinking Legitimacy, Accountability and Effectiveness“. *European Environment* 16 (5):290–306. https://doi.org/10.1002/eet.425.

Baumann-Pauly, Dorothée, Justine Nolan, Auret van Heerden, und Michael Samway. 2017. „Industry-Specific Multi-Stakeholder Initiatives That Govern Corporate Human Rights Standards: Legitimacy assessments of the Fair Labor Association and the Global Network Initiative“. *Journal of Business Ethics* 173:771–87. https://doi.org/10.1007/s10551-016-3076-z.

Belli, Luca. 2017. „Net Neutrality, Zero Rating and the Minitelisation of the Internet“. *Journal of Cyber Policy* 2 (1):96–122. https://doi.org/10.1080/23738871.2016.1238954.

BEREC (Body of European Regulators for Electronic Communications). 2017. „Draft BEREC Report on IP-Interconnection practices in the Context of Net Neutrality“. BoR (17) 111. http://berec.europa.eu/eng/document_register/subject_matter/berec/public_consultations/7092-draft-berec-report-on-ip-interconnection-practices-in-the-context-of-net-neutrality.

Beuth, Patrick. 2013. „Defcon: Das Internet der gehackten Dinge“. Zeit Online. 29. Juli 2013. http://www.zeit.de/digital/internet/2013-07/smart-home-auto-hacker.

Black, Julia. 2002. „Regulatory Conversations“. *Journal of Law and Society* 29 (1):163–96.

BMI (Bundesministerium des Inneren), Hrsg. 2009. „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)“. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/2009/kritis.pdf;jsessionid=7D24D89856B5BA57912B1EB56D484902.1_cid364?__blob=publicationFile&v=3.

BMWI (Bundesministerium für Wirtschaft und Energie), Hrsg. 2017. „Weißbuch Digitale Plattformen: Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe“. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.html.

———. o. J. „Open Data: Mit öffentlichen Daten digitale Wirtschaft fördern“. Zugegriffen 19. Dezember 2017. https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/open-data.html.

Boltanski, Luc., und Laurent. Thévenot. 2006. *On Justification : Economies of Worth*. Übersetzt von Catherine Porter. Princeton, NJ: Princeton University Press.

Boström, Magnus, und Kristina Tamm Hallström. 2013. „Global Multi-Stakeholder Standard Setters: How Fragile Are They?“ *Journal of Global Ethics* 9 (1):93–110. https://doi.org/10.1080/17449626.2013.773180.

Braman, Sandra. 2012. „Internationalization of the Internet by Design: The First Decade“. *Global Media and Communication* 8 (1):27–45. https://doi.org/10.1177/1742766511434731.

Breindl, Yana. 2013. „Internet content regulation in liberal democracies. A literature review.“ DH Forschungsverbund.

Brousseau, Eric, Meryem Marzouki, und Cécile Méadel. 2012. *Governance, regulation and powers on the Internet*. Cambridge: Cambridge University Press.

Buchner, Benedikt. 2016. „Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO“. *Datenschutz und Datensicherheit: DuD*, Nr. 3:155–61.

Bugeja, Joseph, Andreas Jacobsson, und Paul Davidsson. 2016. „On Privacy and Security Challenges in Smart Connected Homes“. In . IEEE. https://doi.org/10.1109/EISIC.2016.21.

Bundeskartellamt. 2015. „Beschluss B6-126/14“. http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2015/B6-126-14.html.

———. 2016. „Arbeitspapier - Marktmacht von Plattformen und Netzwerken“. Az. B6-113/15. Bonn. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.pdf?__blob=publicationFile&v=2.

Bygrave, Lee A. 2015. *Internet governance by contract*. First edition. Oxford, United Kingdom: Oxford Univ Press.

Cameron.Ralph.Khoury. 2017. „Independent Assessment Office of the Ombuds: Internet Corporation for Assigned Names and Numbers (ICANN)“. https://www.icann.org/en/system/files/files/annex-b-ioo-independent-assessment-31jul17-en.pdf.

CIDR Report. 2017. „CIDR REPORT for 18 Dec 17“. CIDR Report. 18. Dezember 2017. http://www.cidr-report.org/as2.0/.

Cisco. 2017. „Cisco Visual Networking Index: Forecast and Methodology, 2016–2021“. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf.

Daigle, Leslie. 2015. „On the Nature of the Internet“. 7. Global Commission on Internet Governance. https://issuu.com/cigi/docs/gcig_paper_no7.

DeNardis, Laura. 2012. „Hidden Levers of Internet Control“. *Information, Communication & Society Information, Communication & Society* 15 (5):720–38.

Dennis Weller, und Bill Woodcock. 2014. „New Approaches to Spectrum Management“. OECD Digital Economy Papers 235. https://doi.org/10.1787/5jz44fnq066c-en.

Diedrich, Oliver. 2017. „Protest gegen DRM im Browser: EFF verabschiedet sich vom W3C“. IX. 19. September 2017. http://www.heise.de/ix/meldung/Protest-gegen-DRM-im-Browser-EFF-verabschiedet-sich-vom-W3C-3835127.html.

Europäische Kommission. 2017. „Public consultation on Building the European Data Economy“. Website der Europäischen Kommission. 2017. https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy.

Faysse, Nicolas. 2006. „Troubles on the way: An analysis of the challenges faced by multi-stakeholder platforms“. In *Natural Resources Forum*, 30:219–29. Wiley Online Library.

FCC (Federal Communications Commission). 2015. *Protecting and Promoting the Open Internet*. https://www.federalregister.gov/documents/2015/04/13/2015-07841/protecting-and-promoting-the-open-internet.

Feick, Jürgen, und Raymund Werle. 2010. „Regulation of Cyberspace“. In *The Oxford Handbook of Regulation*, herausgegeben von Robert Baldwin, Martin Cave, und Martin Lodge, 523–47. Oxford: Oxford University Press.

Fransen, Luc, und Ans Kolk. 2007. „Global Rule-Setting for Business: A Critical Analysis of Multi-Stakeholder Standards“. *Organization* 14 (5):667–84. https://doi.org/10.1177/1350508407080305.

Gasser, Urs, Herbert Burkert, John Palfrey, und Jonathan Zittrain. 2010. „Accountability and Transparency at ICANN: An Independent Review Final Report“. Research Publication No. 2010-13. https://www.icann.org/review-berkman-final-report-20oct10-en.

Genschel, Philipp. 1995. *Standards in der Informationstechnik. Institutioneller Wandel in der internationalen Standardisierung*. Frankfurt/Main: Campus.

Grande, Edgar. 2012. „Governance-Forschung in der Governance-Falle? Eine kritische Bestandsaufnahme“. *Politische Vierteljahresschrift* 53 (4):565–92.

Hofmann, J., C. Katzenbach, und K. Gollatz. 2016. „Between Coordination and Regulation: Finding the Governance in Internet Governance“. *New Media & Society*, März. https://doi.org/10.1177/1461444816639975.

Hofmann, Jeanette. 2010. „Before the Sky Falls Down: A ‘Constitutional Dialogue’ Over the Depletion of Internet Addresses“. In *Anticipating Risk and Organising Risk Regulation*, herausgegeben von Bridhez Hutter, 46–67. Cambridge University Press.

———. 2016. „Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice“. *Journal of Cyber Policy* 1 (1):29–49. https://doi.org/10.1080/23738871.2016.1158303.

———. 2017. „The Multi-Stakeholder Concept as Narrative: A Discourse Analytical Approach“. SSRN Scholarly Paper ID 3070583. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3070583.

Hofmann, Jeanette, und Benjamin Bergemann. 2016. „Die informierte Einwilligung: Ein Datenschutzphantom“. *Spektrum der Wissenschaft Kompakt*, Oktober, 50–59.

Hofmann, Jeanette, Christian Katzenbach, und Kirsten Gollatz. 2016. „Between Coordination and Regulation: Finding the Governance in Internet Governance“. *New Media & Society*, März. https://doi.org/10.1177/1461444816639975.

ICANN (Internet Corporation for Assigned Names and Numbers). 2013. „Second Accountability and Transparency Review Team (ATRT 2) Draft Report & Recommendations“. 13. Dezember 2013. https://www.icann.org/public-comments/atrt2-recommendations-2013-10-21-en.

———. 2016. „CCWG-Accountability Supplemental Final Proposal on Work Stream 1 Recommendations: Annex 08 – Recommendation #8: Improving ICANN's Request for Reconsideration Process". https://community.icann.org/pages/viewpage.action?pageId=58723827.

IEC (International Electrotechnical Commission). 2016. „IoT 2020: Smart and secure IoT platform". http://www.iec.ch/whitepaper/pdf/iecWP-loT2020-LR.pdf.

ISOC (Internet Society). 2017. „2017 Internet Society GLobal Internet Report: Paths to our Digital Future". https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf.

IUCN (International Union for Conservation of Nature). 2008. „Regulatory and Governance Gaps in the International Regime for the Conservation and Sustainable Use of Marine Biodiversity in Areas beyond National Jurisdiction". Marine Series. Gland. https://cmsdata.iucn.org/downloads/iucn_marine_paper_1_2.pdf.

Just, Natascha, und Michael Latzer. 2016. „Governance by algorithms: reality construction by algorithmic selection on the Internet". *Media, Culture & Society* 39 (2):238–58. https://doi.org/https://doi.org/10.1177/0163443716643157.

Kahin, Brian, und James Keller, Hrsg. 1997. *Coordinating the Internet*. London: MIT Press.

Kitchin, Rob. 2017. „Thinking Critically about and Researching Algorithms". *Information, Communication & Society* 20 (1):14–29. https://doi.org/10.1080/1369118X.2016.1154087.

Kleinwächter, Wolfgang. 2012. „WCIT and Internet Governance: Harmless Resolution or Trojan Horse?" *CircleID* (blog). 17. Dezember 2012. http://www.circleid.com/posts/20121217_wcit_and_internet_governance_harmless_resolution_or_trojan_horse/.

Krasner, Stephen D. 1982. *International Regimes*. Cambridge, Mass.: MIT Press.

Lewis, Peter H. 1996. „Limiting a Medium Without Boundaries: How Do You Let the Good Fish Through the Net While Blocking the Bad?" *New York Times*, 15. Januar 1996.

Manske, Julia, und Tobias Knobloch. 2017. *Datenpolitik jenseits von Datenschutz*. Berlin: Stiftung neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/datenpolitik.pdf.

Maple, Carsten. 2017. „Security and privacy in the internet of things". *Journal of Cyber Policy* 2 (2):155–84. https://doi.org/10.1080/23738871.2017.1366536.

Marsden, Christopher T. 2017. *Network neutrality: from policy to law to regulation*. Manchester: Manchester University Press.

Mattioli, Rossella, und Cédric Levy-Bencheton. 2014. „Methodologies for the identification of Critical Information Infrastructure assets and services - Guidelines for charting electronic data communication networks". European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis.

Matzner, Tobias, Philipp K. Masur, Carsten Ochs, und Thilo von Pape. 2016. „Do-It-Yourself Data Protection—Empowerment or Burden?" In *Data Protection on the Move*, herausgegeben von Serge Gutwirth, Ronald Leenes, und Paul De Hert, 24:277–305. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-017-7376-8_11.

Mayntz, Renate. 2009. „The changing governance of large technical infrastructure systems“. In *Über Governance Institutionen und Prozesse politischer Regelung*, herausgegeben von Renate Mayntz, 121–150. Frankfurt: Campus.

Meier-Hahn, Uta. 2016. „Exploring the Regulatory Conditions of Internet Interconnection – A Survey Among Internet Interconnection Professionals“. SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=2740312.

Minerva, Roberto, Abyi Biru, und Domenico Rotondi. 2015. „Towards a definition of the Internet of Things (IoT)“. IEEE. https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

Moog, Sandra, André Spicer, und Steffen Böhm. 2014. „The Politics of Multi-Stakeholder Initiatives: The Crisis of the Forest Stewardship Council“. *Journal of Business Ethics*, Mai. https://doi.org/10.1007/s10551-013-2033-3.

Mörth, Ulrika. 2004. *Soft Law in Governance and Regulation. An Interdisciplinary Analysis*. Cheltenham: Edward Elgar.

Mueller, Milton. 2010. *Networks and states: the global politics of Internet governance*. Information revolution and global politics. Cambridge, Mass: MIT Press.

———. 2015. „Hyper-transparency and social control: Social media as magnets for regulation“. *Telecommunications Policy* 39:804–10. https://doi.org/http://dx.doi.org/10.1016/j.telpol.2015.05.001.

———. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. POLITY PRess.

Mueller, Milton, Brenden Kuerbis, und Hadi Asghari. 2013. „Dimensioning the elephant: an empirical analysis of the IPv4 number market“. *info* 15 (6):6–18. https://doi.org/10.1108/info-07-2013-0039.

Napoli, Philip M. 2015. „Social Media and the Public Interest: Governance of News Platforms in the Realm of Individual and Algorithmic Gatekeepers“. *Telecommunications Policy* 39 (9):751–60. https://doi.org/10.1016/j.telpol.2014.12.003.

NTIA (National Telecommunications and Information Administration). 2014. „NTIA Announces Intent to Transition Key Internet Domain Name Functions“. https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

———. 2016. „IANA Stewardship Transition Proposal Assessment Report“. https://www.ntia.doc.gov/report/2016/iana-stewardship-transition-proposal-assessment-report.

Offe, Claus. 2008. „Governance in einer sich wandelnden Welt“. In *Governance - „Empty signifier“ oder sozialwissenschaft liches Forschungsprogramm?*, herausgegeben von Gunnar Folke Schuppert und Zürn Michael, 61–76. Wiesbaden: VS Verlag für Sozialwissenschaften.

Pasquale, Frank. 2016. „Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power“. *Theoretical Inquiries in Law* 7:487.

Pattberg, Philipp, und Oscar Widerberg. 2015. „Theorising Global Environmental Governance: Key Findings and Future Questions“. *Millennium: Journal of International Studies* 43 (2):684–705. https://doi.org/10.1177/0305829814561773.

———. 2016. „Transnational multistakeholder partnerships for sustainable development: Conditions for success“. *Ambio* 45 (1):42–51. https://doi.org/10.1007/s13280-015-0684-2.

Pohle, Jörg. 2016. „Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen“. *Mediale Kontrolle unter Beobachtung* 5 (1):1–21.

Rentz, Ingo. 2016. „Mark Zuckerberg: Facebook ist ‚kein traditionelles Medienunternehmen‘“. HORIZONT. 22. Dezember 2016. http://www.horizont.net/medien/nachrichten/Mark-Zuckerberg-Facebook-ist-kein-traditionelles-Medienunternehmen-145017.

Reuters. 2017. „Distrustful U.S. allies force spy agency to back down in encryption fight“. *Reuters*, 21. September 2017. https://www.reuters.com/article/us-cyber-standards-insight/distrustful-u-s-allies-force-spy-agency-to-back-down-in-encryption-row-idUSKCN1BW0GV.

Rosenau, James N. 1992. „Governance, Order, and Change in World Politics“. In *Governance without Government: Order and Change in World Politics*, herausgegeben von James N. Rosenau und Ernst-Otto Czempiel, 1–29. Cambridge: Cambridge University Press.

Schmidt, Jan-Hinrik. 2011. *Das neue Netz: Merkmale, Praktiken und Folgen des Web 2.0*. 2., Überarb. Aufl. Kommunikationswissenschaft. Konstanz: UVK Verlagsgesellschaft.

Schulz, Wolfgang. 2017. „Comments on the Draft for an Act improving Law Enforcement on Social Networks (NetzDG)“.

Schulz, Wolfgang, und Kevin Dankert. 2016. *Die Macht der Informationsintermediäre - Erscheinungsformen, Strukturen und Regulierungsoptionen*. Bonn: Friedrich-Ebert-Stiftung. http://library.fes.de/pdf-files/akademie/12408.pdf.

Scott, Ben, Stefan Heumann, und Kleinhans. 2015. „Landmark EU and US Net Neutrality Decisions: How Might Pending Decisions Impact Internet Fragmentation?“ Published by the Centre for International Governance Innovation and Chatham House. 18. Global Commission on Internet Governance. https://www.cigionline.org/sites/default/files/no18.pdf.

Sidley Austin LLP and Adler & Colvin. 2015. „Memorandum Constraining the Sole Member’s Exercise of Statutory Member Rights“. https://community.icann.org/download/attachments/52896826/CCWG%20Memo_%20Constraining%20the%20Exercise%20of%20Statutory%20Rights%20%2800719283xA3536....pdf?version=1&modificationDate=1443816301000&api=v2.

Simon, Tobby. 2017. *Critical Infrastructure and the Internet of Things*. Centre for International Governance Innovation and Chatham House.

Sloot, Bart van der. 2014. „Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation“. *International Data Privacy Law* 4 (4):307–25.

Taylor, Emily. 2015. „ICANN: Bridging the Trust Gap“. GCIG (Global Commission on Internet Governance) and Chatham House. https://www.cigionline.org/sites/default/files/gcig_paper_no9.pdf.

Van Eeten, Michel JG, und Milton Mueller. 2013. „Where is the governance in Internet governance?“ *New Media & Society* 15 (5):720–36.

Varon, Joana, und Niels Ten Oever. 2015. „Human Rights at the IETF“. *IETF Journal* (blog). März 2015. https://www.ietfjournal.org/human-rights-at-the-ietf/.

Vermesan, Ovidiu, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert, u. a. 2011. „Internet of Things Strategic Research Agenda“. In *Internet of Things - Global Technological and Societal Trends*, herausgegeben von Ovidiu Vermesan und Peter Friess, 9–52. Aalborg: River Publishers. http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf.

WGIG (Working Group on Internet Governance). 2005. „Report of the Working Group on Internet Governance“. https://www.wgig.org/docs/WGIGREPORT.pdf.

Wikimedia Commons. 2006. „File:Dns-raum.svg“. Wikimedia Commons. 6. Februar 2006. https://commons.wikimedia.org/wiki/File:Dns-raum.svg.

———. 2017. „File:AS-interconnection.svg“. Wikimedia Commons. 10. Januar 2017. https://commons.wikimedia.org/wiki/File:AS-interconnection.svg.

Woodcock, Bill, und Marco Frigino. 2016. „2016 Survey of Internet Carrier Interconnection Agreements“. Packet Clearing House. https://www.pch.net/resources/Papers/peering-survey/PCH-Peering-Survey-2016/PCH-Peering-Survey-2016.pdf.

Externe Expertise für das WBGU-Hauptgutachten „Unsere gemeinsame digitale Zukunft“
Berlin: WBGU
Verfügbar im Internet unter www.wbgu.de/de/publikationen/publikation/unsere-gemeinsame-digitale-zukunft#sektion-expertisen

Autorin: Prof. Dr. Jeanette Hofmann
Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG) und
WZB-Projektgruppe ‚Politik der Digitalisierung‘
Titel: Internet Governance
Berlin, 2017

Wissenschaftlicher Beirat der Bundesregierung
Globale Umweltveränderungen (WBGU)

Geschäftsstelle
Luisenstraße 46
10117 Berlin

Telefon: (030) 26 39 48 0
E-Mail: wbgu@wbgu.de
Internet: www.wbgu.de
@WBGU_Council

Alle Gutachten können von der Internet-Webseite
https://www.wbgu.de/de/publikationen/alle-publikationen
heruntergeladen werden.