



Wer regiert das Internet?

Die aktualisierte und
erweiterte Neuauflage!

Impressum

12/2019

Friedrich-Ebert-Stiftung

Politische Akademie

FES Medienpolitik

Godesberger Allee 149

53175 Bonn

www.fes.de/medienpolitik

Für diese Publikation sind in der FES verantwortlich

Dr. Johanna Niesyto, Leiterin der FES Medienpolitik,

und

Katrin D. Dapp, Referentin in der FES Medienpolitik

Für diese Publikation ist beim iRights.Lab verantwortlich

Philipp Otto, Geschäftsführer

www.iriights-lab.de

Autoren

Henning Lahmann, Jan Engelmann

Redaktion

Anne Lammers, Jana Maire

Gestaltung und Satz

tigerworx Berlin

Verlag

Friedrich-Ebert-Stiftung, Bonn

ISBN: 978-3-96250-429-8

Die in dieser Publikation zum Ausdruck gebrachten Ansichten sind nicht notwendigerweise die der Friedrich-Ebert-Stiftung.

Creative-Commons-Lizenz: CC BY-NC-ND 4.0

Die Texte dieses Werks sind unter der Creative-Commons-Lizenz vom Typ „Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz“ lizenziert. Um eine Kopie dieser Lizenz einzusehen, besuchen Sie <https://creativecommons.org/licenses/by-nc-nd/4.0/>. Diese Lizenz beinhaltet unter anderem, dass die Texte bei Nennung des/der Autor_innen und dieser Publikation als Quelle ohne Veränderung veröffentlicht und weitergegeben werden dürfen. Ausgenommen von dieser Lizenz sind alle Nicht-Text-Inhalte wie Fotos, Grafiken und Logos.

Wer regiert das Internet?

**Die aktualisierte und
erweiterte Neuauflage!**

Inhalt



- 5 Vorwort**
- 6 Internetregulierung geht uns alle an!**
- 8 Was bedeutet „Regulierung des Internets“?**
- 16 Regulierungsansätze und Gestaltungsmöglichkeiten**
- 22 Akteure im Bereich der Internetregulierung**
- 36 Einschätzung und Ausblick**
- 39 Glossar**
- 40 Literaturhinweise und Links**
- 41 Weiterführende Informationen im Internet**
- 42 Über die Autoren**

Vorwort

Das Internet ist angetreten als ein *globales Freiheitsversprechen*. Der Erfolg des weltweiten Kommunikationsnetzes basiert auf dessen freiheitlicher und offener Architektur. Die Frage, wer das Internet regiert, ist die Schlüsselfrage der digitalen Gesellschaft(en). Dabei sind wir noch immer auf der Suche, wie bestimmte Bereiche des Internets besser geregelt werden können und wer dafür zuständig sein soll. Dies hat sich seit der ersten Auflage dieser Publikation nicht geändert: Internet Governance, die globale Regulierung des Internets, ist und bleibt eine *Suche ohne Ende*.

Bereits 2005 definierte Jeanette Hoffmann Internet Governance als ergebnisoffenen kollektiven Suchprozess, „[...] der darauf abzielt, eine globale regulatorische Leerstelle konzeptionell und institutionell in legitimer Weise zu füllen“. Eine zentrale Bedeutung auf dieser Suche kommt dem Internet Governance Forum (IGF) zu. Das IGF wurde im Jahr 2006 vom Generalsekretär der Vereinten Nationen (UN) ins Leben gerufen und ging aus dem UN World Summit on Information Society (WSIS) hervor. Die UN veranstaltete diesen Gipfel zwischen 2002 und 2005. Das ursprüngliche Ziel war es, die digitale Spaltung zu überwinden. Inzwischen hat sich das IGF zum zentralen internationalen Forum über die Zukunft von Internet Governance und Digitalpolitik entwickelt. Es geht um die grundlegenden Fragen der Offenheit und der Freiheit des Internets und um den Zugang zum Netz. Das IGF ist eine offene Diskussionsplattform zu zentralen rechtlichen, politischen, sozialen und technischen Fragen des Internets. Der Multi-Stakeholder-Ansatz bringt dabei alle relevanten gesellschaftlichen Gruppen an einen Tisch, insbesondere auch bislang unterrepräsentierte Vertreter_innen aus Entwicklungs- und Schwellenländern. Unter dem Motto „One World. One Net. One Vision“ fand das 14. IGF im November 2019 erstmalig in Deutschland statt.

Im Gegensatz zu anderen UN-Formaten fasst das IGF keine bindenden Entscheidungen. Vorrangiges Ziel ist es, den gleichberechtigten und konstruktiven Dialog zwischen Interessenvertreter_innen aus Staaten, internationalen Organisationen, Wissenschaft, Wirtschaft und Zivilgesellschaft zu fördern. Der grundsätzliche Ansatz des IGF ist es also, dass die verschiedenen Akteure aus unterschiedlichen Weltregionen

schaft(en) geht es nämlich um viel. Es geht um Zugang zum Netz, um Menschen- und Bürgerrechte, um soziale, gesellschaftliche, kulturelle und wirtschaftliche Teilhabe aller, um gerechten globalen Handel und darum, dass das „Netz der Netze“ jederzeit sicher ist. Digitalpolitik ist und bleibt Gesellschaftspolitik. Ich danke der Friedrich-Ebert-Stiftung, die mit dieser Publikation Engagierte in der Zivilgesellschaft,

Wie soll das Internet reguliert werden, damit es Teil guter Gesellschaften ist? Und wer soll dafür zuständig sein?

ihre je eigenen Perspektiven einbringen, miteinander diskutieren und so den Entscheidungsprozess in anderen Gremien – zum Beispiel den UN, der Internet Society (ISOC), der Internet Engineering Task Force (IETF), der Organisation für die Vergabe von Domainnamen (ICANN), der Europäischen Union oder der Internationalen Fernmeldeunion (ITU) – voranbringen.

Die freiheitliche und offene Architektur des Internets stand selten so massiv unter Druck wie heute. Nach den Enthüllungen über die Ausspähaktivitäten verschiedener Geheimdienste und angesichts der massiv zunehmenden Cyberangriffe ist die Diskussion um die Rückerlangung und den Erhalt der digitalen Souveränität zwingend geboten. *Die digitale Souveränität darf aber nicht dahingehend umgedeutet werden, dass offene und freie globale Netz infrage zu stellen und Überwachungs- und Zensurinfrastrukturen zu etablieren.*

Internet Governance geht uns alle etwas an. Für die digitale(n) Gesell-

Politiker_innen, Wissenschaftler_innen und Bürger_innen weiterhin ermutigen will, sich an dieser Suche zu beteiligen und auf der Suche zu bleiben – um dieses Freiheitsversprechen einzulösen.

*Dr. Jens Zimmermann, MdB
Digitalpolitischer Sprecher der SPD-
Bundestagsfraktion*



Foto-AG Gymnasium Melle /
CC BY-SA 4.0

Internetregulierung
geht uns alle an!



Das Internet ist mit uns, im Grunde überall. Während stationäre PCs nahezu nur noch im Büroumfeld ihr kümmerliches Dasein fristen, sind Smartphones auf dem Schulhof, Tracking Watches beim Jogging und Sprachassistenzsysteme wie Alexa oder Siri in der Küche oder im Wohnzimmer längst vertraut.

In nahezu allen Bereichen des täglichen Lebens verlassen wir uns auf das Internet und digitale Hilfsmittel. Doch zu den zahllosen Vorteilen, die uns das Netz bietet, gesellen sich fast ebenso viele Herausforderungen für die Gesellschaft – in den einzelnen Ländern auf verschiedene Weise und in unterschiedlichem Ausmaß. Eines gilt jedoch für alle gleichermaßen: Das Internet entwickelt sich nicht von selbst, kann nicht von sich aus den Bürger_innen einen Raum zur freien Entfaltung bieten. Um zu funktionieren, in technischer wie auch politisch-gesellschaftlicher Hinsicht, bedarf es menschlicher Intervention und Steuerung. Das Internet muss reguliert, verwaltet und regiert werden.

Die Gesetze, an die wir uns halten müssen, stammen vom deutschen Gesetzgeber oder von den Institutionen der EU. Was für Internetnutzer_innen in Deutschland gilt, muss daher nicht auch für Brasilianer_innen gelten, die von Rio de Janeiro aus auf Inhalte im Netz zugreifen.

Das Internet ist weltumspannend, aber dezentral organisiert und rechtlich fragmentiert. Je nachdem, von wo aus man online geht, gelten unterschiedliche Regeln. Aber auch die Zugangs-

möglichkeiten oder die Sicherheit bei der Nutzung des Internets sind keineswegs für alle Bürger_innen auf der Welt gleich. Die Situation im Netz spiegelt die politische Situation des jeweiligen Landes. Freiheitsrechte, die zum Beispiel Bürger_innen der EU wie selbstverständlich auch online genießen, mögen für Nutzer_innen in einem Staat mit einem autoritären Regime unerreichbar sein.

Das Politikfeld der Internetregulierung lässt sich in verschiedene Handlungsfelder aufgliedern: Infrastruktur und Entwicklungszusammenarbeit, Sicherheitspolitik, Menschen- und Bürgerrechte sowie Rechtsentwicklung. Dabei ist die Frage relevant, wie die verschiedenen Ziele der Internetregulierung umgesetzt werden sollen: Durch Abkommen zwischen Staaten oder unter Einbeziehung aller Anspruchsgruppen (engl. Stakeholder)? Durch verbindliche Verträge oder lose Verständigungspapiere?

Neben diesen inhaltlichen Aspekten ist insbesondere von Bedeutung, wer für die Internetregulierung verantwortlich sein soll: Internationale Organisationen, in denen Staaten das Sagen haben, oder vielmehr offenere Foren, die auch Vertreter_innen der Privatwirtschaft und der Zivilgesellschaft einbeziehen? Diese Publikation beantwortet die wichtigsten Fragen: Wer regiert das Internet, auf welche Weise und bezüglich welcher Handlungsfelder? Ein angefügtes Glossar erläutert die wichtigsten Fachbegriffe, die im Text vorkommen.

Zentrale Leitfragen der Internetregulierung sind:

Wie können die Freiheitsrechte im Netz möglichst für alle gewährleistet werden?

Wie soll der globale Handel über das Internet aussehen?

Wer sorgt dafür, dass die technische Infrastruktur des Internets auch in Zukunft einwandfrei funktioniert?



Foto: Mario Sixtus. Boy in a Bubble (2) / CC BY-NC-SA 2.0



Was bedeutet
„Regulierung des Internets“?

Wovon sprechen wir, wenn wir uns mit der gegenwärtigen und zukünftigen Gestaltung des Internets befassen? Im Englischen hat sich für den in der Einleitung beschriebenen Politikbereich der Begriff „Internet Governance“ durchgesetzt. Er lässt sich nicht ohne Weiteres ins Deutsche übersetzen. Denn im hiesigen Verständnis umfasst das durch ihn bezeichnete Feld sowohl das „Regieren“, das „Regulieren“ als auch das „Verwalten“ des Internets.

Die zwei Kernfragen der Internetregulierung

Es ist sinnvoll, das Thema in zwei Kernfragen aufzuspalten. Zum einen geht es um die Frage, wer das Internet reguliert, wer also überhaupt dafür zuständig ist (oder sein soll), Entscheidungen in Bezug auf das Netz zu treffen, die dann für alle gelten beziehungsweise auf sämtliche Nutzer_innen des Internets Auswirkungen haben. Hierfür ist es wichtig zu verstehen, dass es sich beim Internet keineswegs um eine in sich abgeschlossene, einheitliche Struktur handelt. Vielmehr verbirgt sich hinter diesem Begriff nichts anderes als ein globales „Netzwerk der Netzwerke“, also der Zusammenschluss sehr vieler einzelner Netzwerke, die auf elektronischem Wege miteinander kommunizieren. Genau aus diesem Grund hat das Internet auch für sich genommen keine zentralisierte Verwaltung oder Steuerung. Wer also für Entscheidungen bezüglich der übergreifenden Struktur zuständig ist, bedarf einer Klärung und versteht sich

keineswegs von selbst. Die wichtigsten Player auf dem Gebiet der Internetregulierung werden mit ihren jeweiligen Rollen im dritten Teil dieser Publikation vorgestellt.

Neben dem „Wer“ der Internetregulierung geht es zweitens um die Frage, was durch die verschiedenen Beteiligten eigentlich genau geregelt werden soll. Zunächst einmal handelt es sich beim Internet ja lediglich um eine technische Struktur. Wie aber bereits einleitend erwähnt, existiert heute wohl kaum eine andere Technologie, die unseren Alltag und unser berufliches Leben so nachhaltig verändert hat. Die Regulierung des Internets auf die Verwaltung, den Ausbau und die technische Überwachung der zugrundeliegenden Infrastruktur zu reduzieren, würde daher zu kurz greifen.

Die vier Ebenen der Internetregulierung

Um die unterschiedlichen inhaltlichen Dimensionen der Regulierung des Internets zu verdeutlichen, bietet es sich an, vier verschiedene Ebenen zu betrachten, aus denen sich das Internet zusammensetzt: die infrastrukturelle, die logische, die anwendungsorientierte und die inhaltliche Ebene.

— Die infrastrukturelle Ebene umfasst die Hardware, die die Grundstruktur des globalen Netzes bildet, also zum Beispiel sämtliche Router, Switches, Server sowie die datenleitenden Vorrichtungen wie Kupfer- oder Glasfaserkabel.

Kernfragen der Internetregulierung:

Regulierung des Internets

Wer setzt die Regeln?

Was wird reguliert?

- Die logische Ebene des Internets bezieht sich auf die technischen Normen und Standards, die Voraussetzung dafür sind, dass die Kommunikation im globalen Maßstab überhaupt möglich ist. Dies sind beispielsweise Ressourcen wie das Internet-Protokoll (IP), die Webadressen und Domain-Namen sowie das dazugehörige Domain Name System (DNS).
- Die Anwendungsebene ist der Bestandteil des Internets, der in erster Linie jene Software-Anwendungen umfasst, anhand derer die Nutzer_innen miteinander sowie mit Systemen und

Webseiten interagieren. Die bekannteste und wichtigste dieser Anwendungen ist das World Wide Web, auf das mittels Internetbrowsern wie Firefox, Chrome oder Safari zugegriffen werden kann.

- Die inhaltliche Ebene ist für Nutzer_innen zentral. Sie umfasst all das, was wir vor uns auf dem Computerbildschirm sehen bzw. womit wir am Screen interagieren, also Text, Ton, Bilder, Videos oder sonstige Multimedia-Inhalte, Virtual-Reality-Umgebungen oder Chat Bots, die mit uns einen Dialog führen.

Von der technischen zur politischen Regulierung des Internets

In den Anfangstagen des Netzes befasste sich die Regulierung des Internets fast ausschließlich mit den ersten beiden Ebenen, also der infrastrukturellen und der logischen. Das Internet wurde vor allem als rein technische Infrastruktur betrachtet. Probleme, die einer Regulierung bedurften, waren daher in erster Linie technischer Natur. Mit der Öffnung des Netzes für kommerzielle und sonstige allgemeine Nutzungen und seiner Relevanz in immer mehr gesellschaftlichen Bereichen ist eine solche enge Auffassung der Regulierung des Internets nicht mehr ausreichend. Die meisten politischen Herausforderungen im Umgang mit dem Internet spielen sich inzwischen auf der inhaltlichen Ebene ab, wie zum Beispiel bei Fragen des Zugangs zu Wissen und Kultur oder der Menschen- und Bürgerrechte im Netz. Deshalb ist heute allgemein anerkannt, dass sich die Regulierung des Netzes auf alle vier Ebenen bezieht. Dabei können durchaus unterschiedliche Akteure für die einzelnen Ebenen primär zuständig sein.

Mit Bezug auf alle vier Ebenen des Internets versuchte sich der von der UN beschlossene und von der Internationalen Fernmeldeorganisation (ITF) durchgeführte Weltgipfel zur Informationsgesellschaft im Jahr 2005 in Tunis, auf dem sich etwa 17.000 Teilnehmer_innen aus 175 Ländern mit der Zukunft des Internets befassten, erstmals an einer umfassenden Definition der Regulierung des Internets, die bis heute weit hin Verwendung findet: Sie umfasst „die durch Regierungen, den Privatsektor und die Zivilgesellschaft in ihren jeweiligen Rollen vorgenommene Entwicklung und Anwendung von einheitlichen Prinzipien, Normen, Regeln, Entscheidungsfindungsprozessen und Programmen, die die Evolution und Benutzung des Internets formen“.

Die vier Ebenen der Internetregulierung:

4

Die inhaltliche Ebene
Nutzerinhalte: Text, Ton, Bilder, Videos,
 Virtual-Reality-Umgebungen ...

3

Die anwendungsorientierte Ebene
Software-Anwendungen:
 World Wide Web und dazugehörige Browser ...

2

Die logische Ebene
Technische Normen und Standards:
 Internet-Protokoll (IP), Domain Name System (DNS) ...

1

Die infrastrukturelle Ebene
Hardware: Router, Switches,
 Server, Kupfer- oder Glasfaserkabel ...

Drei Fragen an Prof. Dr. Laura DeNardis

Fakultätsleiterin des Internet Governance Lab an der American University in Washington, D.C.



Foto: Centre for International Governance Innovation

„Das Ökosystem der Akteure erweitert sich“

Hat sich die vielfältige Ökologie des Internets schleichend dahingehend entwickelt, dass sie maßgeblich durch wenige Technologieunternehmen beeinflusst wird?

Laura DeNardis: Die digitale Welt ist von 2D zu 3D übergegangen, und auch die Internet Governance muss diesen Schritt vollziehen. Die komplexesten und folgenreichsten Kämpfe um die Internet Governance treten nun in der cyber-physischen Welt auf. Das Internet ist von menschlichen Bildschirmen in die materielle Welt der medizinischen Instrumente, Haushaltsgeräte und die sogenannte Industrie 4.0 gesprungen. Dieser Wandel verkompliziert die Frage, was denn als Technologieunternehmen zählt, da alle Unternehmen jetzt gewissermaßen Technologieunternehmen darstellen. Und damit wird auch die Beantwortung der Frage schwierig, welche Governance-Institutionen und Normungsinstitutionen am relevantesten sind.

Welche Auswirkungen hat diese Situation auf den fairen Zugang zu Informationen oder die Meinungsfreiheit?

Anstatt sich zu verkleinern, erweitert sich das Ökosystem der Akteure tatsächlich. Dies erschwert auch die Frage nach der Internetnutzung, da es sich bei vielen „Menschen“ im Internet tatsächlich um Bots handelt und wir längst vom Internet der Dinge sprechen. Die Einbettung des Internets in die physische Welt verschärft die bereits bestehenden Probleme in Bezug auf Privatsphäre, Sprache, nationale Sicherheit, Demokratie und Verbraucher_innenschutz.

Worin sehen Sie die größte Herausforderung für eine gute Governance des Internets?

Bei einem Netzausfall geht es nicht mehr darum, den Zugang zu Kommunikation und Inhalten oder die Strukturen der vernetzten Wirtschaft zu verlieren, sondern möglicherweise um den Verlust von Menschenleben bzw. die Fähigkeit, über das Internet Krieg zu führen und die zivile Infrastruktur zu treffen. Gleichzeitig ist die Sicherheit des Internets der Dinge in der Regel unzureichend. Die Praxis und die Analyse der Internet Governance müssen sich steigern, um diese Herausforderung einer Generation zu meistern.

Prof. Dr. Laura E. DeNardis ist Professorin und Interimsdekanin der School of Communication an der American University in Washington, D.C. Dort ist sie auch Fakultätsleiterin des Internet Governance Lab. Mit einem Hintergrund in Informationstechnik und in Wissenschafts- und Technologiestudien hat sie sechs Bücher und zahlreiche Artikel zu den politischen Auswirkungen der technischen Architektur und Governance des Internets veröffentlicht. Ihr neuestes Buch, „The Internet is Everything“, nimmt verstärkt das Internet der Dinge in den Blick.

Die komplexesten und folgenreichsten Kämpfe um die Internet Governance treten nun in der cyber-physischen Welt auf.



Eine kurze Geschichte des Internets und seiner Regulierung

Die technische Struktur, die wir heute unter dem Namen „Internet“ kennen, begann in den späten 60er Jahren des letzten Jahrhunderts zunächst als Forschungsprojekt des US-amerikanischen Verteidigungsministeriums und einiger Universitäten vor allem in Kalifornien. Zwischen 1984 und 1986 wurde die Struktur durch die National Science Foundation (NSF) zu einem allgemeinen Forschungsnetzwerk ausgebaut, die die lokalen Netzwerke amerikanischer Universitäten zum Zwecke des Informationsaustausches miteinander verknüpfte. Zu dieser Zeit kam auch erstmals der Name „Internet“ in Gebrauch.

Die weltweite Verbreitung des Internets

In den 80er Jahren schloss man erstmals weitere Länder an das Internet an, darunter auch europäische Staaten wie die Niederlande, Italien und Deutschland. Während die NSF noch bis 1991 kommerzielle Nutzungen des Netzes untersagt hatte, lockerten sich die Restriktionen in den folgenden Jahren. Bis Mitte des Jahrzehnts ging das Internet nach und nach in private Hän-

de über. Bis Ende des Jahrhunderts fand das Internet immer größere Verbreitung und kommerzielle Anwendungen hielten Einzug. Auf Betreiben der USA wurde 1998 schließlich die Internet Corporation for Assigned Names and Numbers (ICANN) in Kalifornien gegründet. Diese gemeinnützige Gesellschaft ist bis heute für die Koordinierung des Domain Name System (DNS) und die Zuteilung der IP-Adressen – also für die Pflege der technischen Grundstruktur des Internets – zuständig. Als Untereinheit von ICANN hat sich die Internet Assigned Numbers Authority (IANA) seit Jahrzehnten um administrative und technische Grundfunktionen gekümmert, indem sie etwa Root-Nameserver und neue Standards registriert und veröffentlicht. 2016 lief der Vertrag zwischen dem US-Handelsministerium und ICANN zur Erfüllung dieser Verwaltungsfunktionen aus, und die Aufsicht über IANA wurde auf den privaten Sektor übertragen.

Die Entwicklung der Regulierung auf zwischenstaatlicher Ebene

Im Zuge der Kommerzialisierung des Netzes prägten zunächst zwischenstaatliche, multilaterale Abkommen die Regulierung verschiedener Teilbereiche des Internets. So verabschiedete die Weltorganisation für geistiges Eigentum (WIPO) bereits 1996 die beiden soge-

nannten Internet-Verträge: den WIPO-Urheberrechtsvertrag (WCT) und den WIPO-Vertrag über Darbietungen und Tonträger. Diese Abkommen hatten den Zweck, die Urheberrechtsgesetze der Mitgliedstaaten an das Internetzeitalter anzupassen. Auch im Rahmen der Welt handelsorganisation (WTO) schlossen Staaten völkerrechtliche Verträge, die die Internetregulierung mitbestimmten. So insbesondere das 1995 in Kraft getretene GATS-Abkommen, das den globalen Markt der Telekommunikationsdienstleistungen behandelt. Als weiterer Meilenstein kam das 2001 unterzeichnete, im Rahmen des Europarats ausgehandelte Budapester Übereinkommen hinzu, in dem sich die Staaten zum ersten Mal umfassend mit der Problematik der Cyberkriminalität auseinandersetzten.

Vom UN-Weltgipfel zum IGF

Gleichzeitig zeigte sich zu Beginn des 21. Jahrhunderts endgültig die zentrale Bedeutung des Internets für die Weltgesellschaft jenseits rein kommerzieller Interessen. Um dieser Entwicklung gerecht zu werden, wurde die ITU vom damaligen UN-Generalsekretär Kofi Annan damit beauftragt, einen Weltgipfel zur Informationsgesellschaft (World Summit on the Information Society, WSIS) auszurichten. Dieser fand in zwei Teilen statt, 2003 in Genf und 2005 in Tunis. Wichtigster Beschluss des Gipfels war die Gründung des IGF als permanente Diskussionsplattform zu Fragen der Regulierung des Internets. Daraus sind jährliche Veranstaltungen hervorgegangen, die seit 2006 an wechselnden Standorten stattfinden und mittlerweile unabhängig von der UN geplant und durchgeführt werden. Beim ersten Treffen IGF in Athen (2006) waren die Diskussionsstränge noch auf vier zentrale Aspekte ausgerichtet: Offenheit, Sicherheit, Diversität und Zugang. Im Verlauf der Jahre hat sich das thematische Feld noch wesentlich ausdifferenziert.

**Im Zuge der
Kommerzialisierung des Netzes
prägten zunächst zwischenstaatliche,
multilaterale Abkommen die
Regulierung verschiedener Teilbereiche
des Internets.**

Drei Fragen an Prof. Dr. Jeanette Hofmann

Politikwissenschaftlerin und Internetforscherin am
Wissenschaftszentrum Berlin



Foto: Jason Krüger / CC BY-SA 4.0

„Es gibt immer Experimentierräume für das Andere“

Sie untersuchen seit Jahren die Akteure und Machtmechanismen in der Netzpolitik und haben festgestellt, dass bei jeder institutionellen Herausbildung eines neuen Politikfeldes bestimmte Schutzgüter im Zentrum stehen. Wie ließe sich das für das Feld der Internet Governance beschreiben?

Jeanette Hofmann: Zunächst mal wäre zu klären, ob man im Falle von Internet Governance überhaupt von einem Politikfeld sprechen kann. In den Grundzügen lassen sich einige Merkmale eines beginnenden Politikfeldes erkennen: Es wird ein Problem wahrgenommen, und eine Reihe von Akteuren finden dieses Problem so wichtig, dass sie sich darum kümmern und deshalb immer wieder aufeinandertreffen und über gute Lösungen streiten. Dieses Problem bestand in der offenen Frage, wer die Regeln für das Internet setzen soll. Auch wenn die Akteure fundamental unterschiedlicher Meinung über die Antwort auf diese Frage sind, bilden sie doch eine Subkultur heraus, die sie als Akteure erkennbar macht. Dazu gehört ein Fachjargon, eine bestimmte Expertise, selbst der Humor wird irgendwann speziell. Es hat im Bereich von Internet Governance ja auch anhaltende Prozesse der Institutionenbildung gegeben: ICANN, das IGF und seine nationalen Ableger und entsprechende Zuständigkeiten in Verbänden und nationalen Ministerien. Trotzdem sehe ich bis heute kein verbindendes Schutzgut, das breite gesellschaftliche Unterstützung mobilisieren könnte. Im Gegenteil, den meisten Menschen ist dieser Handlungsbereich entweder unbekannt oder einigermassen egal.

Viele Menschen sehen die Snowden-Enthüllungen rückblickend als eine Art Kipppunkt in der Internetgeschichte. Stecken wir nun in einer neuen Phase, in der es eher um Gefahrenabwehr als um die freiheitlichen Potenziale eines globalen Kommunikationsraums geht?

Wie wir in unseren Interviews ermittelt haben, betrachten viele Expert_innen rückblickend die Snowden-Enthüllungen tatsächlich als Wendepunkt, weil es der kritischen Netzgemeinde in Deutschland nicht gelungen ist, die massenhafte und systematische Verletzung von Grundrechten durch staatliche Organisationen politisch zu nutzen. Ein Bundestagsabgeordneter sagte dazu, man habe als

Bürgerrechtler_in versagt, da es nicht gelungen sei, „unser Fukushima umzusetzen“. Aus Politikfeldperspektive gesprochen, dominieren derzeit die Ideale der angrenzenden Politikfelder: Industrie 4.0, KI-Strategien, aber auch die nationale Sicherheit sowie neuerdings wieder Medienpolitik. Das Schutzgut „Freies und offenes Internet“ wird zwar in besonderen Momenten beschworen, zuletzt etwa in der Auseinandersetzung um die Urheberrechtsreform, aber es fehlt die Kraft, um damit einen öffentlichen Diskurs zu bestimmen.

Derzeit wird viel über die Anwendungspotenziale neuer Technologien gesprochen, z.B. Künstliche Intelligenz oder Blockchain. Inwiefern gibt es für die Zivilgesellschaft die Chance, abweichende Perspektiven abseits der rein ökonomischen stark zu machen?

Es gibt ja schon eine kritische Diskussion um den Einsatz von KI, z.B. die Diskriminierungspotenziale durch verzerrte Trainingsdaten. Bei der Blockchain wiederum herrscht Skepsis gegenüber der libertären Vorstellung, durch sie werde wirtschaftliche oder politische Macht eingegeben. Die kritischen Stimmen werden von der Wirtschaft durchaus gehört, wenn auch vielleicht nicht so interpretiert, wie sich viele das wünschen würden. Ich glaube, das zivilgesellschaftliche Potenzial liegt derzeit vor allem im Aufzeigen von Alternativen. Nicht alle Suchmaschinen, Plattformen und Expert_innensysteme folgen der gleichen Logik. Im Schatten der großen Anbieter gibt es immer Experimentierräume für das Andere und Unerwartete, das im Erfolgsfall dazu beiträgt, dem linearen und eigenlogisch verstandenen Fortschrittsdenken der Politik ein Schnippchen zu schlagen.

Prof. Dr. Jeanette Hofmann, Professorin für Internetpolitik an der Freien Universität Berlin, forscht am Wissenschaftszentrum Berlin für Sozialforschung (WZB) zu den Themen Global Governance, Regulierung des Internets und Digitaler Wandel. Sie ist außerdem Leiterin der WZB-Projektgruppe „Politik der Digitalisierung“, die die Deutung, Aushandlung und Regelung der digitalen Transformation erforscht. Von 2010 bis 2013 war sie Sachverständige in der Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestages. Im Jahr 2017 trug sie zur Gründung des Deutschen Internet-Instituts, dem Weizenbaum-Institut für die vernetzte Gesellschaft, bei.

Politische und inhaltliche Ebenen der Internetregulierung

Unter der Maßgabe, dass sich die Regulierung des Internets nicht auf die technische Administration der Netzwerkinfrastruktur beschränkt, sondern vielmehr auf alle vier Ebenen des Internets bezieht, lassen sich einige Aspekte identifizieren, die Gegenstand gegenwärtiger Internetregulierung sind.

Stabilität der Infrastruktur und Entwicklungszusammenarbeit

Auf technischer Seite geht es zunächst um den weiteren Ausbau und die Sicherung der Infrastruktur. Um als globales Kommunikationsnetzwerk zu funktionieren, muss das Internet zuverlässig und vertrauenswürdig ausgestaltet sein, wie es das 2014 im Anschluss an die genannte Konferenz in São Paulo veröffentlichte Multistakeholder-State-ment der NETmundial-Initiative formuliert hat. Hierbei kommt es insbesondere auch auf die Zusammenarbeit mit Ländern des globalen Südens beim Auf- und Ausbau der Infrastruktur an. Ziel muss es dabei sein, den sogenannten Digital Divide zwischen entwickelten und sich entwickelnden Ländern zu überwinden. Denn noch immer können sehr viele Menschen nicht auf das Internet zugreifen. Dadurch leiden die Mög-

lichkeiten dieser Gesellschaften, sich in wirtschaftlicher Hinsicht fortzuentwickeln. Ein freier und stabiler Zugang zum Netz kann zudem dafür sorgen, dass die Bürger_innen jener Länder Zugang zu mehr politischen Informationen haben, was sich positiv auf die Entwicklung demokratischer Strukturen auswirken kann.

Internet-Sicherheitspolitik

Sicherheitspolitische Anliegen haben in den vergangenen Jahren die Regulierung des Netzes auf internationaler und nationaler Ebene zunehmend geprägt. Hacker-Angriffe auf die Server des Deutschen Bundestags und die IT-Struktur von DAX-Konzernen, sowie die Diskussion um die Spionagegefahr durch den chinesischen Technologiekonzern Huawei beim 5G-Breitbandausbau haben die nationalen Geheimdienste zu Planungen für mögliche Abwehrstrategien und Gegenschläge (Hackbacks) mitangetrieben. Die Relevanz des Themas steigt, die damit verbundene Unsicherheit bezüglich geeigneter Maßnahmenkataloge auch. Eine Studie der Unternehmensberatung Deloitte von 2019, für die deutsche Führungskräfte und Mandatsträger_innen aus Bundestag, Landtagen und dem EU-Parlament befragt wurden, ergab, dass die Manipulation der öffentlichen Meinung durch gezielte Desinformation mittlerweile als wichtigstes Cyber-Risiko angesehen wird – noch vor

Datenbetrug im Internet (70 %), dem Diebstahl privater Daten bzw. Informationen durch Cyber-Angriffe (67 %) oder Computerviren und Schadsoftware (65 %).

Regulatorisch ist das Feld bereits sehr ausgebaut und umfasst nationale IT-Sicherheitsgesetze sowie diverse Richtlinien und Verordnungen auf EU-Ebene. Bei der UN sind im Bereich der Cybersicherheit zwei parallele Arbeitsgruppen eingesetzt worden: die von den USA initiierte UN Group of Governmental Experts (UNGGE) sowie die von Russland vorgeschlagene Open-Ended Working Group (OEWG). Beide sollen überprüfen, wie völkerrechtliche Prinzipien – z.B. das in Artikel 51 in der UN-Charta aufgeführte Recht auf Selbstverteidigung – auch im Internet angewendet werden können. Wenn gleich viele der düsteren Szenarien von tödlichen „Cyber-Kriegen“ bislang bloße Fiktion geblieben sind, gehen die meisten Expert_innen davon aus, dass über das Netz ausgetragene Konflikte zwischen Staaten ebenso wie zwischen Staaten und nichtstaatlichen politischen Gruppen in den kommenden Jahren weiterhin zunehmen werden.

Menschen- und Bürgerrechte im Netz

Darüber hinaus hat sich insbesondere das Thema Menschen- und Bürgerrechte als Handlungsfeld der Regulierung des Internets in den Vordergrund

Handlungsfelder der Internetregulierung:

Infrastruktur und
Entwicklungszusammenarbeit

Menschen- und
Bürgerrechte

Sicherheitspolitik

Rechtsentwicklung

geschoben. Als Katalysator der Debatte dienten hierbei in besonderem Maße die Enthüllungen des NSA-Whistleblowers Edward Snowden im Sommer 2013, die die internationale Öffentlichkeit für die Überwachungstätigkeit der Nachrichtendienste im Internet sensibilisierten. Die durch Snowden ans Licht gebrachten geheimen Dokumente zeigten, dass die Überwachung von Bürger_innen inzwischen eine völlig neue Dimension angenommen hat.

Das Recht auf Privatheit ist das Recht, auch online nicht willkürlich und permanent durch Regierungen und privatwirtschaftliche Akteure überwacht zu werden. Es ist im digitalen Zeitalter zum Abwehrrecht gegen die Datenaggregation und -auswertung von staatlicher oder unternehmerischer Seite geworden und wurde durch die Datenschutz-Grundverordnung der EU von 2018 in besonderer Weise gestützt.

Daneben treten noch weitere menschen- und bürgerrechtliche Prinzipien der Internetregulierung. Zu diesen Rechten gehören insbesondere die Meinungs- und Meinungsäußerungsfreiheit, die Versammlungs- und Vereinigungsfreiheit und die Informationsfreiheit. All diese Bürgerrechte sind im Internet in besonderer Weise gefährdet, vor allem in jenen Ländern mit autokratischen oder sonstigen nicht demokratisch-freiheitlichen Regimen.

Auch das Recht auf Zugang zum Netz sowie das damit verbundene Menschenrecht auf Entwicklung gilt es zu gewährleisten. Denn das Internet spielt eine entscheidende Rolle für die wirtschaftliche und soziale Entwicklung von Staaten und Gesellschaften. Wie kaum eine andere technologische Neuerung kann es beispielsweise Menschen in Armut helfen, sich aus dieser zu befreien.

Rechtsentwicklung

Als übergreifendes Handlungsfeld, das sich auf alle bisher genannten Aspekte bezieht, kann schließlich die Fortentwicklung des Rechts in Bezug auf das Internet gesehen werden. Zwar sind

sich die meisten Expert_innen darin einig, dass fast alle der für die „Offline-Welt“ geschaffenen Regeln auch im Internet Geltung beanspruchen können. Trotzdem weist das Netz insbesondere durch seine technische Beschaffenheit einige Besonderheiten auf, die eine bloße Übertragung der Normen schwierig machen. Deshalb erscheint es – jedenfalls in Teilbereichen – notwendig, neue bzw. angepasste Regeln zu schaffen.

Viele Beobachter_innen bezweifeln, dass es den Staaten in näherer Zukunft gelingt, ein völkerrechtliches Vertragsregime zu schaffen, das umfassend sämtliche rechtlichen Verhältnisse im Netz für alle Beteiligten und Stakeholder verbindlich regelt. Bisherige konkrete Vorschläge für Verträge, die insbesondere von der Russischen Föderation und der Volksrepublik China unterbreitet worden sind, erwiesen sich als unvereinbar mit den genannten Freiheitsrechten der Bürger_innen und standen daher im Konflikt mit bereits geltenden völkerrechtlichen Regeln. Sie wurden deshalb vom Großteil der Staatengemeinschaft zurückgewiesen. Trotzdem sollte die völkerrechtliche Ausgestaltung der Internetregulierung als Ziel nicht aufgegeben werden. Eine entsprechende Entwicklung kann einerseits durch die Entstehung von Gewohnheitsrecht – also ohne die Vereinbarung völkerrecht-

licher Abkommen – geschehen. Bei so entstandenen Regeln handelt es sich um gleichwertiges Völkerrecht. Andererseits ist nicht ausgeschlossen, dass politische Teilbereiche der Internetregulierung durch Verträge zwischen Staaten rechtlich gestaltet werden. Der erfolgreiche Abschluss der Budapester Konvention gegen Datennetzkriminalität hat beispielsweise bereits gezeigt, dass solche internationalen Abkommen zumindest für spezifische Felder des Internets sehr wohl im Bereich des Möglichen liegen.

Selbstverständlich sind völkerrechtliche Normen aber ohnehin nur ein Weg, die Rechtsentwicklung auf dem Feld der Internetregulierung voranzutreiben (s. dazu auch die FES-Publikation „Völkerrecht in Zeiten des Netzes“). Die verschiedenen Ansätze werden im nächsten Teil im Detail dargestellt.

Foto: Cayambe / CC-BY-SA-3.0



Regulierungsansätze und Gestaltungsmöglichkeiten



Alle Staaten und sonstigen Akteure der Internetregulierung sind sich darüber einig, dass das Internet als globale Kommunikationsstruktur internationaler Regulierung bedarf. Wie das geschehen soll und insbesondere durch wen, ist hingegen keineswegs geklärt. Im Folgenden werden verschiedene Ansätze der Internetregulierung anhand von Begriffspaaren vorgestellt. Dabei kommt es durchaus zu Überschneidungen zwischen den Paaren. Zum Beispiel ist der Multistakeholder-Ansatz eine bottom-up-Variante, die für gewöhnlich transnationalen Mechanismen folgt und zumeist zur Schaffung von Soft Law führt. Dennoch sind diese Begriffe keineswegs deckungsgleich. Zum besseren Verständnis der verschiedenen Ansätze der Regulierung des Internets ist eine getrennte Darstellung daher sinnvoll.

Intergouvernemental vs. Multistakeholder

Die beiden Grundansätze für die Regelungsfindung in Bezug auf das Internet sind die intergouvernementale Ebene auf der einen und der Multistakeholder-Ansatz auf der anderen Seite.

Regulierung auf zwischenstaatlicher Ebene

Intergouvernemental bedeutet, dass sich Staaten beziehungsweise deren Regierungen untereinander auf Regelungen verständigen. Dies ist der klassische Weg internationaler Politik – Staatenvertreter_innen kommen auf Konferenzen oder Gipfeln zusammen und besprechen die Problemlage in einem bestimmten politischen Handlungsfeld. Im Anschluss folgen Lösungsvorschläge und Verhandlungen darüber, wie diese Vorschläge in Regelungen gegossen werden können. Die meisten heute geltenden völkerrechtlichen Verträge sind auf diese Weise entstanden, so beispielsweise die Satzung der UN, das Seerechtsübereinkommen oder die Genfer Flüchtlingskonvention. Aber auch Resolutionen der UN-Generalversammlung oder des Sicherheitsrates kommen so zustande. Fast alle relevanten supranationalen Organisationen wie der Europarat, die Afrikanische Union oder die WTO arbeiten in diesem Modus. Auch der Funktionsweise der EU liegt dieses Modell zugrunde. Die Staaten haben hier die volle Kontrolle über das Verfahren der Regelsetzung sowie dessen Ausgang. Auf dem Feld der Internetregulierung ist an erster Stelle die ITU als Beispiel für das intergouvernementale Modell zu nennen.

Wer setzt die Regeln?



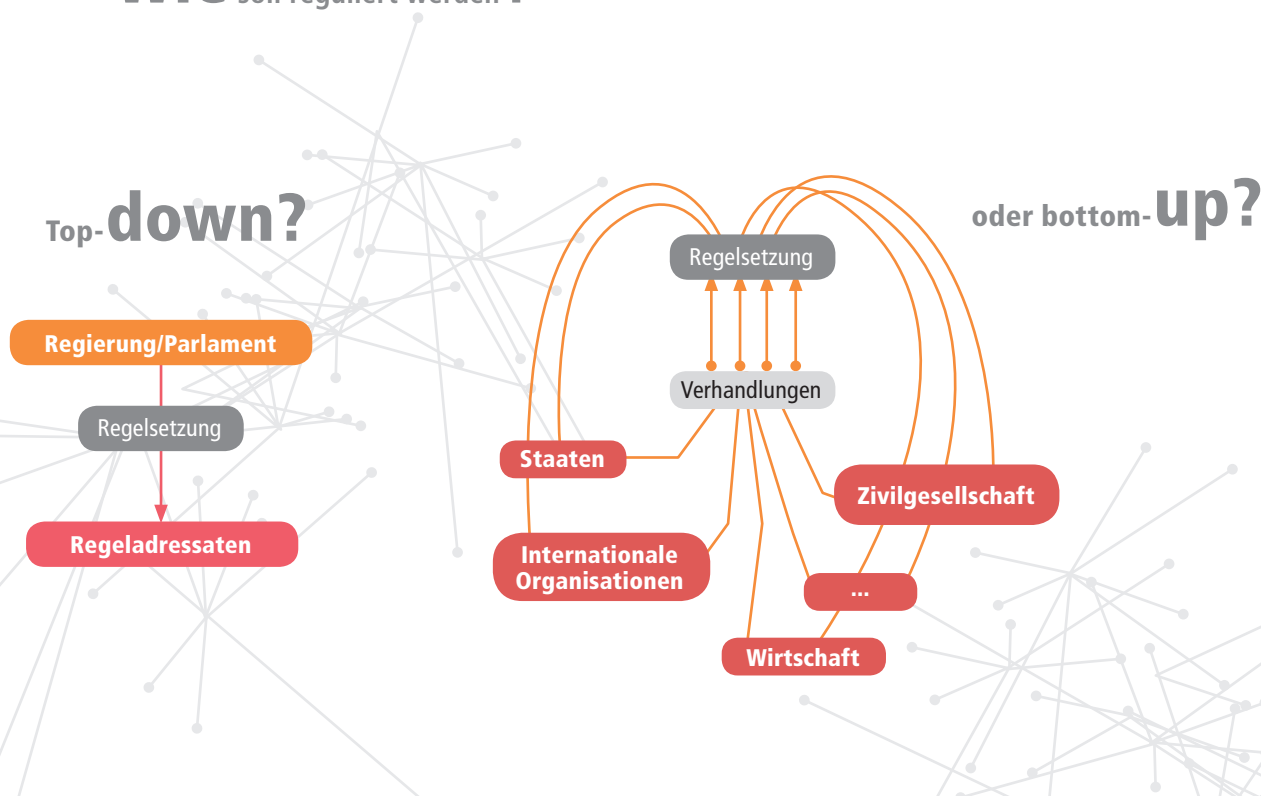
Das Multistakeholder-Modell: Einbeziehung aller Handelnden

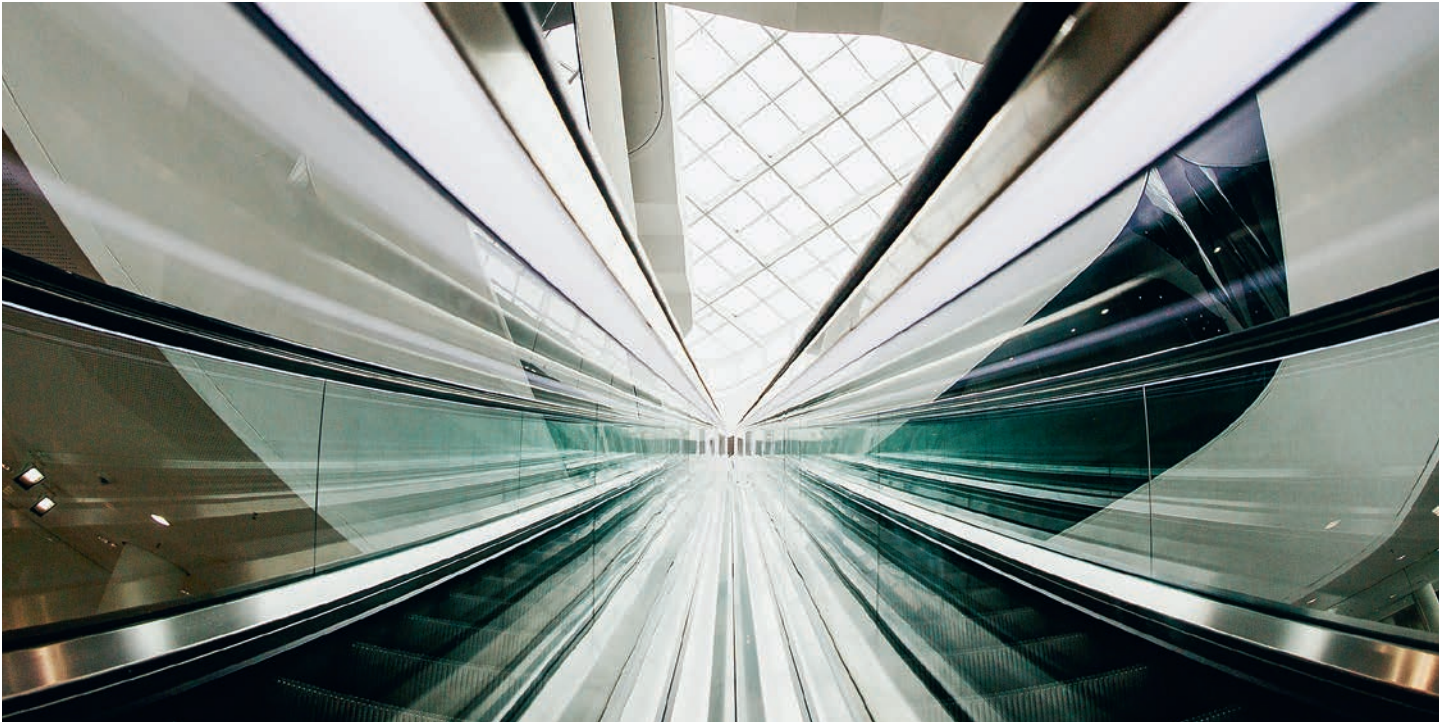
Der im Vergleich noch sehr junge Multistakeholder-Ansatz hingegen versucht, alle Akteure, die von einer Sachlage oder einem politischen Handlungsfeld betroffen sind, als gleichberechtigte Beteiligte in die Entscheidungsfindung einzubeziehen. Wer diese Stakeholder sind, ist von dem jeweiligen Politikfeld abhängig. Auf dem Gebiet der Internetregulierung sind hier insbesondere die Regierungen aller Staaten, die mit dem Internet befassten privatwirtschaftlichen Unternehmen, die Zivilgesellschaft und internationale Organisationen zu nennen. Das Multistakeholder-Modell war zum ersten Mal durch die Working Group on Internet Governance im Anschluss an den ersten Teil des Weltgipfels zur Informationsgesellschaft 2003 in Genf angeregt worden. Es sollte als Kompromiss zwischen den beiden Alternativen einer rein privatwirtschaftlichen und einer ausschließlich öffentlich-staatlichen Regulierung des Internets dienen. Heute wird dieser Ansatz sowohl bei der ICANN als auch beim Internet Governance Forum weiterverfolgt.

Ein fortwährender Streit

Während eine rein privatwirtschaftliche Verwaltung des globalen Netzes auch angesichts der ökonomischen Dominanz von US-amerikanischen IT-Unternehmen heute nicht mehr ernsthaft diskutiert wird, herrscht ein durchaus beachtlicher Disput darüber, welcher der beiden genannten Ansätze auf dem Gebiet der Internetregulierung letztlich zu bevorzugen ist. Während sich insbesondere die westlichen Staaten mit Nachdruck für das Multistakeholder-Modell aussprechen, möchte eine Gruppe von Staaten um die Länder China, Indien, Russland, Iran und Saudi-Arabien das Mandat der ITU auf die allgemeine Verwaltung des Internets ausweiten. Dieser Vorschlag war auf der ITU-Konferenz 2014 in Busan unterbreitet worden. Die genannten Staaten vertraten die Ansicht, dass eine internationale Organisation, die das intergouvernementale Modell verfolgt, am besten geeignet sei, ihre Interessen zu wahren. Gerade aber der Abstimmungsmodus in der ITU bereite den Vertreter_innen der westlichen Länder Unbehagen, da nicht-demokratische Regierungen pro-

Wie soll reguliert werden?





gressive Regelungen im Hinblick auf die Durchsetzung von Freiheitsrechten der Bürger_innen im Internet mit ihren Stimmen relativ leicht blockieren könnten.

Jedoch äußern nicht nur autoritäre Regimes Bedenken gegenüber dem Multistakeholder-Ansatz. Viele Regierungen von Ländern des globalen Südens haben angemerkt, dass die meisten der repräsentierten Stakeholder aus reichen Industrieländern stammen. Wer nicht die nötigen finanziellen Mittel aufbringen könne, um beispielsweise an den entsprechenden Veranstaltungen teilzunehmen, werde nicht ausreichend in den Multistakeholder-Prozess eingebunden. Entscheidungen, die alle Nutzer_innen des Internets betreffen, könnten so ohne die notwendige Repräsentation der ärmeren Staaten geschlossen werden, wodurch ihnen Nachteile entstehen könnten.

Regulierung von oben

Eng verknüpft mit dem soeben dargestellten Begriffspaar sind die zwei Ansätze zur Regelfindung, „top-down“

einerseits und „bottom-up“ andererseits. „Top-down“, wörtlich übersetzt „von oben nach unten“, sind solche Entscheidungsprozesse, die von einer übergeordneten, mit Autorität ausgestatteten Instanz durchgeführt werden. Das klassische Beispiel für solche Prozesse in der Politik sind Gesetze, die durch die gesetzgebende Gewalt – in Deutschland also Bundestag und Bundesrat – beschlossen werden. Die Bundesorgane haben zwar „von unten“ das Mandat zur Gesetzgebung verliehen bekommen, also durch die Bürger_innen in periodisch abgehaltenen Wahlen. Der eigentliche Prozess der Regelfindung findet jedoch in stark formalisierten Prozessen auf der Regierungsebene statt. Die beschlossenen Gesetze wirken dann lediglich „nach unten“ – an den eigentlichen Beschlüssen sind die Bürger_innen nicht direkt beteiligt. Dieses Modell, verbindliche Regeln zu schaffen, ist kennzeichnend für die repräsentative Demokratie. Auf dem Gebiet der Regulierung des Internets kommt es immer dort zum Tragen, wo die Staaten selbst und ausschließlich an den Entscheidungsprozessen beteiligt sind. Das gilt wiederum insbesondere für inter-

gouvernementale Foren und internationale Organisationen, in denen Normen erzeugt werden, die die Staaten und somit mittelbar deren Staatsbürger_innen binden und verpflichten. Für die Internetregulierung ist auch hier die Internationale Fernmeldeunion das typische Beispiel.

Der Multistakeholder-Ansatz als klassisches „bottom-up“

Im Gegensatz dazu ist „bottom-up“ der charakteristische Prozess des Multistakeholder-Ansatzes. Die an der Entscheidungsfindung beteiligten Stakeholder treten als gleichberechtigte Handelnde auf. Das bedeutet im Bereich der Internetregulierung, dass auch Vertreter_innen der Zivilgesellschaft oder der Wirtschaft unmittelbar Einfluss auf den Ausgang der Verhandlungen nehmen können, auch ohne vorherige Übertragung des Mandats auf demokratisch gewählte Vertreter_innen. Diese eher basisdemokratische Variante der Regelfindung hat den Vorteil, dass im Idealfall diejenigen, die von der Entscheidung betroffen sind, während des Prozesses

eine eigene Stimme bekommen. Kritisiert wird an dem Ansatz jedoch mitunter, dass auf diese Weise wirtschaftlich oder anderweitig stärkere Akteure einen unverhältnismäßig großen Einfluss bekommen könnten – eine Gefahr, die in der repräsentativen Demokratie jedenfalls gemindert sei. Zudem neige das letztlich beschlossene Regelwerk dazu, fragmentiert und mitunter in sich nicht widerspruchsfrei zu sein.

Multilateral oder bilateral?

Ein weiteres Begriffspaar, das mit den beiden bereits genannten eng verknüpft ist und sich eignet, Prozesse der Regelungsfindung auf dem Gebiet der Internetregulierung zu unterscheiden, ist „multilateral“ bzw. „bilateral“ auf der einen und „transnational“ auf der anderen Seite.

Multilateral oder bilateral sind Entscheidungsprozesse, die von Regierungen auf zwischenstaatlicher Ebene durchgeführt werden; entweder unter Beteiligung mehrerer Staaten wie bei internationalen Konferenzen oder innerhalb internationaler Organisationen oder aber auch lediglich zwischen zwei Staaten. Bilaterale Prozesse haben

meist den Abschluss eines zweiseitigen Abkommens zum Ziel. Aufgrund der globalen Struktur des Internets sind bilaterale Vereinbarungen, die sich konkret auf dem Gebiet der Internetregulierung bewegen (und beispielsweise nicht nur Fragen zwischenstaatlichen Infrastrukturausbaus im Grenzbereich betreffen), eher selten. Die entscheidenden Arrangements werden in multilateralen Foren ausgearbeitet – wiederum bietet die ITU hier ein gutes Beispiel.

Transnational: über- statt zwischenstaatlich

Als transnational bezeichnet man demgegenüber solche Prozesse, die nicht zwischen Staaten, wohl aber auf überstaatlicher Ebene stattfinden. Sie überschreiten staatliche Grenzen, ohne dass die Regierungen der Staaten allein das Heft in der Hand hätten. Es geht also erneut um die Einbeziehung zivilgesellschaftlicher Akteure in den Entscheidungsprozess. Die Multistakeholder-Modelle der ICANN und des IGF sind in diesem Sinne paradigmatische Beispiele für transnationale Mechanismen in der Internetregulierung. Zudem bietet sich kaum ein regelungsbedürftiges

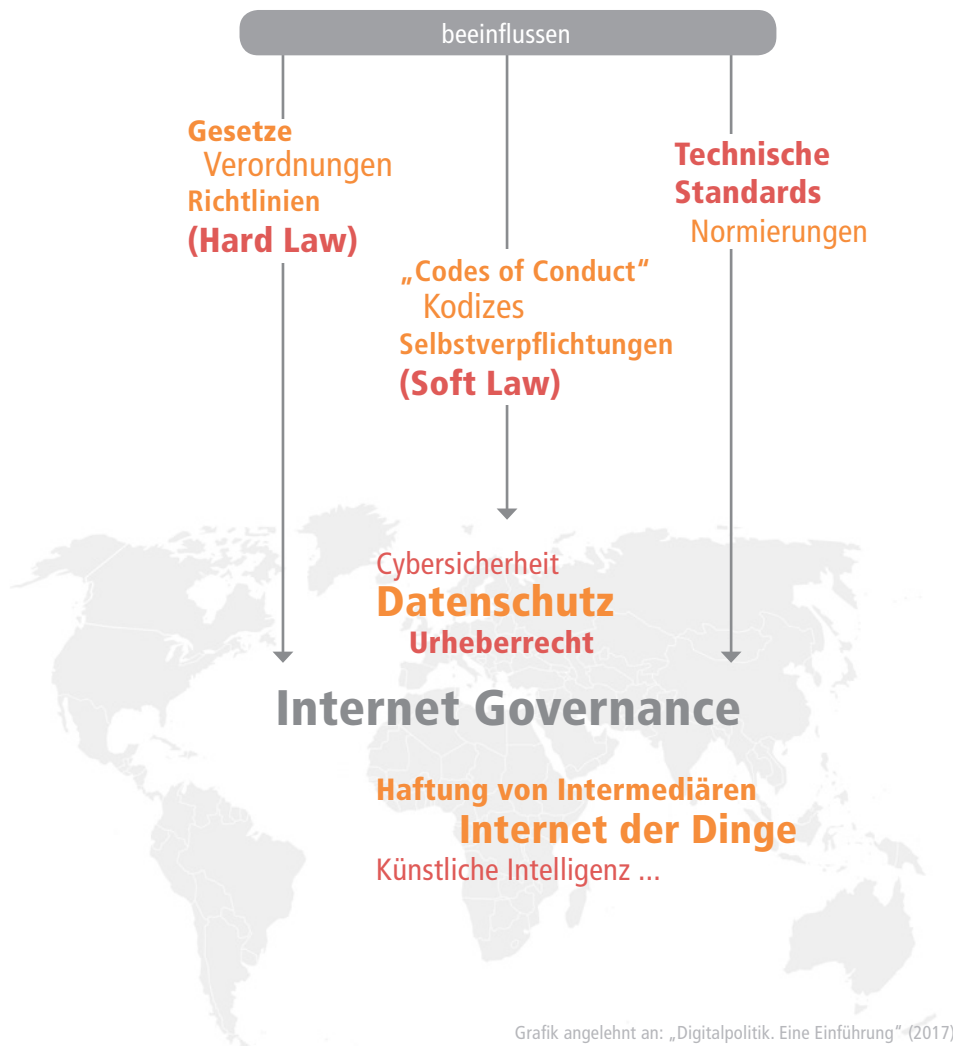
Umfeld mehr für den transnationalen Ansatz an als das Internet, ist es doch strukturell schon staatenübergreifend angelegt. Zwar spielen nationale Grenzen im Netz durchaus eine Rolle – etwa beim Geoblocking von territorial lizenzierten Streaming-Inhalten. Viele der Grundstrukturen des Internets sind aber transnational angelegt, so dass rein nationale Lösungen oft unzureichend bleiben müssen.

Hard Law vs. Soft Law

Schließlich können Regelungen auf dem Gebiet der Verwaltung des Internets entweder dem sogenannten „Hard Law“ oder aber dem „Soft Law“ zuzuordnen sein. Unter Hard Law werden alle diejenigen Normen verstanden, die als eigentliches, „echtes“ Recht zu definieren sind. Das bedeutet, dass sie die jeweiligen Normadressaten tatsächlich zu einem bestimmten Handeln zwingen können beziehungsweise dazu, bestimmte Handlungen zu unterlassen. Dieser Zwang ist auf verschiedenen Wegen durchsetzbar. Die Verurteilung durch ein Gericht ist die naheliegende,



Prinzipien, Stellungnahmen, Resolutionen



durchgesetzt werden können. Gerade auf internationaler Ebene ist Soft Law sehr häufig anzutreffen. Viele Konferenzen oder sonstige Zusammentreffen von Staatenvertreter_innen enden nicht mit verbindlichen Beschlüssen oder gar völkerrechtlichen Verträgen, sondern mit Absichtserklärungen oder Grundsatzvereinbarungen, die einen Konsens zum Ausdruck bringen, ohne dass daraus auch konkretes, anwendbares Recht entstehen würde. Aber auch Resolutionen der UN-Generalversammlung sind zum Beispiel hier einzuordnen. Ihnen fehlt, im Gegensatz zu Resolutionen des Sicherheitsrates, der Zwangscharakter.

Die Vorteile des Soft Law

Gerade auch aufgrund solcher fundamental unterschiedlicher Wertvorstellungen haben unverbindliche Regelwerke häufig weit höhere Chancen, zum Abschluss gebracht zu werden. Daraus sollte man jedoch gerade nicht folgern, dass Soft Law aufgrund seiner Unverbindlichkeit keinerlei Steuerungswirkung hätte. Oft wirken sich erst einmal vereinbarte Prinzipien nachhaltig auf die Handlungsweisen der Adressaten aus. Wenn sich die Regeln erst einmal etabliert haben und sich immer mehr Handelnde an ihnen orientieren und als bindend erachten, kann Soft Law sogar nach und nach Verbindlichkeit erlangen und somit zu Hard Law werden.

aber keineswegs einzige Variante. Gerade bei völkerrechtlichen Regelungen gibt es oft keine gerichtliche Instanz, die für deren Durchsetzung zuständig ist. Daraus folgt aber gerade nicht, dass es sich bei diesen Normen nicht um Hard Law handelt. Verstöße gegen eine Regel sind eben auch auf andere Weise sanktionsfähig, zum Beispiel durch einen Beschluss des Sicherheitsrates der UN.

Um das Internet zu regulieren, bedarf es durchaus einer Vielzahl von Verträgen, Gesetzen und sonstiger Regelungen, die dem Hard Law zuzuordnen sind. Ein Beispiel für einen völkerrechtlichen Vertrag auf dem Gebiet der Regulierung des Internets ist das bereits genannte Budapestener Übereinkommen zu Computerkriminalität, das im Jahr 2001 im Rahmen des Europarates zustande

gekommen ist und eine Reihe von Regeln zur internationalen Bekämpfung von Cyberkriminalität aufstellt. Bemerkenswert an dem Abkommen ist zudem, dass es zwar unter der Federführung des Europarates entstanden, aber dennoch offen in dem Sinne ist, dass auch solche Staaten den Vertrag unterzeichnen können, die nicht Mitglied dieser internationalen Organisation sind. So haben sich bis heute beispielsweise auch die Vereinigten Staaten, Kanada, Japan oder Israel dem Übereinkommen angeschlossen und die darin enthaltenen Regelungen als für sich verbindlich erklärt.

Soft Law hingegen bezeichnet solche Übereinkünfte oder Erklärungen, die zwar Handlungsanweisungen für die Adressaten des Dokuments beinhalten, darüber hinaus aber nicht zwingend

Akteure im Bereich der Internetregulierung



Viele unterschiedliche Akteure tummeln sich auf dem Feld der Internetregulierung. Das hat der vorangegangene Abschnitt bereits gezeigt. Vor allem, wenn man sich dem Multistakeholder-Modell zuwendet, ist es unausweichlich, auch zu untersuchen und zu benennen, wer denn eigentlich die Stakeholder des Internets sind, die bei Fragen der Regulierung Beachtung finden und beteiligt werden sollten. Die wichtigsten werden daher im Folgenden vorgestellt.

Staaten

Als grenzüberschreitende und tatsächlich globale technische Struktur ist das Internet in jedem Land auf staatliche Regulierung angewiesen. Für Internetnutzer_innen gelten stets die Gesetze und sonstigen Regeln desjenigen Landes, in dem sie sich befinden, wenn sie online gehen. Jeder Staat schafft insofern zunächst einmal für sein eigenes Staatsgebiet die für die Internetregulierung spezifischen Gesetze.

Darüber hinaus werden auch die grenzüberschreitenden Internet-Infrastrukturen wie beispielsweise die großen transatlantischen Unterseekabel für den interkontinentalen Datenverkehr von den beteiligten Staaten in Zusammenarbeit bereitgestellt und unterhalten.

Befürworter_innen des intergouvernementalen Modells sehen die Staaten – zusammen mit den internationalen Organisationen, die jedoch erst durch die Staaten und mit ihnen als Mitglieder überhaupt gebildet werden – als allein verantwortlich für die Verwaltung des Internets an. Aber auch die Anhänger_innen des Multistakeholder-Ansatzes gehen für gewöhnlich wie selbstverständlich davon aus, dass die Staaten wichtige Anspruchsgruppen bilden. Abgesandte der Staaten sitzen also im Regelfall mit am Tisch, wenn über Internetregulierung diskutiert wird. Das gilt zum Beispiel für Sitzungen des Advisory Committee der ICANN ebenso wie für Tagungen des IGF.

Zivilgesellschaftliche Akteure

Innerhalb Deutschlands existiert eine Reihe von Interessenverbänden, Think Tanks und Nichtregierungsorganisationen (NGO), die sich im Bereich der Internetregulierung engagieren und als zivilgesellschaftliche Stakeholder identifiziert werden können. Dazu gehören beispielsweise die deutsche Sektion der Internet Society, der Chaos Computer Club oder die Digitale Gesellschaft. Diese gemeinnützigen Vereine befassen sich mit allgemeinen politischen Fragen des Internets und bringen sich in die Debatten beispielsweise dadurch ein, dass sie Studien erstellen, Expert_innenrunden ausrichten oder öffentlichkeitswirksame Aktionen durchführen. Als europäische NGO-Dachorganisation in Brüssel betätigt sich European Digital Rights (EDRi), deren historische Wurzeln vor allem bei Datenschutz- und Überwachungsthemen liegen. In den letzten Jahren haben sich auch die nationalen Sektionen und Freiwilligen-Communities von Wikimedia und der Open Knowledge Foundation immer wieder zu politischen Fragen rund um Freies Wissen und Urheberrecht zu Wort gemeldet.

Vielfalt nimmt zu

Eine kampagnenfähige NGO ist Access Now, die sich vor allem für Meinungsfreiheit, Verschlüsselungstechnologien und Netzneutralität einsetzt. Sie arbeitet auch mit Telekommunikationsunternehmen beim Thema Transparenzberichterstattung zusammen. Die ebenfalls amerikanische Electronic Frontier Foundation, die in Brüssel ein Verbindungsbüro unterhält, geht gerichtlich gegen Verstöße gegen Verbraucher_innenrechte oder die Privatsphäre von Internetnutzer_innen vor. Diese Form der strategischen Prozessführung gehört auch in Deutschland zum Repertoire von NGOs, etwa bei der Gesellschaft für Freiheitsrechte.



Foto: ICANN 2019 Montreal, icannphotos / CC BY-SA 2.0

Daneben sind aber auch Akteure zu nennen, die nicht spezifisch auf Themen des Internets fokussiert sind. Internationale NGOs wie Amnesty International oder Human Rights Watch beispielsweise haben es sich zur Aufgabe gemacht, die Einhaltung der Menschen- und Bürgerrechte im Netz zu überwachen, zu analysieren und einzuordnen – und Alarm zu schlagen, wenn sich die Lage in bestimmten Staaten verschlechtert. Zudem gibt der Washingtoner Think Tank Freedom House den jährlichen Bericht „Freedom on the Net“ („Freiheit im Netz“) heraus, der den weltweiten Status der Freiheit im Internet zusammenfasst und bewertet. Initiativen aus dem Globalen Süden wie z.B. das Centre for Internet & Society oder IT for Change, beide im indischen Bengaluru beheimatet, kümmern sich selbstverständlich ebenso um Fragen der Internet Governance und die Auswirkungen technologischer Innovationen auf demokratische Gesellschaften.

Akteure der Privatwirtschaft

Neben den zivilgesellschaftlichen Akteuren sind auch Unternehmen der Privatwirtschaft sowie ihre Interessenverbände unzweifelhaft Stakeholder der Verwaltung des Netzes. Schließlich liegen die Infrastrukturen des modernen Internets größtenteils und in den meisten Staaten in privater Hand. Das gilt für Zugangsprovider – in Deutschland zum Beispiel die Deutsche Telekom, 1&1 Drillisch oder Vodafone – ebenso wie für große Internetunternehmen wie Google, Facebook oder Amazon. Sie alle haben ein Interesse daran, bei Fragen der Regulierung des Netzes mit am Tisch zu sitzen. Auch die privatwirtschaftlichen Interessenverbände – in Deutschland z.B. der Bitkom oder eco – nehmen an den Prozessen der Internetregulierung teil.

Besonders große und wichtige private Player, die aufgrund ihrer wirtschaftlichen Stellung eine herausragende Bedeutung für die Nutzung des Internets besitzen, sind mitunter selbst und unmittelbar mit Fragen in Teilbereichen der Internetregulierung konfrontiert, die sie entweder aus Eigeninitiative oder infolge von staatlichen Interventionen wie Gerichtsentscheidungen oder Beschlüssen von Kartellbehörden autonom zu regeln haben. So wies der Europäische Gerichtshof Google im Mai 2014 an, das sogenannte „Recht auf Vergessenwerden“ zu implementieren, also Suchergebnisse, die das Recht auf Privatheit von Einzelpersonen verletzen, auf Antrag aus dem Index zu entfernen. Google rief daraufhin ein Advisory Council ins Leben, in dem zwei Vertreter der Geschäftsführung und acht externe Expert_innen (u.a. Wikipedia-Gründer Jimmy Wales und die ehemalige deutsche Justizministerin Sabine Leutheusser-Schnarrenberger) Richtlinien für die Löschpraxis erarbeiten sollten und in schwierigen Einzelfällen hinzugezogen wurden. Im September 2019 machte der Europäische Gerichtshof in einer Folgeentscheidung klar, dass Google nur EU-weit auslisten müsse. Hierbei zeigte sich einmal mehr der Widerspruch zwischen territorial begründeten Rechtskulturen und dem Versuch der Internet Governance, universelle Regeln und allgemeine Verfahrenssicherheit zu schaffen.

Regulierte Selbstregulierung

In Deutschland gab es anlässlich der Verabschiedung des Netzwerkdurchsetzungsgesetzes (2017) eine Kontroverse darum, ob die darin verankerten starren Lösfristen und hohen Bußgelder für soziale Plattformen nicht am Ende dazu führen könnten, dass diese die als problematisch identifizierte Beiträge im Zweifelsfall lieber direkt entfernen, um den schwierigen Prozessen einer Feststellung der Verletzung der Menschenwürde oder der Abwägung zwischen Meinungsfreiheit und Ehrschutz zu entgehen.



Foto: James Gridland - Crowd / CC BY 2.0

Drei Fragen an Ioannis Kouvakas

Legal Officer bei Privacy International in London



Foto: Privat

„Niemand hat Zeit, täglich hunderte Einwilligungserklärungen zu lesen“

Datenmissbrauchsskandale werden in den Medien vor allem anhand großer Internet-Plattformen diskutiert. Ist dieser Fokus Ihrer Ansicht nach gerechtfertigt?

Ioannis Kouvakas: Ja und nein. Im Allgemeinen konzentriert sich die öffentliche Aufmerksamkeit auf große Unternehmen wie Google, Facebook und Amazon, und vielleicht noch um ihre chinesischen Konkurrenten Tencent, Alibaba und Baidu – und das zu Recht. Diese Firmen sind alle in den letzten Jahren unglaublich groß und mächtig geworden. Der Sicherheitsexperte Bruce Schneier hat es einmal schön formuliert: „Bei jedem Artikel über Facebooks unangenehmes Stalker-Verhalten seufzen Tausende von anderen Unternehmen gemeinsam vor Erleichterung auf; darüber, dass Facebook – und nicht sie selbst – im Rampenlicht steht. Facebook ist zwar einer der größten Player in diesem Bereich, jedoch gibt es unzählige andere Unternehmen, die uns für Profit ausspionieren und manipulieren.“ Auch aus diesem Grund haben wir im November 2018 Beschwerden gegen Datenhändler und sogenannte AdTech-Firmen eingereicht.

Die Enthüllungen rund um Cambridge Analytica haben die internationale Öffentlichkeit dafür sensibilisiert, dass Wahlen durch Datenanalysen und Microtargeting hochgradig zu beeinflussen sind. Kann uns die europäische Datenschutz-Grundverordnung (DSGVO) davor schützen?

Es ist wichtig, hier zwei Aspekte zu beachten. Erstens ist die so genannte DSGVO nicht neu. Ja, sie bringt ein höheres Niveau an Transparenz, schafft strengere Garantien für die Zustimmung der Nutzer_innen und die Kontrolle ihrer personenbezogenen Daten und sieht strengere Geldbußen vor. Es ist jedoch nicht das erste Datenschutzinstrument. Der Datenschutz war schon lange vorher vorhanden, und die Datenschutzgesetze in Europa wurden bereits vor Jahrzehnten verabschiedet. Mit anderen Worten: Der Schutz der personenbezogenen Daten der Nutzer_innen ist gegeben, nicht nur wegen der DSGVO, sondern auch wegen einer Reihe anderer oder früherer Rechtsinstrumente.

Zweitens sollten wir, wie bei den anderen Instrumenten, nicht vergessen, dass die DSGVO lediglich ein Gesetz ist – eine Verordnung, um genauer zu sein. Und obwohl sie darauf abzielt, den Schutz personenbezogener Daten zu harmonisieren, obliegt es den Regulierungsbehörden, die Rechte der Nutzer_innen durchzusetzen und zu wahren. Mit anderen Worten, das Gesetz ist nichts ohne seine Durchsetzung. Die lokalen Datenschutzbehörden müssen ihre Befugnisse ausüben und diese Methoden der Datenverarbeitung verurteilen.

Welche Möglichkeiten haben Verbraucher_innen, ihre Privatsphäre gegen den technologisch immer weiter verfeinerten Datenkapitalismus zu schützen?

Wir leben in turbulenten Zeiten – viele Menschen wissen nicht, ob und wie sie ihre Miete bezahlen sollen, ob sie morgen noch einen Job, oder ein Bleiberecht haben. Niemand hat Zeit, täglich hunderte Einwilligungserklärungen zu lesen. Für den Einzelnen ist es derzeit extrem schwierig nachzuvollziehen, was mit den eigenen Daten geschieht, aber ohne starke Datenrechte wird es fast unmöglich, einflussreiche Unternehmen zur Rechenschaft zu ziehen. Datenrechte schützen nicht nur Daten. Sie helfen auch dabei, die Machtungleichgewichte zwischen Menschen, dem Staat und dem Markt auszubalancieren – eine Beziehung, die derzeit durch große Asymmetrien geprägt ist.

Ioannis Kouvakas ist als Jurist bei Privacy International (PI) tätig und arbeitet an einer Vielzahl von Projekten an der Schnittstelle von staatlicher bzw. kommerzieller Überwachung und Datenmissbrauch. Seine Interessen umfassen nationale Sicherheit, Cybersicherheit, Datenschutz, Technologie und Menschenrechte. Bevor er zu PI kam, arbeitete er als Jurist für noyb (europäisches Zentrum für digitale Rechte) und für die Europäische Agentur für Grundrechte (FRA) in Wien.

Drei Fragen an Dr. Matthias C. Kettemann

Rechtswissenschaftler und Spezialist für die normative Ordnung des Internets

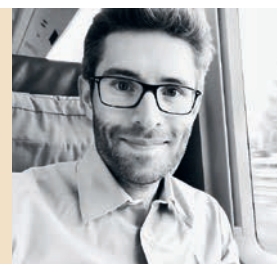


Foto: Privat

„Die kooperative Stoßrichtung ist vielversprechend“

Ist unsere demokratische Öffentlichkeit überhaupt noch ohne sogenannte Informationsintermediäre wie Facebook oder Twitter denkbar?

Matthias C. Kettemann: Ganz zweifellos stellen Informationsintermediäre wichtige Kommunikationsräume zur Verfügung, in denen Beiträge zur öffentlichen Debatte geleistet werden. Besonders die – zumindest in interessierten Kreisen – wahrnehmbare Präsenz einzelner Politiker_innen auf sozialen Medien ermöglicht eine neue Intensität der Interaktion. Koordinierte politische Aktivität, die dann auch offline Ergebnisse zeitigt – man denke an die #metoo- und die Fridays for Future-Bewegungen –, wird durch Online-Kommunikation stark befördert.

Entscheidend sind allerdings auch die sozialen Praktiken und das wirkliche Mediennutzungsverhalten der Menschen. Der Reuters Institute Digital News Report 2019 für Deutschland hat etwa gezeigt, dass auch internetaffine Bevölkerungsteile überwiegend andere Quellen nutzen, um sich zu informieren. Wie auch bisher ist das Fernsehen für 45 Prozent der erwachsenen Internetnutzer_innen die Hauptquelle für Nachrichteninformationen. Nur ein verschwindender Anteil informiert sich ausschließlich online.

Wie könnte man – unterhalb der Schwelle einer gesetzlichen Regelung und jenseits intransparenter Filterpraktiken – die Informationsintermediäre dazu bewegen, verantwortlicher mit ihrer kuratierenden Rolle zwischen Fakten, Behauptungen und Rezipient_innen umzugehen?

Viele Intermediäre würden sich nicht als Kuratoren von Meinungen sehen, da sie sonst sehr schnell in die redaktionelle Verantwortung kämen und ab Kenntnis der Inhalte in Haftung genommen werden könnten. Ihre Algorithmen und Regeln, die bestimmen, welche Inhalte von wem wie gesehen werden können, müssen sich auf Menschenrechte und Grundwerte gründen. Dies kann auch über effektive (regulierte) Selbstregulierungsmechanismen geschehen. Den Rahmen hierzu gab etwa der Europarat, der 2018 über die Empfehlung des Ministerkomitees zu Rolle und Verantwortlichkeiten von Internet-Dienstleistern wichtige Leitlinien für die künftige Ausgestaltung von Regeln für soziale Netzwerke setzte. Besonders der Schutz der Integrität von Wahlen und die Bekämpfung von

Hassrede haben innerhalb der EU zu einem Verhaltenskodex zur Selbstregulierung großer Anbieter geführt. Wenn dieser auch mangels klarer Erfüllungskriterien und Selbstkontrollmechanismen defizitär scheint, ist die normative Stoßrichtung, in Feldern, in denen bindendes Recht alleine die gewünschten Ziele nicht erreichen kann, durch kooperative Regulierungsansätze einzugreifen, prinzipiell vielversprechend.

Gegenwärtig sprechen wir über die Einhegung von Desinformation und Hassrede, weil wir sie als potenziell demokratiegefährdend ansehen. Müssten sich die unterschiedlichen Governance-Akteure dabei nicht verstärken um die Normbildung zu KI und algorithmischen Entscheidungssystemen kümmern?

Es ist empirisch nicht belegt, dass Desinformationen und Hassrede eine Gefahr für „die Demokratie“ darstellen. Gefährlicher sind die Verschiebungen von gesellschaftlichen Referenzrahmen, die Desensibilisierung der politischen Kultur, die Attraktivität antiaufklärerischen Verhaltens und die Nutzung menschenverachtender Terminologie durch Politiker_innen. Diesen Entwicklungen kann alleine durch die stärkere Reglementierung des Einsatzes von Algorithmen bei Intermediären nicht Einhalt geboten werden. Zwar sind komplexe Algorithmen nicht einfach steuerbar, doch haben sich zumindest einzelne Intermediäre dazu bekannt, algorithmisch gesteuert der menschlichen Tendenz entgegenzuwirken, sich mit „Borderline“-Inhalten stark zu beschäftigen (was letztlich dazu führte, dass diese Inhalte oft empfohlen wurden). Im Feld der normativen Steuerung von Algorithmen liegt zurzeit angesichts der Vielzahl von Erklärungen zur ethisch sensiblen Gestaltung von Algorithmen eher das Problem des Standardisierungsüberschwangs vor. Zu viele Normen können auch schaden, wenn nicht klar ist, welche Regulierung individuelle Freiheitsräume schützt und gesellschaftlichen Zusammenhalt fördert.

Dr. Matthias C. Kettemann, LL.M. (Harvard) ist Leiter des Forschungsprogramms „Regelungsstrukturen und Regelbildung in digitalen Kommunikationsräumen“ am Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), Hamburg, sowie Vertretungsprofessor für Öffentliches Recht, Völkerrecht und Menschenrechte an der Universität Heidelberg.

Diese (betriebswirtschaftliche) Handlungsweise wird nicht nur von Netzaktivist_innen als faktisch private Gerichtsbarkeit angesehen. Viele Beobachter_innen befürchten gar einen sogenannten „chilling effect“ (auf Deutsch etwa: entmutigende Wirkung) auf die Freiheit der Meinungsäußerung, sobald immer mehr Nutzer_innen von kritischen Äußerungen im Netz absehen und sich somit in der Ausübung ihrer Grundrechte vorseilend selbstbeschränken.

Auch wenn sich die Gefahr eines solchen „Overblockings“ in der ersten Umsetzungsphase empirisch nicht bestätigen ließ, wurde zwei Jahre nach Inkrafttreten des Gesetzes im Rahmen der Evaluierung erneut darüber diskutiert, ob es im Falle einer Löschung rechtskonformer Inhalte nicht auch ein „Pull-Back-Verfahren“ geben müsse, um den äusserungsrechtlichen Ansprüchen der Geschädigten zu genügen. Zudem wurde die reine Löschung von Inhalten, die Officialdelikte wie z.B. Volksverhetzung oder eine Morddrohung darstellen, als ungenügend kritisiert. In der Folge hat die Große Koalition neben weiteren Änderungen und Klarstellungen auch die Festschreibung einer Meldepflicht an Strafverfolgungsbehörden im Gesetz angekündigt (Stand 11/2019).

Ein Grundproblem, das sich bei der Rechtsdurchsetzung stellt, ist allerdings das Leerlaufen von Auskunftsansprüchen bei erwiesenen Straftaten, da sich die Firmensitze von Facebook und Co. zumeist außerhalb Europas befinden und auf die entsprechenden Rechtshilfeabkommen verweisen. Auch hier hat die Große Koalition eine gesetzliche Klarstellung der Auskunftsverpflichtung angekündigt. Zudem hat die EU-Kommission eine Revision der europäischen Rechtsgrundlagen der e-Commerce-Richtlinie in einem Digital-Service-Act angekündigt (Stand 11/2019). Es ist deshalb davon auszugehen, dass eine verschärfte Plattformhaftung für Hetze und Hassrede mit entsprechenden Auskunftsverpflichtungen ein regulatorischer Konfliktpunkt zwischen den USA und der EU bleiben wird, auch im Kontext der Beratungen der europäischen e-

Evidence-Richtlinie und des amerikanischen Cloud-Acts.

Diskutiert wird im Rahmen der Evaluierung des NetzDG auch eine Weiterentwicklung der Vorgaben hinsichtlich der regulierten Selbstregulierung. Das hier angewandte Grundprinzip ist das einer gesetzlichen Rahmensetzung für die Selbstverpflichtung von Unternehmen, die sogenannte regulierte Selbstregulierung. Dieses Prinzip kommt auch in anderen Politikfeldern zum Einsatz. Im Kontext der Internet Governance lässt sich bereits beobachten, dass kommerzielle Anbieter einen verbindlichen Kodex für ihre Plattformen entwickeln und bei Verstößen zu Maßnahmen greifen, die dann vonseiten einer unabhängigen Aufsicht regelmäßig überprüft werden. In diesem Zusammenhang wurde Mark Zuckerbergs öffentliche Ankündigung einer Verschärfung der hauseigenen „Community Standards“ und der Einsetzung eines unabhängigen Beirats im November 2018 zwar als Schritt in die richtige Richtung begrüßt, gleichzeitig aber als weitere Maßnahme zur Privatisierung der Rechtedurchsetzung kritisch bewertet.

Inter- und supranationale Organisationen

Neben den für Telekommunikation im Allgemeinen oder das Internet im Speziellen ins Leben gerufenen Organisationen, die auf inter- oder transnationalen Ebene angeordnet sind, spielen auch weitere inter- und supranationale Organisationen eine Rolle bei der Regulierung des Internets.

Die Rolle der UN

Die Vereinten Nationen wiederum haben seit Anfang des 21. Jahrhunderts, nachdem die weltweit herausragende Rolle des Internets für das zivile, wirtschaftliche und politische Leben nach und nach offensichtlich geworden war, versucht, eine Vorreiterrolle bei der Internetregulierung einzunehmen. Auf Initiative der Organisation wurde der Weltgipfel zur Informationsgesellschaft (WSIS) in zwei Teilen in Genf (2003) und Tunis (2005) ausgerichtet.



Foto: ITU, R. Farrell / CC BY-SA 2.0

Im Anschluss an die Zusammenkunft in Genf ernannte der damalige UN-Generalsekretär Kofi Annan die Arbeitsgruppe zur Internet Governance (WGIG), die Grundsatzfragen zum Politikfeld klären und Vorschläge für das weitere Vorgehen erarbeiten sollte. Die Ergebnisse der Arbeitsgruppe wurden anschließend in Tunis erörtert. Der zwei-

te Teil des Gipfels führte zur Gründung des IGF, mit dem Ziel, den Diskurs zur Regulierung des Internets zu formalisieren und zu verstetigen.

Aber auch innerhalb der UN selbst spielen Fragen der Regulierung des Internets immer wieder eine Rolle. Besonders hervorzuheben ist in diesem Zusammenhang die von Deutschland

zusammen mit Brasilien im Dezember 2013 in die UN-Generalversammlung eingebrachte Resolution „Das Recht auf Privatheit im digitalen Zeitalter“. Sie stellte als Reaktion auf den NSA-Skandal nach den Enthüllungen des Whistleblowers Edward Snowden in erster Linie klar, dass die Privatsphäre des Individuums auch im Internet vor willkürlichen

Drei Fragen an Moez Chakchouk

stellvertretender Generaldirektor der UNESCO



Foto: Nizarus / CC BY 2.0

„Das Internet ist viel mehr als Infrastruktur und Anwendungen“

Wie ist das Selbstverständnis der UNESCO als Akteurin, was multilaterale Fragen der Internet Governance angeht?

Moez Chakchouk: Die UNESCO erkennt das Potenzial des Internets zur Förderung einer nachhaltigen menschlichen Entwicklung und zum Aufbau inklusiver Wissensgesellschaften sowie zur Verbesserung des freien Informations- und Ideenflusses in der ganzen Welt an. Die UNESCO hat zusammen mit der Internationalen Fernmeldeunion (ITU) auch die Breitbandkommission für digitale Entwicklung ins Leben gerufen. Ziel der Kommission ist es, Strategien zur Beschleunigung des weltweiten Ausbaus von Breitbanddiensten zu definieren und Anwendungen zu untersuchen, mit denen Breitbandnetze die Bereitstellung einer Vielzahl von sozialen Diensten verbessern können, von Gesundheitsdiensten über Bildung bis hin zu Umweltmanagement, Sicherheit und vielem mehr.

Der Ansatz der UNESCO zur Internet Governance basiert auf ihrem universellen Rahmen für das Internet. Internetuniversalität ist ein Konzept, das von der UNESCO im Jahr 2015 angenommen wurde, um die Positionen der Organisation zum Internet zusammenzufassen. Das Konzept erkennt an, dass das Internet viel mehr ist als Infrastruktur und Anwendungen. Es ist ein Netzwerk von wirtschaftlichen und sozialen Interaktionen und Beziehungen, welches das Potenzial aufweist, die Menschenrechte durchzusetzen, Einzelpersonen und Gemeinschaften zu stärken und eine nachhaltige Entwicklung zu erleichtern. Das Konzept basiert auf vier Grundsätzen, nach denen das Internet menschenrechtsbasiert, offen und barrierefrei sein und auf der Beteiligung von vielen Interessengruppen

beruhen sollte. Diese Grundsätze werden als R-O-A-M-Prinzipien (Anm. Akronym aus den Bestandteilen Rights-based, Openness, Accessibility, Multistakeholder participation) abgekürzt. Wenn Sie das Internet auf diese Weise verstehen, können Sie verschiedene Facetten der Internetentwicklung zusammenfassen, die sich mit Technologie, Verwaltungshandeln, Recht und Entwicklung befassen. Durch das Konzept der Internetuniversalität hebt die UNESCO vier getrennte, aber voneinander abhängige Bereiche der Internetpolitik und -praxis hervor, die als „Schlüssel“ für die Bewertung einer besseren Internetumgebung gelten: Zugang zu Informationen und Wissen, Meinungsfreiheit, Datenschutz, ethischen Normen und Verhaltensweisen im Netz.

Der Weltgipfel zur Informationsgesellschaft (WSIS) in Tunis 2005 bedeutete für viele Beobachter_innen eine Initialzündung für die tiefere Beschäftigung mit netzpolitischen Fragen. Bräuchten wir neben dem IGF nicht noch mehr internationale Gesprächsformate für Themen wie Datenschutz und freien Zugang zu Informationen?

Eines der eben genannten Prinzipien des Konzepts der Internetuniversalität bezieht sich auf die Beteiligung von vielen Anspruchsgruppen als wesentliches Element, um den erfolgreichen Aufbau einer auf Menschen ausgerichteten, inklusiven und entwicklungsorientierten Informationsgesellschaft sicherzustellen. Die UNESCO fördert die Entwicklung von Multi-Stakeholder-Prozessen auf nationaler, regionaler und internationaler Ebene, um über den Ausbau

oder sonst ungerechtfertigten staatlichen Eingriffen zu schützen ist.

Das Bestreben, den Multilateralismus in Fragen der Internetregulierung zu stärken, ist der UN in letzter Zeit wieder deutlicher anzumerken. So legte das Generalsekretariat im Sommer 2019 den Bericht „The Age of Digital Interdependence“ vor, der die ein-

jährige Arbeit einer internationalen Expert_innengruppe zusammenfasst. Darin reklamiert die UN selbstbewusst ihre einzigartige Rolle und Befugnis, unterschiedliche Anspruchsgruppen zusammenzubringen und gemeinsam die Normen und Rahmenbedingungen zu schaffen, die eine gerechte digitale Zukunft für alle Menschen gewährleis-

tet. Dieser Anspruch wird im Bericht mit Handlungsempfehlungen und unterschiedlichen Modellen untermauert, wie das Multistakeholder-Modell künftig weiterentwickelt werden könnte. Mit ihren Unterorganisationen könnte die UN tatsächlich wesentlich dazu beitragen, die globale Einhaltung der globalen Nachhaltigkeitsziele (Sustainable Development Goals) bei der digitalen Produktionsweise zu überwachen sowie weitere Normsetzungsprozesse etwa im Bereich Cybersicherheit anzustoßen.

und die Verbreitung des Internets zu diskutieren und dabei zusammenzuarbeiten. Der „International Day for the Universal Access to Information“ alljährlich am 28. September ist eine wichtige Gelegenheit, um Fragen des universellen Zugangs zu Informationen zu erörtern. Er fördert unter anderem das Bewusstsein, dass das Recht auf Informationen von wesentlicher Bedeutung für eine transparente und verantwortliche Regierungsführung und eine Voraussetzung für die Beteiligung der Öffentlichkeit an der Formulierung von Sozialpolitiken und den Entscheidungsprozessen ist.

Wie erleben Sie das Wissensgefälle, was die technische Infrastruktur des Internets angeht?

Infrastruktur- und Technologieentwicklung sind wesentliche Elemente beim Aufbau von Wissensgesellschaften, da Ungleichheiten beim Zugang zu Informationsquellen, -inhalten und -infrastrukturen den globalen Charakter der Informationsgesellschaft in Frage stellen und folglich das Wachstum von Wissensgesellschaften behindern. In Bezug auf die technische Infrastruktur besteht eine Wissenslücke, weshalb die UNESCO das Konzept der Medien- und Informationskompetenz fördert, das auch Fähigkeiten und Kenntnisse im Zusammenhang mit dem Internet umfasst. Das Programm „Information für alle“ (IFAP) setzt sich für ein erweitertes Wissen über eine Reihe von Medien und anderen Informationsstrukturen wie das Internet ein. Die Richtlinien und Strategien der UNESCO für Medien- und Informationskompetenz befürworten auch ein grundlegendes Informationskompetenz-Training, das sich an Jugendliche und Erwachsene an weiterführenden Schulen richtet.

Moez Chakchouk ist stellvertretender Generaldirektor der Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur (UNESCO) sowie Leiter der Kommunikations- und Informationssektion, die auch für die Verwaltung des Internets, die allgemeine Medienentwicklung und die Entwicklung der Künstlichen Intelligenz zuständig ist. Der international anerkannte IKT-Experte ist Ingenieur, studierte in Paris und Tunis und war Spitzenbeamter im tunesischen öffentlichen Sektor. Zuvor war er Vorstandsvorsitzender und CEO der tunesischen Post.

OECD und WTO

Weitere internationale Organisationen, die in diesem Zusammenhang hervorzuheben wären, sind die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) sowie die WTO. Unter der Ägide der 1995 gegründeten WTO ist unter anderem das Übereinkommen zur Informationstechnologie (ITA) geschaffen worden, das fast den gesamten Welthandel mit IT-Produkten in Bezug auf Zölle und Handelshemmnisse reguliert, was jedenfalls mittelbar der Internetregulierung zugeordnet werden kann. Das Allgemeine Abkommen über den Handel mit Dienstleistungen (GATS) der WTO wiederum regelt auch grenzüberschreitende Dienstleistungen im Bereich der Telekommunikation.

Die OECD hat sich verschiedentlich mit Themen der Regulierung des Internets befasst. Bereits 2010 wurden im OECD-Bericht „The Economic and Social Role of Internet Intermediaries“ wegweisende Definitionen und Einschätzungen zum heute allgegenwärtigen digitalen „Plattform-Kapitalismus“ abgegeben. Bei der Ministerkonferenz der Organisation im Juni 2019 in Paris stand denn auch vor allem die digitale Wettbewerbspolitik auf der Agenda.

Die EU

Die Europäische Union ist in unterschiedlichen Handlungsfeldern der Regulierung des Internets aktiv, vor allem

durch ihr gesetzgeberisches Handeln in Bezug auf den europäischen Binnenmarkt. Hervorzuheben ist in diesem Zusammenhang die Digitale Agenda für Europa aus dem Jahr 2010, die den inhaltlichen Bezugsrahmen dafür bildet. So ist denn auch in den letzten Jahren das Bemühen der EU Kommission um ordnungspolitische Eingriffe und Harmonisierungsschritte immer deutlicher hervorgetreten. Dabei wurde die wirtschaftspolitische Optik der Mitgliedstaaten im Rat des öfteren durch eine stärker auf Verbraucher_inneninteressen und Beteiligungsrechte hin orientierte Sichtweise des Parlaments ausbalanciert. Die wichtigsten einschlägigen Rechtsakte aus den letzten Jahren waren die Datenschutz-Grundverordnung (2018), die Urheberrechtsrichtlinie (2019) sowie die noch in der Diskussion befindliche e-Privacy-Verordnung. Die neue Kommission unter Führung der deutschen Präsidentin Ursula von der Leyen hat mit der digitalpolitischen Kompetenzzuweisung an die dänische Wettbewerbskom-

missarin Margrethe Vestager das Zeichen gesetzt, dass weitere Regulierungsschritte folgen werden, etwa bei der Ausarbeitung der geplanten Plattformgesetzgebung („Digital Services Act“) oder beim Thema Digitalsteuer, das intern für einige Kontroversen sorgen dürfte.

International Telecommunication Union (ITU)

Die Internationale Fernmeldeunion, die bereits 1865 unter dem Namen Internationaler Telegraphenverein gegründet wurde, ist seit 1947 eine Sonderorganisation der UN mit Sitz in Genf. Ihr Mandat umfasst in erster Linie die technischen Aspekte der Telekommunikation. Dazu gehört beispielsweise die globale Koordination der Verteilung der Radiofrequenzen, die internationale Kooperation in Bezug auf



Foto: ITU, D. Woldu / CC BY-SA 2.0

Drei Fragen an Laura-Kristine Krause

Co-Vorsitzende von D64 und Geschäftsführerin von More in Common



Foto: Privat

„Den größten Hebel sehe ich auf europäischer Ebene“

Gibt es eigentlich ein spezifisch sozialdemokratisches Augenmerk auf bestimmte Aspekte der Internetregulierung?

Laura-Kristine Krause: Freiheit, Gerechtigkeit, Solidarität – all das sind Werte, die auch und gerade im Internetzeitalter zu wahren sind. Deshalb ist ein sozialdemokratisches Augenmerk auf Digitalisierung sehr wichtig, bedeutet aber auch, dass neu verhandelt werden muss, was die Wahrung dieser Werte in der Praxis bedeutet. Denn eine digitalisierte Welt braucht in Teilen neue Rezepte und Ansätze, um diese alten (aber hochaktuellen!) Werte zu verwirklichen.

Das gilt zum Beispiel für das gesellschaftliche Miteinander in einer digitalen Gesellschaft und den Umgang mit einem digitalen Kapitalismus, aber besonders für die digitalisierte Arbeitswelt: Die Digitalisierung erlaubt Menschen eine größere Flexibilität und Eigenständigkeit in ihrer Erwerbstätigkeit und lässt zum Beispiel mit Solo-Selbstständigkeiten etwas zur Normalität werden, was auf den ersten Blick wie ein Rückschritt hinter sozialdemokratische Errungenschaften wirken mag. Aufgabe von Sozialdemokratie ist es aber sicherzustellen, dass soziale Standards gewahrt bleiben, ohne sich gegen gesellschaftliche Veränderungen zu sperren.

Was sollte Deutschland Ihrer Meinung nach tun, um eine möglichst breite Teilhabe an den Diskussionen um die Zukunft des Internets sicherzustellen?

In erster Linie sollte die Zukunft des Internets noch viel selbstverständlicher im Rahmen von fachpolitischen Debatten mitgedacht werden. Viel zu oft noch werden digitalpolitische Fragen „separat“ unter Digitalpolitiker_innen diskutiert, anstatt als Teil von Zukunftsdebatten in den jeweiligen fachpolitischen Strängen mitbearbeitet zu werden. Hinsichtlich der möglichst breiten Teilhabe von Menschen an diesen Diskussionen ist es außerdem wichtig, Zukunftsdebatten zur Digitalisierung nicht als technisch-abstrakte Debatten aufzubauen, die möglicherweise abschreckend wirken, sondern als das, was sie im Grunde sind: wichtige Beiträge zu unserer aller Zukunft, zur Zukunft unserer Gesellschaft und zur Zukunft unseres Wohlstandes.

Glauben Sie angesichts der Globalität des Internets an die Wirksamkeit nationalstaatlicher Einzelgesetze, die – zumindest potenziell – einen Wettbewerb um die besten Lösungen in Gang setzen können?

Natürlich ist es wichtig, Regulierungsansätze zu digitalpolitischen Fragen auch auf nationalstaatlicher Ebene zu verfolgen, allerdings immer mit besonderem Blick darauf, was sinnvoll ist und tatsächlich die Chance hat, die avisierten Ziele zu erreichen. Den potenziell größten Hebel für einen Wettstreit um die besten Lösungen sehe ich nicht auf der nationalstaatlichen, sondern auf der europäischen Ebene, da hier das Potenzial besteht, aufgrund der Größe des digitalen Binnenmarktes tatsächlich prägende und richtungsweisende Dinge auf den Weg zu bringen. Bestes Beispiel dafür ist die in Deutschland ja wenig geschätzte Datenschutz-Grundverordnung, die aufgrund ihrer Wirkbreite einen Regulierungsmaßstab weit über die Grenzen der EU gesetzt hat, an den sich auch zahlreiche Akteure zum Beispiel in den USA nun halten. Um diese Rolle der EU als „Pionierreguliererin“ aber tatsächlich zu stärken und auszubauen, wäre es aber nötig, dass sich nationalstaatliche Regulierer noch viel stärker konstruktiv an den digitalpolitischen Debatten auf EU-Ebene beteiligen. Hier ist – gerade was den Wettbewerb um beste Lösungen angeht – noch viel Luft nach oben, wie auch die Verabschiedung der EU-Urheberrechtsrichtlinie gezeigt hat.

Laura-Kristine Krause ist Co-Vorsitzende des SPD-nahen Think Tanks D64 – Zentrum für digitalen Fortschritt. Daneben ist sie ehrenamtliches Mitglied des Landesrats für Digitalisierung und Kultur des Landes Rheinland-Pfalz und des Digitalbeirats Brandenburg. Hauptberuflich ist Krause Gründungsgeschäftsführerin von More in Common Deutschland. Zuvor war sie als Programmleiterin des Think Tanks Das Progressive Zentrum und als Senior Associate bei einer Strategieberatung tätig. Frühere berufliche Stationen absolvierte sie u.a. im Wahlkampfteam von Hillary Clinton.

die Umlaufbahnen der Telekommunikationssatelliten, die Entwicklung weltweiter technischer Standards oder auch die Koordination der Zusammenarbeit mit Ländern des globalen Südens beim Ausbau ihrer kommunikationstechnischen Infrastruktur. Der Organisation steht seit 2015 der Chinese Houlin Zhao als Generalsekretär vor.

Die ITU steht allen Staaten offen und hat 193 Mitglieder. Obwohl neben den Staaten selbst auch private Unternehmen und Organisationen wie Netzbetreiber, Hersteller technischer Geräte oder auch Forscherverbände Mitglied werden können, folgt die ITU dem intergouvernementalen Modell und nicht dem Multistake-

holder-Ansatz. Die nichtstaatlichen Mitglieder haben lediglich beratenden und beobachtenden Status, sind jedoch nicht stimmberechtigt. Abstimmungen erfolgen im Normalfall nach dem Mehrheitsprinzip. Oberstes Organ der ITU ist die Konferenz der Regierungsbevollmächtigten, die alle vier Jahre stattfindet.

Drei Fragen an Prof. em. Wolfgang Kleinwächter

Deutscher Doyen des Themas Internet Governance



Foto: republica / CC BY-SA 2.0

„Es gibt keine Alternative zu einem kollektiven Ansatz“

Inwieweit steht der „digitale Autoritarismus“, der sich etwa in Ländern wie China oder Russland zeigt, im Gegensatz zu den Ambitionen der UN, neue Architekturen für eine globale digitale Zusammenarbeit zu schaffen?

Wolfgang Kleinwächter: Die neue Komplexität der Internet-Governance spiegelt den politischen Mainstream Ende der 2010er Jahre wider: Der digitale Neo-Nationalismus wächst. The Freedom House hat seinen Jahresbericht 2018 mit dem Titel „The Rise of Digital Authoritarianism“ versehen. Immer mehr Regierungen betrachten globale internetbezogene politische Fragen hauptsächlich aus nationaler Sicht. Sie wollen den grenzüberschreitenden Datenfluss kontrollieren, da sie befürchten, dass die grenzenlose Kommunikation die nationale Sicherheit, die heimische digitale Wirtschaft oder die lokale Kultur untergräbt. Stichworte sind „Cyber-Souveränität“, „Nationale Internet-Segmente“ oder „Mein Land zuerst“. Ziel ist es, die Grenzen wieder einzuführen, die die Informationsrevolution beseitigt hatte, als TCP / IP- und DNS-basierte Netzwerke den gesamten Globus umfassten.

Viele Regierungen glauben nicht mehr an globale Lösungen zur Bekämpfung von Cyberterrorismus, grenzüberschreitender Cyberkriminalität oder digitaler Dominanz. Sie bevorzugen einseitige Aktionen innerhalb ihrer eigenen Gerichtsbarkeit. Russland hat ein staatlich kontrolliertes DNS aufgebaut, China filtert schädliche Inhalte. Iran, Saudi-Arabien und Indien führen strenge Gesetze zur Datenlokalisierung ein. Die USA schließen Huawei vom Aufbau von 5G-Netzwerken aus. Frankreich strebt eine digitale Digitalsteuer an. Deutschland drängt Facebook, gefälschte Nachrichten und Hassre-

den zu blockieren. Und Regierungen in vielen Entwicklungsländern setzen das gesamte Internet außer Betrieb, sobald etwas passiert, was ihnen nicht gefällt. 22 von 51 afrikanischen Staaten haben in den letzten fünf Jahren die Konnektivität unterbrochen.

Bedeutet das, dass wir Rückwärtsschritte machen und Barrieren wieder einführen, die durch die digitale Revolution eigentlich beseitigt wurden?

Ein fragmentiertes Internet würde den Wert des globalen Netzwerks verringern, zu Instabilität im Cyberspace führen, Innovation und Wirtschaftswachstum verringern, nationalen Protektionismus fördern, lokale Zensur und Überwachung anregen. Es würde Türen für neue Formen der Konfrontation zwischen nationalen Internet-Segmenten öffnen, einschließlich Netzwerkkriegen mit einer neuen Generation von Cyberwaffen. Heutzutage sehen einige Regierungen das globale Internet weniger als Chance für eine Win-Win-Situation, sondern eher als Nullsummenspiel mit Gewinner_innen und Verlierer_innen. Sie glauben, dass sie die nationale politische Stabilität gewinnen (und die lokale Macht stärken) können, wenn sie das Internet regulieren, indem sie die damit verbundenen wirtschaftlichen und sozialen Aktivitäten in ihrem Hoheitsgebiet einschränken. Aber dieser Ansatz hat eine Kehrseite. Die Wiedereinführung nationaler Grenzen in den globalen Cyberspace schafft nicht wirklich mehr Sicherheit. Sie führt zu einer Illusion von Kontrolle, entspricht jedoch nicht den Realitäten des Informationszeitalters. Wie bei der Umwelt löst isoliertes Handeln die globalen Probleme der Menschheit nicht.

Seit Anfang des Jahrhunderts hat sich die ITU darum bemüht, auf dem Gebiet der Regulierung des Internets Fuß zu fassen. So war sie eine der vier UN-Organisationen, die 2003 und 2005 den Weltgipfel zur Informationsgesellschaft ausrichtete. Trotzdem ist die Rolle der ITU bislang größtenteils auf technisch-infrastrukturelle Fragen beschränkt.

Die ITU als Haupt-verwalterin des Internets?

Auf Initiative von Russland, China und Indien wurden auf der Weltkonferenz zur internationalen Telekommunikation 2012 in Dubai erstmals konkrete Vorschläge zur Änderung des ITU-Gründungsvertrages unterbreitet, um

das Mandat der Organisation unter anderem auf jene Funktionen auszuweiten, die bislang von der ICANN übernommen worden waren. Die genannten Staaten brachten als Hauptargument die Sorge zum Ausdruck, die Vereinigten Staaten würden zu viel Einfluss auf die private kalifornische Organisation ausüben. Der Vertragsentwurf wurde nicht nur von den westlichen Ländern und vom Europäischen Parlament, sondern auch von Akteuren der Privatwirtschaft scharf kritisiert. So veröffentlichte beispielsweise Google eine Erklärung, die die Vorschläge als einen Angriff auf das freie und offene Internet verurteilte.

Auf der ITU-Konferenz 2014 im südkoreanischen Busan versuchten die genannten Staaten, das Mandat der Organisation entsprechend auszuweiten und sogar Themen wie das Recht auf Privatheit und staatliche Überwachungstätigkeit einzubeziehen. Die Vorhaben wurden von der Gruppe der westlichen Staaten unter Federführung der USA mit Verweis auf das befürwortete Multistakeholder-Prinzip verhindert. Bei der ITU-Konferenz 2018 in Dubai stellten die ITU-Mitgliedstaaten einen Fahrplan für 2020 bis 2023 auf und diskutierten vor allem über grundlegende Fragen des digitalen Wettbewerbs wie Marktzutrittsbarrieren oder Fusionskontrollen.

Der französische Präsident Macron hat beim IGF 2018 in Paris einen „innovativen Multilateralismus“ in Fragen der Internetregulation ausgerufen. Würde das nicht zwingend bedeuten, eine noch stärkere Einbeziehung von nicht-staatlichen Akteuren in den wichtigsten Foren der internationalen Politik – UN, WTO, G20 – zu sichern?

Das UN High Level Panel on Digital Cooperation spricht über das Zeitalter der digitalen Interdependenz. Interdependenz meint, dass kein Land mehr isoliert leben kann. Dies bedeutet auch, dass Lösungen nur durch eine verstärkte Zusammenarbeit aller Beteiligten, d.h. Regierungen, Unternehmen, Zivilgesellschaft und der technischen Community, gefunden werden können. Dies wiederum heißt, dass Lösungen nur gefunden werden können, wenn die Sektoren Cybersicherheit, digitaler Handel, Menschenrechte und Technologie – die vier Bereiche der digitalen Welt – miteinander verknüpft sind. Es gibt keine Alternative zu einem ganzheitlichen und kollektiven Ansatz. Innovativer Multilateralismus braucht Weisheit und Mut, aber vor allem politisch guten Willen, der in unserer Zeit selten geworden ist. Digitaler Unilateralismus bietet niedrig hängende Früchte. Aber diese Früchte sind vergiftet. Digitaler Unilateralismus kann die Aufrüstung des Cyberspace, digitale Handelskriege und massive Menschenrechtsverletzungen im Internet auslösen. Er kann die Stabilität im Cyberspace untergraben – ein Raum, der heute von mehr als der Hälfte der Menschheit genutzt wird. Der Cyberspace wurde vom Menschen gemacht. Für zukünftige Generationen ist der Cyberspace jedoch Teil des gemeinsamen Erbes der Menschheit, ihres Ökosystems als natürliche Umwelt. Und man sollte keinen Zweifel daran haben, dass Instabilität im Cyberspace genauso gefährlich ist wie der Klimawandel.

Wolfgang Kleinwächter ist emeritierter Professor für Internet Policy an der Universität Aarhus. Er ist Mitglied der Global Commission on Stability in Cyberspace, war Mitglied des ICANN Board (2013 bis 2015) und Sonderbotschafter der Net Mundial Initiative (2014 bis 2016). Außerdem berät er zahlreiche Gremien und Institutionen zum Thema Internet Governance und Sicherheit – darunter die Vereinten Nationen, das Internet Governance Forum und die EU.

Internet Corporation for Assigned Names and Numbers (ICANN)

Die ICANN wurde 1998 auf Initiative des US-amerikanischen Handelsministeriums gegründet. Ihr Sitz ist im kalifornischen Los Angeles. Sie ist eine private gemeinnützige Organisation, die im Auftrag des Handelsministeriums das Domain Name System des Internets verwaltet. Das DNS ist ein globales Netzwerk von Datenbanken, das die Domain Names und die ihnen zugeordneten IP-Adressen verzeichnet. Daher



Foto: Kranich, pixabay.com / CC0

wird das DNS auch als das Telefonbuch des Netzes bezeichnet.

Die ICANN untersteht keiner direkten staatlichen Kontrolle. Sie hat aber auch keine staatlichen Kompetenzen. Geltungskraft erlangen ihre Regelungen in Bezug auf das Netz daher, indem zivilrechtliche Verträge mit anderen Organisationen, vor allem in anderen Staaten, abgeschlossen werden. Wie bereits wiederholt angemerkt, ist die Organisation eines der Hauptbeispiele für das Multistakeholder-Modell. Zentrales Organ ist das 21-köpfige Board of Directors, das die wichtigen Entscheidungen nach Beratungen mit einem Komitee trifft. Es setzt sich aus Vertreter_innen von Regierungen von insgesamt 110 Staaten zusammen. An den Entscheidungsprozessen wirken darüber hinaus Vertreter_innen aus der Privatwirtschaft, der Tech-Community, der Wissenschaft und der Zivilgesellschaft mit.

Kompatibilität mit EU-Recht?

Kurz nach Inkrafttreten der europäischen Datenschutz-Grundverordnung (DSGVO) im Mai 2018 klagte die ICANN vor dem Landgericht Bonn gegen einen deutschen Domain-Registral. Es ging um die juristische Klärung, ob das Unternehmen weiterhin dazu verpflichtet werden könnte, vollständige administrative und technische Kontaktinformationen – sogenannte WHOIS-Daten – für neue Registrierungen zu sammeln, so wie dies grundsätzlich im Rahmen einer Registrar-Akkreditierung bei der ICANN vereinbart wird. Das Gericht stellte dazu fest, dass eine datensparsamere Handhabung ausreiche, um etwaigen Missbrauch zu verhindern. Zu der Frage, ob die von ICANN geforderte Datenübermittlungspraxis einen Verstoß gegen die DSGVO darstelle, äußerte das Gericht sich jedoch nicht. Daraufhin kündigte die ICANN an, die Gespräche mit der Europäischen Kommission und den europäischen Datenschutzbeauftragten im Hinblick auf die Integrität der WHOIS-Dienste fortzusetzen.

Internet Governance Forum (IGF)

Das Internet Governance Forum ist als der Inbegriff des Multistakeholder-Ansatzes auf dem Gebiet der Internetregulierung beschrieben worden. Gegründet im Jahr 2006 als Hauptergebnis der Weltgipfel zur Informationsgesellschaft 2003 und 2005, stellt das IGF das erste tatsächlich global ausgerichtete und verstetigte Forum für Debatten um die Regulierung des Netzes dar. Die Initiative der UN zur Gründung des IGF war auch dadurch motiviert, dass ein Gegengewicht zur von den USA dominierten ICANN geschaffen werden sollte. Im Gegensatz zur ICANN hat das IGF jedoch kein Mandat, um verbindliche Beschlüsse zu treffen.

Das IGF kommt zu jährlichen Treffen zusammen und lädt Vertreter_innen der Regierungen sowie der anderen oben aufgezählten Stakeholder ein, sich an den Diskussionen zur Regulierung des Internets zu beteiligen. Im November 2019 fand das IGF erstmalig in Deutschland statt.

Organisatorisch unterteilt sich das IGF in ein Sekretariat, das seinen Sitz in den UN-Gebäuden in Genf hat, und die Multistakeholder Advisory Group (MAG), die mit der Aufgabe betraut ist, die jährlichen Treffen organisatorisch und inhaltlich vorzubereiten. Dabei wird sie vom Sekretariat unterstützt. Die Gruppe kommt zu diesem Zweck dreimal jährlich für jeweils zwei Tage zusammen. Die MAG besteht heute aus insgesamt 56 Mitgliedern und setzt sich zusammen aus Vertreter_innen aller Stakeholder. Es wird versucht, in jedem Jahr ungefähr ein Drittel der Vertreter_innen aus jeder der einzelnen Stakeholder-Untergruppen auszutauschen. Daneben gibt es derzeit 17 regionale und subregionale IGFs. Das übergeordnete Ziel dieser Ableger ist die Schaffung zusätzlicher Dialogräume, in denen verschiedene Akteure Fragen zum Internet diskutieren können, die den Bedürfnissen ihrer jeweiligen Communities entsprechen. Einen dieser Gesprächs-

sammenhänge bildet der Europäische Dialog über Internet Governance (EuroDIG), der versucht, nationale Perspektiven zusammenzuführen und europäische Leitbilder und Haltungen zum Internet zu formen.

Institutionalisierung des Internet Governance Forum Deutschland

Seit Gründung des IGF wurden nationale Foren gegründet. Das deutsche Forum des IGF, das Internet Governance Forum Deutschland (IGF-D), besteht als lose Struktur seit 2008. Es fördert die offene Meinungsbildung im Sinne des Multistakeholder-Ansatzes und organisiert eine jährliche Konferenz, die die nationalen Akteure im Bereich der Internetregulierung zusammenbringt. Wie das internationale Forum hat es die Aufgabe, den Dialog bezüglich der Regulierung des Internets – nur eben auf nationaler Ebene – voranzutreiben.

Seit Anfang 2016 wird das IGF-D von einem Beirat begleitet und durch ein Sekretariat unterstützt. Der Beirat besteht aus Vertreter_innen aus Politik, Wissenschaft, Wirtschaft und Zivilgesellschaft. Er berät das IGF-D bei seiner Arbeit und stellt diese öffentlichkeitswirksam dar. Das Sekretariat ist in der Geschäftsstelle von Reporter ohne Grenzen angesiedelt.

Wohin geht die Entwicklung?

Die UN schlägt in ihrem Bericht „The Age of Interdependence“ drei Entwicklungspfade vor, wie eine geeignete Architektur für die globale digitale Kooperation aussehen könnte:

— Das Modell „IGF plus“ geht davon aus, dass die Einbindung von mehr Regierungs- und Unternehmensvertreter_innen zu konkreteren Ergebnissen führen würde, wenn man die Diskus-

sionsstränge entsprechend moderiert. Dazu könnten neue Gremien (Advisory Board, Trust Fund) und neue Funktionalitäten eingerichtet werden. Ein „Cooperation Accelerator“ soll die themenzentrierte Zusammenarbeit in einer Vielzahl von Institutionen, Organisationen und Prozessen beschleunigen, indem er Konvergenzpunkte zwischen bestehenden Koalitionen ermittelt und Fragen identifiziert, um die neue, möglichst multidisziplinäre Gruppen gebildet werden. Ein „Policy Incubator“ soll das derzeit fehlende Bindeglied zwischen den Dialogplattformen zur Ermittlung von Regelungslücken und

zu verstetigen. Ein „Network of Networks“ hätte demgegenüber die koordinierende Rolle, wiederkehrende Foren für den Austausch zu organisieren. Sobald Normen verfügbar sind, könnten die jeweiligen Regierungsbehörden Durchsetzungsmechanismen festlegen und diese als Blaupausen verwenden.

— Das Modell „Digital Commons Architecture“ orientiert sich an der Allmende-Bewegung, die Gemeingüter nach bestimmten Prinzipien schützen und aufrechterhalten möchte. Diese Perspektive wird zunehmend auch in datenethischen Debatten oder beim Thema KI in Stellung gebracht. Pro-

Drei Modelle für die globale digitale Kooperation schlägt die UN vor:

IGF plus Distributed Co-Governance- Architecture Digital Commons

den bestehenden politischen Entscheidungsgremien bilden, indem er die Diskussion in Schwung hält, ohne selbst rechtsverbindliche Entscheidungen treffen zu können.

— Das Modell „Distributed Co-Governance-Architecture“ will die erprobte Praxis horizontaler Netzwerke dazu nutzen, um die drei Stufen von Regelungsbedarf, Implementierung und Rechtsdurchsetzung voneinander zu entkoppeln und arbeitsteilig zu behandeln. Die selbstverwalteten, offenen „Digital Cooperation Networks“ sollen sich um die Gestaltung digitaler Normen kümmern. Die „Network Support Platforms“ dürfen sich dabei nicht inhaltlich einmischen, sondern lediglich die Netzwerke dabei unterstützen, effizient zu arbeiten und die Partizipation

zedural sollen diese Debatten durch „Multistakeholder Tracks“ und jährliche Treffen, unterstützt durch ein Sekretariat bei der UN, kanalisiert werden. Dieses Vorgehen legt keine technischen Lösungen fest, sondern schlägt lediglich Modelle und Standards für Verantwortlichkeiten vor. Es könnte potenziell auch die Sammlung und Diskussion von weltweiten Lösungswegen bei der Umsetzung bestehender Normen in bestimmten Bereichen befördern.

Die drei genannten Modelle weisen als Grundmuster das Multistakeholder-Prinzip auf und könnten flexibel miteinander kombiniert werden. Es wird interessant sein zu beobachten, ob diese Vorschläge ihren Niederschlag in der praktischen Ausgestaltung der Internet Governance finden.

Einschätzung und Ausblick





In immer schnelleren Zyklen verändern digitale Innovationen das Leben in unserer Gesellschaft. Neue Technologien aus dem Bereich des maschinellen Lernens und der KI oder Blockchain-Anwendungen stellen bisherige regulatorische Paradigmen auf den Prüfstand. Viele dieser Anwendungen wandern schnell in andere Sektoren – von Landwirtschaft, Bankenwesen, Klimaschutz über digitale Bildung, e-Government und e-Health bis hin zu intelligenten Verkehrs- und Energiesystemen.

Lösungen für gesellschaftliche Herausforderungen werden selten in abgegrenzten Wissenssilos gefunden. Das Nachdenken über die digitale Gesellschaft ist daher international, interdisziplinär und internet-basiert. Zumindest sollte es das sein. Die internationale Politik hat sich indes Höhenkamm-Events wie die alljährlichen Treffen in Davos geschaffen, um die großen Linien der Wirtschaftspolitik und Wettbewerbsbedingungen im Bereich der digitalen Wertschöpfung zu zeichnen. Dort wird deutlich: Im Hinblick auf das Internet befinden wir uns längst nicht mehr in einer regulatorischen Wüste, sondern in einem zunehmend kartierten Gebiet, in dem viele Claims bereits abgesteckt sind.

Internet Governance in all ihren Facetten war schon immer ein umkämpftes Terrain. Jahrelang drehte sich die Debatte um die Frage, ob die internationale Netzpolitik eher durch Multi-Stakeholder-Vereinbarungen oder multilaterale Verträge geregelt werden sollte. Der hohe Ausstoß nationaler Rechts-

vorschriften zu Cybersicherheit, Überwachung, Inhaltsfilterung oder der Besteuerung von datengetriebenen Unternehmen hat zu neuen Kontroversen geführt. Zur Bearbeitung dieser Konfliktlinien braucht es Akteure, die einander vertrauen und lösungsorientiert miteinander diskutieren. Und genau an dieser Stelle hakt es gegenwärtig.

Eine alte Debatte, neu entfacht

Die USA, die jahrzehntelang eine Vorreiterrolle für die Freiheit des Internets innehatte, hat unter der Trump-Regierung ihren „America First“-Ansatz in eine nationale Cyber-Strategie übersetzt. Diese Robustheit ähnelt der Haltung von China und Russland, die dem von Emmanuel Macron auf dem IGF 2018 geforderten „innovativen Multilateralismus“ einen neo-nationalistischen Unilateralismus entgegensetzen. „Diese globale Debatte“, schreibt Wolfgang Kleinwächter, „hat bereits Anfang der neunziger Jahre begonnen. Sie kreiste in den ersten Jahren um das Management kritischer Internetressourcen. Aber seit der Tunis-Agenda von 2005, die den Multistakeholder-Ansatz einführte, hat sich die Diskussion auf alle Bereiche der globalen Politikgestaltung ausgeweitet: von Sicherheit über Handel bis hin zu Menschenrechten. Vor 20 Jahren war das Internet ein technisches Problem mit politischen Auswirkungen. Jetzt ist es eine politische Frage mit einer technischen Komponente.“

**Das Nachdenken über die
digitale Gesellschaft
ist international,
interdisziplinär und
internet-basiert.**

Aus Sicht der Europäer_innen bildete der Fall Snowden eine Art „Realitätsschock“ (Sascha Lobo), in jedem Fall eine mentale Zäsur. Spätestens mit den NSA-Enthüllungen ist klar geworden, dass das freie und offene Internet eine Struktur darstellt, die immer neu erkämpft werden muss. Die erste mit und im Internet aufgewachsene Alterskohorte musste erkennen, dass das Leitbild einer informationellen Selbstbestimmung und damit die Abwesenheit von Zensur, Repression und Überwachung keine Selbstverständlichkeiten sind. Und so handelt sie, teilweise mit ganz analogen Mitteln: Jugendliche Europäer_innen gingen zu Hunderttausenden auf die Straße, um den Artikel 17 der EU-Urheberrechtsrichtlinie oder das Handelsabkommen ACTA zu bekämpfen, weil sie ihren Freiraum im Netz bedroht sahen. Eigentlich eine fruchtbare Zeit für Internet Governance, so möchte man meinen.

Kontrollverlust und Gestaltungsmut

Das Gegenstück zur Freiheit bildet die Angst vor Kontrollverlust. Und diese umfasst längst nicht mehr nur jene Industrien, deren Geschäftsmodelle im Zuge der Digitalisierung obsolet geworden sind. Auch diejenigen, die im Internet eine zweite, zusätzliche Schicht demokratischer Öffentlichkeit zu erkennen glaubten, sehen nun mit Sorge die Häufung von Desinformationskampagnen auf sozialen Plattformen. Der traditionelle Journalismus in redaktionellen Medien muss mit neuen Recherche- und Vermittlungsformen dagegenhalten, will er den Zeitenwechsel überstehen.

Alle Akteure der Internetregulierung sind aufgerufen, sich an der Quadratur des Kreises zu versuchen: der Versöhnung von Meinungs- und Informationsfreiheit mit der Verhinderung justiziabler Inhalte oder Falschbehauptungen. Diese komplexe Herausforderung könnte bereits mittelfristig zum Lackmustest der gerade erst erwachten digitalen Öffentlichkeit mit ihren inter-

aktiven Rückkanälen, Beschleunigungszwängen und Beteiligungsmöglichkeiten werden.

Zudem gilt es, die Diversität im Ökosystem des Internets zu erhalten. Die gegenwärtige Marktdominanz der US-amerikanischen „Gang of Four“ (Google, Amazon, Facebook, Apple) und dem alten Riesen Microsoft verbirgt den Blick darauf, dass es neben diesen „Kontinenten“ auch ganz andere viele kleine Inseln gibt, deren Gründungsidee nichts mit Datenaggregation und deren kommerzieller Verwertung zu tun hatte. Eigentlich ein Wunder, dass die spendenfinanzierte Online-Enzyklopädie Wikipedia sich bis heute unter den TOP 10 der meistbesuchten Internetseiten weltweit hält.

Das Multistakeholder-Modell ausbauen?

Tendenzen von autoritären Regimen wie China, das sich eine „Great Firewall“ für unliebsame Inhalte schuf, muss energisch widersprochen werden. Vor allem aber gilt es, die zugrundeliegende Struktur des Internet stabil zu halten und seine Aufspaltung in ein sogenanntes „Splinternet“, das durch geografische Grenzen verschiedener Länder aufgeteilt und durch lokale Gesetze reglementiert wird, zu vermeiden. Denn dies wäre unzweifelhaft das Ende seiner ursprünglich universalen Idee.

Die Kräfte für ein offenes und freies Internet sind nach wie vor vorhanden und wachsen sogar. Dies ist ablesbar am Wachstum der zivilgesellschaftlichen Akteure und auch den Bemühungen im privaten Sektor (mitsamt den politischen und unternehmensnahen Stiftungen), zu neuen Beteiligungsverfahren und erhöhter Transparenz zu kommen. Selbst die UN, deren Entscheidungskraft im Sicherheitsrat seit Jahren gelähmt ist, ruft zu neuen Initiativen auf. Im UN-Bericht „The Age of Interdependence“ heißt es:

„Eine effektive digitale Zusammenarbeit erfordert, dass der Multilateralismus trotz der gegenwärtigen Belastungen gestärkt wird. Dazu gehört auch,

dass der Multilateralismus durch Multistakeholderismus ergänzt wird – eine Zusammenarbeit, an der nicht nur Regierungen, sondern auch ein weitaus breiteres Spektrum anderer Akteure aus Zivilgesellschaft, Wissenschaft, Technologie und Privatsektor beteiligt sind. Wir müssen die unterschiedlichsten Stimmen einbringen, insbesondere aus Entwicklungsländern und traditionell marginalisierten Gruppen wie Frauen, Jugendlichen, Indigenen, ländlichen Bevölkerungsgruppen und älteren Menschen.“

Für die Beibehaltung des Multistakeholder-Modells sowohl bei der ICANN als auch in Diskussionsforen wie dem IGF sprechen also gute Gründe. Denn nur dieser Ansatz kann gewährleisten, dass die Stimmen der gesamten Netzcommunity Gehör finden. Transnationale Entscheidungsprozesse und Bottom-up-Regelsetzungsmechanismen entsprechen der diversifizierten Stakeholder-Struktur des Internets und werden den tatsächlichen Interessensgeflechten besser gerecht als multilaterale, allein durch Regierungen top-down oktroyierte Normsetzungen für die Regulierung des Netzes.

Glossar

ACTA (Anti-Counterfeiting Trade Agreement): ein geplantes multilaterales Handelsabkommen auf völkerrechtlicher Ebene, mit dem u.a. internationale Standards im Kampf gegen Produktpiraterie und Urheberrechtsverletzungen gesetzt werden sollten. Nach viralen Kampagnen im Internet und Massendemonstrationen in zahlreichen europäischen Städten lehnte das EU-Parlament ACTA im Juli 2012 mit großer Mehrheit ab.

Advocacy: Aktivität einer Person bzw. Gruppe, die darauf abzielt, Entscheidungen in politischen, wirtschaftlichen und sozialen Systemen und Institutionen indirekt – im Gegensatz zu direktem Lobbying – zu beeinflussen, indem Fakten und Botschaften zur Aufklärung der Öffentlichkeit genutzt werden. Instrumente dieser „Themenanwaltschaft“ durch NGOs oder Verbände können Medienkampagnen, Preise, öffentliche Auftritte oder Forschungsergebnisse sein.

Afrikanische Union (AU): Internationale Organisation mit Sitz in Addis Abeba (Äthiopien) und Johannesburg (Südafrika), die sich für die Kooperation der Staaten Afrikas einsetzt. Ihr gehören sämtliche Staaten des Kontinents mit Ausnahme Marokkos an.

Browser: Computerprogramm mit der Hauptaufgabe, Webseiten des World Wide Web auf dem Gerät des Endnutzers darzustellen. Webbrowser dienen als Benutzeroberfläche für die meisten Webanwendungen. Bekannte Browser sind Google Chrome, Microsoft Internet Explorer, Mozilla Firefox oder Apple Safari.

Confidence Building: bezeichnet in der internationalen Politik alle solchen Maßnahmen, die dem Zweck dienen, Spannungen zwischen Staaten abzubauen, die ansonsten die Gefahr politischer Krisen bis hin zu bewaffneten Konflikten in sich bergen würden.

Cyber-Angriff: bezeichnet als Oberbegriff sämtliche schädlichen Handlungen, die mittels Informationstechnologie im Cyberspace durchgeführt werden. Die Motive für Cyber-Angriffe können krimineller oder politischer Natur sein.

Cyber- oder Computerkriminalität: Gemeint sind diejenigen Straftaten, die sich entweder gegen Infrastrukturen der Informations- und Kommunikationstechnologie richten oder aber mit Hilfe dieser begangen werden. Die „Tatwaffen“ sind also ein Netzwerk sowie ein oder mehrere daran angeschlossene Computer.

Cyber-Sicherheit: Unter diesen Begriff lassen sich sämtliche Maßnahmen fassen, die dazu dienen sollen, Computer, Netzwerke und andere Infrastrukturen der Informations- und Kommunikationstechnologie vor Angriffen zu schützen.

Cyberspace: Der Begriff wird oft als Synonym für das Internet verwendet. Er ist aber weiter zu fassen als Metapher für die Gesamtheit des virtuellen Raums, in dem Kommunikation zwischen Computern beziehungsweise Computernetzwerken stattfindet.

Datenschutz-Grundverordnung (DSGVO): Rechtsakt der Europäischen Union, der am 25. Mai 2018 in sämtlichen Mitgliedstaaten wirksam wurde und die Regeln für die Verarbeitung personenbezogener Daten europaweit vereinheitlicht hat. Sie ersetzt die aus dem Jahr 1995 stammende Richtlinie 95/46/EG und sieht hohe Bußgelder bei etwaigen Verstößen gegen europäisches Datenschutzrecht vor. Durch das „Marktortprinzip“ wird festgeschrieben, dass auch außereuropäische Anbieter von Waren und Dienstleistungen wie z.B. Internetplattformen oder Cloud-Services, die innerhalb der EU agieren, automatisch der DSGVO unterliegen und ihre internen Verfahren und Policies dementsprechend anpassen müssen.

Digital Divide: Dieser Begriff stammt aus der Politikwissenschaft und bezeichnet eine wirtschaftliche oder soziale Ungleichheit im Hinblick auf den Zugang zu modernen Informations- und Kommunikationstechnologien. Dies kann sich sowohl auf Zustände zwischen unterschiedlichen Bevölkerungsgruppen und Regionen als auch auf Unterschiede zwischen Staaten beziehen.

Domain-Name: derjenige Teil einer Internetadresse (wie zum Beispiel `www.fes.de`), der die Adresse als einer bestimmten Domain identifiziert. Domains sind administrative Einheiten im Netzwerk, die auf verschiedenen Ebenen angesiedelt sein können. Das Beispiel zeigt, dass die Webseite der Friedrich-Ebert-Stiftung der Top-Level-Domain „.de“ angehört, also der Domain der höchsten Ebene, die Webseiten in Deutschland umfasst.

Domain Name System (DNS): Als eines der technischen Kernstücke der Internet-Infrastruktur ist es die Hauptaufgabe des DNS, die Domain-Namen in IP-Adressen zu übersetzen. Damit können Anfragen von Nutzer_innen in ihrem Webbrowser, die mittels Eingabe der Internetadresse erfolgen, einer ganz bestimmten IP-Adresse im Netzwerk zu geordnet werden.

Europarat: 1949 gegründete internationale Organisation, die 47 europäische Staaten als Mitglieder umfasst. Ihr Sitz ist das französische Straßburg. Sie dient der regionalen politischen Kooperation der Staaten Europas. Kernstück ist die im Rahmen des Europarats abgeschlossene Europäische Menschenrechtskonvention mit dem zugehörigen Europäischen Menschenrechtsgerichtshof.

GATS-Abkommen: das Allgemeine Abkommen über den Handel mit Dienstleistungen (englisch „General Agreement on Trade in Services“, GATS), ein internationales Abkommen, das im Rahmen der WTO geschlossen wurde. Es regelt den grenzüberschreitenden Handel mit Dienstleistungen und zielt darauf ab, diesen zu liberalisieren.

Geoblocking: im Internet eingesetzte Technologie, mittels derer bestimmte Inhalte in festgelegten geografischen Gebieten gesperrt werden können. So ist es beispielsweise in Deutschland nicht möglich, bestimmte Videos auf der Plattform YouTube anzuschauen, obwohl diese in Dänemark oder Polen frei verfügbar sind.

Hackivismus: zusammengesetzt aus „Hacking“ und „Aktivismus“. Der Begriff bezeichnet politischen Aktivismus, der mithilfe von Computern und Netzwerken durchgeführt wird.

Informationsintermediäre: Netzwerkplattformen, Suchmaschinen und andere Dienste, die Informationen im Internet sammeln, strukturieren und gewichten. Insofern erbringen sie eine zentrale Funktion für die Auffindbarkeit von Inhalten im Netz. Für Nutzer_innen bieten sie wertvolle Orientierung, faktisch agieren sie aber auch als vorselektierende Filter. Die dabei zum Einsatz kommenden algorithmischen Systeme sind Gegenstand einer breiten Debatte, insbesondere im Zusammenhang mit der Verbreitung von Desinformation in den sozialen Medien.

Internet: weltumspannendes System, das verschiedene Computernetzwerke miteinander verbindet. Auf diese Weise kann jeder an das Internet angeschlossene Computer mit jedem anderen kommunizieren. Die wichtigsten Anwendungen, die über das Internet ausgeführt werden können, sind das World Wide Web sowie E-Mail- oder Telefondienste.

Internet-Protokoll (IP): das Netzwerkprotokoll, das die Grundlage des Internets bildet. Es ermöglicht, dass Datenpakete von einem ans Netzwerk angeschlossenen Computer zu einem bestimmten anderen gesendet werden können.

IP-Adresse: die jedem ans Internet angeschlossenen Computer individuell zugewiesene Adresse, die auf dem Internet-Protokoll basiert. Durch sie können an jeden Computer über das Netz einzeln Datenpakete gesendet werden.

Internationale Fernmeldeunion (ITU): internationale Organisation, die sich mit den technischen Aspekten der Telekommunikation befasst. Sie hat 191 Mitgliedstaaten und ist eine Sonderorganisation der UN mit Sitz in Genf.

National Security Agency (NSA): größter US-amerikanischer Geheimdienst, der mit der Aufgabe betraut ist, weltweit elektronische Kommunikation zu überwachen, zu entschlüsseln und auszuwerten. Das Ausmaß dieser Überwachung wurde 2013 durch die Enthüllungen des ehemaligen Angestellten Edward Snowden bekannt.

Netzneutralität: technische Gleichbehandlung von Daten bei der Übertragung im Internet, die einen diskriminierungsfreien Zugang für alle Nutzer_innen sicherstellt. Das sogenannte „Best-Effort-Prinzip“ soll gewährleisten, dass Zugangsprovider wie z.B. die Deutsche Telekom die jeweilige Übertragungsrate von z.B. Netflix-Filmen nicht zugunsten eigener Inhalte (z.B. Streaming von Fußballspielen) drosseln dürfen. Ein „Zero-Rating“, d.h. die kostenfreie Überlassung von Inhalten durch Dienste-Anbieter, verstößt nach Meinung von Netzkativist_innen ebenso gegen den Grundsatz der Gleichbehandlung.

Nichtregierungsorganisation: meist abgekürzt als NGO (vom Englischen Non-Governmental Organisation), bezeichnet der Begriff sämtliche durch zivilgesellschaftliche Initiative gegründeten Vereine oder Interessengruppen, die sich im Normalfall politischen Themen wie beispielsweise der Wahrung der Menschenrechte oder dem Umweltschutz verschrieben haben. Viele größere NGOs haben Beobachtungs- oder Beratungsstatus bei den Vereinten Nationen und anderen internationalen Organisationen.

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD): internationale Organisation mit 35 Mitgliedstaaten, die sich für Demokratie und freie Marktwirtschaft einsetzt. Die 1948 als OEEC gegründete Organisation hat ihren Sitz in Paris.

Roadmap: wörtlich übersetzt „Straßenkarte“, bezeichnet der Begriff besonders in der (internationalen) Politik heute allgemein einen Projektplan für ein längerfristiges politisches Vorhaben, in dem übersichtsartig die für die Zielerreichung notwendigen Schritte aufgeführt werden.

Router: Netzwerkgeräte, die Datenpakete zwischen Netzwerken oder zwischen einem Computer und einem Netzwerk weiterleiten. Sie kommen zumeist zum Einsatz, um Endgeräte wie PCs oder Notebooks an das Internet anzuschließen.

Switch: Gerät in der Netzwerktechnologie, das verschiedene Teile des Netzwerks miteinander verbindet.

Think Tank: gelegentlich auch „Denkfabrik“, bezeichnet ein für gewöhnlich nichtstaatlich organisiertes Institut, das sich mittels der Erstellung von Studien, Analysen und Strategien in sozialen, wirtschaftlichen oder politischen Fragestellungen beratend am politischen Meinungsbildungsprozess beteiligt.

Welthandelsorganisation (WTO): 1994 aus dem GATT hervorgegangene internationale Organisation, die sich mit Handels- und Wirtschaftspolitik auf globaler Ebene befasst. Ihr Sitz ist Genf.

Weltorganisation für geistiges Eigentum (WIPO): 1967 gegründete internationale Organisation mit Sitz in Genf, die den Zweck verfolgt, die Rechte an immateriellen Gütern weltweit zu sichern. Die Teilorganisation der UN hat 188 Mitgliedstaaten.

Whistleblower: Hinweisgeber_in, der/die Zugang zu geheimen Informationen eines Unternehmens, einer Organisation oder einer staatlichen Stelle hat und diese öffentlich macht, mit dem Ziel, dessen bzw. deren für unrechtmäßig oder unethisch erachteten Praktiken aufzudecken. Eine EU-Richtlinie zum Schutz von Hinweisgeber_innen von 2019 muss in den nächsten Jahren von den Mitgliedstaaten in nationales Recht umgesetzt werden.

Whois: Protokoll, mit dem Informationen zu Internet-Domains und IP-Adressen sowie deren Eigentümer_innen abgefragt werden können. Aus Datenschutzgründen können die Inhaber_innen von .de Domains bereits seit Ende des vergangenen Jahrzehnts nicht mehr über das whois-Protokoll abgefragt werden, sondern nur noch über die Homepage des DENIC (Deutsches Network Information Center), welches die Top-Level-Domain .de verwaltet.

World Wide Web (WWW): 1989 vom englischen Wissenschaftler Tim Berners-Lee erschaffener Internetdienst, der Dokumente und andere Ressourcen mittels Webseiten bereitstellt, die über sogenannte Hyperlinks miteinander verbunden sind. Es wird mit Hilfe von Webbrowsern auf Endgeräten dargestellt. Das WWW ist ein Teil des Internets, aber keineswegs mit diesem deckungsgleich.

Zugangsprovider: Unternehmen, das Kund_innen den Zugang zum Internet ermöglicht.

Literaturhinweise und Links

Balleste, Roy: Internet Governance – Origins, Current Issues, and Future Possibilities, 2015.

Betz, Joachim und Kübler, Hans-Dieter: Internet Governance – Wer regiert wie das Internet?, 2013.

Centre for International Governance Innovation und Chatham House (Hg.): Global Commission on Internet Governance – One Internet, 2016, <https://www.cigionline.org/publications/one-internet>.

Deloitte (Hg.): Cyber Security Report 2019. Teil 1: Fake News und Schlüsseltechnologien – wachsende Herausforderungen, <https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html>.

DeNardis, Laura: The Global War for Internet Governance, 2014.

DeNardis, Laura: The Internet is Everything. Freedom and Security in a World with No Off Switch, 2020 (im Erscheinen).

Esch, Johanna: Internationale Internet-Governance. Das Internet als Herausforderung für etablierte Medienpolitik, in: Aus Politik und Zeitgeschichte 40-41 (2018), S. 35-40, <http://www.bpb.de/apuz/276561/internationale-internet-governance-das-internet-als-herausforderung-fuer-etablierte-medienpolitik?p=all>.

Hölig, Sascha und Hasebrink, Uwe: Reuters Institute Digital News Report 2019 für Deutschland – Ergebnisse für Deutschland. Unter Mitarbeit von Julia Behre, 6/2019 (Arbeitspapiere des HBI Nr. 47), <https://www.hans-bredow-institut.de/de/publikationen/reuters-institute-digital-news-report-2019-ergebnisse-fuer-deutschland>.

Hofmann, Jeanette: Multi-Stakeholderism in Internet Governance: Putting Fiction into Practice, Journal of Cyber Policy, S. 29 - 49 (2016), 10.1080/23738871.2016.1158303.

Hofmann, Jeanette: Constellations of trust and distrust in Internet governance, in: Europäische Kommission (Hg.), Trust at Risk: Implications for EU Policies and Institutions, 2017, S. 85-98, <https://publications.europa.eu/en/publication-detail/-/publication/e512c11b-e922-11e6-ad7c-01aa75ed71a1/language-en/format-PDF/source-104354701>.

Jaume-Palasi, Lorena und Pohle, Julia und Spielkamp, Matthias (Hg.): Digitalpolitik. Eine Einführung. Eine Publikation des Wikimedia Deutschland e.V. und iRights.international, mit Unterstützung von ICANN, 2017, https://irights.info/wp-content/uploads/2017/05/Digitalpolitik_-_Eine_Einfuehrung.pdf.

Kettemann, Matthias C.: Völkerrecht in Zeiten des Netzes. Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht. Herausgeber: Friedrich-Ebert-Stiftung, Politische Akademie, Medienpolitik, 2015, <http://library.fes.de/pdf-files/akademie/12068.pdf>.

Kettemann, Matthias C.: Internationale Regeln für soziale Medien. Menschenrechte wahren und Desinformation bekämpfen, in: Global Governance Spotlight 2 (2019), <https://www.sef-bonn.org/de/publikationen/global-governance-spotlight/22019.html>.

Kleinwächter, Wolfgang: Internet Governance Outlook 2019: Innovative Multilateralism vs. Neo-Nationalistic Unilateralism, in: Circle ID (8.1.2019), http://www.circleid.com/posts/20190108_internet_governance_2019_innovative_multilateralism_vs_neo/.

Kurbalija, Jovan: An Introduction to Internet Governance, 6. Auflage 2014.

Masters, Jonathan: What Is Internet Governance?, 2014, <http://www.cfr.org/internet-policy/internet-governance/p32843>.

NETmundial (Hg.): NETmundial Multistakeholder Statement, 2014, <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Dokument.pdf>.

OECD (Hg.): The Economic and Social Role of Internet Intermediaries, 2010, <https://www.oecd.org/internet/ieconomy/44949023.pdf>.

Schulz, Wolfgang und Dankert, Kevin: Die Macht der Informationsintermediäre. Erscheinungsformen, Strukturen und Regulierungsoptionen, FES Medienpolitik Studie, 2016, <https://library.fes.de/pdf-files/akademie/12408.pdf>.

Weber, Rolf H.: Proliferation of 'Internet Governance', 2014, <http://ssrn.com/abstract=2809874>.

Singer, Peter W. und Brooking, Emerson T.: LikeWar. The Weaponization of Social Media, 2018.

United Nations (Hg.): The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation, 2019, <https://eucyberdirect.eu/wp-content/uploads/2019/10/un-high-level-panel-digital-cooperation-2019.pdf>.

Zuckerberg, Mark: A Blueprint for Content Governance and Enforcement (15.11.2018), <https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/>.

Weiterführende Informationen im Internet

Afrikanische Union (AU):
<http://www.au.int>

Europarat (Council of Europe, COE):
<http://www.coe.int/de>

Freedom on the Net:
<https://freedomhouse.org/report-types/freedom-net>

GATS-Abkommen:
<http://www.bmz.de/de/themen/welthandel/welthandelssystem/WTO/GATS/index.html>

Internationale Fernmeldeunion (ITU):
<http://www.itu.int/en>

Internet Corporation for Assigned Names and Numbers (ICANN):
<https://www.icann.org>

Internet Governance Forum (IGF):
<http://www.intgovforum.org>

Internet Governance Forum Deutschland (IGF-D):
<http://www.intgovforum-deutschland.org>

Internet-Governance-Radar:
<https://internet-governance-radar.de/>

Multistakeholder Advisory Group (MAG):
<http://www.intgovforum.org/cms/mag>

National Security Agency (NSA):
<https://www.nsa.gov>

NETmundial Initiative:
<https://www.netmundial.org>

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD):
<http://www.oecd.org>

Welthandelsorganisation (WTO):
<https://www.wto.org>

Weltorganisation für geistiges Eigentum (WIPO):
<http://www.wipo.int>

Über die Autoren



Foto: Henning Lahmann

Henning Lahmann ist Senior Policy Advisor beim iRights.Lab. Zudem war er fünf Jahre lang als wissenschaftlicher Mitarbeiter am Walther-Schücking-Institut für Internationales Recht in Kiel und an der Universität Potsdam beschäftigt. Während dieser Zeit promovierte er im Völkerrecht zu Fragen der transnationalen Cybersicherheit und der Anwendbarkeit völkerrechtlicher Regelungen im Cyberspace.



Foto: Die Hoffotografen / CC-BY-SA-4.0

Jan Engelmann arbeitet als Policy Advisor beim iRights.Lab und unterstützt die Geschäftsführung in strategischen Fragestellungen sowie bei der Organisationsentwicklung. Zuvor war er als Geschäftsführer beim Whistleblower-Netzwerk, der Social Reporting Initiative und Wikimedia Deutschland tätig.

Die Friedrich-Ebert-Stiftung

Die Friedrich-Ebert-Stiftung (FES) wurde 1925 gegründet und ist die traditionsreichste politische Stiftung Deutschlands. Dem Vermächtnis ihres Namensgebers ist sie bis heute verpflichtet und setzt sich für die Grundwerte der Sozialen Demokratie ein: Freiheit, Gerechtigkeit und Solidarität. Ideell ist sie der Sozialdemokratie und den freien Gewerkschaften verbunden. Als gemeinnützige Einrichtung gestalten wir unsere Arbeit eigenständig und unabhängig. Die FES fördert die Soziale Demokratie vor allem durch:

- politische Bildungsarbeit zur Stärkung der Zivilgesellschaft
- Politikberatung
- internationale Zusammenarbeit mit Auslandsbüros in über 100 Ländern
- Begabtenförderung
- das kollektive Gedächtnis der Sozialen Demokratie mit u.a. Archiv und Bibliothek

www.fes.de

Bestellung/Kontakt

medienpolitik@fes.de
www.fes.de/medienpolitik



Angelehnt an den Leitsatz „Netzpolitik ist Gesellschaftspolitik“ folgt diese Publikation der Idee, dass Internet Governance alle etwas angeht. Das offene und freie globale Netz darf nicht infrage gestellt werden. Überwachungs- und Zensurinfrastrukturen dürfen nicht etabliert werden. Für die digitalen Gesellschaften hat die Regulierung des „Netzes der Netze“ längst eine politische Dimension bekommen. Menschen- und Bürgerrechte und Fragen der sozialen, gesellschaftlichen, kulturellen wie wirtschaftlichen Teilhabe aller Menschen stehen ganz oben auf der Agenda. Die Publikation gibt einen Überblick über Akteure und Handlungsfelder und verdeutlicht, dass es das kollektive Engagement mehr denn je braucht, um Internet Governance weiterzuentwickeln, das Multistakeholderprinzip und den Multilateralismus zu stärken und der Fragmentierung des Netzes zu begegnen.

