Bedrohte Menschenrechte im Cyberraum

Anja Mihr

Die Umsetzung grundlegender Freiheitsrechte, sozialer und wirtschaftlicher Menschenrechte und der Ziele für nachhaltige Entwicklung (Sustainable Development Goals – SDGs) sind ohne das Internet heute nicht mehr denkbar. Jedoch gelang es der Staatengemeinschaft bislang nicht, Menschenrechte sowohl offline als auch online ausreichend zu schützen und zu fördern. Daher verabschiedete die UN-Generalversammlung im Dezember 2015 eine Resolution, die der Förderung und dem Schutz der Menschenrechte im Internet neue Regeln geben soll.

Im digitalen Zeitalter wird der internationale Menschenrechtskodex der Vereinten Nationen immer dann bemüht, wenn Regierungen bei der Bekämpfung von Sicherheitsrisiken im Internet nicht weiterkommen. Menschenrechte sind häufig das letzte Mittel beim Miteinander im ›staatenlosen‹, anarchischen Cyberraum[1]. Wenn staatliche Behörden und die nationale Rechtsprechung es nicht schaffen, Internetkriminalität zu verhindern, appellieren staatliche Stellen gerne an die individuelle Verantwortung des Nutzers. Dementsprechend sollte jeder Nutzerin und jedem Nutzer der freie Zugang zu Informationen, Schutz der Privatsphäre, Chancen der persönlichen, beruflichen und privaten Entwicklung, das Recht auf Meinungsfreiheit sowie auf Arbeit und Gesundheit gewährt werden. Im Umkehrschluss sollten Nutzerinnen und Nutzer damit verantwortungsbewusst umgehen.

Zu den Regierungen als einzige maßgebliche Akteure, die diese Rechte schützen, fördern oder verletzen, sind andere Akteure hinzugekommen: Nutzerinnen und Nutzer, private Unternehmen oder kriminelle Organisationen. Sie alle sollen miteinander Frieden, Freiheit und Sicherheit des Internets aushandeln und damit für einen allen gleichermaßen zugänglichen Internetzugang im Cyberraum Sorge tragen. Der Staat als einziger Garant für den Schutz der Menschenrechte im Internet hat sich *de facto* schon lange von dieser Rolle verabschiedet.

Heute zählen die Sicherheitsrisiken und die Verletzung der grundlegenden Freiheitsrechte im Cyberraum zu den Prioritäten jeder gesellschaftspolitischen Debatte. Dem tragen die hastigen Aktivitäten der Vereinten Nationen spätestens seit der Gründung des Internet Governance Forums (IGF) im Jahr 2005 Rechnung.[2] Trotz aller Appelle und Resolutionen internationaler Organisationen in den letzten Jahren und der wiederholten Beteuerung aller staatlichen und nichtstaatlichen Akteure, dass Menschenrechte sowohl offline als auch online gültig seien, gelang es der Staatengemeinschaft nicht, das Menschenrecht auf Privatsphäre zu harmonisieren. Auch die im Jahr 2013 verabschiedete ›Charta der Menschenrechte und Prinzipien für das Internet‹ im Auftrag des IGFs änderte daran zunächst nichts.[3] Die UN hofften, die Ursachen dafür mit einer neuen Resolution zu benennen und Anreize zu schaffen, diese zu beheben.

Aus Anlass einer Evaluierung des IGFs durch die Gruppe der Vereinten Nationen für die Informationsgesellschaft (United Nations Group on the Information Society – UNGIS) verabschiedete die UN-Generalversammlung im Dezember 2015 die umfassende Resolution 70/125 zu Multistakeholder-Ansätzen und Teilhabe im Internet.[4] Entsprechend dieser Resolution soll eine Informationsgesellschaft aufgebaut werden, die die nachhaltige Entwicklung und die Lebensqualität jedes Einzelnen fördert. Das Internet, so die Staatenvertreterinnen und Staatenvertreter, spiele dabei mehr denn je eine wesentliche Rolle und die Informations- und Kommunikationstechnologie leiste einen bereichsübergreifenden Beitrag, schnellere Fortschritte bei den Zielen für nachhaltige Entwicklung zu erwirken. Nur wenn private Nutzerinnen und Nutzer, Unternehmen, Wissenschaftlerinnen und Wissenschaftler sowie Regierungen zusammenarbeiten, gelingt die Umsetzung der Ziele für nachhaltige Entwicklung (Sustainable Development Goals – SDGs). Betrachtet man die Tragweite und Ehrgeizigkeit dieser Ziele, so hängt letztlich auch die Zukunft und das Weiterbestehen der Vereinten Nationen von der Verwirklichung der Ziele ab.

Dr. Anja Mihr, geb. 1969, ist Gründerin und Leiterin des HUMBOLDT-VIADRINA Centers on Governance through Human Rights in Berlin. Sie vertritt zudem den Franz-Haniel Chair of Public Policy an der Willy-Brandt-School of Public Policy der Universität Erfurt.

1 Als Cyberraum (Cyberspace) wird ein virtueller mehrdimensionaler Raum bezeichnet, der mithilfe von Computern oder mobiler Technologie ›betreten‹ werden kann. Das Internet ist ein Netzwerk von Dienstanbietern, Plattformen oder Nutzerinnen und Nutzern, die im Cyberraum kommunizieren und sich vernetzen.

2 Siehe zur Gründung: Wolfgang Kleinwächter, Globalisierung und Cyberspace. Der Weltgipfel über die Informationsgesellschaft weist den Weg, VN, 1–2, 2006, S. 38–44, sowie www.intgovforum.org

3 Siehe dazu Internet Rights and Principles Coalition, Die Charta der Menschenrechte und Prinzipien für das Internet, United Nations, 2013, www.internetrightsandprinciples.org/site/wp-content/uploads/2014/06/IRPC_booklet_29May2014_German.pdf

4 Vgl. UN-Dok. A/RES/70/125 v. 16.12.2015.

Resolution 70/125 sieht die Neuverteilung von Verantwortlichkeiten, Entscheidungsbefugnissen, Einfluss und der Systemordnung vor. Ziel ist es, das Internet neutral, für alle zugänglich und sicher zu machen sowie Cyberkriminalität und Cyberterror zu verhindern. Gleichzeitig soll der Zugang zum Internet die persönliche Entwicklung aller Menschen ermöglichen. Jeder Mensch hat eine Rolle und Verantwortung, so die Resolution, nicht nur Regierungen. Waren es bis dato vor allem Regierungen und staatliche Einrichtungen, die im Sinne der Menschenrechte verantwortlich zu handeln hatten, ist diese Verantwortung in den letzten Jahren fast schleichend an andere, zumeist private und nichtstaatliche Akteure abgegeben worden.[5] Noch existieren allerdings weder lokal, regional, international, global noch ›cyberal‹ entsprechende Umsetzungs- und Einhaltungsmechanismen. Als Erfolg ist immerhin zu werten, dass sich Staaten wie China, Russland, Singapur, die Türkei oder die USA davon verabschiedet haben, zu glauben, sie könnten das Internet allein kontrollieren. Internet Governance ist Multistakeholder-Governance: Jeder Akteur darf bei der Norm- und Regelsetzung mitmischen und übernimmt Verantwortung bei der Einhaltung oder Nichteinhaltung dieser Regeln. Was für Wissenschaftlerinnen und Wissenschaftler sowie internetaffine Personen keine neue Erkenntnis ist, war auf Staatenebene noch bis letztes Jahr umstritten. Nicht umsonst ist im Jahr 2015 zum ersten Mal beim jährlich tagenden Internet Governance Forum das Thema Menschenrechte und Verantwortung auf die Agenda gekommen. Auch das NATO Cooperative Cyber Defence Centre of Excellence in Tallin, das sich zuvor ausschließlich mit Sicherheitsfragen befasst hat, beschäftigt sich seit letztem Jahr mit dem Thema.[6]

Waren es bis dato vor allem Regierungen, die im Sinne der Menschenrechte verantwortlich zu handeln hatten, ist diese Verantwortung in den letzten Jahren zumeist an private und nichtstaatliche Akteure abgegeben worden.

Die Resolution liest sich daher wie ein lang überfälliges Eingeständnis der Realität. In Zeiten von nicht zu lokalisierenden Nutzern und Domainbesitzern, von Hasspredigern, Terrornetzwerken und Anbietern von Kinderpornografie wäre es fatal, auf nationalstaatliche Kompetenz in Fragen von Sicherheit und Frieden zu beharren. Internet Governance beruht entsprechend des Vorschlags der UNGIS auf dem Multistakeholder-Ansatz für erstens mehr Verantwortlichkeit aller Akteure, zweitens mehr Transparenz und Freiheitsrechte für alle Nutzerinnen und Nutzer und drittens mehr Teilhabe von Akteuren durch Cybertools, wie zum Beispiel das Internet, Smartphones und andere mobile Geräte. Kurz: Internet Governance bedeutet verantwortungsbewusster Umgang aller Akteure im Internet. Wer diesen Umgang einfordern, einhalten oder überwachen soll, ist noch offen. Genau darum geht es jedoch bei dem Thema Menschenrechte im Cyberraum und damit auch im Internet. Wer hat die Interpretationshoheit, wer darf daran teilhaben und wer setzt die Ergebnisse im Anschluss daran um? Welche globalen, unabhängigen, transparenten und rotierenden Mechanismen braucht es, um allen Akteuren gerecht zu werden? Auch hier versucht die UN-Generalversammlung seit dem Jahr 2013, ein multistakeholder-basiertes Governance-System zu schaffen.[7]

Die Pflicht, die Menschenrechte im Cyberraum zu schützen, wird aus dem Prinzip der territorialen Souveränität abgeleitet.

Warum Internet Governance?

Bereits in Resolution 68/167 zu Sicherheitsfragen und der Privatsphäre im Internet aus dem Jahr 2013 forderte die Generalversammlung die Regierungen auf, Maßnahmen zu ergreifen und die Menschenrechte auf der ›Datenautobahn‹ zu schützen.[8] Es sollten ›Verkehrsregeln‹ für die Nutzung des virtuellen Raums eingeführt werden. Entsprechend den internationalen Menschenrechtsrechtsverträgen soll das Sammeln und die Weiterverarbeitung von persönlichen Daten unter gleichen und für alle nachvollziehbaren Kriterien offen gelegt werden. Was sich damals noch wie Wunschdenken anhörte, hat in den letzten zwei Jahren durch unzählige nationale und einige internationale Gerichtsentscheidungen an Format gewonnen. Es handelt sich dabei um Präzedenzfälle, die möglicherweise den Weg zu einem internationalen ›Cyber- oder Internetgerichtshof‹ bereiten könnten.

Denn die Möglichkeiten nationaler Gerichtsbarkeit im Fall von Internetkriminalität sind schon lange ausgeschöpft. Das neue globale Rechts- oder Leitungssystem ist jedoch noch nicht etabliert und legitimiert, geschweige denn souverän.[9] Internationale Rechtssysteme wie die des Seerechts, der Raumfahrt oder der extraterritorialen Verpflichtungen sind noch staatenzentriert, werden jedoch oft als Beispiele für die zukünftige Entwicklung einer ›Cyberjustiz‹ zu Rate gezogen. Nationale Grenzen, Staatszugehörigkeiten oder ein Eintrag in ein Handels- und Vereinsregister in einem bestimmten Land spielen dann keine Rolle mehr, sondern allein die Tat und die Verantwortlichkeit – so der Wunsch der Visionäre: eine ›geteilte Verantwortlichkeit‹, wie sie bereits seit langem im Klima- und Menschenrechtsregime Thema ist.[10]

Die Pflicht, die Menschenrechte im Cyberraum zu schützen, wird aus dem Prinzip der territorialen Souveränität abgeleitet. Der Internationale Gerichtshof (IGH) in Den Haag hat argumentiert, dass aufgrund der (bisherigen) territorialen Souveränität Menschenrechte im Cyberraum zu schützen seien, wenn Unternehmen ihre Server innerhalb der eigenen Staatsgrenzen betreiben. Da diese Server stets auch physisch lokalisiert sind, müssen Regierungen aktiv werden – auch wenn sie damit nur beschränkt Rechte schützen.[11] Während Unternehmen wie Google, Twitter, Youtube oder Facebook die Verantwortung für ihre Angebote tragen müssen – egal in welchem Land oder auf See –, sollten Staaten die Betreiber von Servern zur Verantwortung ziehen,

auch wenn deren Angebot nicht die eigene Bevölkerung betrifft.

Als Reaktion auf die Debatte, ob Internet-Souveränität und -Legitimität staatliche Institutionen schwächt oder stärkt, hat der damalige UN-Sonderberichterstatter über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung Frank William La Rue bereits im Jahr 2013 empfohlen, die Kommunikations-, Daten- und Informationsflüsse zu überprüfen. Es solle untersucht werden, inwiefern diese nicht nur Freiheit einschränken, sondern auch die Grundwerte einer demokratischen Gesellschaft angreifen. Allerdings sollten nur unabhängige, durch die UN initiierte Überprüfungsmechanismen darüber befinden.[12]

Schülerinnen und Schüler der Rhodes Park School in Lusaka, Sambia, bereiten im Computerlabor im Rahmen eines Projekts des Insitute for International Cooperation and Development (IICD) einen Lernzirkel vor. Foto: IICD/flickr.com

Chancen für die Menschenrechte

Am Ende überrascht es wenig, dass die UN-Generalversammlung das Internet kurz nach der Verabschiedung der 17 SDGs im September 2015 als Wegbereiter für deren Verwirklichung benannt hat. Ob Bildung, Armutsbekämpfung, Gesundheit, Frieden und Gerechtigkeit, Bekämpfung des Klimawandels oder der Geschlechterungleichheit: Ohne Zugang zum Internet sind diese Ziele nicht zu verwirklichen. In Resolution 70/125 wird deshalb der Multistakeholder-Prozess als Chance für einen holistischen, auf Menschenrechten basierenden Weg zur Umsetzung der SDGs gesehen. Der Entscheidungs- und Umsetzungsprozess soll ermöglichen, dass sowohl Frauen als auch Männer gleichen und neutralen Zugang zum Internet haben. Bislang sind nur knapp 40 Prozent aller Internetnutzer Frauen. Zudem sollen entsprechend Resolution 70/125 in den nächsten Jahren mindestens zwei Milliarden Menschen erstmalig Zugang erhalten, vor allem in den Entwicklungsländern. Erst dann hätten die SDGs eine reelle Chance, ansatzweise bis zum Jahr 2030 realisiert zu werden.

Dies ist jedoch nur in Zusammenarbeit mit internationalen, nationalen, lokalen und privaten oder zivilgesellschaftlichen Akteuren über das Internet möglich. Nur im ›cyberalen‹ Raum können alle ihr Menschenrecht auf Informationszugang, freie Meinungsäußerung und Teilhabe an gesellschaftlichen Prozessen als Schlüssel für ihre berufliche Entwicklung, zur Teilhabe an wissenschaftlichem Fortschritt, zur Bildung, zur Gesundheit und gesunder Umwelt, zum Ausleben ihrer Kultur oder zur Geschlechterneutralität nutzen. Das Völkergewohnheitsrecht kann die Grundlage sein, diese globalen Werte und Normen auch in jene Länder zu übermitteln, die internationale Menschenrechtsverträge nicht ratifiziert haben. Ein neutrales Internet, wie es die Teilnehmenden des IGF im November 2015 in Brasilien gefordert haben, ist dabei nur die technische Voraussetzung, die jedoch von staatlichen Behörden allein nicht gewährleistet werden kann.[13]

Alle Akteure sind laut Generalversammlung verpflichtet, nicht nur in ihren eigenen Ländern, sondern auch in von Krieg, Gewalt, Armut und Naturkatastrophen gebeutelten Ländern in ein neutrales Internet zu investieren. So wie einst der Straßen-, Hafen- oder Schienenbau der Schlüssel zum Wiederaufbau oder zur Entwicklung einer Gesellschaft war, ist es heute die freie, neutrale und allen zugängliche ›Datenautobahn‹. Unternehmen wie Microsoft oder

5 Ronald J. Deibert/Masashi Crete-Nishihata, Global Governance and the Spread of Cyberspace Controls, Global Governance, 18/2012, S. 339–361.

6 Vgl. Dokumentation zum Workshop on ›Human Rights in Cyberspace‹ des NATO Cooperative Cyber Defence Centre of Excellence unter www.ccdcoe.org/workshop-human-rights-cyberspace.html

7 Tim Maurer, Cyber Norm Emergence at the United Nations – An Analysis of the UN**'s Activities Regarding Cybersecurity, Discussion Pa**per #2011–11, Belfer Center for Science and International Affairs Harvard Kennedy School, www.belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

8 Vgl. UN-Dok. A/RES/68/167 v. 18.12.2013.

9 Zu den rechtlichen Rahmenbedingungen: Tatiana Tropina/Nicolas von zur Mühlen, in diesem Heft: S. 56–60.

10 Jaqueline Lipton, Rethinking Cyberlaw. A New Vision for Internet Law, Cheltenham 2015.

11 Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, in: Christian Czosseck/Rain Ottis/Katharina Ziolkowski (Eds.), 4th International Conference on Cyber Conflict, Tallinn 2012, S. 7–13, www.ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf

12 UN Doc. A/HRC/23/40 v. 17.4.2013.

13 Siehe dazu Internet Governance Forum, The 10th Internet Governance Forum (IGF), Chair's Summary, 10.–13. November 2015, João Pessoa, Brasilien, www.intgovforum.org/cms/10th%20IGF%20Chairs%20Summary_Finalv2.pdf

Google können nicht mehr frei entscheiden, ob sie in ein Land investieren oder ihre Dienstleistung anbieten wollen, sondern sind quasi dazu verpflichtet, zu investieren und am Gemeinwohl orientiert zu handeln. Gleichzeitig wird im letzten Abschnitt der Resolution 70/125 beim Thema Internet Governance davon ausgegangen, dass selbst autokratische Regime sich dem Multistakeholder-Ansatz öffnen und damit zumindest minimale Good-Governance-Standards umsetzen. Denn um Datenfreiheit und Datenschutz in Zukunft zu garantieren, braucht es ein Mindestmaß an Transparenz, Rechenschaftslegung und Partizipation durch und mit privaten und staatlichen Akteuren.

Es geht um das Thema, wie viel Schutz, Zugang oder Begrenzung von Freiheit für eine Gesellschaft gut sind und wann unter dem Vorwand ›Sicherheit‹ die freie Entwicklung eingeschränkt wird.

Unternehmen wie Microsoft und SAP, Anbieter wie Google und Yandex sowie soziale Netzwerke wie Facebook, Renren in China oder d1g.com in den arabischen Ländern sollten überall verfügbar beziehungsweise frei zugänglich sein. Neutral bedeutet auch, dass jeder Mensch gleichen und freien Zugang zu Informationen und Kommunikation erhält, der für seine Entwicklung notwendig ist. Zusatzangebote sollen über das Mindestangebot hinaus den Unternehmen ihren Profit garantieren. Der ungehinderte Zugang in Landes- und Minderheitensprachen sowie ein ortsunabhängiger Zugang mit allen Endgeräten gehören ebenfalls dazu. Freier und kostenloser Zugang zu den neusten Anbaumethoden von Getreide in Afrika südlich der Sahara in lokalen Dialekten ist dabei ebenso wichtig wie freier Zugang für Jugendliche zu Informationen und Bildungsangeboten, ohne dabei permanenter Werbung und Manipulation ausgesetzt zu sein. Gerade beim Kampf gegen die rasante Klimaveränderung und ihre dramatischen Folgen kann ein neutrales, politik-, religions- und kommerziell unabhängiges Internet viel bewirken.

Ob bei der Bekämpfung und Aufklärung von Ebola in Westafrika oder dem Zika-Virus in Lateinamerika: Das Internet ist auch beim Recht auf Gesundheit nicht mehr wegzudenken. Junge Menschen erhalten über das Internet Chancen auf Bildung und Ausbildung, die sie sich offline niemals hätten leisten können. Dabei setzen Anbieter nicht mehr auf Computer als Zugangstechnik, sondern auf Smartphones mit Satelliten- oder gar drohnengesteuertem Zugang zum Internet.

Es gibt keine Notwendigkeit für eine eigene digitale Menschenrechtscharta. Vielmehr gilt es, ein effizienteres Internet-Governance-Regime aufzubauen.

Der Austausch zwischen Kulturen kann zu mehr Frieden beitragen. Gleichzeitig erhalten jedoch auch autoritäre Regierungen, radikale und religiöse Hassparteien Zugang zu den Nutzerinnen und Nutzern und können diese beeinflussen. Es geht immer um das Thema, wie viel Schutz, Zugang oder Begrenzung von Freiheit für eine Gesellschaft gut sind und wann unter dem Vorwand ›Sicherheit‹ die freie Entwicklung eingeschränkt wird. Diese Diskussion ist so alt wie die Idee der Menschenrechte selbst und nicht allein auf das Internet beschränkt. Sie wird im Cyberraum allerdings stärker geführt, da es hier (noch) kein Steuerungs- und Sanktionssystem gibt. Die Kommunikation im Internet ist oft anonym, was nicht nur die vielbeschriebenen Risiken, sondern auch Chancen birgt. Mehr Frauen, Mädchen und Angehörige von marginalisierten Gruppen beteiligen sich an politischen Debatten im Internet. Es bietet denjenigen Zugang, die sich aufgrund gesellschaftlicher Zwänge und Diskriminierung bislang nicht trauten, sich am politischen Prozess zu beteiligen. Die Frauenbewegungen in Saudi-Arabien, die Blogger-Bewegung in Bangladesch oder die Aktivisten des ›Arabischen Frühlings‹ und die Indio-Bewegung ›Amazonas Watch‹ sind ohne den freien Zugang zum Internet nicht denkbar. Menschen mit Behinderung erhalten Zugang zur beruflichen und politischen Teilhabe, ohne dass dabei alltägliche Hemmnisse ein Hindernis darstellen. Angehörige von ethnischen oder religiösen Minderheiten mischen sich in politische Debatten ein, um ihr Land, ihre Kultur und ihre Ressourcen zu schützen, und sie profitieren von der internationalen Solidarität.

Es gibt daher keine Notwendigkeit für eine eigene digitale Menschenrechtscharta, wie noch vor wenigen Jahren diskutiert. Vielmehr gilt es, ein effizienteres Internet-Governance-Regime aufzubauen. Dabei einigen sich private, öffentliche oder internationale Akteure gemeinsam auf Kriterien, denen entsprechend sie einen Teil des Cyberraums ›besiedeln‹ und ihre Rollen und Verantwortlichkeiten festlegen. Bei Nichteinhaltung drohen selbst auferlegte Sanktionen – erst dann kann der Multistakeholder-Ansatz funktionieren. Bislang ist jedoch offen, wer festlegt, welche Akteure sich in welcher Weise an diesem Aushandlungsprozess beteiligen.

Negative Auswirkungen des Internets auf die Menschenrechte

Vor allem der Schutz der Privatsphäre und privater Daten ist ein Kernanliegen von Internet Governance. Der Missbrauch oder Diebstahl von privaten Gesundheits- und Kreditkartendaten oder Cybermobbing führten bereits in vielen Fällen zum existenziellen Ruin einzelner Nutzer und nicht selten zu Todesfällen, ohne dass die Täter erkannt oder verurteilt werden konnten. Privatsphäre ist jener persönliche Raum, in dem wir unsere Persönlichkeit selbstbewusst und frei entwickeln und unsere Fähigkeiten und Möglichkeiten ausschöpfen, unsere Gesundheit erhalten sowie soziale Beziehungen mit Familie und Freunden ohne Einfluss von außen unterhalten können.[14] Daher bedeutet Privatsphäre im Cyberraum, das Internet als Werkzeug für private Zwecke zu verwenden, ohne zu fürchten, dass Dritte ohne Zustimmung auf unsere Daten zugreifen, sie verkaufen oder öffentlich machen. Hier wird deutlich, warum die UN-Generalversammlung den Multistakeholder-Ansatz

so hoch bewertet, denn private Unternehmen sind häufig die einzigen Akteure, die Daten von potenziellen Tätern zugänglich machen können. Gleichzeitig haben Regierungen die Sorge, ihren Einfluss auf Unternehmen zu verlieren, da diese sich im Cyberraum zunehmend staatlicher Kontrolle entziehen.

Freiheits- und Persönlichkeitsrechte im Internet sind beim Datenschutz, bei der Cybersicherheit, der Cyberüberwachung oder dem Cyberkrieg durch Cyberviren besonders zu schützen. Staatliche und nichtstaatliche Akteure sind an dieser Kriminalität im Internet gleichermaßen beteiligt. Gesetzesvorhaben wie der amerikanische ›Stop Online Piracy Act‹ (SOPA) beziehungsweise der PROTECT IP Act, das amerikanische Überwachungsprojekt PRISM oder das multilaterale Handelsübereinkommen zur Bekämpfung von Produkt- und Markenpiraterie (Anti-Counterfeiting Trade Agreement – ACTA) gehören zu den unzähligen verzweifelten Versuchen, die staatliche Kontrolle über den grenzenlosen Datenfluss wiederzuerlangen. Es ist ein Wettlauf gegen die Zeit, den staatliche Stellen allein nicht gewinnen können.

Andere Grundfreiheiten und Menschenrechte, die in diesem Zusammenhang behandelt werden, sind der freie Ausdruck des Glaubens, der politischen Meinung, von Forschungsdaten, geistigem Eigentum, der freie und gleichberechtigte Zugang zu Informationen und der Schutz der Privatsphäre. Darüber hinaus geht es um den Schutz und die Sicherheit, frei von Belästigung und Verfolgung im Internet zu agieren. Geistiges Eigentum und Kreativität müssen geschützt werden, gleichzeitig jedoch der Gemeinschaft im Sinne ihrer Entwicklung in angemessener Weise zugeführt werden.[15] Oberstes Prinzip dabei ist, dass die veröffentlichten Mitteilungen und Informationen die Menschenrechte anderer nicht verletzen. Dies ist Abwägungssache und bis dato lag die Entscheidung darüber allein in der Hand nationaler oder internationaler Gerichte.

Das oft proklamierte ›Recht auf Internet‹, das den Privatpersonen jederzeit den Zugang zum Internet ermöglichen soll, und das ›Recht auf Vergessen‹, das sicherstellt, dass private Daten privat bleiben und jederzeit gelöscht werden können, sind inzwischen Bestandteil von Internet Governance geworden, ohne dass es einer eigenen Internetcharta oder Ähnlichem bedurfte. Der Gerichtshof der Europäischen Union (EuGH) hat im Mai 2014 eine Grundsatzentscheidung getroffen, die diesen Ansatz untermauert.[16] Allerdings gilt die Entscheidung nur für die EU und eine globale Lösung steht noch aus. Dies gilt auch für die Entscheidung des EuGH aus dem Jahr 2015 zum Thema ›sicherer Hafen‹ für Datenübermittlung in die USA.[17] Dies sind Präzedenzfälle, auf die sich zukünftige Rechtsprechungen berufen werden. Grundsätzlich geht es bei all diesen Entscheidungen um die anteilige Verantwortung verschiedener Akteure, Staaten, Unternehmen sowie Nutzerinnen und Nutzer beim Schutz der Daten im Internet.

Im Jahr 2011 hat die Forschungsabteilung des Europäischen Gerichtshofs für Menschenrechte bereits eine klare Richtung vorgegeben, indem sie dem Datenschutz eine prinzipielle Vorrangstellung einräumte.[18] Es hängt viel davon ab, wer über die Grenzen der Informationsfreiheit entscheidet. Je mehr diese Akteure im Sinne des Multistakeholder-Ansatzes in Zukunft am Aushandeln dieser Rechtsgrundsätze beteiligt sind, desto wahrscheinlicher wird dieses Ergebnis von den Nutzern angenommen.

Nach Bekanntwerden vieler Fälle von Cyberspionage und Internetkriminalität im Jahr 2013 betonte der damalige UN-Sonderberichterstatter über die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung, dass Datenschutz und Meinungsfreiheit miteinander verknüpft seien. Ohne ausreichende Gesetzgebung und Rechtsnormen zur Gewährleistung der Privatsphäre können Sicherheit und Anonymität der Kommunikation für Journalistinnen und Journalisten, Menschenrechtsaktivisten und Whistleblower nicht gewährleistet werden.[19] Dass Regierungen Verfahren gegen den Whistleblower Edward Snowden, den Wikileaks-Gründer Julian Assange oder gegen die Plattform netzpolitik.org eingeleitet haben, war eine Bankrotterklärung der nationalen Sicherheitsapparate und Rechtsysteme, die allesamt mit ihrer neuen Rolle im Multistakeholder-System überfordert sind.

Das ›Recht auf Internet‹ und das ›Recht auf Vergessen‹ sind Bestandteil von Internet Governance geworden.

Ausblick

Die rund 3,5 Milliarden Nutzerinnen und Nutzer des Cyberraums machen die Hälfte der Weltbevölkerung aus. Der Cyberraum ist ein grenzenloser öffentlicher Raum ohne Regierung, in dem Menschen, unabhängig von ihrer Staatsbürgerschaft, ethnischen Herkunft, politischen Orientierung, ihrem Geschlecht oder sonstigem Hintergrund kommunizieren und interagieren. Dies erinnert fast schon an ein ›Failed state‹-Szenario. Gleichzeitig ist die

14 Anja Mihr, Good Cyber Governance. The Human Rights and Multi-Stakeholder Approach, in: Georgetown Journal of International Affairs, 2014, S. 24–34.

15 Vgl. Marcia V.J. Kran/Geraldine Fraser-Moleketi, Global Consultation on Governance and the Post-2015 Framework: Concept Note, 7.10.2012, www.worldwewant2015.org/node/277876

16 Urteil des EuGH, C-131/12, 13.5.2014.

17 Urteil des EuGH, ECLI:EU:C:2015:650, 6.10.2015.

18 Declaration by the Committee of Ministers on Internet Governance Principles, Adopted by the Committee of Ministers on 21 September 2011.

19 Heintschel von Heinegg, a.a.O (Anm. 11).

Drei Fragen an **Thomas Fitschen**

Was sind die wichtigsten Themenfelder der Cyber-Außenpolitik der Bundesregierung und wo finden sich die Vereinten Nationen in der digitalen Agenda?

Die deutsche Cyber-Außenpolitik hat drei Kernziele: Erstens wollen wir erreichen, dass die wirtschaftlichen Chancen der Digitalisierung in Deutschland und in weniger entwickelten Teilen der Welt genutzt werden. Zweitens setzen wir uns dafür ein, dass die Menschenrechte online wie offline geschützt werden. Hierzu zählt unser Engagement zum Schutz der Privatsphäre. Dies ist nur möglich, wenn wir – drittens – gemeinsame Lösungen für neue Bedrohungen finden. Vertrauensbildung und die Stärkung des Völkerrechts sind die entscheidenden Stichworte. Unsere Aktivitäten in den UN, in der Europäischen Union und in Organisationen wie der OSZE spiegeln sich in der ›Digitalen Agenda‹ wider. Für Deutschland ist besonders wichtig, dass die Kontrolle über das Internet dem Multistakeholder-Prinzip folgt. Wir müssen sicherstellen, dass das Netz offen und nicht fragmentiert bleibt. Auch die ›digitale Spaltung‹ zwischen den Industrie- und Entwicklungsländern muss beseitigt werden. Das ist auch der Auftrag der Überprüfungskonferenz WSIS+10 im Dezember 2015.

Deutschland hat mit Brasilien bei den Vereinten Nationen Initiativen zum Schutz der Menschenrechte im Cyberraum eingebracht. Was wurde erreicht?

Im Jahr 2013 haben Deutschland und Brasilien eine Initiative zum Schutz der Privatsphäre im digitalen Zeitalter in der Generalversammlung gestartet. In einer im Dezember 2014 verabschiedeten Resolution stellte die Generalversammlung fest, dass die (Menschen-)Rechte, die alle im täglichen Leben haben, auch online geschützt werden müssen. Das klingt ganz einfach, aber in den Jahren zuvor hätten längst nicht alle Staaten dieser Aussage zugestimmt. Auch bei den Beschlüssen des Menschenrechtsrats, die im Jahr 2015 zur Einsetzung eines Sonderberichterstatters über das Recht auf Privatheit führten, waren unsere beiden Länder die treibenden Kräfte. Wir haben die entsprechenden Entscheidungen vorbereitet und in mehreren Paneldiskussionen in Genf und New York auch den Austausch mit Wissenschaft und Zivilgesellschaft ermöglicht. Uns war klar, dass das Thema politisch sensibel ist. Aber in langen Verhandlungen konnten wir erreichen, dass am Ende alle Staaten zustimmten.

Die Bundesregierung möchte ein ›Völkerrecht des Netzes‹ definieren. Welche Rolle spielen die Vereinten Nationen?

Die Vereinten Nationen sind der wichtigste Ort für den Dialog über diese Frage. Die Generalversammlung hat bereits mehrere Gruppen von Regierungssachverständigen eingesetzt, die eine Bestandsaufnahme machen und den Staaten Empfehlungen unterbreiten sollten. In diese Gruppe hat der UN-Generalsekretär auch einen deutschen Experten aus dem Cyber-Koordinierungsstab des Auswärtigen Amtes berufen. Nach schwierigen Anfangsjahren kam die Gruppe im Jahr 2015 zu dem Schluss, dass die Normen des Völkerrechts auch im Cyberraum gelten, und machte Vorschläge für Grundregeln verantwortlichen Verhaltens von Staaten sowie für Maßnahmen zur Vertrauensbildung. Auch dies war nicht selbstverständlich und setzt dem zwischenstaatlichen ›Verkehr‹ im Netz wichtige Leitplanken.

Dr. Thomas Fitschen, geb. 1959, ist seit 2015 der Beauftragte im Auswärtigen Amt für die Vereinten Nationen, Cyber-Außenpolitik und Terrorismusbekämpfung.

›Internetgemeinde‹ die am schnellsten wachsende Bevölkerungsgruppe in der Geschichte der Menschheit in einem fast anarchischen Cyberraum. Internet Governance ist daher zu Recht als Weg aus dem Dilemma erkannt worden, jedoch steckt sie noch in den Kinderschuhen.

Die Internetnutzer, von denen zwei Drittel in sogenannten entwickelten Ländern leben, erledigen im Cyberraum ihre täglichen Geschäfte, tauschen Wissen, organisieren Kampagnen und ihr Privatleben. Dies alles ohne gemeinsame grenzüberschreitende Regeln, Gesetze, Regierung, Durchsetzungs- oder Kontrollmechanismen, Gerichte oder Polizei, die die Aktivitäten der Menschen in diesem Bereich schützen könnten.

Beachtlich scheint es, dass es eine Staatenallianz aus den Vereinigten Arabischen Emiraten (VAE) und Lettland war, die den Multistakeholder-Prozess bislang vorantrieb. Demokratieschwache Länder wie die VAE, Pakistan, China oder Nigeria, in denen es keine freie Zivilgesellschaft, jedoch eine schnell wachsende junge Internetgemeinde gibt, die alle bisherigen Normen der Gesellschaft in Frage stellt, setzen sich für einen Multistakeholder-Ansatz ein, um diesen kontrollieren zu können. Dies kann als ein Zugeständnis gewertet werden. Allerdings ist fraglich, ob die Staatenvertreter im Dezember 2015 wirklich einen Multistakeholder-Ansatz im Sinne des Begriffs vor Augen hatten oder nicht eher einen staatenzentrierten Ansatz, bei dem lediglich die eine oder andere Internetfirma zurate gezogen werden kann, wann immer es öffentlichkeitswirksam wäre.

Allen Bemühungen zum Trotz, die *terra incognita* Cyberraum zivilisiert zu ›besiedeln‹ und diesem Raum einheitliche Regeln und Vorschriften zu geben, steht Internet Governance noch am Anfang. Das Internet- oder Cyberregime ist allerdings neben dem Klimaregime das am schnellsten wachsende globale Regime. Es ist gerade einmal 20 Jahre her, dass John Perry Barlow im Jahr 1996 die erste ›Unabhängigkeitserklärung des Cyberspace‹ veröffentlichte.[20] In dieser Erklärung wies er bereits auf die Gefahren hin, über die wir uns heute weltweit Sorgen machen. Barlow war sich sicher, dass die Internetgemeinde ihre eigenen Gesellschaftsverträge entwickeln werde, um zu bestimmen, wie sie mit den Problemen umgehen solle. Für ihn stand dabei allerdings stets fest, dass die Problemlösung auf Grundlage der Menschenrechte gefunden werden müsse. Er sollte Recht behalten.

20 John Perry Barlow, A Declaration of the Independence of Cyberspace, Davos 1996, www.eff.org/cyberspace-independence