Völkerrecht in Zeiten des Netzes

Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht

FRIEDRICH EBERT STIFTUNG
Medienpolitik

Herausgeber
Friedrich-Ebert-Stiftung
Politische Akademie
Medienpolitik

Godesberger Allee 149
53175 Bonn

Autor
Dr. Matthias C. Kettemann, LL.M. (Harvard)
Goethe-Universität Frankfurt am Main
Exzellenzcluster „Die Herausbildung
normativer Ordnungen“

Redaktion
Norbert Bicher, Indira Kroemer

Gestaltung und Satz
Pellens Kommunikationsdesign GmbH, Bonn

Fotos
Sergey Nivens/fotolia.com; suze/photocase.de

Druck
bub Bonner Universitäts-Buchdruckerei, Bonn

Printed in Germany 2015

Die Position des Autors gibt nicht in jedem Fall die Position der Friedrich-Ebert-Stiftung wieder.

ISBN-Nr: 978-3-95861-328-7

Matthias C. Kettemann

Völkerrecht in Zeiten des Netzes

Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht

Inhaltsverzeichnis

Vorwort

Das weltweite Netz war und ist ein globales Freiheitsversprechen, ein Ort der Freiheit und der freien und offenen Kommunikation, ein Ort der bürgerlichen und unternehmerischen Selbstentfaltung, ein Ort des Zusammenlebens. Es war und ist ein schöner Traum, dass die digitale Gesellschaft eine offene, demokratische und pluralistische Gesellschaft ist – ein vernetzter Kontinent Europa und eine vernetzte Weltgesellschaft. Der Erfolg des weltweiten Kommunikationsnetzes basiert auf dessen freiheitlicher und offener Architektur. Doch dieser Traum und dieses Freiheitsversprechen sind angesichts der Enthüllungen der vergangenen beiden Jahre über die flächendeckende Ausspähung durch ausländische Nachrichtendienste, aber auch angesichts der Erkenntnisse über Grenzüberschreitungen der eigenen Dienste in Gefahr.

Seit mehr als zwei Jahren wissen wir von den Möglichkeiten ausländischer Geheimdienste und von der Existenz von Überwachungsprogrammen wie „PRISM“ und „TEMPORA“. Mit „PRISM“ soll die NSA auf die Serverdaten der großen Internetunternehmen zugreifen können. Unter dem Namen TEMPORA soll das eng mit der NSA kooperierende britische Government Communications Headquarters (GCHQ) den Datenstrom von mehr als 200 der wichtigen Transatlantik-Glasfaser-Verbindungen überwachen. Seitdem verging kaum eine Woche ohne neue Enthüllungen über die Ausspähaktionen und die Instrumente britischer und amerikanischer Geheimdienste. Bis heute reißen die Enthüllungen über Programme mit Namen wie „XKeyscore“ oder „Boundless Informant“ zur flächendeckenden Kommunikationsüberwachung, über die Überwachung von Regierungsmitgliedern und -institutionen, von Botschaften, Unternehmen und

Medien sowie von Bürgerinnen und Bürgern weltweit nicht ab. Inzwischen wissen wir, dass die ersten Enthüllungen zu „PRISM“ und „TEMPORA“ lediglich die Spitze des Eisberges darstellten – und vermutlich kennen wir bis heute nur einen Bruchteil des Ausmaßes. Was wir aber heute wissen: Nachrichtendienste sind in der Lage, weltweit nahezu die gesamte elektronische Kommunikation auszuspionieren – und sie tun dies auch in großem Umfang. Dies ist ein beispielsloser Angriff auf die Grund- und Freiheitsrechte von Bürgerinnen und Bürgern und eine Gefährdung einer offenen, freien und demokratischen Gesellschaft. Zugleich haben diese Enthüllungen das Vertrauen in die Informations- und Kommunikationstechnik und insbesondere in die weltweite Vernetzung nachhaltig erschüttert.

Auch aus Sicht der Vereinten Nationen hat die Überwachung der elektronischen Kommunikation besorgniserregende Ausmaße angenommen: die bestehenden Massenüberwachungsprogramme seien als Bruch der Menschenrechte anzusehen. In ihrem Bericht „The right to privacy in the digital age“ betont die UN-Hochkommissarin für Menschenrechte, Navi Pillay, dass diese Praxis wichtige Prinzipien, die den Kern jedermanns Persönlichkeitsrechte betreffen, in Frage stellen.

Eigentlich hätten diese Enthüllungen der vergangenen beiden Jahre eine Zäsur darstellen müssen. Doch wenn man sich fragt, was seitdem tatsächlich passiert ist, müssen wir feststellen, dass es bislang kaum politische Konsequenzen gegeben hat. Zwar wird endlich die Frage um den Erhalt bzw. in vielen Bereichen die Rückgewinnung digitaler Souveränität und technologischer Kompetenz diskutiert. Eine Debatte aber auf internationaler Ebene über die Grenzen der gegenseitigen Ausspähung und über mögliche rechtliche Konsequenzen steht weiterhin aus.

In ihrem Koalitionsvertrag haben sich CDU/CSU und SPD auf Folgendes verständigt:

> „Um die Grund- und Freiheitsrechte der Bürgerinnen und der Bürger auch in der digitalen Welt zu wahren und die Chancen für die demokratischen Teilhabe der Bevölkerung am weltweiten Kommunikationsnetz

zu fördern, setzen wir uns für ein Völkerrecht des Netzes ein, damit die Grundrechte auch in der digitalen Welt gelten. Das Recht auf Privatsphäre, das im Internationalen Pakt für bürgerliche und politische Rechte garantiert ist, ist an die Bedürfnisse des digitalen Zeitalters anzupassen."

Die Friedrich-Ebert-Stiftung hat dankenswerterweise Dr. Matthias C. Kettemann gebeten, ein Gutachten zu der Fragestellung „Bedarf es eines ‚Völkerrechts des Netzes'" zu erstellen. Ziel des Gutachtens ist es, aufzuzeigen, ob es eines expliziten „Völkerrechts des Netzes" bedürfe und wie dieses ausgestaltet sein müsse. Das Gutachten kommt zu dem Ergebnis, dass der Terminus zwar zu kurz greife, dass es aber sehr wohl eines solchen „Völkerrechts des Netzes" im Sinne eines auf staatliche und nichtstaatliche Aktivitäten mit Bezug zum Internet anwendbaren internationalen Normenbestandes bedarf, um Freiheit und Sicherheit effektiv zu schützen. Es komme vor allem darauf an, das bestehende Völkerrecht vollumfänglich anzuwenden. Denn: Es sei weniger das ‚Völkerrecht des Netzes' lückenhaft, es sind vielmehr die völkerrechtswidrigen Handlungen einzelner Staaten, die das Recht auf Privatsphäre verletzen und den Charakter des Internets als Vertrauensraum gefährden.

Dr. Matthias C. Kettemann macht mit seinem Gutachten deutlich, dass es des Zusammenspiels und des Ineinandergreifens von nationalem Recht, europäischem Recht und Völkerrecht bedarf, um über die verschiedenen Regelungsregimes und um allen faktischen Schwierigkeiten des Mehrebenensystems zum Trotz die Grundrechte zu gewährleisten und Rechtsschutz zu garantieren. Wir müssen das Recht auf allen Ebenen weiterentwickeln, um die geltenden Grund- und Freiheitsrechte auch in der digitalen Welt wirksam zu schützen und die demokratische Teilhabe am weltweiten Kommunikationsnetz zu verstärken – und wir müssen das Recht auch durchsetzen. Die im Offline-Zeitalter geltenden Wertevorstellungen müssen für das 21. Jahrhundert fit gemacht und die bestehenden technischen Strukturen diesen Vorgaben angepasst werden. Notwendig ist quasi ein allgemeines „Screening" aller rechtlichen Vorgaben mit digitalen Bezügen auf nationaler, europäischer und internationaler Ebene,

um bestehende Lücken und Aktualisierungsbedarfe oder auch Umsetzungsdefizite erkennen und diesen begegnen zu können.

Dazu brauchen wir in Europa und mit den USA einen Dialog über den Wert der offenen, freien und demokratischen digitalen Gesellschaft – für den wir gemeinsam eintreten. Eine freie, offene und demokratische Gesellschaft setzt voraus, dass es Räume gibt, in denen man sich unbeobachtet bewegen und in denen man unbeobachtet kommunizieren kann. Wenn es diese Räume nicht mehr gibt, wenn jeder und jede ständig fürchten muss, ohne Anlass beobachtet, ausspioniert und hinsichtlich möglicher Verhaltensauffälligkeiten durchleuchtet zu werden, führt dies dazu, dass sich die Menschen in ihrer Kommunikation nicht mehr frei fühlen und dass in solchen Situationen eine Form der Selbstzensur greift. Der Staatsrechtler Dieter Grimm hat dies einmal wie folgt skizziert: „Der allwissende Staat wird schnell zum allmächtigen Staat. Freiheit gibt es dagegen nur im begrenzten Staat." Und genau darum muss es wieder gehen: den Staat und seine Nachrichtendienste in die Grenzen zu weisen.

Lars Klingbeil, MdB
Netzpolitischer Sprecher
der SPD-Bundestagsfraktion

Kurzzusammenfassung in 20 Thesen

Zum Bedarf nach einem „Völkerrecht des Netzes“

1. Die Staaten der Welt haben sich darauf geeinigt, dass der Aufbau einer menschenzentrierten, entwicklungsorientierten Informationsgesellschaft nur unter Berücksichtigung der Ziele und Grundsätze der Charta der Vereinten Nationen und der Achtung des Völkerrechts und der Menschenrechte funktionieren kann.
2. Das bestehende Völkerrecht ist vollumfänglich auf das Internet anzuwenden.
3. Der Fokus auf das Völkerrecht ist unterkomplex; die Normen der Internet Governance, deren Ziel es ist, die Integrität des Internets und dessen Potenzial zur Entfaltung der menschlichen Entwicklung zu sichern, sind weit vielfältiger als suggeriert wird: Code und hybride Regelungsarrangements sind Teil der normativen Infrastruktur.
4. Es bedarf indes sehr wohl eines „Völkerrechts des Netzes“ – im Sinne eines auf staatliche und nichtstaatliche Aktivitäten mit Bezug zum Internet anwendbaren internationalen Normenbestandes, um Freiheit und Sicherheit effektiv zu schützen.
5. Begriffliche Unsicherheiten in politischen Dokumenten (Regierungserklärung, Digitale Agenda) sind problematisch, da sie den Blick auf die wirklichen (und bestehenden) Herausforderungen der Anwendung des Völkerrechts auf staatliche und nichtstaatliche Aktivitäten mit Bezug zum Internet verstellen.

Zu den inhaltlichen Anforderungen an ein „Völkerrecht des Netzes“

6. Voraussetzung für die Ausübung der Menschenrechte im Internet sind der Zugang zum Internet (der durch Infrastrukturmaßnahmen sicherzustellen ist) und der Zugang zu Internet-Inhalten (die vor Zensur zu schützen sind). Innerstaatlich ist das Recht auf Internetzugang grundrechtlich als Ausfluss des Würdegebots und des Sozialstaatprinzips geschützt.

7. Alle Menschenrechte, die offline gelten, gelten auch online.
8. Der Schutz des Privatlebens – auch im Internet – schafft die Voraussetzungen für die Ausübung der Meinungsäußerungsfreiheit; beide Rechte sind eng verquickt; die Meinungsäußerungsfreiheit (und ihre korrelierenden Freiheiten, wie die Informationsfreiheit) ist das katalysierende Menschenrecht im Internet, das die Realisierung aller anderen Menschenrechte ermöglicht.
9. Nicht das Völkerrecht des Netzes ist lückenhaft; es sind die völkerrechtswidrigen Handlungen einzelner Staaten, die das Recht auf Privatsphäre verletzen und den Charakter des Internets als Vertrauensraum gefährden; ein neuer Vertrag schafft keine Abhilfe.
10. Demokratische Teilhabe am Internet kann dadurch gefördert werden, dass Einzelne verstärkt in globale Prozesse der Internet Governance integriert werden.
11. Der Multistakeholder-Ansatz ist eine genuin neue Art der normativen Entwicklung; er findet seine Verwirklichung in der Entwicklung und Anwendung durch Regierungen (Staaten), den Privatsektor (Unternehmen) und die Zivilgesellschaft (Individuen) in ihren jeweiligen Rollen von Instrumenten und Prozessen zur Regelung des Internets.
12. Demokratische Teilhabe am Internet setzt Zugang voraus. Mehr als die Hälfte der Menschheit hat noch immer keinen Zugang zum Internet. Bis 2020 will die UNO alle Menschen ans Netz holen; auch die deutsche Regierung hat sich zum Breitbandausbau deutschlandweit bis 2018 bekannt. Beide Prozesse sind zu überwachen und zu fördern.
13. Accountability (Rechenschaftspflicht) meint im Kontext der Internetregulierung, dass die formalen und informellen Institutionen der Internet Governance sich gegenüber allen Stakeholdern rechtfertigen müssen.
14. Dem Völkerrecht des Netzes sind klare inhaltliche Richtlinien für die nationale Politik zu entnehmen: Aus dem Prinzip der Offenheit und Freiheit der Netze lässt sich eine abgestufte daseinsvorsorgliche Verpflichtung zugunsten eines möglichst unregulierten Zugangs zu möglichst flächendeckend bereitgestellten öffentlichen WLAN-Netzen ableiten.

Zum Zusammenspiel von nationalem Recht, europäischem Recht und Völkerrecht

15. Im Internet herrschen viele verschiedene Regelungsregime; allen faktischen Schwierigkeiten des Mehrebenensystems zum Trotz verbleibt die Pflicht, Grundrechte zu gewährleisten und Rechtsschutz zu garantieren, maßgeblich bei den Staaten.
16. Alle Normen der Internet Governance müssen sowohl ihrem Produktionsverfahren als auch ihrem Gehalt nach rechtstaatlichen Standards zumindest in ihren Wesenszügen genügen.
17. Die normative Ordnung des Internets (bei der es sich um ein Gemisch von Rechtsordnungen und Regelungsarrangements handelt) ist defizitär – doch dies sind alle anderen Rechtsordnungen auch; die Dynamik sozialer Prozesse bedingt responsive Regulierung.
18. Das gemeinsame Ziel aller normativen Maßnahmen muss es sein, das Vertrauen in die Integrität des Internets wiederherzustellen.
19. Resolutionen und Berichte helfen bei der Kristallisierung völkergewohnheitsrechtlicher Pflichten mit Bezug zum Internet. Der effektive Schutz einer menschenrechtssensibleren Kommunikationsordnung setzt kein „neues“ Völkerrecht voraus.
20. Systematisierungs- und Evaluierungsleistungen der Wissenschaft können angesichts der sprunghaft wachsenden Normenproduktion im Mehrebenensystem durch öffentliche und private Normproduzenten entscheidende Beiträge leisten.

Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfrMRK	Afrikanische Konvention für die Rechte der Menschen und Völker
AJIL	American Journal of International Law
AMRK	Amerikanische Menschenrechtskonvention
BRICS	Brasilien, Russland, Indien und China
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
DNS	Domain Name System
EGMR	Europäischer Gerichtshof für Menschenrechte
EJIL	European Journal of International Law
EMRK	Europäischen Menschenrechtskonvention
EuGH	Gerichtshof der Europäischen Union
FISA	Foreign Intelligence Surveillance Act
GA	General Assembly
GAC	Governmental Advisory Committee
GG	Grundgesetz
GGE	Gruppe von Regierungsexperten für Entwicklungen im Feld der Information und Telekommunikation im Kontext von Informationssicherheit
GV	Generalversammlung
HRIA	Human Rights Impact Assessments
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	Information and Communcation Technologies
IGF	Internet Governance Forum
ILC	International Law Commission
IP	Internet Protocol

IPbpR	Internationaler Pakt über bürgerliche und politische Rechte (Zivilpakt)
IT	Informationstechnologie
ITU	Internationale Telekommunikations-Union
JZ	Juristenzeitung
MIND	Multistakeholder Internet Dialog
OHCHR	Office of the UN High Commissioner for Human Rights
Res.	Resolution
TISA	Trade in Services Agreement
TTIP	Transatlantic Trade and Investment Partnership Agreement
TPP	Trans-Pacific Partnership Agreement
UNESCO	United Nations Economic, Social and Cultural Organization
UNO	United Nations
URL	Uniform Resource Locator
WGIG	Working Group on Internet Governance
WLAN	Wireless Local Area Network
WSIS	Weltgipfel zur Informationsgesellschaft (2003 und 2005)
WSIS+10	Review-Treffen zum Weltgipfelprozess zur Informationsgesellschaft (2015)
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Rechtsvergleichung

I. Zielsetzung

Ich wurde von der Friedrich-Ebert-Stiftung e.V., Abteilung Politische Akademie, Medienpolitik, beauftragt, ein wissenschaftliches Gutachten zu erstellen, das die Frage beantwortet, ob es eines „Völkerrechts des Netzes" explizit bedürfe (III.A) und wie dies ausgestaltet werden müsste, um die geltenden Grund- und Freiheitsrechte (insbesondere bezogen auf die Privatsphäre im digitalen Zeitalter) zu schützen (III.B.1.–3.) und die Chancen für eine demokratische Teilhabe am weltweiten Kommunikationsnetz zu verstärken (III.B.4.). Außerdem wurde ich gebeten zu bewerten, ob es im Zusammenspiel von nationalem, europäischem und internationalem Recht Regelungs- oder Umsetzungsdefizite gebe (III.C.2) – und falls ja, welche normativen Ansätze auf welcher Ebene zu verfolgen seien (III.C.3).[1]

Zunächst erfolgt eine kurze Einführung in die Rechtsgeschichte des Internets (II.A.) und die Rolle des Rechts in der Technikregulierung (II.B.). Die Einleitung schließt mit einem Überblick über zwei Regierungsdokumente – Koalitionsvertrag und Digitale Agenda –, in beiden findet das „Völkerrecht des Netzes" prominent Erwähnung (II.C.). Leider herrschte bei den Verfassern Unklarheit darüber, was das Wesen des „Völkerrechts des Netzes" ausmacht und welche Zwecke ihm zugeschrieben werden können. Diese Unklarheit zu beheben und herauszuarbeiten, was das „Völkerrecht des Netzes" wirklich leisten kann, ohne es mit unerfüllbaren Aufgaben zu überfrachten, ist Ziel dieses Gutachtens.

1 Das Gutachten stützt sich auf meine bisherigen Forschungen und Publikationen zu dem Thema und namentlich auf meine Habilitationsschrift, die ich als Habilitand am Exzellenzcluster „Die Herausbildung normativer Ordnungen" an der Goethe-Universität Frankfurt am Main anfertige. Sämtliche URLs wurden zuletzt am 1.10.2015 abgerufen.

II. Einführung
Internationale Internetregulierung zwischen Semantik, Normativität und Politik

A. Recht und Governance im Internet

Das Konzept der „digitalen Welt“ suggeriert eine neue Lebensrealität jenseits des staatlichen Territoriums, in der Recht bzw. Menschenrechte nicht gälten – beides ist falsch. Der „Cyberspace“ ist keine rechtliche *terra nullius*.[2] Recht (und Völkerrecht) gelten online wie offline. Menschenrechte gelten online wie offline. Das *Ob* der Geltung ist unbestritten; das *Wie* der Anwendung des geltenden Rechts und das *Wohin* der rechtspolitischen Entwicklung werden in Folge im Mittelpunkt stehen.

Zunächst zur Terminologie: Das „Internet“ ist ein globales Netzwerk von Netzwerken, das unter Verwendung eines gemeinsamen Protokolls weltweite Kommunikation ermöglicht.[3] Der Begriff Internet ist eine kombinierter Begriff, der sich aus *interconnection* of *networks* bzw. *internetwork* ableitet.[4] „Das Internet“ besteht also aus verschiedenen, miteinander verbundenen „Internets“.[5] Wenn in Folge vom „Internet“ die Rede ist, dann ist immer das globale Netzwerk der Netzwerke gemeint.

Die Governance des Internets (oder „Internet Governance“) umfasst die „Entwicklung und Anwendung durch Regierungen, den Privatsektor und die Zivilgesellschaft, in ihren jeweiligen Rollen, von gemeinsamen Prinzipien, Normen, Regeln, Entscheidungsfindungsprozessen und Programmen, die die Weiterentwicklung und Verwendung des Internets gestalten“.[6] Verschiedene komplexe Aspekte der Internetarchitektur – wie das System der IP-Adressenverwaltung, der Zuweisung der Nummern und Namen, das Management der DNS Root Zone File[7] – fallen ebenso unter

die Internet Governance wie im Kern völkerrechtliche Fragen, wie die Grenzen staatlicher Souveränität über Internetressourcen, der Schutz der Privatsphäre online und die Bekämpfung von Hassrede im Netz.

Besonders die rechtsförmige Behandlung von Fragen der internationalöffentlichen Internetpolitik gewinnt in letzter Zeit an Bedeutung. Der Grund dafür ist die digitale Konvergenz. Einst sahen wir Filme auf unseren Fernsehern oder im Kino, hörten Musik auf dem CD-Player, kauften und lasen gedruckte Zeitungen, schalteten das Radio an, gingen in Bibliotheken, um gedruckte Bücher auszuleihen und telefonierten mit Festnetztelefonen. Heute verwenden wir für all diese Tätigkeiten zunehmend das Internet und internetbasierte Dienste, sei es am Computer, auf einem elektronischen Lesegerät oder am Smartphone.[8] Mit dem Internet der Dinge wird sich dieser Trend nur verstärken. Die verschiedenen Medien – TV, Bücher, Radio, CDs, Zeitungen – hatten je eigene Regimes, Regeln und Akteure. Nun weisen sie normativ einen gemeinsamen Nenner auf: die Lieferung von Inhalten durch IP-basierte Dienste.[9]

Das Völkerrecht des Netzes ist kein neues Rechtsgebiet.[10] 2009 popularisierte Robert Uerpmann-Wittzack den Begriff „Internetvölkerrecht“,[11] das „all rules of public international law pertaining to the functioning and use of the internet“[12] umfasse. Andere Autoren schrieben vom „supranational cyberspace law“ oder „supranational Internet law“, das sich gemeinsam mit einem „customary law of the Internet“ entwickle.[13] Im Kern ist das „Völkerrecht des Netzes“ ein praktischer Begriff für die Summe völkerrechtlicher Regeln, die auf internetbezogene Sachverhalte Anwendung finden. Allerdings suggeriert der Begriff eine umfassende Regelungsabsicht „des Internets“ durch ein Rechtsgebiet. Doch es kann nicht ein Völkerrecht des Netzes geben. Das *Umwelt*völkerrecht beruht auch nicht auf einem Vertrag und klärt unter Ausschluss genereller (völkerrechtlicher) Regeln und anderer Regime, wie der Menschenrechte, völkerrechtlich relevante Fragen des Umgangs mit natürlichen Ressourcen.

„Völkerrecht des Netzes“, Völkerrecht des Internets, Internetvölkerrecht bzw. Internationales Internetrecht sind mögliche Begriffe für den Bestand

an (völkerrechtlichen) Normen, die sich auf das Internet und menschliche Aktivitäten im Internet beziehen. Angesichts der gewählten Formulierung in Koalitionsvertrag, Digitaler Agenda und Gutachtensauftrag geht dieses Gutachten in Folge aber vom Begriff „Völkerrecht des Netzes“ aus.[14]

B. Responsivität charakterisiert die Technikregulierung

Recht ist responsiv. Neue Technologien ziehen neue Regeln mit sich. Zwölf Jahre, nachdem Samuel Morse in New York 1838 das erste funktionstüchtige Telegrafensystem präsentiert hatte, unterzeichneten Österreich, Preußen, Bayern und Sachsen den Staatsvertrag über die Bildung des „deutsch-österreichischen Telegraphenvereins“,[15] um „dem öffentlichen wie dem Privatverkehre Ihrer respectiven Staaten die Vortheile eines nach gleichmäßigen Grundsätzen geregelten Telegraphensystemes zuzuführen“[16].

Innovationen der Informations- und Kommunikationsordnung mit den Mitteln des Völkerrechts zu regulieren, hat mithin Tradition. Dennoch wird beizeiten Kritik daran laut, neuen technischen Entwicklungen sogleich ein neues Teilrechtsgebiet – etwa ein „Völkerrecht des Netzes“ – angedeihen zu lassen.[17] Besser, so etwa Frank H. Easterbrook in einer bekannten Kritik eines eigenen Rechtsregimes für den „Cyberspace“, sei es, allgemeine Regeln anzuwenden.[18] Allerdings liegt Easterbrooks Ansatz der Fehlschluss zugrunde, dass die Benennung eines neuen Teilrechtsgebietes einen normativen Neubeginn notwendig macht. Das würde in der Tat zu einer Fragmentierung des Rechts(systems) führen. Diese Gefahr kann allerdings vermieden werden, wenn das Recht sich an neue soziale Entwicklungen dergestalt anpasst, dass, wo möglich, bestehende Regeln angewandt bzw. durch die Wissenschaft und Judikatur präzisiert werden und, nur wo nötig, neue Regeln entwickelt werden; wobei stets generelle Regeln des Gesamtsystems teilsystemimmanente Zentrifugalkräfte zügeln.[19]

C. Das „Völkerrecht des Netzes“ als politisches Desiderat

Dies ist der Hintergrund, vor dem, sowohl im Koalitionsvertrag von 2013 als auch in der Digitalen Agenda 2014–2017, ein „Völkerrecht des Netzes“ gefordert wird. Die Quellen belegen, dass die Bedeutung völkerrechtlicher Internetregulierung unterschiedlich verstanden wird; ihre Kritik bereitet den Boden für die folgenden Teile des Gutachtens, weshalb sie nun kritisch präsentiert werden.

Im Koalitionsvertrag bekennen sich CDU, CSU und SPD unter dem Titel „IT-Infrastruktur und digitaler Datenschutz“ zur Stärkung und Gestaltung der deutschen und europäischen Internet-Infrastruktur „als Vertrauensraum“: zum Zweck, „Freiheit und Sicherheit im Internet zu schützen“.[20] Das „Völkerrecht des Netzes“ wird doppelt funktional konzipiert:

> „*Um* die Grund- und Freiheitsrechte der Bürgerinnen und der Bürger auch in der digitalen Welt zu wahren und die Chancen für die demokratischen Teilhabe der Bevölkerung am weltweiten Kommunikationsnetz zu fördern, setzen wir uns für ein *Völkerrecht des Netzes* ein, *damit* die Grundrechte auch in der digitalen Welt gelten.“[21]

Die Koalition will sich also „für ein Völkerrecht des Netzes“ einsetzen (was impliziert, dass es keines gebe) mit drei Zielen: 1. Grundrechtsschutz; 2. Wahrung von demokratischen Teilhaberechten am weltweiten Kommunikationsnetz; und 3. um die Geltung der Grundrechte „in der digitalen Welt“ sicherzustellen.

Auch die Digitale Agenda vom August 2014[22] bestätigt, dass internationale Normen angesichts der Globalität des Netzes essenziell sind:

> „Die Schaffung von Regeln und Rahmenbedingungen für das globale Netz kann nicht alleine auf nationaler Ebene erfolgen, sondern muss auf europäischer und internationaler Ebene eingebettet und flankiert werden.“[23]

Unklar wird es dann, wenn „Klarheit“ gefordert wird. So heißt es in der Digitalen Agenda weiter:

> „Wir wollen Klarheit über das anwendbare „Völkerrecht des Netzes“ herstellen, um die geltenden Grund- und Freiheitsrechte auch in der digitalen Welt wirksam zu schützen und die Chancen für eine demokratische Teilhabe am weltweiten Kommunikationsnetz zu verstärken.“[24]

Bemerkenswert ist wieder die funktionale Betrachtung: Es wird „Klarheit“ erwünscht über das anwendbare (daher implizit präexistente) „Völkerrecht des Netzes“, um Menschenrechte zu schützen (die aber schon gälten) und Teilhabechancen zu verstärken. Während im Koalitionsvertrag ein „Völkerrecht des Netzes“ also erst zu schaffen ist, werden in der Digitalen Agenda schärfere Konturen eingefordert.[25]

Die Bekenntnisse in Koalitionsvertrag wie Digitaler Agenda, auch wenn ihnen vom Telos (Grundrechtsschutz stärken, Völkerrecht des Netzes bewusster konturieren) zuzustimmen ist, sind problematisch, weil sie nicht der Problemabschichtung in einem komplexen normativen Feld dienen, sondern begrifflich unstimmig und inhaltlich zumindest unscharf sind.[26] Drei Gründe legen diese Bewertung nahe; ihre Diskussion strukturiert den Hauptteil des Gutachtens (III.):

- Der Fokus auf das Völkerrecht ist unterkomplex; die Normen der Internet Governance sind weit vielfältiger als suggeriert wird (III.A.1).
- Es bedarf eines „Völkerrechts des Netzes“, um Freiheit und Sicherheit im Internet zu schützen (III.A.2.)
- Es existiert schon ein Normenbestand, der als „Völkerrecht des Netzes“ bezeichnet werden kann (III.A.3.).

2 Stephan Hobe, Cyberspace – der virtuelle Raum, in Josef Isensee, Paul Kirchhof et al. (Hrsg.), Handbuch des Staatsrechts, Band XI: Internationale Bezüge, 3. Aufl. (2013), § 231.

3 Matthias C. Kettemann, Internet Governance, in Dietmar Jahnel, Peter Mader, Elisabeth Staudegger (Hrsg.), IT-Recht, 3. Aufl. (Wien: Verlag Österreich, 2013), 43-63.

4 Lydia Parziale et al., TCP/IP Tutorial and Technical Overview, 8. Aufl. (IBM: IBM Redbooks, 2006), 4.

5 Vgl. RFC 675 (Vinton Cerf, Yogen Dalal, Carl Sunshine), Specification of Internet Transmission Control Program, December 1974, http://tools.ietf.org/html/rfc675. Im Englischen wird die Unterscheidung klarer: „The Internet" besteht nur einmal; es beinhaltet aber unzählige „internets".

6 Arbeitsgruppe über Internet Governance (WGIG), Bericht der Arbeitsgruppe (2005), Abs. 10, http://www.wgig.org/docs/WGIGREPORT.pdf.

7 Karl Auerbach, Deconstructing Internet Governance (2004), http://www.cavebear.com/archive/rw/deconstructting-internet-governance-ITU-Feb26-27-2004.htm.

8 Zur Medienkonvergenz einführend: Milton N. Mueller, Networks and States. The Global Politics of Internet Governance (Cambridge, MA: MIT Press, 2010), 9.

9 Vgl. ibid., 10.

10 Vgl. Antonio Segura-Serrano, Internet Regulation and the Role of International Law, Max Planck Yearbook of United Nations Law, Vol. 10 (Den Haag: Brill, 2006), 191-272.

11 Robert Uerpmann-Wittzack, Internetvölkerrecht, Archiv des Völkerrechts 47 (2009) 3, 261-283. Ähnlich: Joanna Kulesza, International Internet Law (London: Routledge, 2012).

12 Robert Uerpmann-Wittzack, Principles of International Internet Law, German Law Journal (2010) 11, 1245-1263 (1245), http://www.germanlawjournal.com/index.php?pageID=11&artID=1293.

13 Przemysław Paul Polański, Customary Law of the Internet: in the Search for a Supranational Cyberspace Law (Den Haag: T.M.C. Asser, 2007). Wobei hier zu bemerken ist, dass die Verwischung der Unterschiede zwischen Völkerrecht (also internationalem) Recht und supranationalem Recht nicht unproblematisch ist.

14 Das „Völkerrecht des Netzes" ist im Vergleich zur Internet Governance spezifisch juristisch aufgeladen und blendet Staatsrecht und Unionsrecht aus. Allerdings lassen sich die Lenkungskräfte im Internet nicht analysieren, wenn diese Dimensionen der Internet Governance ignoriert werden. Im Folgenden werde ich, wo nötig, auf die „politischen" Aspekte der Internet Governance eingehen, da sich nur vor der Hintergrundfolie der Gesamtheit normativer Herausforderungen im Internet die Bedeutung des Völkerrechts des Netzes abhebt. Im Lichte des Gutachtensauftrags verbleibt der Fokus aber auf völkerrechtlichen Fragen des Netzes.

15 Staatsvertrag zwischen Oesterreich, Preußen, Baiern und Sachsen vom 25. Juli 1850 über die Bildung des deutsch-österreichischen Telegraphenvereins, Allgemeines Reichs-Gesetz und Regierungsblatt für das Kaiserthum Österreich, Nr. CXXVII vom 30.9.1850, 266ff.

16 Ibid., Präambel.

17 Siehe Frank H. Easterbrook, Cyberspace and the Law of the Horse, University of Chicago Law School, Chicago Unbound (1996), 207ff.

18 Ibid., 213. Kritisch zu Easterbrooks Ansatz statt vieler: Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach, Harvard Law Review 113 (1999), 501ff (502).

19 Diese Debatte wird unter dem Titel der Fragmentierung des Völkerrechts sehr lebendig geführt. Siehe einführend den von Martti Koskenniemi finalisierten Bericht der International Law Commission (ILC), Fragmentation of International Law: Difficulties Arising from the Diversivication and Expansion of International Law, Report of the Study Group of the International Law Commission (Martti Koskenniemi), A/CN.4/L.682 vom 13.4. 2006, http://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf. Aber siehe: Mads Andenas, Eirik Bjorge (Hrsg.), A Farewell to Fragmentation: Reassertion and Convergence in International Law (Cambridge: Cambridge University Press, 2015) (mit Beiträgen, die zeigen, wie über internationale Gerichte dem Völkerrecht normative Zentrumsbindung eingeschrieben wird).

20 Deutschlands Zukunft gestalten: Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Legislaturperiode (Dezember 2013), 103, https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf (im Folgenden: „Koalitionsvertrag (2013)“).

21 Koalitionsvertrag (2013), 104 (Hervorhebungen durch den Verfasser).

22 Bundesregierung, Digitale Agenda 2014-2017, August 2014, http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (im Folgenden: „Digitale Agenda“).

23 Ibid., 35.

24 Ibid., 36 (Hervorhebung des Verfassers).

25 Auch auf den Informationsseiten zur Digitalen Agenda ist von der „Weiterentwicklung des ‚Völkerrecht des Netzes‘ und des Menschenrechtsschutz[es]“ die Rede – wiederum eine implizite Anerkennung dessen Existenz (Bundesministerium für Wirtschaft und Energie, Digitale Agenda (Informationsseite), http://www.bmwi.de/DE/Themen/Digitale-Welt/digitale-agenda.html (Hervorhebung des Verfassers).

26 Christian Walter, Cyber Security als Herausforderung für das Völkerrecht, JZ 14/2015, 685 - 693 (686).

III. Analyse

A. Bedarf es eines „Völkerrechts des Netzes"?

A.1. Der Fokus auf das Völkerrecht ist unterkomplex: Die „Internet Governance" ist nicht nur völkerrechtlich determiniert

Um Regulierungsansätze an das Internet zu verstehen, müssen wir uns bewusst machen, welche genuin eigene „Rechtsgeschichte" das Internet aufweist. In der Frühphase der Regulierung des Internets und von Handlungen mit Onlinebezug dominierten soziale Regeln.[27] Im Internet in seiner ersten Entwicklungsphase involvierte Programmierer sandten seit 1969 sog *Requests for Comments (RFCs)* aus, und Beschlussfassung über technische Standards wurde auf Grundlage von „rough consensus" durchgeführt. Erst 1994, nach Versuchen der Privatisierung des Domainnamensystems durch die US-Regierung, wurden Trends zu einer Verrechtlichung spürbar. Die so angelegte Distanz zu formalem Recht in der Internet Governance beeinflusst bis heute die Rolle des *soft law* sowie den Trend zur Selbstregulierung durch Multistakeholderprozesse.

Parallel zur Anwendung nationalen Rechts auf Sachverhalte mit Internetbezug entwickelten sich Normen der Internet Governance. Diese bestehen in der allgemein akzeptierten Definition von Internet Governance aus geteilten Prinzipien, Normen und Regeln, Entscheidungsfindungsmechanismen, Programmen und Codes – und innerhalb der Normen finden sich auch solche des Völkerrechts, aber eben nicht nur diese.

Anders als in vielen traditionelleren Regelungsmaterien spielen im Bereich der Internet Governance auch Programme und Codes eine bedeutende Rolle. Codes legen bestimmte Befehlsabfolgen fest, aber auch diese haben

eine menschenrechtliche Relevanz. Codes legen (oft natürlich in Befolgung entsprechender gesetzlicher Vorgaben) fest, ob Daten gespeichert werden, Suchmaschinenanbieter IP-Adressen protokollieren oder soziale Netzwerke den Ort veröffentlichen, von wo ein Update gepostet wird. Auch Algorithmen rücken zunehmend in den Fokus der Wissenschaft und werden auf ihre ethische und rechtliche Relevanz befragt.

Prinzipien (oder Grundsätze) der Internet Governance haben sich als zentrales regulatives Instrument zur Gestaltung des Internets entwickelt.[28] Einen normativen Höhepunkt (wenn auch keinen Endpunkt) fand die Entwicklung der Grundsätze der Internet Governance 2014 in den NETmundial Prinzipien (oder Prinzipien von Sao Paolo), die in einem lange andauernden Vorbereitungsprozess konzipiert und beim bis dato weltweit repräsentativsten Treffen zu Internet Governance vorgestellt wurden. Sie bestehen aus „gemeinsamen Prinzipien" und „wichtigen Werten", die beitragen zu einem „inclusive, multistakeholder, effective, legitimate, and evolving Internet governance framework".[29]

Dazu gehören Menschenrechte, der Schutz der Intermediäre, die Förderung kultureller und sprachlicher Vielfalt, die Sicherung eines einheitlichen und unfragmentierten Netzwerks der Netzwerke mit offener und verteilter Architektur, das eine befähigende Umgebung für Innovation darstellt und in dem offene Standards herrschen. Zu den Verfahrensprinzipien zur Weiterentwicklung der Internet Governance zählen der Erklärung zufolge der Multistakeholder-Charakter der Prozesse, eine offene, partizipative, konsensorientierte Governance, Transparenz, Accountability, der einschließende Charakter von Prozessen und Institutionen, ein verteiltes und dezentralisiertes Regelungs-Ökosytem und der kollaborative und partizipative Charakter von Diskursprozessen.

Diese Prinzipien sind formal nicht bindend; ihnen wohnt allerdings – alleine schon angesichts der legitimierenden Wirkung der Prozeduralisierung von Legitimität durch die Multistakeholderstruktur – eine gewissen Bindungskraft inne, die durch stete Bezugnahme auf sie in anderen normative Instrumenten und Prozessen nur erhöht wird.[30]

A.2. Es bedarf dennoch eines „Völkerrechts des Netzes“, weil nur Völkerrecht die Integrität des Internets legitim und effektiv schützen kann

Die Attraktivität des Völkerrechts ist ungebrochen. Aktuell stehen etwa die USA und China in Verhandlungen über einen völkerrechtlichen Vertrag über das Verbot von Cyberangriffen gegen kritische Infrastruktur. Gleichinhaltlich wäre ein entsprechendes Verbot auch über eine internetsensible Auslegung des gewohnheitsrechtlichen Interventionsverbots möglich, aber ein Vertrag schafft – in den Augen gerade mächtiger bzw. traditionellen Souveränitätskonzepten verbundedner Staaten – (Rechts)Sicherheit.[31] Die Ubiquität und grenzenlose Natur der Technologie, auf der das Internet beruht, macht eine nur einzelstaatliche Regulierung wirkungsarm; außer liefe ein Vertrauen auf nur nationale Regelungen auf die Gefährundung der Integrität des Internets hinaus – genau wie mangels koordinierter Aktion gegen den Klimawandel mittels Völkerrecht die Gefahren der Erderwärmung nicht gebannt werden könnten. Völkerrecht ist nötig, um die Integrität des Internets, die im Gemeinschaftsinteresse aller Staaten liegt, legitim und effektiv zu sichern.

Das ist keine neue Erkenntnis. Der Konsens hinsichtlich der Bedeutung von Völkerrecht für die Integrität des Internets wird schon in den Schlusserklärungen der Weltgipfel zur Informationsgesellschaft 2003 (Genf) und 2005 (Tunis) sichtbar. In der *Geneva Declaration of Principles* von 2003 (bestätigt im *Tunis Commitment* von 2005[32]) drücken Staaten ihren Wunsch aus,

> „to build a people-centred, inclusive and development-oriented Information Society, […] enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, *premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.*“[33]

Ähnliche Verwendungen der Staatengemeinschaft, diesmal einer regionalen, liest man bei der 2014 von der Europäischen Kommission veröffentlichten Mitteilung, die den EU-Ansatz an die Internet Governance und globale Internet-Politik darlegt.[34] Auch Deutschland bekennt sich durch sein vom Grundgesetz getragenes Rechtssystem zur Rolle des Völkerrechts „als Maßstab der Gerechtigkeit und des angemessenen Interessenausgleichs in den internationalen Beziehungen."[35] Gerade in einem Bereich wie der Regulierung des Internets muss mit Mitteln des Rechts – des Völkerrechts – Interessenausgleich auf Grundlage fairer Regeln betrieben werden. Das verpflichtet auch deutsche Behörden: Das Grundgesetz nimmt in Art. 23 GG Staatsorgane in die Verantwortung, nicht nur passiv auf Entwicklungen des Völkerrechts zu warten und diese dann zu rezipieren, sondern aktiv an der Bewältigung von weltgesellschaftlicher Herausforderungen mitzuwirken – und die Regulierung des Internets fordert ohne Zweifel bestehende normative Akteure und Regime heraus. Darüber hinaus bürgen das Würdegebot (Art. 1. Abs. 1 GG) und die generelle Grundrechtsbindung der deutschen Staatsgewalt auch in grenzüberschreitenden Sachverhalten für eine entwicklungsoffene und dynamische Grundrechtsensibilität aller Rechtssysteme, die unter deutsche Beteiligung entstehen.[36]

Jellinek formuliert die Erkenntnis von der Notwendigkeit des Völkerrechts zur Schaffung eines fairen Interessensausgleich als das „objective Principe"[37], das ein Zusammenleben Normsetzung basierend auf einer geteilten „Rechtsanschauung" nötig mache. Völkerrecht existiert, weil es notwendig ist; Völkerrecht regelt das Internet, weil dies nötig ist. Es ist das *ius necessarium* einer internationalen Gemeinschaft, in der das Internet eine bedeutende Rolle für viele Aspekte des wirtschaftlichen, sozialen und kulturellen, bürgerlichen und politischen Lebens spielt.

Die Integrität des Internets liegt im Gemeinschaftsinteresse aller Staaten – das hat wichtige rechtliche Folgen für jene Staaten, die kritische Infrastrukturen kontrollieren, wie die USA. Die Sicherheit, Stabilität, Robustheit, Resilienz und Funktionalität des Internets (also seine Integrität) sind im Lichte der technologischen Entwicklung inzwischen

Voraussetzung für das reibungslose Ablaufen nationaler volkswirtschaftlicher Prozesse und des internationalen Wirtschafts- und Finanzsystems, transnationaler Kommunikationsinfrastrukturen, Energienetze, nationaler, regionaler und internationaler Verteidigungsinfrastrukturen und natürlich auch Voraussetzung für die volle Realisierung aller Menschenrechte, der menschlichen Sicherheit und der menschlichen Entwicklung.[38]

A.3. Aber es gibt schon ein „Völkerrecht des Netzes" dergestalt, dass das Völkerrecht auf das Internet anzuwenden ist

Schon seit 1998 (dem Jahr der Gründung von ICANN und dem Beginn der Internationalen Politisierung und Verrechtlichung der Internet Governance) und in Folge jährlich wurde die Relevanz des Völkerrechts für das Internet auf Ebene der UNO-Generalversammlung thematisiert.[39] Seit 2010 erschienen darüber hinaus vier Berichte einer Group of Governmental Experts (GGE) für Entwicklungen im Feld der Information und Telekommunikation im Kontext von Informationssicherheit, die sich kooperativen regelbasierten Maßnahmen zur Bekämpfung von Online-Gefahren auf internationaler Ebene widmen und an denen Deutschland sich intensiv beteiligt.[40]

Deutlich wurde erstmals der Bericht von 2013,[41] in dem die GGE festhielt, dass die Anwendung von Normen, die aus dem bestehenden Völkerrecht abgeleitet werden, „essenziell" ist, um Risiken für den Weltfrieden und die internationale Sicherheit und Stabilität zu minimieren.[42] Völkerrecht und die Charta der Vereinten Nationen seien „applicable and […] essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [=information and communication technology] environment."[43] Dies gelte auch für den völkerrechtlichen Schutz der Souveränität und der Verantwortung, die dieser entfließe,[44] sowie der Menschenrechte.[45] Allerdings wies die GGE auch darauf hin, dass das Völkerrecht des Netzes noch nicht ausgereift sei.[46] In seinem Kommentar zur Arbeit der GGE für 2014 unterstrich Deutschland,[47] dass der Fortschritt hinsichtlich der „laws and rules that apply to use of [ICTs]" willkommen sei.

Von zentraler Bedeutung für das Völkerrecht des Netzes ist der Bericht der GGE von 2015,[48] der im Konsens von einer repräsentativen Gruppe von staatlichen Experten angenommen wurde, die unter anderem China, Deutschland, Russland und die USA umfasste.[49] Die GGE bestätigte erneut, dass Völkerrecht einen essenziellen Rahmen für die nationale Nutzung von Informations- und Kommunikationstechnologien darstelle.[50] Besonders hob die Gruppe dabei hervor:[51]

- Staaten verbleibt die Jurisdiktion über die informations- und kommunikationstechnologische (IKT)-Infrastruktur in ihrem Territorium.
- In der Nutzung von Information- und Kommunikationstechnologien müssen Staaten neben anderen Prinzipien des Völkerrechts jene der staatlichen Souveränität, souveränen Gleichheit, friedlichen Streitbeilegung und das Interventionsverbot respektieren. Alle völkerrechtlichen Verpflichtungen bleiben bestehen, insbesondere hinsichtlich des Schutzes von Menschenrechten und Grundfreiheiten.
- Die internationale Gemeinschaft strebt danach, IKTs auf friedliche Weise „for the common good of mankind“ zu nutzen; die Satzung der Vereinten Nationen ist vollumfänglich anwendbar auf das Internet.
- Staaten dürfen keine Proxies (Stellvertreter) verwenden, um Völkerrecht zu übertreten und dürfen nicht zulassen, dass ihr Territorium zu derartigen Handlungen missbraucht wird. Sollte eine derartige Handlung gesetzt werden, müssen sie ihrer völkerrechtlichen Verantwortlichkeit gerecht werden.

In seinem Bericht für 2015 an die GGE unterstrich Deutschland, dass Völkerrecht, „supplemented by non-binding norms that define and shape expectations“[52], die „minimum baseline that guides responsible state behavior in cyberspace“ darstellen sollte. Mit den non-binding norms spricht Deutschland Empfehlungen der Grupppe an für „voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment.“[53]

Das Völkerrecht ist also in seiner Gänze auf das Internet anzuwenden.[54] Die Gesamtheit der Normen, die anwendbar sind, können wir als „Völkerrecht des Netzes“ bezeichnen.

A.4. Zwischenfazit

Dieser Abschnitt war der Frage gewidmet, ob es eines Völkerrechts des Netzes bedarf. Die kurze Antwort lautet: Es bedarf eines Völkerrechts des Netzes, aber es besteht schon ein Normenbestand, der als „Völkerrecht des Netzes“ bezeichnet werden kann.

Recht ist dem Wesen nach responsiv. Neue soziale Realitäten schaffen Regelungsbedürfnisse. Rechtliche Zentrifugalkräfte sind eine Gefahr; diese Gefahr kann allerdings vermieden werden, wenn, wo möglich, bestehende Regeln angewandt bzw. durch die Wissenschaft und Judikatur präzisiert werden und nur dort, wo nötig, neue Regeln entwickelt werden.[55] Auch regimespezifische Meta-Regeln (also Regeln über die Regelproduktion) können normativen Zentrifugalkräften entgegenwirken, in dem sie Prinzipien aus dem allgemeinen Völkerrecht importieren).

Im Koalitionsvertrag bekennen sich CDU, CSU und SPD zur Stärkung und Gestaltung der deutschen und europäischen Internet-Infrastruktur „als Vertrauensraum“ zum Zweck, „Freiheit und Sicherheit im Internet zu schützen“. Nicht nur der Raum, auch das „Völkerrecht des Netzes“ wird doppelt funktional konzipiert. Diese begrifflichen Unsicherheiten und die formale Instrumentalisierung des Völkerrechts des Netzes sind problematisch, da sie den Blick auf die wirklichen (und bestehenden) Herausforderungen der Anwendung des Völkerrechts auf staatliche und nichtstaatliche Aktivitäten mit Bezug zum Internet verstellen. Außerdem beruhen sie auf einem unzutreffenden Verständnis des Verhältnissen von Menschenrechten und Völkerrecht des Netzes.

Zugleich ist der Fokus auf das Völkerrecht unterkomplex; die Normen der Internet Governance sind weit vielfältiger als suggeriert wird. Von besonderer Bedeutung sind Grundsätze der Internet Governance, die

unterschiedlichen rechtlichen Charakter haben. Ihr gemeinsames Hauptziel ist es, die Integrität des Internets zu sichern.

Es bedarf eines „Völkerrechts des Netzes", um Freiheit und Sicherheit im Internet zu schützen. Die Staaten der Welt haben sich schon im Prozess der Weltgipfel der Informationsgesellschaft (2003–2005) darauf geeinigt, gemeinsam den Aufbau einer menschenzentrierten, einschließenden, entwicklungsorientierten Informationsgesellschaft anzustreben, gestützt auf „Ziele und Grundsätze der Charta der Vereinten Nationen, das Völkerrecht und den Multilateralismus sowie unter voller Achtung und Einhaltung der Allgemeinen Erklärung der Menschenrechte."

Das „Völkerrecht des Netzes" muss nicht neu erfunden werden. Es existiert schon ein Normenbestand, der als „Völkerrecht des Netzes" bezeichnet werden kann. Bestehendes Völkerrecht ist einfach technologiesensibel anzuwenden. Dieser Ansatz ist in Lehre wie Staatenpraxis im Wesentlichen unwidersprochen. Zuletzt bestätigte die repräsentative UN-Gruppe von Regierungsexperten für Informationssicherheit in ihrem Bericht von 2015, dass Völkerrecht einen essenziellen Rahmen für die nationale Nutzung von Informations- und Kommunikationstechnologien darstelle.

Es wird wohl nie ein kohärentes, auf eine Rechtsquelle zurückzuführendes „Völkerrecht des Netzes" geben; aber das ist auch nicht nötig, um Freiheit und Sicherheit im Internet effektiv zu schützen – dafür reicht der Bestand an Normen, der beschreibend „Völkerrecht des Netzes" genannt werden kann; er reicht, er ist aber auch unersetzlich.

B. Inhaltliche Anforderungen an ein „Völkerrecht des Netzes"

B.1. Einleitung

Wie oben in III.A. ausgeführt, ist die Bezeichnung des für staatliche und menschliche Aktivitäten im Internet anzuwendenden Normenbestandes als „Völkerrecht des Netzes" durchaus legitim. Wenn hier von „inhaltlichen

Anforderungen“ die Rede ist, ist damit gemeint, welche zentralen Prinzipien und Werte der für das Internet relevante internationale Normenbestand reflektieren sollte. Das „Völkerrecht des Netzes“ stellt wie erläutert einen normativen Bestandteil der Internet Governance dar. Die Internet Governance hat ausweislich der Verpflichtungserklärung von Tunis das Ziel des Aufbaus einer menschenzentrierten, einschließenden und entwicklungsorientierten Informationsgesellschaft. Gemeinsame Grundsätze lassen sich auch der Erklärung von Sao Paolo sowie dem GGE-Bericht von 2015 entnehmen. Diese geben in einer Gesamtschau den Rahmen für das „Völkerrecht des Netzes“ vor und definieren seine inhaltlichen Konturen.

Im Folgenden sollen aber, dem Gutachtensauftrag entsprechend, vor allem die Verpflichtungen aller Stakeholder, besonders der Staaten, auf die Menschenrechte (und besonders auf das Recht auf Privatsphäre) interessieren. Allerdings sei bemerkt, dass andere grundlegende Prinzipien der Internet Governance mit Wirkung auf das Völkerrecht – wie besonders der Schutz der Intermediäre[56] – auch menschenrechtliche Fragen berühren. Dagegen wäre ein alleiniger Fokus auf menschenrechtliche Fragen in der größeren, politischen Debatte um die Zukunft der Internetregulierung verfehlt; nicht alles lässt sich auf Fragen des Menschenrechtsschutzes reduzieren, auch wenn Ziel und Zweck jeder Rechtsordnung der Schutz (der Würde) des Menschen ist. Das gilt natürlich auch für das Völkerrecht (generell; und jenes „des Netzes“). Die ultimative Einheit des Völkerrechts, dessen Sinnhorizont, ist das menschliche Wesen; und der „ultimate concern for the human being“ des Völkerrechts Essential.[57]

B.2. Schutz und Sicherung des Internetzugangs als Grundvoraussetzung der Realisierung aller Menschenrechte

Ohne Zugang zum Internet (Infrastrukturdimension) und Zugang zu Internet-Inhalten (Inhaltsdimension) können Menschen nicht am Möglichkeitsraum des Internets teilnehmen. Der Menschenrechtsrat der Vereinten Nationen hat zuletzt 2012 und 2014 Staaten aufgerufen, „to

promote and facilitate access to the Internet".[58] Er berief sich dabei unter anderem auf einen bedeutenden Bericht des UN-Sonderberichterstatters für Meinungsäußerungsfreiheit, Frank La Rue, von 2011,[59] der Internetzugang als Grundbedingung zur Ausübung der Kommunikationsfreiheiten anerkannte: „the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression".[60] Gleichzeitig ist die Meinungsäußerungsfreiheit aber auch ein „enabler" anderer Rechte, darunter wirtschaftlicher, sozialer und kultureller Rechte, wie das Recht auf Bildung, und bürgerlicher und politischer Rechte, wie die Versammlungsfreiheit.[61]

Voraussetzung für all die Ausübung der Menschenrechte im Internet sind also der Zugang zum Internet (der durch Infrastrukturmaßnahmen sicherzustellen ist) und der Zugang zu Internet-Inhalten (der vor Zensur zu schützen ist). Völkerrecht schützt beide Zugangsdimensionen. Artikel 19 Abs. 2 des Zivilpaktes garantiert die Verbindungstechnologien mit seinem Verweis auf den Schutz von Meinungsäußerung durch „any […] media of [one's] choice".[62] Die Menschenrechtskommission bestätigt dies in ihrem General Comment No. 34 zu Artikel 19.[63]

Während in manchen Staaten bereits ein Recht auf Internetzugang gesetzlich festgeschrieben ist oder sich aus dem Recht dogmatisch ableiten lässt,[64] ist eine explizite Kodifizierung weder national noch international Voraussetzung für das Bestehen des Rechts. Die völkerrechtlichen Verpflichtungen stecken den Rahmen ab, innerhalb dessen Deutschland die Sicherung des Internetzugangs garantieren muss.[65] Ein Recht auf Zugang lässt sich dogmatisch (für den deutschen Rechtsraum) als objektiv-rechtliche Grundrechtswirkung sowohl als eigenständiges Recht, umfasst vom Grundrecht auf Gewährleistung eines menschenwürdigen Existenzminimums (Art. 1 Abs. 1 iVm Art. 20 Abs. 1 GG) aber auch als rechtlich geschützte Vorbedingung der Ausübung anderer Rechte konstruieren.[66] Angesichts der zentralen Rolle, die das Internet inzwischen einnimmt,[67] entspricht diese Grundrechtswirkung einer positiven Leistungspflicht des Staates: ein unmittelbar verfassungsrechtlicher Leistungsanspruch[68] auf Gewährleistung eines menschenwürdigen Existenz-

minimums, die auch die „Sicherung der Möglichkeit zur Pflege zwischenmenschlicher Beziehungen und zu einem Mindestmaß an Teilhabe am gesellschaftlichen, kulturellen und politischen Leben umfasst."[69] Zwischenmenschliche Beziehungen werden angesichts der Kommunikationsmöglichkeiten der Informationsgesellschaft maßgeblich über das Internet gepflegt. Es liegt am Gesetzgeber, die „jeweiligen wirtschaftlichen und technischen Gegebenheiten" zu beachten und „die soziale Wirklichkeit zeit- und realitätsgerecht im Hinblick auf die Gewährleistung des menschenwürdigen Existenzminimums zu erfassen, die sich etwa in einer technisierten Informationsgesellschaft anders als früher darstellt."[70]

Das Recht auf Internetzugang in der Praxis zu verwirklichen ist auch wichtig für die menschliche Entwicklung. In der *Agenda for Sustainable Development* für 2030 bekennen sich die Staaten der Vereinten Nationen dazu, bis 2020 universellen und leistbaren Internetzugang in Entwicklungsländern zu sichern.[71] Hier müssen auch Staaten im Rahmen ihrer Verpflichtung zur Umsetzung des Rechts auf Entwicklung tätig werden.

Dominierende Technologieunternehmen stehen im Hinblick auf das Recht auf Zugang als Voraussetzung zur Ausübung anderer Menschenrechte in einer abgestuften menschenrechtlichen Verantwortung, die in den *Guiding Principles on Business and Human Rights: Implementing the United Nations „Protect, Respect and Remedy"* Framework expliziert wird.[72] Insbesondere dürfen sie nicht Menschenrechte durch unternehmerische Tätigkeit verletzen oder durch ihre Produkte dazu beitragen.

B.3. Schutz der Grund- und Freiheitsrechte

B.3.1. Prinzipiell: Was offline gilt, gilt online

Es ist eigentlich ganz einfach. Alle Menschenrechte, die offline gelten, gelten auch online.[73] Dies bestätigt nicht zuletzt der Menschenrechtsrat der Vereinten Nationen in seinen zwei einschlägigen Resolutionen von 2012 und 2014.[74] Gleichlautend heißt es jeweils in Absatz 1:

> „the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".

Das Gleiche liest man in der Resolution zum Recht auf Privatleben im digitalen Zeitalter: „the same rights that people have offline must also be protected online, including the right to privacy."[75] Auch die Menschenrechtskommission wendet Artikel 19 des Zivilpaktes unaufgeregt auf das Internet an:

> „Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3."[76]

Dieses klare Bekenntnis zur technologischen Neutralität des Menschenrechtsschutzes wurde vom Europäischen Gerichtshof für Menschenrechte in seiner *Yildirim*-Entscheidung nachvollzogen.[77] Er wendet regelmäßig die EGMR als „living instrument" in Lichte der „present-day conditions" an, wobei aber natürlich Rücksicht auf die technologischen Besonderheiten des Internets zu nehmen ist.[78] Hinsichtlich des Internets ist im Bereiche der Meinungsäußerungsfreiheit besonders die Verstärkungswirkung von veröffentlichten (problematischen) Äußerungen, wie hate speech, zu beachten. Besonders Faktoren wie Einfluss einer Meinungsäußerung, Zugang, Dauer und Asynchronizität der Informationen sind Teile der „Spezifizität" von internetbezogenen Äußerungen online.

B.3.2. Im Besonderen: Recht auf Privatleben (und Datenschutz)

Das Recht auf Privatsphäre ist auf Ebene der Menschenrechte geschützt durch Artikel 12 der Allgemeinen Erklärung der Menschenrechte, die inzwischen großteils als Völkergewohnheitsrecht angesehen wird, sowie

Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte (IPbpR) und Artikel 8 der Europäischen Menschenrechtskonvention (EMRK).[79] Das Recht auf Datenschutz ist international – außer durch eine entsprechende Konvention des Europarates – nicht explizit verankert, wird aber als spezifisch ausgestalteter Teilbereich des Rechts auf Achtung der Privatsphäre angesehen.

Artikel 8 EMRK schützt den Freiheitsraum des Einzelnen, der notwendig ist, um die Persönlichkeit frei zu entfalten und hat sowohl eine abwehrrechtliche als auch eine gewährleistungsrechtliche Dimension (Schutzpflichtwirkung).[80] Staaten müssen also nicht nur von Eingriffen in die Privatsphäre Abstand nehmen, sondern auch gewährleisten, dass andere soziale Akteure (und andere Staaten) die Privatsphäre Einzelner nicht verletzen.[81]

Artikel 17 IPbpR in seiner Auslegung durch den Menschenrechtsausschuss hat eine ähnliche Wirkung. Dem im Koalitionsvertrag geäußerten Wunsch – „Das Recht auf Privatsphäre, das im Internationalen Pakt für bürgerliche und politische Rechte garantiert ist, ist an die Bedürfnisse des digitalen Zeitalters anzupassen“[82] – ist der Ausschuss, dem Grunde nach, schon 1988 nachgekommen, als er festgehalten hat,[83] dass Überwachungsmaßnahmen („whether electronic or otherwise“) von allen Arten von Kommunikationen mit den üblichen Ausnahmen verboten seien.[84] Staaten müssten einen Rechtsrahmen schaffen, um Eingriffe „by natural or legal persons“ zu verbieten.[85] Es geht bei der Bewertung der Massenüberwachung durch die NSA auch weniger um die Frage der Auslegung von Artikel 17 (höchstens der Frage seiner extraterritorialen Wirkung, die von den USA – im Gegensatz zur Mehrheitsmeinung – zurückgewiesen wird[86]), sondern vielmehr um die Umsetzung dieser Verpflichtungen in der Praxis.[87] Nicht das Völkerrecht des Netzes ist hier (notwendigerweise) lückenhaft; es sind die völkerrechtswidrigen Handlungen durch die USA und die anderen „Five Eyes“-Staaten sowie europäische Staaten, die eng mit diesen kooperiert haben, die das Recht auf Privatsphäre im Internetzeitalter und den Charakter des Internets als Vertrauensraum gefährden.[88]

Auch der Menschenrechtsrat der Vereinten Nationen zeigte sich in seiner aktuellsten Resolution zum Recht auf Privatleben im digitalen Zeitalter „ernsthaft in Sorge“ im Lichte des

> „negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights.“[89]

Auf Ebene der Vereinten Nationen initiierten Deutschland und Brasilien 2013 unter dem Eindruck der Enthüllungen über die Überwachung deutscher und brasilianischer Regierungsmitglieder und -ämter eine Resolution der Generalversammlung über das Recht auf Privatsphäre im digitalen Zeitalter, in der mit klaren Worten die Sorge der Staatengemeinschaft über den negativen Einfluss von widerrechtlicher und willkürlicher Überwachung auf die Menschenrechte Ausdruck findet und die an die Rechtfertigungspflicht für Eingriffe in Menschenrechte – auch und gerade im Internet – erinnert.[90]

Das Urteil des EuGH im Fall *Schrems* reiht sich nahtlos ein. Luxemburg hob damit die „Safe Harbour“-Entscheidung der Kommission auf[91] und entzog dem millionenhaften Transfer von Daten europäischer Nutzer in die USA die rechtliche Grundlage. Mit Entscheidung vom 6.10.2015[92] rügte der EuGH die Kommission, weil sie es verabsäumt hatte festzustellen, dass die USA – durch nationales Recht oder internationale Verpflichtungen – ein angemessenes grundrechtliches Schutzniveau gewährleisten.[93]

Der Entscheidung vorangegangen war ein Rechtsstreit des österreichischen Privacy-Aktivisten Max Schrems, der versucht hatte, über den die Datenschutzbehörde Irlands, des Sitzes von Facebook, eine Überprüfung der Rechtmäßigkeit der Datenbewegungen zwischen Europa und den USA zu erreichen. Das schlussendlich befasste irische Höchstgerichte legte schließlich vor.

Der EuGH unterstrich, dass jeder Eingriff in die Charta-Grundrechte nach Artikel 7 (Privatleben) und 8 (Datenschutz) klar und präzise umrissen sein müsse, sich auf das absolut Notwendige beschränken müsse[94] und gleichzeitig wirksame Rechtsschutzmöglichkeiten für die Betroffenen zur Verfügung stehen müssten, zumal es sich um personenbezogenen Daten handelt, die automatisch verarbeitet werden. Eingriffe in das Privatleben und den Schutz personenbezogener Daten – hier führt der EuGH seine Judikatur von *Digital Rights Ireland*[95] fort – müssten sich auf das „absolut Notwendige" beschränken.

Die Rechtslage in den USA entspräche diesen Anforderungen nicht. Überschießend sei eine Regelung, „die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen […] ohne irgendeine Differenzierung, Einschränkung oder Ausnahme" ermöglicht.[96] Gerade Reglungen, die Behörden gestatteten, „generell auf den Inhalt elektronischer Kommunikation zuzugreifen" verstoßen gegen den Wesensgehalt des durch Artikel 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens.[97] Deshalb war auch keine Verhältnismäßigkeitsprüfung (wie noch in Digital Rights Ireland) nötig. Es ist auch beachtenswert, dass schon der abstrakt normierte Zugriff („access") behördenseitig ausreicht, um eine Wesensgehaltsverletzung festzustellen, und nicht erst das tatsächliche Prozessieren der Daten. Auch verletzt sei, so der EuGH, Art. 47 der Grundrechtecharta, das ein Grundrecht auf wirksamen gerichtlichen Rechtsschutz, festschreibt, da für EU-Bürger keine Möglichkeit bestehe, bei US-Behörden Zugang zu (oder Löschung von) den sie betreffenden personenbezogenen Daten zu erlangen. Eine wirksame gerichtliche Kontrolle zur „Gewährleistung der Einhaltung des Unionsrechts" sei „dem Wesen eines Rechtsstaats inhärent".[98]

Das Urteil, das im Wesentlichen den Ausführungen in den Schlussanträgen von Generalanwalt Yves Bot[99] folgte, unterstreicht die Bedeutung von Privatleben und Datenschutz als Menschenrechte, bestätigt die Bedeutung, die der EuGH europäischer Datenhoheit beimisst und stellt eine Fortführung der multidimensionalen datenschutzfreundlichen Judikaturlinie des EuGH dar.[100] Schon in Digital Rights Ireland hatten die

Europarichter betont, dass Eingriffe – besonders solche, die Datensammlung ohne Differenzierung, Einschränkung oder Ausnahme vorsehen – regelmäßig Grundrechte verletzten, weil sie sich nicht auf das „absolut Notwendige" beschränkten. In *Digital Rights Ireland* hatte der EuGH übrigens auch gerügt, dass die RL zur Vorratsdatenspeicherung keine Speicherung im Unionsgebiet vorgeschrieben hatte.[101] Man sieht hier den Kern einer judiziellen Resouveränisierung der Datenlandschaft im Internet mit dem EuGH als Vorfechter der europäischen Datenhoheit.

Mit Schrems schützt der EuGH Privatleben und Datenschutz (und das Recht auf wirksamen gerichtlichen Rechtsbehelf) gegen Handlungen der EU-Organe und anderer Staaten; in *Google Spain* und *Google*[102] fokussiert er auf die Pflichten von Unternehmen (Linklöschpflichten von Suchmaschinenbetreibern als Ausfluss der Rechte auf Privatleben und Datenschutz, außer gegenläufige Interesse der Öffentlichkeit wiegen stärker); und in *Rynes*[103] erstreckte er seine Judikatur auch auf Aktivitäten von Privaten (private Videoüberwachung im öffentlichen Raum ist ein Eingriff in das Datenschutzrecht; diesem korrespondiert eine staatliche Schutzpflicht). Damit hat der EuGH in nur zwei Jahren einen umfassende multidimensionale, tendenziell expansive Datenschutzjudikatur entwickelt, die bedeutende extraterritoriale Wirkungen zeitigt.

B.3.3. Rechtspolitische Überlegungen

Der Schutz des Privatlebens – auch im Internet – ist ein „gateway" für die Meinungsäußerungsfreiheit.[104] Nur wer sich sicher fühlt, kann frei kommunizieren, sich eine Meinung bilden und diese äußeren. Beide Rechte sind daher eng miteinander verquickt und bekräftigen einander. In dieser Sicht spielen auch Verschlüsselungstechnik und Anonymität eine kritische Rolle für den Realisierung der Menschenrechte online.[105]

Im Gutachtensauftrag wird unter anderem die Frage gestellt, wie ein „Völkerrecht des Netzes" ausgestaltet werden müsse, um die Grund- und Freiheitsrechte im Allgemeinen und besonders die Privatsphäre im digitalen Zeitalter besser zu schützen. Daher werden im Folgenden einige (völker)rechtspolitische Überlegungen angestellt.

Es gebricht nicht am Recht. Wie der Menschenrechtshochkommissar der Vereinten Nationen in einem Bericht über das Recht auf Privatleben im Internet eindeutig festhält, ist die Staatenpraxis das Problem:

> *„International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy,* including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data. Practices in many States have, however, revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy."[106]

Die Snowden-Enthüllungen haben „chilling effects"auf die Nutzung des Internets und unser Verständnis vom Internet als einer Technologie, um positiven sozialen Wandel hin zu einer Informationsgesellschaft auf Grundlage der Menschenrechte zu bewirken.[107] Die sozialen Kosten der Massenüberwachung sind weit höher als ihre Erträge. Gerade die Schwächung von Verschlüsselungsstandards oder die codierte Öffnung von Hintertüren für staatliche Stellen kann negative Folgen für die nationale Sicherheit haben. Der im September 2015 angenommene Schaake-Bericht des Europäischen Parlamentes unterstreicht die Bedeutung von Verschlüsselungstechnologien für die Privatsphäre und fordert unter anderem ein Recht auf Verschlüsselung und die Einführung von „end to end"-Verschlüsselungsstandards für sämtliche Kommunikationen.[108]

Demokratische Gesellschaften waren schon lange von Spionage und Terrorismus bedroht. Schon 1978 urteilte der EGMR *in Klass und andere gegen Deutschland,* dass die

> „existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[109]

Allerdings bedeute dies nicht, dass Staaten Menschenrechte ignorieren könnten oder in der Wahl ihrer Mittel und der Intensität der Überwachung gänzlich frei wären: Im Bewusstsein, dass entsprechende Gesetze die Gefahr in sich bärgen „[of] undermining or even destroying democracy on the ground of defending it", könnten Staaten nicht tun, was sie wollten „in the name of the struggle against espionage and terrorism".[110] So unterstrich der EGMR in *Shimovolos gegen Russland* die Notwendigkeit von „detailed rules on the application of secret measures of surveillance, especially as the technology available for use is continually becoming more sophisticated."[111]

Um den Schutz der Privatsphäre im Internet zu verstärken, müssen Staaten im Lichte dieser Ausführungen ihre nationalen Gesetze und Politiken auf Übereinstimmung mit ihren menschenrechtlichen Verpflichtungen – nach EMRK und Zivilpakt (und einschlägigem europäischem Primärrecht und insb. der Grundrechtecharta), jeweils in aktueller Auslegung durch EGMR, Menschenrechtsausschuss (und EuGH) – überprüfen. Normative Maßnahmen zur Behebung von Lücken müssen im Rahmen von leicht zugänglichen, offenen, gesellschaftlichen Diskussionsprozessen entwickelt werden.

Jedes Gesetz, das Datensammlung ermöglicht, muss sich an anerkannten menschenrechtlichen Kriterien (wie Spezifizität und Zweckbindung) messen lassen. Die Bedingungen, unter denen gesammelte Daten mittels Selektoren durchsucht werden dürfen, müssen öffentlich diskutiert werden. Selektoren müssen veröffentlicht werden, um eine diskriminierungsfreie Anwendung sicherzustellen. Der Einsatz von Selektoren, die bestimmten Personen zugeordnet werden können, muss noch höhere Schutzschranken passieren.

Der EGMR hat in wichtigen Urteilen aufgezeigt, welche Pflichten Staaten hinsichtlich des Schutzes der Privatsphäre haben. Besonders einschlägig sind *Weber and Saravia v. Germany, Klass and Others v. Germany* (Richterliche Kontrolle von Überwachungsmaßnahmen), *Bucur and Toma v. Romania* (Schutz von Whistleblowern), *Iordachi and others v. Moldova* (enge Defi-

nition der „nationalen Sicherheit“ zur Legitimierung von Eingriffen) und *El-Masri v. the former Yugoslav Republic of Macedonia* (extraterritoriale Wirkung der EMRK; Bedeutung demokratischer Kontrolle von Nachrichtendiensten).[112]

Demokratische Kontrolle von Sicherheits- und Nachrichtendiensten ist wichtig für den Schutz der Menschenrechte und der Rechtstaatlichkeit. Der Menschenrechtskommissar des Europarates empfiehlt die Aufnahme eines nationalen Dialoges über Möglichkeiten zur Sicherstellung der Kontrolle durch Recht.[113] Ähnliche Forderungen stellt die Venedig-Kommission des Europarates auf.[114]

Zusammenfassend lässt sich sagen, dass der Schutz des Rechts auf Privatleben zentral für die Weiterentwicklung einer entwicklungsorientierten und menschenzentrierten Informationsgesellschaft ist. Mangelndes Vertrauen in eine geschützte private Sphäre höhlt mit den Kommunikationsfreiheiten auch die zentralen partizipativen Rechte an der Informationsgesellschaft aus. Das Recht auf Privatleben schafft den Freiraum, alle anderen Rechte auszuüben.[115] Der historisch gesehen für die Entwicklung der Menschenrechte zentrale Kampf um eine staatsfreie Sphäre des Privaten muss, um das Recht auf eine „unternehmensfreie“ Sphäre erweitert, ins Zentrum von Bemühungen um den Menschenrechtsschutz im Internet rücken.

Um dies zu erreichen, müssen alle Stakeholder an der Entwicklung von Normen mit Internetbezug teilhaben können. Dies setzt Modelle der demokratischen Legitimierung von Internet Governance-Normen voraus und stellt das in Normenvokabular wie Rechtsfortbildungsverfahren staatenorientierte klassische Völkerrecht westfälischer Prägung vor große Herausforderungen.

B.4. Verstärkung der demokratischen Teilhabe am weltweiten Kommunikationsnetz

B.4.1. Partizipation im Multistakeholder-Modell als Teilhabe-Äquivalent

Demokratie ist ein völkerrechtlich höchst umstrittener Begriff. Politisch oszilliert der Begriff zwischen „Lebensform“[116] und leerer Bekenntnisformel[117]. Völkerrechtlich ist inzwischen[118] allerdings weitgehend anerkannt, dass sie als „teleologisches Prinzip“[119] des Völkerrechts gelten kann, das flankiert wird von einem Menschenrecht auf demokratische Governance und besonders periodische, geheime, faire und freie Wahlen, das aus dem Recht auf Selbstbestimmung in den gemeinsamen Artikel 1 Zivil- und Sozialpakt, Artikel 21 der Allgemeinen Erklärung der Menschenrechte sowie Artikel 25 des Zivilpaktes in seiner Auslegung und nachfolgender Praxis,[120] und den regionalen Verbriefungen (Artikel 10 Abs. 2 EMRK; Artikel 13, 15, 16 AMRK, Artikel 10, 11 AfrMRK) abgeleitet werden kann.[121]

Die Realisierung demokratischer Partizipationsansprüche im Rahmen von transnationalen Steuerungsprozessen ist indes genuin schwierig. Demokratische Teilhabe am Internet kann grundsätzlich dadurch gefördert werden, dass Einzelne verstärkt an globalen Prozessen der Internet Governance teilnehmen – selbst oder durch Repräsentanten. Verfahren der Internetpolitik sind komplex und laufen parallel auf diversen Ebenen mit weit divergierenden Normierungszielen ab. Das kann zu kognitiver Überforderung und in Folge Interessensverlust und Partizipationsverweigerung führen. Das grundsätzliche Bekenntnis der internationalen Gemeinschaft zur Integration aller Stakeholder ist aber unbestritten.

Da Demokratie im Kontext des Internets vor großen begrifflichen Herausforderungen steht, nimmt die Multistakeholderstruktur als Institutionalisierung qua Verfahren von demokratischen Ansprüchen der Stakeholdergruppen an Governance-Entscheidungen mit Internetbezug eine zentrale Rolle in der normativen Ordnung des Internets ein. Alle – gerade auch Bürger – haben ein demokratisches Teilhabeinteresse am Internet und dessen Regulierung, ein „Stake“, ein wertunterlegtes Interesse am Regelungsergebnis und in Hinblick auf den Regelungsprozess, dessen

Respekt – prinzipiell – eine Integration aller Stakeholder in allen Phasen des normativen Prozesses voraussetzt. Dieses wird dann auch im Multistakeholder-Ansatz durchgesetzt, der seine Verwirklichung findet in der Entwicklung und Anwendung durch Regierungen (Staaten), den Privatsektor (Unternehmen) und die Zivilgesellschaft (Individuen) in ihren jeweiligen Rollen von Instrumenten und Prozessen zur Regelung des Internets.[122]

Der Multistakeholderprozess als inklusiver Ansatz der Internet Governance Policy-Gestaltung ist mit wenigen Ausnahmen (ordnungspolitischer Initiativen souveränitätsbewusster Regierungen) unumstritten. Durch die derart erzielte Bündelung der legitimationsstiftenden Wirkung der Beteiligung von Staaten, dem Privatsektor und der Zivilgesellschaft (Input-Legitimität) und Verfahren, die eine gleichberechtigte Interaktion in Regelungsprozessen ermöglichen (Throughput-Legitimität), sind auch die Regelungsergebnisse besonders legitim (Output-Legitimität).[123] Die Regelungsergebnisse von Internet Governance-Prozessen sind aufgrund ihrer Legitimität auch im Großen und Ganzen effektiv, was wiederum ihre Legitimität befördert.

Die Verwendung von Multistakeholder-Prozessen und von Mehrebenendiplomatie (oder „mehrdimensionaler Diplomatie“) ist auch aus anderen Rechtsregimen bekannt.[124] Die Integration der Zivilgesellschaft in den Verhandlungsprozess in den Römischen Statuten des Internationalen Strafgerichtshofs hat hier Beispielcharakter, wie auch die Entstehung umweltvölkerrechtlicher Regularien mit expliziten Beteiligungsrechten nichtstaatlicher Akteure (allerdings nur als NGOs organisierter).[125] Es ist aber das Völkerrecht des Netzes, das den Multistakeholderismus als normativen Ansatz ins allgemeine Völkerrecht kraftvoll einführt und eine Desintermediatisierung des Einzelmenschen bewirkt. Internetbezogene Regeln, die ohne Beteiligung aller Stakeholder entwickelt werden, werden – häufig – als illegitim wahrgenommen. Dies hat das Beispiel des Anti-Produktpiraterie-Abkommen (ACTA) gezeigt; dies illustriert auch die zivilgesellschaftliche Opposition gegenüber TTIP und TISA.

Die Debatte um das optimale Design von Multistakeholder-Strukturen wird heftig geführt. Zentrale Verbesserungspotenziale für internetbezogene Multistakeholder-Prozesse liegen im Abbau von Informationsdisparitäten zwischen Akteuren und Akteursgruppen (wobei staatliche Informationsmonopole durch Informationsfreiheitsgesetze aufgeweicht werden), im Aufbau von Vertrauen zwischen den Stakeholdergruppen als Voraussetzungen für einen konstruktiven Diskurs,[126] und in der Identifizierung und Marginalisierung von „bad actors", die sich zwar am Diskursprozess beteiligen, diesen aber inhaltlich oder durch Verfahrenstricks obstruieren.[127]

Auf lokaler und regionaler Ebene sind „Governance Groups", die sich aus verschiedenen Stakeholdern zusammensetzen inzwischen zu einem effektiven und legitimen Modell der Regulierung geworden.[128] Empirische Studien legen nahe, dass die Repräsentativität der Gruppe und eine starke Leadership des Diskussionsprozesses entscheidende Faktoren auf dem Weg zu erfolgreichen normativen Outcomes darstellen.[129] Wie diese Erkenntnisse für die Internet Governance übersetzt werden können, steht zurzeit zur Debatte.

Globale zivilgesellschaftliche Bewegungen haben in historischer Sicht schon vieles bewegt: vom Verbot des interkontinentalen Sklavenhandels bis zum Frauenwahlrecht sind wichtige soziale Fortschritte – zunächst – durch nichtstaatliches Engagement initiiert worden. In Bezug auf das Internet kommt als ergänzendes Element die Bedeutung der nichtstaatlichen Standardsetzung hinzu. Es kann durchaus sein, dass sich langfristig aus den nun präsenten ersten globalen Initiativen um Aspekte der Internet Governance eine Weltzivilgesellschaft[130] entwickelt – und einen Weltbürger entstehen lässt, der sich in den Diskursräumen des Internets bewegt und dort seine demokratischen Teilhaberechte einfordert und auslebt.[131]

Je inklusiver das Internet, desto eher kann dieser Prozess Wirkung zeitigen. Zugang ist also Voraussetzung für demokratische Teilhabe.

B.4.2 Demokratische Teilhabe am Internet setzt Zugang zum Internet voraus

Demokratische Teilhabe am Internet setzt Zugang voraus. Mehr als die Hälfte der Menschheit hat noch immer keinen Zugang zum Internet. Einem aktuellen Bericht von ITU und UNESCO zufolge sind 3,2 Milliarden Menschen online. Das bedeutet aber auch, dass 4 Milliarden Menschen noch nicht ins Internet kommen. Breitband-Internet sei aber eine „foundation for sustainable development“,[132] was auch die UNO-Staaten selbst anerkannten, die sich im Rahmen der Sustainable Development Goals dazu verpflichteten, Internetzugang für alle bis 2020 zu sichern. Selbst in entwickelten Gesellschaften müssen allerdings noch Maßnahmen gesetzt werden, um Breitbandausbau flächendeckend zu erreichen.

Diesen als „Universaldienst“ zu definieren, wäre ein erster Schritt. Ein Bericht des Broadband Opportunity Council von 2015 im Auftrag von US-Präsident Obama kommt zu dem Schluss, der Zugang zu Breitband-Internet habe sich inzwischen zu einer „core utility“ entwickelt und sei gleich zu bewerten wie Wasser, Abwasserversorgung und Elektrizität als „essential infrastructure for communities“.[133] Auch die deutsche Regierung hat sich in der Digitalen Agenda zum Breitbandausbau bekannt: 2,7 Milliarden Euro stehen dafür bereit.[134] Bis 2018 sollen in ganz Deutschland Zugangsraten von mindestens 50 Mbit pro Sekunde erreicht sein.[135] Dieser Prozess ist zu überwachen und zu fördern.

Die Sicherstellung von schnellem Internetzugang, gekoppelt mit einem möglichst flächendeckenden WLAN-Netz, ist Voraussetzung für eine Verstärkung der demokratischen Teilhabe am Internet. Daher ist auch die Verabschiedung des Referentenentwurfs des Telemediengesetzes durch das Kabinett nicht unproblematisch, da die Neufassung der Störerhaftung in § 8 und die Konzipierung der Haftungsprivilegien für Host-Provider in § 10 Rechtsunsicherheit schaffen.[136]

Zugang ist Voraussetzung für die Stärkung der Rolle des Internets zur Förderung von demokratischer Partizipation in nationalen und interna-

tionalen Diskursräumen sowie – potenziell – zur Stärkung der demokratischen Legitimation internetbezogener Normierungsprozesse. Es ist Aufgabe des Staates, sowie abgestuft der internationalen Gemeinschaft, in der Umsetzung des Rechts auf Entwicklung und der Verpflichtung auf nachhaltige Entwicklungsziele Internetzugang für alle zu schaffen. Zugang alleine reicht indes nicht; der Staat muss auch die Privatheit und Sicherheit der Kommunikation im Internet respektieren und gewährleisten – auch gegen Private und Drittstaaten. Das geht unter anderem durch die Förderung von Verschlüsselungstechnologien.

B.4.3. Ein Recht auf Verschlüsselung befördert demokratische Teilhabe

Diskussionen über ein Grundrecht auf Verschlüsselung, die angesichts der deutschen Pionierstellung durch das Grundrecht auf IT-Sicherheit einen Impetus erfahren haben,[137] müssen forciert und international geführt werden. Ein Recht auf Verschlüsselung ist Ausfluss des Rechts auf Privatleben.[138] Angesichts der systemischen Überwachung von Internetkommunikation ist ein Grundrecht sowohl auf Verschlüsselung als auch auf Wahl der Verschlüsselungsmethode bedeutsam: als eine Art „Recht der digitalen Selbstverteidigung".[139] Das Wissen, geschützt kommunizieren zu können, kann das Interesse an demokratischer Teilhabe am Internet verstärken. Staaten müssen sich – in negativer Wirkung des Rechts auf Verschlüsselung – Versuchen enthalten, „back doors" in Verschlüsselungstechnologien einzubauen oder Bürger von deren Gebrauch abzubringen.

Während der britische Premierminister Cameron und der FBI-Direktor James Comey codierte „Schlüssel" für Geheimdienste zur Überwindung von Verschlüsselung fordern,[140] liegt dem US-Kongress ein Gesetz – der Secure Data Act – vor, der es Behörden verbieten würde, Vulnerabilitäten in Sicherheitstechnologie vorzuschreiben.[141] Diese sog. Hintertüren (‚backdoors') sind, so auch UN-Sonderberichterstatter Kaye, kein menschenrechtlich vertretbarer Weg:

> „It is a seemingly universal position among technologists that there is no special access that can be made available only to government

> authorities […] In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online."[142]

Welche Folgen dies haben kann, zeigt die Veröffentlichung des Master Keys der amerikanischen Transportsicherheitsverwaltung (TSA) für Gepäck und dessen Nachdruck durch Aktivisten auf einem 3D-Drucker.[143] Der Schutz von Verschlüsselungstechnik und dessen verstärkter Einsatz schützen die Privatsphäre und mit ihr die Vorbedingung zur Ausübung der Meinungsäußerungsfreiheit. Beide sind damit wichtige Fundamente für die Realisierung demokratische Teilhabeperspektiven.

B.4.4. Accountability als Element demokratischer Legitimation

Accountability oder Rechenschaftspflicht meint im Kontext des Internets, dass die formalen und informellen Institutionen, die relevant sind in Internet Governance und Internetpolitik-Prozessen, sich gegenüber der in Multistakeholderstrukturen organisierten internationalen Gemeinschaft rechtfertigen müssen. So kann über das Ziel, die demokratische Legitimation von in privaten oder hybriden Regimen entstandenen Normen zu heben, die demokratische Teilhabe aller Stakeholder gesichert werden. Entscheidungen dieser Formationen sind nach allgemein anerkannten Grundsätzen der Menschenrechte, der Rechtstaatlichkeit und der Demokratie zu treffen.[144] Diese Grundsätze sind für die Beurteilung der Legitimität aller Akte der Ausübung international-öffentlicher Gewalt bzw. International Public Authority entscheidend;[145] doch selbst wenn nicht öffentliche Gewalt ausgeübt, sondern eher durch (formlose oder nur schwach prozeduralisierte) Macht auf den „Raum der Gründe" (für bestimmtes Verhalten)[146] anderer Stakeholder eingewirkt wird, sind diese zumindest relevant. Im Detail wird etwa gefordert, dass alle Akteure einzubeziehen sind und sich alle Institutionen der Internet Governance an die Grundsätze der guten Verwaltung, einschließlich der Transparenz und der Rechenschaftspflicht, halten müssen.[147]

Dieser Anspruch – dass alle Stakeholder, auch Einzelne, ein Recht auf Rechenschaftspflicht gegenüber normativen Akteuren der Internet Go-

vernance haben, ohne dass ein Staat dieses Recht mediatisieren müsste – kann auch als Recht auf Rechtfertigung ausgedeutet werden. So hat Rainer Forst ein Recht jedes Menschen postuliert, dass er weder Normen noch gesellschaftlichen Verhältnissen unterworfen ist, die ihm gegenüber nicht angemessen gerechtfertigt werden können.[148]

Natürlich ist die „Rechtfertigung" von Politiken eine Frage der Macht.[149] ICANN ist ein mächtiger Akteur und war historisch in der Lage, sich gegenüber Zweifel an seiner Legitimität effektiv zu wehren. Dies liegt auch an ICANNs Ressourcenausstattung.

> „Wer über größere und stärkere ökonomische Ressourcen oder Gewaltmittel verfügt, wer mit Hilfe moderner Informationstechnologien normative Gründe strategisch erfolgreich verbreiten oder gegen Kritik erfolgreich immunisieren, die politische Agenda bestimmen und den politischen Prozess mit je eigenen Themen und Gründen erfolgreich beeinflussen kann, wer ganze Bevölkerungsgruppen in Abhängigkeit bringen oder Eliten zu Klienten machen kann, hat größere Chancen, seine normative Ordnung gegenüber anderen durchzusetzen und gegen Kritik, Dissidenz und Widerstand zumindest über längere Zeiträume zu immunisieren."[150]

Die Überprüfung dieser normativen Gründe verläuft in Prozessen der Überprüfung der Accountability einer Formation bzw. deren Entscheidungen, was einen Rekurs auf die „Demokratie" bzw. demokratische Legitimation zunächst unnötig macht. In einer Studie zur Accountability von internationalen Organisationen hat die International Law Association Prinzipien der Accountability entwickelt, deren Anwendung die „demokratische Teilhabe" von Bürgern auch an nicht-traditionellen internationalen Organisationen bzw. privaten oder hybriden Regelungsformen und -formationen verstärken kann. Zu diesen gehören Prinzipien wie Good Governance (Transparenz, Informationszugang, partizipatorischer Entscheidungsfindungsprozess, nachvollziehbare Finanzgebarung), Good Faith, Verfassungsartigkeit und institutionelle Balance, Kontrolle, Begründungszwang, prozedurale Regularität, Objektivität und Unparteilich-

keit, und Due Diligence.[151] Durch Prozeduralisierung kann dergestalt gesichert werden, dass informelle Regulierung und nicht formal legitimierte Formationen dennoch Normen produzieren, die als demokratisch legitimiert gelten können.[152]

Ein beispielhafter Anwendungsfall für Accountability-Prüfungen im Völkerrecht des Netzes ist der Transitionsprozess der Kontrolle der IANA-Funktionen[153] Die Diskussionen werden hier parallel in zwei Bereichen geführt: zur Frage der Transition der IANA-Funktionen und zur Hebung der Accountability von ICANN. Die mit letzterer Frage befasste Cross Community Working Group (CCWG) kam zu dem Schluss, dass sich der ICANN-Vorstand in Zukunft stärker nach den Vorschlägen der Stakeholder zu richten hätte, dass diese die Statuten entwerfen dürften sowie die Möglichkeit haben sollten, Entscheidungen des Boards vor Gericht anzufechten und Board-Mitglieder auszutauschen.[154] ICANNs Vorstand, der Empfehlungen zu dem Bericht abgeben kann, lehnte die Maßnahmen zur Accountability-Steigerung ab.[155]

Diese Diskussion zeigt beispielhaft, wie komplex es ist, eine Rechtfertigungsordnung selbst für eine Organisation zu konzipieren, die schon lange unbestritten zentrale Aspekte der Internetarchitektur verwaltet und deren Rolle in der Fällung von Entscheidungen im internationalöffentlichen Interesse unbestritten ist. Wie schwierig ist es erst, die Verwaltung inzwischen zumindest halböffentlicher sozialer Räume durch die Betreiber sozialer Netzwerke und die Entwicklung ethischer Prinzipien für Algorithmisches Entscheiden einer Rechtfertigungspflicht gegenüber einer internationalen Multistakeholder-Struktur zu unterwerfen. Dennoch muss dieser Weg gegangen werden, wenn das Recht auf Rechtfertigung jedes Einzelnen gegenüber allen Normenproduzenten nicht für die normative Ordnung des Internets aufgeben werden soll.

B.5. Zwischenfazit

In diesem Abschnitt standen die inhaltlichen Anforderungen an ein „Völkerrecht des Netzes“ im Vordergrund. Zunächst ist dem Völkerrecht

des Netzes (und den staatlichen Grundrechten) ein Menschenrecht auf Internetzugang zu entnehmen. Denn ohne Zugang zum Internet (Infrastrukturdimension) und Zugang zu Internet-Inhalten (Inhaltsdimension) können Menschen nicht ihre Menschenrechte realisieren. In der Agenda for Sustainable Development für 2030 bekennen sich die Staaten der Vereinten Nationen dazu, bis 2020 universellen und leistbaren Internetzugang in Entwicklungsländern zu sichern; und bis 2018 – so will es die Digitale Agenda – soll in Deutschland flächendeckend Breitbandzugang erreicht sein.

Der Schutz der Privatsphäre im Internet ist Voraussetzung für die Ausübung der Meinungsäußerungsfreiheit; diese wiederum ist ein Katalysator für die Realisierung aller anderen Menschenrechte im Online-Kontext. Trotz unterschiedlicher Gewichtungen des Privaten (und des Datenschutzes) auf globaler Ebene sind gewisse normative Konvergenzen auszumachen. Doch schon jetzt gebricht es nicht an Normen: Die systemische Massenüberwachung der Internetkommunikation durch die USA und ihre Partner ist nach geltendem Recht unkompliziert als Völkerrechtsverstoß zu beurteilen. Dennoch müssen Staaten handeln. Sie stehen in der Pflicht, ihre nationalen Gesetze und Politiken auf Übereinstimmung mit ihren menschenrechtlichen Verpflichtungen zu prüfen und insbesondere Gesetze, die Datensammlung ermöglichen, an den anerkannten menschenrechtlichen Kriterien messen zu lassen. Gleichzeitig müssen Staaten ihre Sicherheits- und Nachrichtendiensten verstärkt demokratischer Kontrolle unterziehen. Internationale Kooperation zwischen den USA und der EU können – so sie menschenrechtlich sensibel ablaufen – wichtige Schritte zum Schutz des Rechts auf Privatsphäre und des Datenschutzes online darstellen.

Demokratische Teilhabe am Internet kann durch verstärkte Teilnahme des Einzelnen an den globalen Prozessen der Internet Governance realisiert werden. Das Bekenntnis der internationalen Gemeinschaft zur Integration aller Stakeholder im Rahmen von Multistakeholder-Ansätzen prozeduralisiert inhaltliche Anforderungen an die Internet Governance.

Die Sicherstellung von schnellem Internetzugang, gekoppelt mit einem möglichst flächendeckenden WLAN-Netz, sind wichtig für die demokratische Teilhabe am Internet. Dies muss auch bei rechtspolitischen Entwicklungen beachtet werden. Gleichzeitig sind internationale Diskussionen über ein Grundrecht auf Verschlüsselung als Ausfluss des Rechts auf Privatleben weiter zu forcieren.

Accountability oder Rechenschaftspflicht meint im Kontext des Internets, dass die formalen und informellen Institutionen, die relevant sind in Internet Governance und Internetpolitik-Prozessen, sich gegenüber der in Multistakeholderstrukturen organisierten internationalen Gemeinschaft rechtfertigen müssen. Die Diskussion um die Stärkung der Accountability von ICANN zeigt beispielhaft, wie komplex es ist, internationale Ordnungen zu konzipieren, die von Multistakeholderstrukturen auf ihre Rechtfertigung befragt werden können.

C. Das Zusammenspiel von nationalem Recht, europäischem Recht und Völkerrecht

C.1. Einführung

Das Konzept der Geschlossenheit der Rechtsordnung im Sinne der ausschließlichen Geltung des von Normunterworfenen legitimierten Rechts in einem nationalstaatlichen System ist eine Fiktion.[156] Das mit dem modernen Verfassungsstaat entstandene staatliche Rechtsparadigma wird herausgefordert durch die Globalisierung und die Relativierung von Territorialitäten durch Informations- und Kommunikationstechnologien.[157]

Das heißt jetzt nicht, dass der Staat vergeht: „Der virtuelle Raum bedeutet […] nicht das Ende des souveränen Verfassungsstaates“[158]. Der Staat – durch Legislative, Exekutive und vor allem Judikative – muss sich auf seine zentralen Funktionen besinnen und seine Bürger schützen, ohne dabei aber deren Rechte zu verletzen. Das heißt, dass Staatsrecht auch weiterhin eine zentrale Rolle bei der Regulierung von internetbezogenen Sachver-

halten einnimmt. Gleichzeitig herrschen im Internet verschiedene Regelungsregime – also Ansammlungen von Normen unterschiedlicher Natur, Urheberschaft und Bindungswirkung.

Die Regeln, auf denen die Internet Governance beruht, speisen sich aus einer Gemengelage von öffentlichen Rechtsquellen (staatlichem Recht, Europarecht und völkerrechtlichen Vorgaben) sowie privaten und hybriden Normenquellen (Standards, Codes, Allgemeinen Geschäftsbedingungen).[159] Das Normengefüge der Internet Governance beeinflusst das Völkerrecht, supranationale Rechtssetzer (wie die EU) und zahlreiche nationale Rechtsregime (wie das Internetstrafrecht und den Datenschutz), nimmt aber gleichzeitig Entwicklungen aus diesen Regimen wieder auf. In diesem „Regelungsmosaik" ist die Kohärenz des Freiheitsschutzes schwierig zu garantieren.[160] Als komplizierender Faktor kommt noch hinzu, dass im Internet spontane, dezentrale, private Rechtsregime entstanden sind, in denen weder traditional noch charismatisch und nicht einmal regelmäßig rational legitimierte Akteure und Institutionen international-öffentliche Gewalt ausüben.[161]

C.2. Bestehen normative Defizite in der Regulierung und Umsetzung?

Wann ist eine Rechtsordnung defizitär? Jede Rechtsordnung ist im Fluss und passt sich ständig neuen Gegebenheiten an; sich wandelnde Konzeption von Sozialmoral schaffen beispielsweise inkrementell steigenden Änderungsdruck; die gesellschaftliche Willensbildung und die Rechtsordnung sind daher kommunizierende Gefäße mit einem Verzögerungsfaktor.[162] Entscheidend ist also die Frage des Vergleichsobjekts: defizitär im Vergleich zu einer anderen bestehenden Rechtsordnung? Oder einer idealen Rechtsordnung?

Die Antwort kann sinnhaft nur lauten: defizitär im Vergleich zu einer Rechtsordnung, die so gestaltet ist, dass sie die angestrebten Ziele der internationalen Gemeinschaft für die Informationsgesellschaft, nämlich deren entwicklungsorientierte, menschenrechtssensible Ausgestaltung

auf Grundlage der Charta der Vereinten Nationen, des Völkerrechts und der Allgemeinen Erklärung der Menschenrechte sicher erreichen kann. In Regulierung und Umsetzung bestehen also dann normative Defizite, wenn die normative Ordnung des Internets – das transnationalisierte Recht, bestehend aus Völkerrechtsregeln, Europarecht, Staatsrecht, privaten Rechtsregimen und *soft law* – diese Ziele nicht legitim und effektiv erreicht. Diese bestehen in der Tat.

C.3. Wie können diese überwunden werden?

C.3.1. Zur Identifikation der passenden Ebene zur Normproduktion

Angesichts der Vielzahl betroffener Akteure und der sinkenden Relevanz von Grenzen im Internet ist es eine Herausforderung, die „passende" normative Ebene – global, regional, national – zur Normierung bestimmter internetbezogener Sachverhalte zu identifizieren. Regelmäßig ist nämlich nicht nur eine Ebene betroffen, und allen drei Ebenen könnte legitim ein Normierungsinteresse unterstellt werden. Dies sei am Beispiel der lokalen Speicherpflicht für Nutzerdaten illustriert.[163]

Am 1.9.2015 trat ein neues russisches Gesetz in Kraft, das eine Datenlokalisierungspflicht (*Data Localization Rule*) beinhaltet: Daten mit Bezug zu russischen Bürgern müssen auf Servern in Russland gespeichert werden; die russische Datenschutzagentur *Roskomnadzor* muss informiert werden, wo sich die Daten physisch befinden.[164] Hier trifft staatliches Recht auf den völkerrechtlichen Schutz der freien Internetkommunikation und der Freiheit des Internets als globale Kommunikationsinfrastruktur.[165] Auf europäischer Ebene stellte nun der EuGH im Fall *Schrems* fest, dass das Datenschutzniveau in anderen Staaten „angemessen" sein müsse (d. h. ein der Union „der Sache nach gleichwertig[es]",[166] wenn ein Transfer von Daten europäischer Nutzer gestatten werden sollte. Die Gleichwertigkeit substanziiert der EuGH in Folge unter Rückgriff auf europäisches Datenschutzrecht (um gleichzeitig zu betonen, dass das Schutzniveau nicht *ident* sein müsse).[167] Damit schreibt der EuGH seine expansive Datenschutzjudikatur fort und setzt einheitlich – „angemessene" – Schutzstandards für „europäische" Daten, ob in Europa oder als Exportartikel,

fest. Diese Schutzstandards entfalten extraterritoriale Wirkung. Gleichzeitig lässt sich das Urteil als Plädoyer für europäische Datenhoheit lesen. Sollte dies einem umfassenden, multidimensionalen Grundrechtsschutz sicherstellen, ist allerdings – etwa im Rahmen der Datenschutzgrundverordnung – dringend eine Lücke normativ zu füllen. Die nach außen hin nun vom EuGH unterstrichenen datenschutzrechtlichen Grundsätze und der hohe Schutzstandard kann von diesen nicht auf nationale Sachverhalte angewandt werden (vgl Art 51 Abs 1 GRC). Weiterhin besteht keine europarechtliche Grundlage für die Bewertung von mitgliedstaatlichen Datenzugriffsregelungen, wie des Artikel 10-Gesetzes, auf Grundrechtskonformität.[168] Das ist ein Widerspruch, den es aufzulösen gilt, will die EU weiterhin glaubhaft als Verfechterin von hohen Datenschutzstandards auftreten. Zusammen mit den Folgen des Urteils für die Verhandlungen über die völkerrechtliche Verträge TTIP und TISA zeigt dieses Beispiel die Verbundenheit der Rechtsordnungen; Fragen des Datenschutzes kann keine Rechtsordnung (mehr) alleine normieren.

Als grundsätzliches Prinzip der normativen Ordnung des Internets kann wohl die Subsidiarität gelten, die sich im regionalen Integrationsrecht erfolgreich etabliert hat und mit Abstufung auch für das Verhältnis der Ebenen global, regional, national in Bezug auf das Internet Anwendung finden kann. Grundsätzlich soll daher gelten, dass eine Regelung auf bürgernächster Ebene vorzunehmen ist, außer gute Gründe (globale Harmonisierungsnotwendigkeit) sprechen dafür, dass globale Regelungen vorzuziehen sind. Der Nachteil der subsidiären Normierung liegt natürlich in der Förderung unterschiedlicher normativer Ansätze, die nur mit Mühen miteinander in Einklang zu bringen sind. Dies widerspricht der globalen, interoperativen Natur der Informations- und Kommunikationstechnologien, die Grenzen ja gerade überwinden. Als Minimalanforderung an subsidiäre normativen Ansätze muss daher in jedem Fall eine starke responsive Komponente gefordert werden, die Rechtsordnungen füreinander öffnet.[169]

Darüber hinaus kommt im Internet noch die Frage auf, ob eine Regelung durch öffentliches Recht oder durch private Regime stattzufinden hat. Weiters komplizierend kommt hinzu, dass gerade im Bereich der Internet Governance das Entstehen von Normen oft nicht zentral steuerbar ist.

Eingedenk dieser Herausforderungen werden im Folgenden dennoch ebenenspezifisch ausgewählte normative Perspektiven zu einer menschenrechtssensibleren und entwicklungsorientierten Adaptierung von Facetten der normativen Ordnung des Internets durch das nationale Recht, für die supranationale Ebene (EU) und im Völkerrecht beleuchtet.[170]

C.3.2. Ausgewählte normative Perspektiven[171]

C.3.2.1. Nationale Ebene

Kritiker der staatlichen Regulierung des Internets stellen vor allem die Wirksamkeit von zentraler Regulierung im Vergleich zu dezentraler entstehenden, „natürlich" sich entwickelnden privaten Rechtsregime in Frage.[172] Dem ist aber nicht so. Eine Studie zur Wirkung des Grundgesetzes im Internet diagnostiziert kaum Defizite im rechtlichen und grundrechtlichen Rahmen, solange die Sachverhalte „rein national" seien.[173] Die grundgesetzliche Werteordnung sei „in die sozial-ethischen Grundanschauungen der deutschen Gesellschaft eingegangen, dass bereits auf diese Weise […] der Rechtsfrieden auch unter Privaten (auch im Internet) gesichert scheint." Sobald Sachverhalte allerdings die Grenzen Deutschlands überschreiten, lassen sich grundrechtliche Positionen nicht leicht verteidigen. Der problematische Schluss der Studie, dem zuzustimmen ist: In Internetsachverhalten mit einem internationalen Bezug (und das ist die Mehrheit) kann sich der Einzelne „nicht auf die Garantenstellung des Staates hinsichtlich seiner Grundrechte verlassen". [174]

Dies ist problematisch, da Internetnutzerinnen und -nutzer aufgrund der Ubiquität des Internets nicht zwischen staatlichen, europäischen und internationalen Sachverhalten unterscheiden können. Wer könnte wissen, auf welchen Servern und in welchen Clouds[175] jene Daten gesichert sind, die abgerufen werden; wer könnte nachvollziehen, auf welchem Wege die Datenpakete einer E-Mail ihren Weg zum Empfänger finden; – gerade die Dezentralität des Internets und die Endnutzer-zu-Endnutzer-Konzeption der grundlegenden Architektur bedeutet auch, dass die geografische Festlegung von Handlungen und Zuschreibung von Verantwortlichkeiten an private und staatliche Akteure schwer fällt.[176] Dies bedeutet natürlich nicht, dass Territorialität als völkerrechtliches Leit-

prinzip hinsichtlich *jurisdiction to prescribe* und *enforce* irrelevant wird.[177] Lediglich die Handlungsmöglichkeiten (und damit -pflichten) des Staates werden eingeschränkt.[178] *Schliesky et al.* führen dazu richtig aus, dass die Steuerungsfähigkeit von Nationalstaaten zu Zeiten der Globalisierung begrenzt sei:

> „[W]er die Vorteile der Globalisierung, der zunehmenden Vernetzung, der auf Ubiquität sowie Raum- und Zeitunabhängigkeit basierenden Dienste nutzt, muss sich im Gegenzug vergegenwärtigen, dass er nicht in gleicher Weise Schutz des Staates beanspruchen kann wie in rein nationalen Sachverhalten."[179]

Dass der Nationalstaat nicht effektiv sämtliche Grundrechtspositionen sichern kann, immunisiert die für das Internet einschlägigen Rechtsordnungen allerdings noch nicht gegen Kritik. Im nationalen Recht gilt es zunächst, die Wirkmächtigkeit der Grundrechte für internetbezogene Sachverhalte zu erhöhen. Hier sind verschiedene normative Ansätze möglich,[180] wobei am sinnvollsten erscheint, dass Wissenschaft und Gerichtspraxis die Schutzpflichtdimension des Staates inhaltlich weiterentwickeln[181] sowie die Drittwirkung der Grundrechte in der Praxis effektuieren – dies kann maßgeblich über das AGB-Recht (hier: §§ 307ff BGB) ablaufen.

Darüber hinaus ist bestehendes Recht internetsensibel zu adaptieren und internetbezogene Gesetze menschenrechtsbewusst zu reformieren. Novellen wie jene des Telemediengesetzes zeigen indes auf, dass den rechtlichen Herausforderungen der Informations- und Kommunikationstechnologien immer noch nicht gerecht wird. Dringend wäre auch eine Reform der rechtlichen Einschränkungen für Fernmeldeüberwachung geboten.

Im Interesse der Vollständigkeiten seien an dieser Stelle auch faktische Maßnahmen angeführt,[182] die von Seiten deutscher Institutionen zu setzen wären, um die angestrebten Ziele der Informationsgesellschaft (Sicherung der Stabilität, Integrität und Funktionsfähigkeit des Internets zum Zwecke des Erhalts und Ausbaus einer globalen, befähigenden

Kommunikationsinfrastruktur) zu erreichen.[183] Der Aufbau eigener Dienste, wie DeMail, und Infrastrukturen, wie eine „Bundes-Cloud", kann grundrechtlich positive Wirkungen zeitigen.[184] Lokale Speicherungen können zu einem erhöhten Schutzniveau für Bürgerinnen- und Bürgerdaten führen und sind im Bereich hoheitlicher Aktivitäten sicher nötig. Allerdings ist es nicht zielführend, eine Duplizierung von kommerziellen nichtdeutschen Diensten (zumindest nicht auf *öffentliche* Kosten) anzustreben – dies wäre auch mit Blick auf die Ubiquität von Internetangeboten nicht sachgerecht. Hier wäre wieder darauf zu verweisen, dass an der Grundrechtsensibilität bestehender Dienste zu arbeiten ist und mittels *bestehender* völkerrechtlicher Verpflichtungen und des wachsenden Bewusstseins für die multidimensionale Wirkung der Grundrechte sowie die Verpflichtungen privater Akteure auf diese eine Erhöhung des grundrechtlichen Schutzniveaus zu erreichen ist.

Ein wichtiger Schritt zur Hebung des Vertrauens in (auch nichtdeutsche) Internet-Produkte und -Dienstleistungen kann in der Verstärkung der Bekanntheit und Nutzung der Zertifizierungen und Konformitätsbewertungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) liegen,[185] das eine erhöhte Vertrauenswürdigkeit – gerade in Hinblick auf die Nutzung von Kundendaten – sicherstellen kann.[186] Im Licht der Popularität von Stiftung Warentest in der deutschen Konsumöffentlichkeit muss es verwundern, dass – namentlich in Post-*Snowden*-Zeiten und trotz regelmäßiger öffentlicher Diskussionen über die Überwachungskapazitäten und Kooperationspraxis des Bundesnachrichtendienstes – die Grundrechtskonformität von Internetangeboten nicht ebenso Interesse weckt und Akkreditierungs- und Zertifizierungsinstitutionen und -prozesse für Internetprodukte und Internetdienstleistungen eingefordert werden.

Staaten müssen sich ernsthaft mit der Frage beschäftigen, welche Maßnahmen sie rasch setzen können, um das Vertrauen in die Integrität des Internets wiederherzustellen. Die Global Commission on Internet Governance, eine Studiengruppe zur Zukunft der Internetregulierung, fokussierte in ihrem Vorschlag für einen neuen Sozialvertrag entsprechend stark auf die Verknüpfung von Schutz der Privatsphäre und Sicherheit.

Staaten müssten tätig werden, um das Privatleben und den Datenschutz stärker zu sichern; jede Überwachung einer strikten Notwendigkeits- und Verhältnismäßigkeitsprüfung zu unterziehen; Transparenz bei Überwachungsmaßnahmen und Rechtsschutzwege zu garantieren; Online-Daten zu schützen und Konsumenten zu sensibilisieren; Vertrauen in Big Data-Lösungen zu heben; private Kommunikationen verstärkt zu schützen; keine Backdoors zu privaten Daten einzuführen; good practices im Bereich Cybersecurity zu heben und gemeinsam verstärkt gegen Cybergefahren zusammenzuarbeiten.[187] Detaillierter finden sich die Prinzipien, die angewendet werden sollten auf eine menschenrechtssensible Überwachung von Internet Kommunikation, auch in den *International Principles on the Application of Human Rights to Communications Surveillance* (May 2014)[188]. Diese wiederum zeigen auf, welch normatives Potenzial nichtstaatliche Stakeholder als Normenaggregateure und Normenpromotoren haben könnte. Das Völkerrecht hat sich diesen zu öffnen, will es sich nicht kurzsichtig erweisen gegenüber neuen normativen Dynamiken, die relevant sind für die Regulierung von Fragen, die im internationalöffentlichen Interesse liegen.

C.3.2.2. Europäische Ebene

Die EU hat mit ihrem bindenden und nichtbindenden Rechtsbestand einen bedeutenden Einfluss auf die normative Entwicklung mitgliedstaatlichen Rechts und auf die Lebensrealitäten der Unionsbürger. Wolfgang Hoffmann-Riem ist daher zuzustimmen, wenn er auch die Union in der Pflicht sieht, im Bereich ihrer Kompetenzen „für die Funktionsfähigkeit von existenzwichtigen Infrastrukturen – wie denen der Information und Kommunikation – zu sorgen."[189] Dieser Pflicht ist sie, gemeinsam mit den Mitgliedstaaten, je nach Kompetenzlage auch gemeinsam, Subsidiarität respektierend nachzukommen.

Neben den USA und der Koalition aus Russland und den BRICS ist die EU der einzige normative Player in der Entwicklung des Internetvölkerrechts, der sich bewusst für eine grundrechtssensible Ausgestaltung einsetzt. Von gleichrangiger Bedeutung ist das klare Bekenntnis der EU zur Multistakeholderstruktur der Internet Governance, das von anderen

Akteuren zwar auch abgeleistet, aber nicht ebenso überzeugend umgesetzt wird. Daher steht die EU in der Pflicht, „politisch-wirtschaftliche Gegenmachtpotentiale“[190] aufzubauen, ohne die grundrechtssensible Positionen in der Gestaltung internationaler Internetpolitik nicht durchzusetzen sind.

Internationale Kooperation zwischen den USA und der EU sind ein wichtiger Schritt zum Recht auf Privatsphäre und Datenschutz online.[191] Das ‚Umbrella Agreement‘ zwischen den USA und der EU über den Schutz persönlicher Informationen im Zusammenhang mit der Verbrechensbekämpfung ist ein wichtiger erster Schritt. Es enthält klarere Regeln zur Nutzung der übermittelten Daten, der Nichtdiskriminierung, der Weiterübermittlung (nur nach Zustimmung der europäischen Datenquellbehörde) und der richterlichen Kontrolle.[192] Das Europäische Parlament hat klar gemacht, dass es erst zustimmen würde, wenn die Rechtslage in den USA dergestalt verändert wird, dass europäischen Datensubjekte ein Recht auf einen wirksamen Rechtsbehelf im Sinne von Artikel 47 GRC eingeräumt wird.[193] Im Zusammenhang der Verhandlungen wurde auch der Vorschlag geäußert, dass die USA der Datenschutz-Konvention des Europarates (Nr. 108) beitreten könnten.[194] Ein Hauptproblem verbleibt indes: Trotz der positiven Signalwirkung des ‚Umbrella Agreements‘ ist dies nicht anzuwenden auf Behörden, die mit Fragen der nationalen Sicherheit befasst sind (also Geheimdienste) und betrifft auch nicht Daten, die auf Grundlage nationaler Gesetze (wie des Foreign Intelligence Surveillance Act, FISA) gesammelt werden.[195]

Das *Schrems*-Urteil wird auch die nächsten Verhandlungsrunden zu TTIP und TISA beeinflussen. Der Verweis des EuGH auf seine ständige Rechtsprechung, wonach die Union eine „Rechtsunion“ sei und die Möglichkeit, die Handlungen aller Organe an Primärrecht und insbesondere Grundrechten zu messen,[196] kann als Indiz dafür gesehen werden, dass der EuGH ein „Workaround“ um seine hohen Datenschutzstandards durch die Kommission über völkerrechtliche Verträge nicht akzeptieren würde.[197]

Aufgrund ihrer Kompetenz im Bereich des Wettbewerbsrechts hat die EU-Kommission darüber hinaus eine hervorgehobene Rolle in der Überprüfung des Marktvorgehens großer IT-Unternehmen. Nach fünf Jahren der Vorprüfung hat die Kommission nun ein Verfahren gegen Google eröffnet und Beschwerdepunkte gegen den Preisvergleichsdienst (comparative shopping service) übermittelt und ein Verfahren wegen des Android-Betriebssystens eingeleitet.[198] Im Kern wirft die Kommission Google einen Verstoß gegen Artikel 102 AEUV vor, der die missbräuchliche Ausnutzung einer marktbeherrschenden Stellung verbietet,[199] indem es seinen eigenen Preisvergleichsdienst auf seinen allgemeinen Suchergebnisseiten im Europäischen Wirtschaftsraum (EWR) systematisch bevorzugt. Das Verfahren ist noch in einer frühen Phase.

Auch in Rechtssetzungsverfahren der EU wird der Datenschutz herausgefordert. Der Europäische Datenschutzbeauftragte hat den aktuellen Entwurf einer Richtlinie über die Nutzung von Fluggastdaten durch europäische Behörden kritisiert und mehrere Verletzungen von Grundrechten gerügt.[200] Schließlich gibt auch die mangelnde Offenheit der EU-Verhandlungspraxis bei Verträgen und Rechtsinstrumenten mit Internetbezug (namentlich TISA und TTIP) Anlass zu Sorge.

C.3.2.3. Globale Ebene

Die Entwicklung des Völkerrechts schreitet langsam voran. Wie oben dargelegt, ist es aber das Völkerrecht „des Netzes“, das den Grundrahmen für die normative Ordnung des Internets bietet und bieten muss. Nur dem Völkerrecht sind (in letzter Instanz) Anforderungen zu entnehmen an das Ergebnis und die Verfahren zur Entwicklung von Normen dies- und jenseits der staatlichen Grenze. Besonders transnationale Regelungsarrangements und informelle Regulierungsansätze können nur über das Völkerrecht auf Legitimität überprüft werden. Nur das Völkerrecht kann in internationalen Konstellationen Freiheit und Sicherheit garantieren. Deshalb ist es nur konsequent, dass sich die Staaten der Welt schon bei den Weltgipfeln zur Informationsgesellschaft explizit dazu bekannt haben, eine Informationsgesellschaft auf Grundlage des Völkerrechts anzustreben, und der aktuelle Bericht der Regierungsexperten für die UNO die zentrale Rolle des Völkerrechts bestätigt.

Die Welt ist global vernetzt. Daher kann effektiver Schutz von Grundrechten auch in primär nationalen Fällen nur durch entsprechenden Schutz auf globaler Ebene – durch Völkerrecht – gewährleistet werden. In Hinblick auf die systemische Massenüberwachung der Internetkommunikation gehe ich daher von einer Notwendigkeit der Neukonzeption des Freiheitsschutzes in der globalen Dimension aus.[201] Dies bedeutet aber nicht, dass zwingend neue Regeln zu setzen sind. Vorschläge wie jener von Joseph Cannataci, dem neu berufenen Sonderberichterstatter für das Recht auf Privatleben (eine neue „Genfer Konvention" zum Schutz von Daten und zur Verhinderung massiver Internet-Kommunikationsüberwachung[202]) und jener von Bundeskanzlerin Merkel („globales Datenschutzabkommen nach dem Vorbild des Kyoto-Protokolls zum Klimaschutz")[203] sind weder sinnvoll noch tragfähig. Es bestehen bereits, wie ausgeführt, ausreichend Normen, die Staaten die Grenzen ihrer Überwachungskompetenzen aufzeigen. Es geht nicht darum, neues Recht zu schaffen, sondern das bestehende anzuwenden. Darüber hinaus würde sich – gerade angesichts der absehbaren Verweigerungshaltung der USA – die Sinnfrage eines derartigen Abkommens stellen. Völkerrechtspolitisch sinnvoll wäre es dagegen, die Anwendung geltender Normen – etwa die extraterritoriale Anwendung der Garantien des Zivilpakts durch alle Staaten, auch die USA – konsequent zu betreiben.

Von besonderer Bedeutung in dem Prozess der Konkretisierung und Ausdifferenzierung bestehender Normen sind Resolutionen der Organe der Vereinten Nationen, namentlich des Menschenrechtsrates und der Generalversammlung. Darüber hinaus wächst ein Bestand an Berichten von Experten, Expertengremien und Einrichtungen von Internationalen Organisationen an, der kaum mehr überschaubar ist. Zwar können diese zunächst nur als punktuelle Einlassungen gesehen werden, doch ein sensibilisierter Blick durch die Brille des postwestfälischen Völkerrechts fördert die Erkenntnis zu Tage, dass hier ein Prozess der Kristallisierung völkergewohnheitsrechtlicher Pflichten verläuft – der über einen internationalen normativen Dialog der verschiedenen Stakeholder Einfluss auf den Pfad der normativen Entwicklung nimmt. Mittelfristig werden auf diese Weise völkergewohnheitsrechtliche Normen stabilisiert.

Zentrales Regelungsziel des Völkerrechts muss es sein, wie oben gezeigt, die Stabilität und Sicherheit der Ressource Internet im globalen-öffentlichen Interesse zu garantieren. Dies muss klarer in völkerrechtspolitischen Diskursen zum Ausdruck kommen. Um mit dem Bericht der GGE von 2015 zu schließen:

> „An open, secure, stable, accessible and peaceful ICT environment is essential for all [..] to reduce risks to international peace and security. […] ICTs provide immense opportunities for social and economic development and continue to grow in importance for the international community."[204]

Das Recht der „international community", das Völkerrecht gemeinsam mit den je einschlägigen anderen Rechtskategorien in einem normativen Mehrebenensystem, muss dieser Herausforderung nachkommen.

C.3.2.4. Querschnittsmaterien

Ein Recht auf Zugang zum Internet, das als Vorbedingung des international geschützten Rechts auf Meinungsäußerungs- und Informationsfreiheit Substanz gewinnt, setzt eine grundlegende staatlich garantierte Kommunikationsinfrastruktur voraus. Staatsrecht und Völkerrecht (und auch Europarecht) spielen hier ineinander. Aber nicht nur die Umsetzung des Rechts auf Internetzugang, dessen Realisierung für alle bis 2020 nun Teil der *Agenda 2030* geworden ist, ist nur als Querschnittsmaterie zu konzipieren. Das bedeutet indes nicht, dass Staaten nicht mehr verpflichtet wären. Da es in der klassischen Konzeption des Völkerrechts vordergründig Staaten sind, die dessen Weiterentwicklung verantworten, ergeben sich aus Forderungen an das im Internet herrschende Recht auch Handlungsaufträge an staatliche Stellen. Diesen kommen sie aber nicht immer nach – besonders im Hinblick auf andere Global Players: transnationale Technologieunternehmen.

Unternehmen der Internetwirtschaft sind bislang großteils kaum rechtlich bindenden Anforderungen an ihre Transparenz unterworfen – nicht ihren Kunden gegenüber und auch nicht demokratisch legitimierten

Institutionen. Selbst der Markt versagt, da es – selbst in der Vorverfahrensphase Jahre dauernde Wettbewerbsverfahren gegen IT-Unternehmen zeigen es auf – angesichts der Netzwerkeffekte und technologischer „Lock-ins" erfolgreicher Programme (wenn auch durch Interoperabilität gemäßigt) kaum marktförmige Wege gibt, Machtasymmetrien zu kompensieren. Die Nutzer werden zwar durch Kommunikationstechnologien befähigt, kritische Gegendiskurse zu initiieren, die die Gegenstände jener Diskurse sein sollten; doch die „crowd" verfügt einfach nicht über die nötige Organisationsdichte und kommunikative Gegenmacht, um marktimmanente Selbstregulierungskräfte zur Entfaltung zu bringen.[205] Hier müssen alle Rechtsordnungen lückenfüllend eingreifen und die Anwendung der Prinzipien der Corporate Social Responsibility in Form der *UN Guiding Principles on Business and Human Rights* auf globale Player im Internet sicherstellen.

Hinsichtlich ICANNs Bindung an Menschenrechte bestehen schon einige Vorarbeiten, die nutzbar gemacht werden können – gerade auch in Bezug auf die Bindung ICANNs an Menschenrechte und demokratische Werte.[206] Im aktuellen Prozess der Reform von ICANN stellen sich menschenrechtliche Schutzfragen in besonderer Schärfe;[207] wirklich in Frage gestellt wird die „corporate and social responsibility to respect human rights" aber nicht mehr.[208]

Unternehmen haben eine wichtige Rolle für den Schutz von Menschenrechten im Internet. Das Völkerrecht des Netzes umfasst *soft law-Standards,* die diese ausbuchstabieren. Viele Unternehmen bekennen sich aktiv zum Schutz der Menschenrechte.[209] Damit können sie sich aber weder gegen Kritik an negativen Folgen für Menschenrechte in anderen Geschäftsbereichen (oder für andere Menschenrechte) immunisieren noch ihre entsprechenden Verpflichtungen aufweichen. Transparenzberichte von Unternehmen müssen klarer und eindeutiger sein, ihre Berichte unter dem UN-System (*UN Guiding Principles Reporting Framework*[210]) müssen verstärkt auf ihre menschenrechtlichen Herausforderungen im Internet Bezug nehmen.

Von Unternehmen – wie übrigens auch von Staaten – sollten im vermehrten Maße die Durchführung von Human Rights Impact Assessments (HRIA) bzw. Regulatory Impact Assessments vor der Einführung neuer Produkte oder der Setzung neuer Regeln gefordert werden.[211]

Menschenrechtliche Verpflichtungen von Unternehmen erstrecken sich auch auf die Regelung von Algorithmen. Forschungen zeigen, dass diese – zwar objektiv neutral programmiert – negative soziale Folgen zeitigen und menschenrechtliche Fortschritte im Bereich der Gleichbehandlung von Mann und Frau[212] und der sozialen und wirtschaftlichen Rechte[213] wieder rückgängig machen können.

Offene Fragen stellen sich weiters im Bereich der menschenrechtssensiblen Ausgestaltung von Big Data[214] und des *Internets of Things*. Die Regelung von Big Data wirft etwa Fragen zum Eigentum an Daten, Insolvenzrecht, Urheberrecht, Datenschutzrecht, Vertragsrecht, Informationshaftungsrecht, Steuerrecht, Strafrecht, Produkthaftungsrecht, Roboterrecht, dem Recht der Datenmarktplätze und Medizinrecht auf.[215] Nur in einer normativen Gesamtschau können etwa die Zugriffsmöglichkeiten ausländischer Behörden auf in Clouds gespeicherter Daten europäischer Nutzer problematisiert werden. Zufolge einer Studie von 2014 steckt „Big Data […] in Deutschland noch in den Kinderschuhen".[216] Studien in den USA zeigen aber, dass Big Data-Anwendungen Konsumenten, besonders verletzliche Bevölkerungsschichten, benachteiligen kann.[217] Zu diesem Schluss kommt auch ein Bericht des Weißen Hauses von 2014.[218]

Auch die flächendeckende Einführung des Internets der Dinge stellt das Rechtssystem vor Herausforderungen. Nach aktuellen Berichten[219] zirkulierte ein Ministerium einen (von einem Chiphersteller inspirierten) Plan für ein problematisches „Identitätssicherheitsgesetz für das Internet der Dinge".[220]

Nur durch internationale Zusammenarbeit kann weiters die Rolle von Unternehmen in der Umsetzung von – teils gegenläufigen – Gerichtsentscheidungen geklärt werden. Diese müssen Wege finden, um sich über

die Umsetzung von nationalen und regionalen Entscheidungen zu verständigen sowie gegenläufige normative Entwicklungen zu identifizieren.[221] Es ist problematisch, Unternehmen die Umsetzung von Urteilen mit maßgeblicher Wirkung auf die Archivfunktion des Internets und die für den öffentlichen Diskurs relevanten Daten alleine zu überlassen.

Paradebeispiel für diese normative Herausforderung ist die Umsetzung des unscharf „Recht auf Vergessen" genannten Anspruchs aus dem *Google Spain*-Urteil des EuGH,[222] dass Datenschutzbehörden Suchmaschinenbetreiber anweisen, erforderliche Maßnahmen zu ergreifen, um Einzelpersonen betreffende personenbezogene Daten (Links zu anderen Artikeln) aus ihrem Index zu entfernen und den Zugang zu diesen Daten in Zukunft zu verhindern.[223] Mangels klarerer Aussagen im Urteil griff das Unternehmen zurück auf einen selbst zusammengestellten Expertenbeirat.[224] Dieser war weder formal legitimiert noch hat er zu mehr Transparenz bei der Umsetzung der Löschpflichten geführt.[225]

Angesichts normativer Herausforderungen wie dieser und generell der sprunghaften wachsenden Normenproduktion im Mehrebenensystem durch öffentliche und private Normproduzenten wächst daher die Bedeutung von Systematisierungs- und Evaluierungsleistungen. Die Wissenschaft steht hier in der Verantwortung, unterstützt und gefördert von den Staaten, die Voraussetzungen für einen Dialog der Gerichte und Organisationen über Grundprinzipien des „Völkerrechts des Netzes" und über die darüber hinaus in internetbezogenen Fällen anzuwendenden Normenbestände zu führen. Drei erfolgreiche Projekte dienen der Illustration dieses Punktes:

- Die *NETmundial Solutions Map* ist eine kollaborative Plattform, auf der nach Themen geordnet Links zu „Lösungen" für Herausforderungen der Internetregulierung gesammelt werden.[226] So finden sich etwa für das Problem „Internetzugang" zurzeit[227] fünf Lösungen, darunter „Aquila (Facebook's Internet Drone)".[228]
- Das *Internet&Jurisdiction Project*[229] stellt einen Dialogprozess zwischen allen Stakeholdern zum Thema Jurisdiktionskonflikte online zur

Verfügung und sammelt und synthetisiert weltweit normative Ansätze an die Internetregulierung. Das Ziel des Projekts ist es, ein *Transnational Due Process Framework* zu entwickeln, das „interoperable procedural interfaces" enthält, um Transparenz, Due Process and Menschenrechtsschutz zu sichern.[230] Zu diesem Zweck hat das I&J Project eine Prinzipiensammlung zur Lösung von Jurisdiktionskonflikten entwickelt. Das ist ein Beispiel für einen Ebenen übergreifenden rechtsvergleichenden Ansatz.

- Thematisch spezifisch ist die *World Intermediary Liability Map* (WILMAP) des Center for Internet and Society der Stanford Law School, das einen Überblick zum rechtlichen Status (mit einem Fokus auf Haftung und Haftungsfreistellung) von Intermediären weltweit gibt.[231]

C.4. Zwischenfazit

Mit der Globalisierung und der verstärkten Nutzung des Internets in allen Lebensbereichen sind sowohl das staatliche Rechtsparadigma als auch das Konzept der Einheit der Rechtsordnung weder deskriptiv (so ist es) noch normativ (so sollte es sein) haltbar. Weder bedeutet dies aber das Ende des (dem Prinzip nach) souveränen Verfassungsstaates noch führt dies in die Anarchie. Der Staat – durch Legislative, Exekutive und vor allem Judikative – muss sich weiterhin auf seine zentralen Funktionen besinnen und seine Bürgerinnen und Bürger schützen, ohne deren Rechte zu verletzen – auch in Sachverhalten, die Grenzen überschreiten oder „im Internet" stattfinden. Wobei selbst jede Handlung, jeder Datenstrom, jede Cloud einen Territoriumsbezug hat, mag er auch schwer festzumachen sein. Das Internet bringt auch keine Ohnmacht des Rechts mit sich. Lediglich die Trennschärfe in der Normenproduktion zwischen den Ebenen global-regional-national und zwischen privaten und öffentlichen gesetzten und durchgesetzten Normen ist nicht mehr gegeben. Im Internet herrschen viele verschiedene Regelungsregime – also Ansammlungen von Normen unterschiedlicher Natur und Bindungswirkung. In dieser Gemengelange ist es schwierig, für Rechtsschutz zu sorgen; allen faktischen Schwierigkeiten des Mehrebenensystems zum Trotz verbleibt die Pflicht aber maßgeblich bei den Staaten.

Die normative Ordnung des Internets (bei der es sich um ein Gemisch von Rechtsordnungen und Regelungsarrangement handelt) ist dergestalt defizitär, als sie die angestrebten Ziele der internationalen Gemeinschaft für die Informationsgesellschaft, nämlich deren entwicklungsorientierte, menschenrechtssensible Ausgestaltung auf Grundlage der Charta der Vereinten Nationen, des Völkerrechts und der Allgemeinen Erklärung der Menschenrechte nicht ohne Änderungen erreichen kann. Aber da in dieser Sicht jede Rechtsordnung defizitär (und optimierbar) ist, stellt diese Feststellung noch kein Unwerturteil dar.

Von zentraler Bedeutung ist es hingegen, die drängendsten Rechtsfragen zu identifizieren und die passende Ebene zur Normierung identifizieren. Als grundsätzliches Prinzip kann die Subsidiarität gelten: Regelungen sind daher auf bürgernächster Ebene vorzunehmen, außer gute Gründe (globale Harmonisierungsnotwendigkeit) sprechen dafür, dass eine globale Regelung vorzuziehen ist. Faktische Maßnahmen – die Förderung von Selbstregulierungsmaßnahmen, die Stärkung der Medienkompetenzen der Nutzer, der Aufbau eigener Infrastrukturen und Dienste – müssen rechtliche Maßnahmen flankieren; das gemeinsame Ziel aller staatlichen Maßnahmen muss es sein, das Vertrauen in die Integrität des Internets wiederherzustellen.

Die EU hat mit ihrem bindenden und nichtbindenden Rechtsbestand einen bedeutenden Einfluss auf die normative Entwicklung mitgliedstaatlichen Rechts und auf die Lebensrealitäten der Unionsbürger und ist neben den USA und losen Staatenverbunden wie BRICS einer der wichtigsten normativen Player in der Entwicklung des Internetvölkerrechts. Die EU steht damit in der Verantwortung, global grundrechtssensible Positionen in der Gestaltung internationaler Internetpolitik durchzusetzen. Aufgrund ihrer Kompetenz im Bereich des Wettbewerbsrechts hat die EU-Kommission auch eine wichtige Funktion in der Überprüfung des Marktvorgehens großer IT-Unternehmen.

Das Völkerrecht muss im Internet nicht neu erfunden werden. Vorschläge eines neuen Vertrages über Datenschutz sind weder sinnvoll noch

tragfähig. Es bestehen bereits ausreichend Normen, die Staaten die Grenzen ihrer Überwachungskompetenzen aufzeigen.

Einschlägig sind hier insbesondere der Zivilpakt in dessen Auslegung durch das Menschenrechtskomitee und die EMRK in ihrer Auslegung vermittels des Fallrechts des EGMR. Von besonderer Bedeutung im Prozess der Granulierung des menschenrechtlichen Schutzbestandes sind Resolutionen und Berichte von internationalen Organisationen und ihren Organen. Resolutionen und Berichte können zwar auch als punktuelle Einlassungen gesehen werden, doch in einer Gesamtschau ist hier ein Prozess der Kristallisierung völkergewohnheitsrechtlicher Pflichten zu erkennen.

Nur durch internationale Zusammenarbeit aller Stakeholder können Unternehmen, ihre Daten und ihre Algorithmen demokratischer Kontrolle unterworfen werden. Urteile, die Unternehmen viel Spielraum in der Etablierung privater Umsetzungsstandards überlassen, sind nicht hilfreich. Bedeutend sind hingegen angesichts der sprunghaft wachsenden Normenproduktion im Mehrebenensystem durch öffentliche und private Quellen die Systematisierungs- und Evaluierungsleistungen der Wissenschaft.

27 Siehe im Einzelnen: Matthias C. Kettemann, Internet Governance, in Dietmar Jahnel, Peter Mader, Elisabeth Staudegger (Hrsg.), IT-Recht, 3. Aufl., (Wien: Verlag Österreich, 2013), 43–63.

28 Siehe Matthias C. Kettemann, Grotius goes Google: Der Einfluss der Internet Governance auf das Völkergewohnheitsrecht, in Christoph Vedder (Hrsg.), Tagungsband 37. Österreichischer Völkerrechtstag 2012, (Wien: Peter Lang Verlag, 2013), 89–104. Einflussreich war die Erklärung des Ministerkomitees des Europarates über die Grundsätze der Internet Governance vom 21.5.2012. Vgl. auch Germany, Federal Foreign Office, Commissioner for International Cyber Policy, German Government Proposal on Global Internet Principles (2014), http://content.netmundial.br/contribution/german-government-proposal-on-global-internet-principles/32 (siehe auch Annex I). An dem Beispiel der Globalen Internetprinzipien der Deutschen Regierung sieht man, dass neue Prinzipienvorschläge Rückgriff nehmen auf ‚erfolgreiche' normative Vorgänger. Das suggeriert eine gewisse positive normative Pfadabhängigkeit und macht den Prozess der Kristallisierung (auch) völkergewohnheitsrechtlicher Normen via Reiteration von soft law augenfällig.

29 NETmundial, NETmundial Multistakeholder Statement, 24 April 2014, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.
30 Siehe dazu im Detail III.B.4.4.
31 Heise.de, USA und China wollen Vertrag zur Begrenzung von Cyberangriffen, 20.9.2015, http://www.heise.de/newsticker/meldung/USA-und-China-wollen-Vertrag-zur-Begrenzung-von-Cyberangriffen-2822083.html#mobile_detect_force_desktop.
32 WSIS, Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, 18 November 2005, Abs. 2.
33 WSIS, Geneva Declaration of Principles (2003), Abs. 1 (Hervorhebung des Verfassers).
34 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Internet-Politik und Internet-Governance Europas Rolle bei der Mitgestaltung der Zukunft der Internet-Governance, COM/2014/072 final.
35 Christian Tomuschat, Staatsrechtliche Entscheidung für die internationale Offenheit, in Isensee/Kirchof (Hrsg.), HStR XI3 (2013), § 226 Rz 4.
36 Ibid., Rz 5 - 7.
37 Georg Jellinek, Die rechtliche Natur der Staatsverträge. Ein Beitrag zur Juristischen Construction des Völkerrechts (Wien 1880), 43.
38 Matthias C. Kettemann, The Common Interest in the Protection of the Internet: An International Legal Perspective, in Wolfgang Benedek, Koen de Feyter, Matthias C. Kettemann, Christina Voigt (Hrsg.), The Common Interest in International Law (Antwerpen: Intersentia, 2014), 167-184.
39 Developments in the field of information and telecommunications in the context of international security, A/RES/53/70 vom 4.1.1999, Abs. 2 lit. c, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70.
40 Für eine Dokumentation der Berichte einzelner Staaten siehe Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, http://www.un.org/disarmament/topics/informationsecurity.
41 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 vom 24.6.2013.
42 Ibid., Abs. 16.
43 Ibid., Abs. 19.
44 Ibid., Abs. 20. Vgl. auch Abs. 23, der die Staatenverantwortlichkeit anspricht: „States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs."
45 Ibid., Abs. 21.
46 Ibid., Abs. 16.
47 Germany, Report on Developments in the Field of Information and Telecommunications in the Context of International Security (Res. 68/243), https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/Germany.pdf.
48 Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, A/70/174 vom 22.7.2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (im Folgenden: „GGE-Bericht (2015)").
49 Mitglieder: Belarus, Brasilien, China, Kolumbien, Ägypten, Estland, Frankreich, Deutschland, Ghana, Israel, Japan, Kenia, Malaysia, Mexiko, Pakistan, Russische Föderation, Spanien, Vereinigtes Königreich und USA.

50 GGE-Bericht (2015), Ibid., Abs. 25.
51 Ibid., Abs. 28 a)-f).
52 Germany, Report on Developments in the Field of Information and Telecommunications in the Context of International Security" (RES 69/28), https://unoda-web.s3.amazonaws.com/wp-content/uploads/2015/08/GermanyISinfull.pdf.
53 Ibid., Abs. 13.
54 Der Rahmen dieser Studie erlaubt nicht, im Detail auf alle anwendbaren völkerrechtlichen Rechtssätze einzugehen. Vgl statt dessen Michael N. Schmitt und Liis Vihul, The Nature of International Law Cyber Norms, Tallinn Paper No. 5 (NATO CCD COE), 2014, 16, https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf; Katharina Ziolkowski, General Principles of International Law as Applicable in Cyberspace, in Katharina Ziolkowski (Hrsg.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (Tallinn: NATO CCD COE Publications, 2013), 135-184 (151–152).
55 Kohärenz, dies sei angemerkt, ist nur eine „formal and abstract virtue." Wie Martti Koskenniemie so schön schreibt: „For a legal system that is regarded in some respects as unjust or unworkable, no added value is brought by the fact of its being coherently so" (ILC, Fragmentation-Bericht (2006), 491).
56 Vgl. EGMR 16. 6. 2015, 64569/09 (Delfi AS v Estland; Entscheidung vom 10.10.2013 der GK zugewiesen am 17. 2. 2014) (Die Rechte und Interessen Anderer und der Gesellschaft als Ganze erlaubt es den Vertragsstaaten, unter bestimmten Bedingungen Intermediäre (hier: ein Internet News-Portal) in die Haftung zu nehmen) (vgl. zu der Problemlage: Staudegger, Haftungsprivilegierung des Hostproviders oder Medieninhaberschaft – tertium non datur?, ALJ 2015, 4); sowie EuGH, Google Spain und Google, C-131/12, Urteil des Gerichtshofes (Große Kammer) vom 13. Mai 2014 (Linklöschpflichten für Suchmaschinenbetreiber unter bestimmten Bedingungen bejaht) (statt vieler: Gerhard Spindler, Durchbruch für ein Recht auf Vergessen(werden)? – Die Entscheidung des EuGH in Sachen Google Spain und ihre Auswirkungen auf das Datenschutz- und Zivilrecht, JZ 69/2014, 981–991).
57 Vgl. Malcolm N. Shaw, International Law, 5. Aufl. (Oxford: Oxford University Press, 2003), 232.
58 Menschenrechtsrat, Resolution 26/13, The promotion, protection and enjoyment of human rights on the Internet, 20.6.2014, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/26/L.24; Menschenrechtsrat, Resolution 20/8, The promotion, protection and enjoyment of human rights on the Internet, 16.7.2012, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8.
59 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27 vom 16.5.2011, http://www2.ohchr.org/english/bodies/hrcouncil/ docs/17session/A.HRC.17.27_en.pdf.
60 Ibid., Abs. 20.
61 Mary Rundle and Malcolm Birdling, Filtering and the International System: A Question of Commitment, in Ronald Deibert et al. (Hrsg.), Access Denied: The Practice and Policy of Global Internet Filtering (Cambridge, MA: MIT Press, 2008), 73-102.
62 Molly K. Land, Toward an International Law of the Internet, Harvard International Law Journal, 54 (2013), 393-458.
63 Menschenrechtskommission, Allgemeiner Kommentar zu Art. 19 IPbpR, CCPR/C/GC/34 vom 12.9.2011, Abs. 15: „States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto."
64 Vgl EGMR, Yildirim v. Türkei (18.12.2012), No. 3111/10, Abs. 31: "in theory" bestehe ein derartiges Recht in mehr als zehn Mitgliedstaaten des Europarates.

65 BVerfG, 1 BvL 10/10; 1 BvL 2/11 vom 18.7.2012, Rn. 94; BVerfG, 1 BvL 10/12 vom 23.7.2014, Rn. 74 („Dem Gesetzgeber steht ein Gestaltungsspielraum zu […]; [dabei] ist er auch durch völkerrechtliche Verpflichtungen gebunden.“)

66 Neben dem Recht auf Internetzugang ist nach dieser Sicht übrigens auch die Sicherheit und Integrität der Kommunikationssysteme als objektiv-rechtliche Vorbedingung der Ausübung kommunikativer Rechte geschützt (dazu sehr instruktiv Wolfgang Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, 69 JZ 2/2014, 53-63 (53).

67 So etwa Bundesgerichtshof, Urteil des III. Zivilsenats vom 24.1.2013, III ZR 98/12.

68 BVerfG, 1 BvL 1/09 vom 9.2.2010, Rn. 136: „Die verfassungsrechtliche Gewährleistung eines menschenwürdigen Existenzminimums muss durch ein Parlamentsgesetz erfolgen, das einen konkreten Leistungsanspruch des Bürgers gegenüber dem zuständigen Leistungsträger enthält.“

69 Ibid., Rn. 135.

70 Ibid., Rn. 138. Dieser Ansatz wird bestätigt in Hinblick auf Leistungen für Asylwerber durch BVerfG, 1 BvL 10/10; 1 BvL 2/11 vom 18.7.2012, Rn. 92 (Leistungsanspruch aus Art. 1 Abs. 1 GG […] hängt von […] den jeweiligen wirtschaftlichen und technischen Gegebenheiten [ab]“); ebenso BVerfG, 1 BvL 10/12 vom 23.7.2014, Rn. 74 („Grundrecht […] bedarf […] der Konkretisierung und stetigen Aktualisierung durch den Gesetzgeber [ausgerichtet] an dem jeweiligen Entwicklungsstand des Gemeinwesens und den bestehenden Lebensbedingungen im Hinblick auf die konkreten Bedarfe der Betroffenen“).

71 Vereinte Nationen, Transforming Our World. The 2030 Agenda for Sustainable Development, https://sustainabledevelopment.un.org/content/documents/7891Transforming%20Our%20World.pdf, Ziel 9.c.: „Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.“

72 Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, A/HRC/17/31 vom 21.3.2011, Annex.

73 Vgl schon die Beiträge in Rikke F. Jørgensen (ed.), Human Rights in the Global Information Society (Cambridge, MA: MIT Press, 2006); eine Übersicht bei Wolfgang Benedek, Menschenrechte in der Informationsgesellschaft, in André Zwierlein, Nicole Zillien (Hrsg.), Informationsgerechtigkeit. Theorie und Praxis der gesellschaftlichen Informationsversorgung (Berlin: De Gruyter, 2012), 69-88.

74 Menschenrechtsrat, Resolution 26/13, The promotion, protection and enjoyment of human rights on the Internet, 20.6.2014, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/26/L.24; Menschenrechtsrat, Resolution 20/8, The promotion, protection and enjoyment of human rights on the Internet, 16.7.2012, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8. Ein kurze Analyse der Resolution von 2012 bei Matthias C. Kettemann, The UN Human Rights Council Resolution on Human Rights on the Internet: Boost or Bust for Online Human Rights Protection, Human Security Perspectives (2012) 1, 145-169.

75 Menschenrechtsrat, Resolution 28/16, The Right to Privacy in the Digital Age, A/HRC/RES/28/16 vom 1.4.2015, Abs. 3.

76 Vgl Menschenrechtskommission, Allgemeiner Kommentar Nr. 34 zu Art. 19 IPbpR, CCPR/C/GC/34 vom 12.9.2011, Absatz 43.

77 EGMR, Yildirim (2012); Europarat, Parlamentarische Versammlung, Resolution 1877 on the protection of freedom of expression and information on the Internet and online media, Res. 1877 (2012), http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=18323&lang=en.

78 EGMR, Stoll v. Schweiz (10.12.2007), No. 69698/01, Abs. 104 mit weiteren Nachweisen; siehe auch Wolfgang Benedek und Matthias C. Kettemann, Freedom of Expression on the Internet (Straßburg: Council of Europe Publishing, 2014), 24f.
79 Zum grundrechtlichen Schutz der Privatsphäre im europäischen Recht, siehe sogleich.
80 Christoph Grabenwarter, Katharina Pabel, Europäische Menschenrechtskonvention, 5. Aufl. (München: Beck, 2012), 226 (mit weiteren Nachweisen).
81 Siehe die exzellente Zusammenfassung bei Helmut Philipp Aust, Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014, 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages, https://www.bundestag.de/blob/282870/fc52462f2ffd254849bce19d25f72fa2/mat_a_sv-4-1_aust-pdf-data.pdf.
82 Koalitionsvertrag (2013), 104.
83 Menschenrechtskomitee, Allgemeiner Kommentar No. 16 (1994), Abs. 21.
84 Ibid., Abs. 8.
85 Ibid., Abs. 9.
86 Siehe die Antwort der USA auf die Empfehlungen im Rahmen des Universal Periodic Review, Addendum of the United States of America to the Report of the Working Group on its Universal Periodic Review (16.9.2015), https://geneva.usmission.gov/2015/09/01/addendum-of-the-united-states-of-america-to-the-report-of-the-working-group-on-its-universal-periodic-review: Auf einen besseren Schutz des Privatlebens zielende Empfehlungen werden insoweit unterstützt,
„as they recommend respect for ICCPR Article 17, which applies to individuals within a state's territory and subject to its jurisdiction. Our Constitution and laws contain appropriate protections for privacy of communications, consistent with our international human rights obligations, and we publicize our policies to the extent possible, consistent with national security needs. We frequently update and draft new laws, regulations, and policies to further protect individuals' privacy."
Eine extraterritoriale Anwendung wird ausgeschlossen.
87 Ähnlich: Marko Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, Harvard International Law Journal 56 (2015) 1, 81-146, http://www.harvardilj.org/wp-content/uploads/561Milanovic.pdf.
88 Vgl. Europarat, Parlamentarische Versammlung, Komitee für Rechtsangelegenheiten und Menschenrechte, Bericht – Mass surveillance, Rapporteur Mr. Pieter Omtzigt, Doc. 13734 vom 18.3.2015, http://www.coe.int/t/dghl/standardsetting/media/Conf-FoE-2015/Report%20on%20Mass%20Surveillance%20of%20Mr%20Pieter%2 0Omtzigt.pdf
89 Menschenrechtsrat, Resolution 28/16, The Right to Privacy in the Digital Age, A/HRC/RES/28/16 vom 1.4.2015.
90 Generalversammlung, The Right to Privacy in the Digital Age, Resolution 68/167, A/RES/68/167 vom 21.1.2014.
91 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens".
92 EuGH, Rs. C-362/14, Schrems v. Data Protection Commissioner, Urteil vom 6.10.2015.
93 Ibid., Rn. 97-98.
94 Ibid., Rn. 92.
95 EuGH, Rs C-293/12 and C-594/12, Digital Rights Ireland und Seitlinger u.a., Urteil vom 8.4.2014.
96 EuGH, Schrems (2015), Rn. 93.
97 Ibid., Rn. 94.
98 Ibid., Rn. 95.

99 EuGH, C-362/14, Maximillian Schrems/Data Protection Commissioner. Schlussanträge von Generalanwalt Yves Bot.
100 Vgl. Lorna Woods, Schrems v Data Protection Commissioner, Key Aspects of the Judgment, The International Forum for Responsible Media Blog, 7.10.2015, https://inforrm.wordpress.com/2015/10/07/case-law-cjeu-schrems-v-data-protection-commissioner-key-aspects-of-the-judgment-lorna-woods.
101 EuGH, Rs C-293/12 and C-594/12, Digital Rights Ireland und Seitlinger u.a., Urteil vom 8.4.2014.
102 EuGH, Rs C-131/12, Google Spain und Google, Urteil vom 13.5.2014
103 EuGH, Rs C-212/13, František Ryneš/Úřad pro ochranu osobních údajů, Urteil vom 11.12.2014.
104 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32 vom 22.5.2015, www.ohchr.org/EN/HRBodies/HRC/RegularSessions/ Session29/Documents/A.HRC.29.32_AEV.doc.
105 Ibid., Abs. 17.
106 OHCHR, The right to privacy in the digital age, A/HRC/27/37 vom 3.6.2014, Abs. 47, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (Hervorhebung des Verfassers).
107 Dies betrifft speziell die EU: Report on human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries (2014/2232(INI)), Committee on Foreign Affairs Rapporteur: Marietje Schaake, 3.6.2015, Abs. 3: „the active complicity of certain EU Member States in the NSA's mass surveillance of citizens and spying on political leaders, as revealed by Edward Snowden, has caused serious damage to the credibility of the EU's human rights policy and has undermined global trust in the benefits of ICTs."
108 Ibid., Abs. 61-62.
109 EGMR, Klass und andere v. Deutschland, No. 5029/71 vom 6.9.1978, Abs. 48.
110 Ibid., Abs. 49.
111 EGMR, Shimovolos v. Russia, No. 30194/09 vom 28.11.2011, Abs. 68.
112 Weitere Einsichten, besonders in Hinblick auf die Aktivitäten der „Five Eyes"-Staaten, versprechen die Fälle Big Brother Watch and Others v. the United Kingdom (Appl. No. 58170/13) and Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (Appl. No. 62322/14).
113 Council of Europe Commissioner for Human Rights Democratic and effective oversight of national security services (Mai 2015), Abs. 18, http://www.coe.int/t/dghl/standardsetting/media/Conf-FoE-2015/Commissioner%20for%20Human%20Rights_Democratic%20and%20effective%20oversight%20of%20national%20security%20services.pdf.
114 European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, adopted by the Venice Commission at its 102nd Plenary Session (20.-21.3.2015), http://www.coe.int/t/dghl/standardsetting/media/Conf-FoE-2015/Venice%20Commission_Study%20No%20719_2013.pdf, Study No. 719/2013, CDL-AD(2015)006.
115 Ausführungen zur Rolle des EU-Rechts und der EU zum Schutz des Privatlebens – bezogen auf die Kooperation mit den USA und das Schrems-Verfahren vor dem EuGH um Facebook-Nutzerdatenweitergabe an die USA – finden sich unter III.C.3.2.2.
116 Sidney Hook, Democracy as a Way of Life, in: John N. Andrews u. Carl A. Marsden (Hrsg.), Tomorrow in the Making (New York: Whittlesey House, 1939), 31-46.
117 Wendy Brown, We Are All Democrats Now, The Kettering Review (2011) 29, 44-52.

118 Noch 1996 hieß es seitens der Vereinten Nationen – und das in der Agenda for Democratization (meine Hervorhebung): „it is not for the United Nations to offer a model of democratization or democracy or to promote democracy in a specific case." (UN, Agenda for Democratization, A/51/761 vom 20.12.1996, Abs. 10).

119 Niels Petersen, Demokratie als teleologisches Prinzip: Zur Legitimität von Staatsgewalt im Völkerrecht (Frankfurt am Main: Springer, 2009).

120 Eine ausführliche Übersicht findet sich bei OHCHR, Compilation of documents or texts adopted and used by various intergovernmental, international, regional and sub-regional organizations aimed at promoting democracy, http://www.ohchr.org/english/law/compilation_democracy/index.htm.

121 Thomas Franck, The Emerging Right to Democratic Governance, AJIL 1992, 46-91.

122 Im Kontext der Internet Governance wird Multistakeholderismus verstanden als „the study and practice of forms of participatory democracy that allow for all those who have a stake and who have the inclination to participate on equal footing in the deliberation of issues and the design of policy. While they may assign implementation to a single stakeholder group, implementers are accountable to the decision making stakeholders." (Internet Governance Forum (IGF) 2014, Best Practice Forum on Developing Meaningful Multistakeholder Mechanisms, http://www.intgovforum.org/cms/documents/best-practice-forums/developing-meaningful-multistakeholder-participation-mechnisms/410-bpf-2014-outcome-document-developing-mean ingful-multistakeholder-mechanisms).

123 Vgl. die gute Übersicht über die Prozeduralisierung von Legitimation in transnationalen Konstellationen bei Michael Zürn, Martin Binder, Matthias Ecker-Ehrhardt, Katrin Radtke, Politische Ordnungsbildung wider Willen, Zeitschrift für Internationale Beziehungen 14 (2007) 1, 129-164 (154ff, 157).

124 Wolfgang Benedek, The Relevance of Multi-Stakeholder Approach and Multi-Track Diplomacy for Human Rights Diplomacy, in Michael O'Flaherty et al. (Hrsg.), Human Rights Diplomacy: Contemporary Perspectives (London: Stroud, 2011), 251-261 (253).

125 Dorothea Baur, NGOs as Legitimate Partners of Corporations. A Political Conceptualization (Heidelberg: Springer, 2012).

126 So mit einigen Anforderungen mehr schon Jürgen Habermas: „Gültig sind genau die Handlungsnormen, denen alle möglicherweise Betroffenen als Teilnehmer an rationalen Diskursen zustimmen könnten" (Jürgen Habermas, Faktizität und Geltung (Frankfurt am Main: Suhrkamp, 1992), 138). Auch die Bedingungen zur Herstellung eines idealen Diskurses klingen ähnlich den Anforderungen an Multistakeholder-Diskurse: Potentielle Teilnehmer sollen die gleichen Chancen haben, sich im Diskurs einzubringen, sie können in alle ihnen relevanten Themen ansprechen, sie müssen in der Lage sein, ihre Einstellungen zum Ausdruck zu bringen und sie müssen in der Lage, sich zu widersetzen. Schon 2003 bezog Michael Froomkin Habermas auf das Internet: Michael A. Froomkin, Habermas@discourse.net: Toward a Critical Theory of Cyberspace, Harvard Law Review 116 (2003), 749-873.

127 IGF, Best Practice Forum on Developing Meaningful Multistakeholder Mechanisms (2014) (supra). Gerade die Frage der ‚bad actors' ist kontrovers. Nur schwerlich lässt sich zwischen der (auch) emotionalen Äußerung valider Gegenargumente und inhaltlicher Obstruktion unterscheiden. Auch die Diskussion der Legitimität der Beteiligung von GONGOs – governmental non-governmental organizations – fällt hier hinein. Viele sind recht betrachtet staatliche Akteure. Bekannte Beispiele sind die Myanmar Women's Affairs Federation, die harsche Kritik an Nobelpreisgewinnerin Aung San Suu Kyi übte, und aus den Frauen der Generäle von Myanmars Ex-Militärjunta bestand; die kirgisische Assocation of Non-commercial and Nongovernmental Organizations; Bolivarian Circles, die Hugo Chavez unterstützten; und Chongryon, ein Netzwerk nordkoreanischer ‚zivilge-

sellschaftlicher' Organisationen in Japan, das von der Regierung Nordkoreas kontrolliert wird (vgl. Moisés Naím, Democracy's Dangerous Impostors, Washington Post, 21.4. 2007, A17; siehe auch Moisés Naím What Is a GONGO? How government-sponsored groups masquerade as civil society, Foreign Policy, 13.10.2009, http://foreignpolicy.com/2009/10/13/what-is-a-gongo).

128 Ryan Budish, Sarah Myers West, Urs Gasser, Designing Successful Governance Groups: Lessons for Leaders from Real-World Examples, August 2015, Berkman Center Research Publication No. 2015-11, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2638006.

129 Ryan Budish, Sarah Myers West, Urs Gasser, Multistakeholder as Governance Groups: Observations from Case Studies, January 14, 2015, Berkman Center Research Publication No. 2015-1, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549270.

130 Von Konzept der Weltzivilgesellschaft zu unterscheiden ist jenes der regimespezifischen (nichtstaatlichen) Zivilverfassungen (Gunther Teubner, Globale Zivilverfassungen, ZaöRV 63 (2003), 1 (22)). Allerdings ist es möglich, dass sich vermittels responsiver und reflexiver, sich einander öffnender und zunehmend vernetzter Zivilverfassungen, auch eine globale Zivilgesellschaft entwickelt. Schon jetzt in nationalen Kontexten eine gesellschaftliche Atomisierung festzustellen, gekoppelt mit einer zunehmender Ausdifferenzierung und Komplexifizierung von Fragen und Prozessen sozialer Regulierung, die zivilgesellschaftliches Engagement benötigen. Perspektiven globaler Vernetzung könnten bei vielen Bürgern eher zu kognitiver Überforderung und sodann zu Partizipationsverweigerung führen.

131 Julian Nida-Rümelin, Das Internet als Chance, die Konturen einer Weltzivilgesellschaft zu entwickeln, Multistakeholder Internet Dialog (MIND), Volume 5 (Berlin, Juni 2013), http://www.collaboratory.de/w/Das_Internet_als_Chance,_die_Konturen_einer_Weltzivilgesellschaft_zu_entwickeln: „Das Internet bietet zumindest eine Chance, die Konturen einer Weltzivilgesellschaft zu entwickeln. Noch ist die Internetkommunikation nicht hinreichend inklusiv, um von einer über die Internetkommunikation etablierten Weltbürgerschaft zu sprechen. Aber die jüngste[n] Entwicklung[en] weisen – trotz aller Kommerzialisierung – in diese Richtung."

132 Broadband Commission for Digital Development (ITU/UNESCO), State of Broadband 2015, http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf.

133 Broadband Opportunity Council, Report and Recommendation, 20.8.2015, https://www.whitehouse.gov/sites/default/files/broadband_opportunity_council_report_final.pdf.

134 Digitale Agenda, Fortschrittsbericht im Kabinett: Digitale Agenda kommt voran, http://www.digitale-agen da.de/Content/DE/Artikel/2015/09/2015-09-15-digitale-agenda-fortschrittsbericht.html;jsessionid=3009D8E76 F601E311790AF2F08A4B7E1.s1t2.

135 Bundeministerium für Verkehr und digitale Infrastruktur, Dobrindt fördert Kommunen mit Milliarden-Programm für den Breitbandausbau, http://www.bmvi.de/SharedDocs/DE/Artikel/DG/eckpunkte-des-milliarden-foerderprogramms-breitbandausbau.html

136 Vgl. Dieter Frey, Matthias Rudolph, Jan Oster, Gutachten: Rechtliche Bewertung des Gesetzentwurfs zur Neuregelung der Host-Providerhaftung, im Auftrag von eco – Verband der deutschen Internetwirtschaft e.V., https://www.eco.de/wp-content/blogs.dir/150913-gutachten-host-providerhaftung-2015000545.pdf

137 Julia Gerhards, (Grund-)Recht auf Verschlüsselung? (Frankfurt am Main: Nomos, 2010).

138 Bericht von Sonderberichterstatter Kaye, A/HRC/29/32 vom 22.5.2015, passim und Abs. 5: „Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief."

139 Andreas Fischer-Lescano, Der Kampf um die Internetverfassung, JZ 20 (2014), 965-974 (974).

140 Vasudevan Mukunth, A Call for a New Human Right, the Right to Encryption, 2.6.2015, TheWire,http://thewire.in/2015/06/02/a-call-for-a-new-human-right-the-right-to-encryption-2976.
141 Secure Data Act, S. 135 – 114th Congress (2015-2016): „To prohibit Federal agencies from mandating the deployment of vulnerabilities in data security technologies“, vorgelegt am 8.1.2015, https://www.congress.gov/bill/114th-congress/senate-bill/135/text.
142 Bericht von Sonderberichterstatter Kaye, A/HRC/29/32 (2015), Abs. 8.
143 Peter König, Heise Online, Hack mit 3D-Drucker: TSA-Generalschlüssel für Gepäck, 10.9.2015, http://www.heise.de/make/meldung/Hack-mit-3D-Drucker-TSA-Generalschluessel-fuer-Gepaeck-2810177.html.
144 Gerd Winter, Transnationale informelle Regulierung: Gestalt, Effekte und Rechtstaatlichkeit, in Gralf-Peter Calliess (ed.), Transnationales Recht (Tübingen: Mohr Siebeck, 2014), 95-112 (108), spricht von „rule of law“, die die Willkür der „subkutan“ ausgeübten Macht beschränken muss.
145 Armin von Bogdandy, General Principles of International Public Authority: Sketching a Research Field; German Law Journal 9 (2008) 11, 1910-1938, http://www.germanlawjournal.com/article.php?id=1048; weiterführend: Armin von Bogdandy, Prinzipien von Staat, supranationalen und internationalen Organisationen, § 232 (275-304), in Isensee/Kirchof (Hrsg.), HStR XI3 (2013) (zugleich Armin von Bogdandy, Prinzipielles zur Pluralität normativer Ordnungen. Zu den Anforderungen an die Ausübung öffentlicher Gewalt, Normative Orders Working Paper 1/2013).
146 Rainer Forst und Klaus Günther, Die Herausbildung normativer Ordnungen. Zur Idee eines interdisziplinären Forschungsprogramms, in Rainer Forst und Klaus Günther (Hrsg.), Die Herausbildung normativer Ordnungen. Interdisziplinäre Perspektiven (Frankfurt/New York: Campus, 2011), 11-30 (16).
147 Beispielhaft: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Internet-Politik und Internet-Governance Europas Rolle bei der Mitgestaltung der Zukunft der Internet-Governance, COM/2014/072 final.
148 Rainer Forst, Das Recht auf Rechtfertigung. Element einer konstruktivistischen Theorie der Gerechtigkeit (Frankfurt am Main: Suhrkamp, 2007).
149 Rainer Forst und Klaus Günther, Die Herausbildung normativer Ordnungen. Zur Idee eines interdisziplinären Forschungsprogramms, in Rainer Forst und Klaus Günther (Hrsg.), Die Herausbildung normativer Ordnungen. Interdisziplinäre Perspektiven (Frankfurt/New York: Campus, 2011), 11-30 (16).
150 Klaus Günther, Normativer Rechtspluralismus – Eine Kritik, Normative Orders Working Paper 03/2014 (2014), 8.
151 International Law Association, Accountability of International Organisations (1996 - 2004), http://www.ila-hq.org/en/committees/index.cfm/cid/9, 1-2 (mit ausführlicher Diskussion der Prinzipien im Bericht).
152 Instruktives zur Ausgestaltung von Beteiligungsrechten zur Rückbindung von Entscheidungsprozessen an gesellschaftliche Willensbildungsprozesse (um die Besonderung des Staates zivilgesellschaftlich einzuholen) bei Andreas Fisahn, Demokratie und Öffentlichkeitsbeteiligung (Tübignen: Mohr Siebeck, 2002), 216f.
153 Dies sind das Management von Internet Protocol (IP)-Adressen, das Management der Protokoll-Parameter und die Verwaltung der Root Zone, auf deren Ausübung die USA verzichten wollen, wenn ein stabiles multistakeholderbasiertes Modell entwickelt werden kann, das eine Vereinnahmung durch andere Regierungen vermeidet, von allen Stakeholdern unterstützt werden kann und die Offenheit des Internets bewahrt.

154 Milton Mueller, ICANN Accountability: A Three Hour Call Trashes a Year of Work, 6.9.2015, http://www.internetgovernance.org/2015/09/06/icann-accountability-a-three-hour-call-trashes-a-year-of-work.
155 ICANN, CCWG/Board Dialogue Meeting, 2.12.2014, https://community.icann.org/pages/viewpage.action?pageId=56133316. Auch Mitglieder des Regierungsbeirats von ICANN (GAC – Governmental Advisory Committee), kritisierten mehrheitlich dessen Aufnahme als ‚first among equals' in einen neuen Mechanismus und befürworteten die Beibehaltung des Status quo, in dem der GAC nicht bindende, aber wirkungsvolle Empfehlungen an den ICANN-Vorstand abgibt (Milton Mueller, GAC as „First Among Equals": The Danger in the Accountability Plan, 29.8.2015, http://www.internetgovernance.org/2015/08/29/gac-as-first-among-equals-the-danger-in-the-accountability-plan).
156 Klaus Günther, Normativer Rechtspluralismus – Eine Kritik, Normative Orders Working Paper 03/2014 (2014), 1.
157 Lars Viellechner, Transnationalisierung des Rechts (Weilerswist: Velbrück, 2013), 99, dessen Beitrag unter der jüngeren Literatur zur Transnationalisierung (gerade auch mit Bezug zum Internet) begriffsprägend war. Besonders einlässlich seine Ausführungen zum Regime der Domainvergabe durch ICANN (127 ff).
158 Stephan Hobe, Cyberspace – der virtuelle Raum, in: Isensee/Kirchof (Hrsg.), HStR XI3 (2013), § 271, Rn. 44.
159 Vgl. zur Einführung in den Begriff Matthias C. Kettemann, Internet Governance, in Dietmar Jahnel, Peter Mader, Elisabeth Staudegger (Hrsg.), IT-Recht, 3. Aufl., (Wien: Verlag Österreich, 2013), 43-63.
160 Wolfgang Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, 69 JZ 2/2014, 53-63 (63).
161 Matthias Goldmann, Internationale öffentliche Gewalt. Handlungsformen internationalen Institutionen im Zeitalter der Globalisierung (Heidelberg: Springer, 2015).
162 Manchmal preschen Gerichte allerdings auch vor, was zu Rechtsverweigerung führen kann. Vgl. Matthias C. Kettemann, How to Implement Controversial Court Decisions: International Constitutional Lessons from Brown v. Board of Education for the Austrian Cases on Topographical Signs in Carinthia, International Constitutional Law Online Journal (ICL Online), vol. 4 (2010), 590-623.
163 Entsprechende Pflichten finden sich auch in verschiedenen Jurisdiktionen: Australisches Recht limitiert den Export von gesundheitsbezogenen Daten; Südkorea verlangt, dass geographische Daten lokal gespeichert werden; Vietnam zwingt Unternehmen zu einer lokal gespeicherten Sicherheitskopie (vgl., sehr kritisch diesen Entwicklungen gegenüber, Anupam Chander, Uyen P. Le, Breaking the Web: Data Localization vs. the Global Internet, UC Davis Legal Studies Research Paper Series No. 378 (April 2014), 1: „Data localization requirements threaten the major new advances in information technology—not only cloud computing, but also the promise of big data and the Internet of Things."
164 Michael Malloy, Pavel Arievich, Russia's data localization requirement will take effect September 1, Data Protection, Privacy and Security Alert (US), 8 July 2015, https://www.dlapiper.com/en/us/insights/publications/2015/07/russia-data-localization-requirement.
165 Daniel Joyce, Internet Freedom and Human Rights, EJIL 26 (2015) 2, 493-514.
166 EuGH, Schrems, Rn. 73.
167 Ibid.
168 Peters, EuGH erklärt Safe-Harbour für ungültig – Was folgt daraus für die europäischen Sicherheitsbehörden?, 13.10.2015, http://www.juwiss.de/74-2015.
169 Vgl. Viellechner, Transnationalisierung (2013), 265ff.
170 Angesichts der Vielzahl an Regelungsmaterien mit Internetbezug müssen diese natürlich auf einige wichtige beschränkt bleiben.

171 Diese verstehen sich in Ergänzung der schon unter III.B.3.3. erwähnten rechtspolitischen Erwägungen.
172 Winter, Transnationale informelle Regulierung (2014), 96.
173 Utz Schliesky, Christian Hoffmann, Anika D. Luch, Sönke E. Schulz, Kim Corinna Borchers, Schutzpflichten und Drittwirkung im Internet. Das Grundgesetz im digitalen Zeitalter (Baden-Baden: Nomos, 2014), 146.
174 Ibid, 147.
175 Zumal Clouds ja nicht – wie der Begriff ‚Wolke' suggeriert – ohne Territoriumsbindung sind. Daten müssen physisch gespeichert werden; dies geschieht in der Regel in großen Serverfarmen.
176 So David Bethlehem, The End of Geography: The Changing Nature of the International System and the Challenge to International Law, EJIL 25 (2014) 1, 9-24. Siehe aber die zu Recht geäußerte Kritik bei David S. Koller, The End of Geography: The Changing Nature of the International System and the Challenge to International Law: A Reply to Daniel Bethlehem , EJIL 25 (2014) 1, 25-29, sowie Carl Landauer, The Ever-Ending Geography of International Law: The Changing Nature of the International System and the Challenge to International Law: A Reply to Daniel Bethlehem, EJIL 25 (2014) 1, 31-34.
177 So zutreffend Christian Walter, Cyber Security als Herausforderung für das Völkerrecht, JZ 14/2015, 685-693 (691ff.).
178 In der Hess-Entscheidung, BVerfGE 55, 349ff, führt das BVerfG aus, dass die Involvierung anderer Staaten in Sachverhalte dazu führen kann, dass grundrechtlich geschützte Rechtspositionen nicht ohne weiteres durchgesetzt werden können, da die Außenpolitik und das Völkerrecht Grenzen setzen.
179 Schliesky et al. (2014), 181.
180 Ibid., 150ff.
181 Ibid.: Es sei der Rechtswissenschaft „vordringlichste Aufgabe", „dogmatische Grundlagen, Maßstäbe und Grenzen der staatlichen Schutzpflichten weiterzuentwickeln" (156).
182 Vgl. für einen Überblick über sinnvolle Maßnahmen zur Steigerung von inklusiven Informationsgesellschaften: UNESCO, UNESCO Internet Study: Keystones to Foster Inclusive Knowledge Societies (2015), http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/unesco-internet-study.
183 Schliesky et al. (2014), 167-179.
184 So Bundesinnenminister Thomas de Maizière in einer Rede vor dem IT-Sicherheitskongress, zit. nach Thomas Rudl, Bundesregierung beschließt IT-Konsolidierung der Bundesverwaltung und will „Bundes-Cloud", Netzpolitik.org, 20.5.2015, https://netzpolitik.org/2015/bundesregierung-beschliesst-it-konsolidierung-der-bundesverwaltung.
185 Diese Kompetenzen kommen dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), BGBl 2009 I Nr. 54 vom 14.8.2009 idF IT-Sicherheitsgesetz, BGBl 2015 I Nr. 31 vom 24.7.2015, und der Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) zu.
186 Vgl. BSI, Zertifizierung und Konformitätsbewertung, https://www.bsi.bund.de/DE/Themen/Zertifizierungund Anerkennung/zertifizierungundanerkennung_node.html.
187 Statement by the Global Commission on Internet Governance, Toward a Social Compact for Digital Privacy and Security, Wednesday, April 15, 2015, https://www.ourinternet.org/publication/toward-a-social-compact-for-digital-privacy-and-security; Global Commission on Internet Governance, Toward a Social Compact for Digital Privacy and Security (2015), https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Social_Compact.pdf.

188 International Principles on the Application of Human Rights to Communications Surveillance, Final Version (May 2014), https://necessaryandproportionate.org/text.
189 Wolfgang Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, 69 JZ 2/2014, 53-63 (61).
190 Ibid.
191 Streng genommen handelt es sich um Völkerrecht, aber ich behandle den Vertrag hier, da für Mandat wie Inhalt der Verhandlungen europäisches Recht relevant ist.
192 European Commission, Questions and Answers on the EU-US data protection „Umbrella agreement", 8.11.2015,http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.
193 Dies ist durch den Judicial Redress Act of 2015, http://judiciary.house.gov/_cache/files/8a28056b-387e-46f2-8c80-655249f4ae8f/hr-1428.pdf, geplant. Vgl. Francesca Bignami, The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs (May 15, 2015), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf.
194 Marc Rotenberg, On International Privacy: A Path Forward for the US and Europe, Harvard International Review (Juni 2014), http://hir.harvard.edu/archives/5815.
195 Vgl. die Kritik bei Peter Schaar, Leaky Umbrella, EAID-Blog (Europäische Akademie für Informationsfreiheit und Datenschutz), 18.9.2015, http://www.eaid-berlin.de/?cat=8.
196 EuGH, Schrems (2015), Abs. 60.
197 Vgl. Steve Peers, The party's over: Eu data protection law afte rthe Schrems Safe Harbour judgment, 7.10.2015, http://eulawanalysis.blogspot.be/2015/10/the-partys-over-eu-data-protection-law.html.
198 Europäische Kommission, Wettbewerb, Antitrust Case 39740 „Google Search", http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740.
199 Europäische Kommission, Kartellrecht: Kommission übermittelt Google Mitteilung der Beschwerdepunkte zu seinem Preisvergleichsdienst, Brüssel, 15 April 2015, http://europa.eu/rapid/press-release_MEMO-15-4781_de.htm.
200 European Data Protection Supervisor, Opinion 5/2015, Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 24.9.2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-24_PNR_EN.pdf.
201 So auch Hoffmann-Riem, JZ 2/2014, 62.
202 Adam Alexander, Digital surveillance ‚worse than Orwell', says new UN privacy chief, 24.8.2015, http://www.theguardian.com/world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief (mit starken Worten: Der Guardian zitiert ihn unter anderem damit, dass „British surveillance oversight [is] ‚a joke'; […]the situation is worse than anything George Orwell could have foreseen."
203 FAZ, Spähaffäre: Merkel regt globales Datenschutz-Abkommen an, 20.7.2013 http://www.faz.net/aktuell/politik/spaehaffaere-merkel-regt-globales-datenschutz-abkommen-an-12288963.html („Bundeskanzlerin Angela Merkel [hat] ein globales Datenschutzabkommen nach dem Vorbild des Kyoto-Protokolls zum Klimaschutz angeregt. […] In einem Zusatzprotokoll könnte ein Bekenntnis zu einem zeitgemäßen und weitreichenden Datenschutz verankert werden").
204 GGE-Bericht 2015, Abs. 2-3.
205 So auch Hoffmann-Riem, JZ 2/2014, 63.

206 Europarat (Thomas Schneider and Monika Zalnieriute), ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values, Dezember 2014, DGI(2014)12, https://www.coe.int/t/informationsociety/Source/DGI_2014_12E%20Report%20ICANN%20and%20Human%20Rights%20updated%208%20Oct%202014.pdf.

207 Siehe die beiden Berichte: Article 19, ICANNs Corporate Responsibility to Respect Human Rights, Februar 2015, http://www.article19.org/data/files/medialibrary/37845/ICANN-PAPER-WEB.pdf und Article 19, Issue report for the Cross Community Working Party on ICANN's Corporate and Social Responsibility to Respect Human Rights: Practical recommendations for ICANN, Juni 2015, https://www.article19.org/data/files/medialibrary/38003/ICANN_report_A5-for-webv2.pdf.

208 Cross Community Working Party on ICANN's Corporate and Social Responsibility to Respect Human Rights (CCWP-HR), Oktober 2015, https://www.article19.org/data/files/medialibrary/38148/ICANN_CS_to_respect_ HR_report_ALL_FINAL-PDF.pdf.

209 Etwa im Rahmen der Global Network Initiative, https://www.globalnetworkinitiative.org, die den Telecommunications Industry Dialogue on Freedom of Expression and Privacy, http://www.telecomindustrydia logue.org, organisiert. Die GNI hat u.a. Prinzipien (http://globalnetworkinitiative.org/principles) und Richtlinien zu deren Implementierung (http://globalnetworkinitiative.org/implementationguidelines) entwickelt. Siehe auch GNIs Jahresbericht für 2014: GNI 2014 Annual Report (2015), https://globalnetworkinitiative.org/sites/default/files/2014%20Annual%20Report.pdf.

210 UN Guiding Principles Reporting Framework, http://www.ungpreporting.org.

211 Als Beispiele für „Tools", nach denen diese Prüfungen stattfinden können, zählen etwa Danish Institute for Human Rights Compliance Assessment Tool, https://hrca2.humanrightsbusiness.org; und International Finance Corporation (IFC), Human Rights Impact Assessment and Management Tool, http://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/guide+to+human+rights+impact+assessment+and+management.

212 University of Washington, Who's a CEO? Google image results can shift gender biases, EurekAltert, (paper presented at Association for Computing Machinery's CHI 2015 conference), 9.4.2015, http://www.eu rekalert.org/pub_releases/2015-04/uow-wac040915.php (Bildersuche nach „CEO" zeigt 11 Prozent Frauen, obwohl 27 % von US-CEOs weiblich sind; dies beeinflusst die Wahrnehmung der Rolle von Frauen in der Wirtschaft).

213 Amit Datta, Michael Carl Tschantz, and Anupam Datta, Automated Experiments on Ad Privacy Settings, A Tale of Opacity, Choice, and Discrimination, Proceedings on Privacy Enhancing Technologies 2015 (1), 92–112, http://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf (Werbungen für Jobs mit hohen Einkommen werden Männern häufiger gezeigt als Frauen).

214 Vgl. Viktor Mayer-Schönberger und Kenneth Cukier, Big Data. A Revolution that will transform how we live, work and think (Oxford: OUP, 2013).

215 Vgl. die Beiträge in Thomas Hoeren (Hrsg.), Big Data und Recht (München: C.H.Beck, 2014).

216 Thomas Hoeren, Fazit, in ibid., 135.

217 Nathan Newman, How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population, Journal of Internet Law 18 (2014) 6, 11.

218 Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, May 2014, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. Dieser wartet auf S. 60 mit einer interessanten Policy Recommendation auf: „Extend Privacy Protections to non-U.S. Persons. The Office of Management and Budget should work with departments and agencies to apply the Privacy Act of 1974 to

non-U.S. persons where practicable, or to establish alternative privacy policies that apply appropriate and meaningful protections to personal information regardless of a person's nationality." Das wird ja auch vom Europäischen Parlament als Vorbedingungen zu dessen Zustimmung zum 'Umbrella Agreement' gefordert.

219 Kai Biermann, Internet of Things: Ein Ausweis für jeden vernetzten Toaster?, 17.9.2015, http://www.zeit.de/digital/internet/2015-09/internet-sicherheit-identitaet-nxp.

220 Ein Antrag auf Aktenauskunft wurde eingebracht. Vgl. Thomas Rudl, Eckpunktepapier für Identitätssicherheitsgesetz, 17.9.2015, https://fragdenstaat.de/anfrage/eckpunktepapier-fur-identitatssicherheitsgesetz.

221 Agnes Callamard, Are Courts re-inventing Internet Regulation?, Global Freedom of Expression @ Columbia University Discussion Paper (Mai 2015), https://globalfreedomofexpression.columbia.edu/wp/wp-content/uploads/2015/06/A-Callamard-AreCourts-reinven-ting-Internet-regulation-May-6-2015.pdf?37c4ff.

222 EuGH, Rs C-131/12 vom 13.5.2014, Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González.

223 Am Tag der Veröffentlichung des Delinking-Formulars erhielt Google 12.000 Anfragen (Spiegel Online, Google-Formular: 12.000 Löschanträge am ersten Tag, 31.5.2014, http://www.spiegel.de/netzwelt/netzpolitik/google-12-000-loeschantraege-am-ersten-tag-a-972612.html). Bis Ende September 2015 gingen ca. 320.000 Anfragen ein, und Gogle hat 1,14 Millionen URLs auf Entfernungsnotwendigkeit analysiert. 41 Prozent der URLs werden im Durchschnitt auch entfernt (Google, Google Transparency Report, European privacy requests for search removals (Stand: 28.9.2015), http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en).

224 Google, Google Experten-Beirat (Advisory Council to Google on the Right to be Forgotten, Final Report, 6.2.2015, https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view.

225 Siehe Kritik bei Open Letter to Google from 80 Internet Scholars, Release RTBF Compliance Data, 14.5.2015, https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd.

226 NETmundial Solutions Map (Beta), Mapping Internet Governance Actors, Issues, Solutions, and Resources, https://map.netmundial.org.

227 28.9.2015.

228 NETmundial Solutions Map, Viewing Solution, Aquila, https://map.netmundial.org/map/view/777.

229 Internet&Jurisdiction Project (Bertrand de la Chapelle, Paul Fehlinger), http://www.internetjurisdiction.net (gefördert von öffentlichen und privaten Stellen).

230 Internet&Jurisdiction Project, Progress Report 2013/2014, http://www.internetjurisdiction.net/progress-report-2013-14.

231 Stanford Law School, Center for Internet and Society, World Intermediary Liability Map, http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap.

IV. Zusammenfassung

Die Entwicklung des Völkerrechts, so der Internationale Gerichtshof im Gutachten zu *Reparation for Injuries*, „has been influenced by the requirements of international life".[232] Im Licht dieser Anforderungen – mehr kollektives Staatenhandeln – erschien es 1949 angebracht, den Vereinen Nationen Rechtspersönlichkeit, unabhängig von jener der Mitgliedstaaten, zuzuerkennen.

Völkerrecht darf und muss sich wandeln im Einklang mit den „needs" der internationalen Gemeinschaft.[233] Deren Anforderungen haben sich seit der Erfindung des WWW und der Kommerzialisierung, Politisierung und Militarisierung des Internets sowie der Medienkonvergenz bei gleichzeitiger Digitalisierung ganzer Lebensbereiche substanziell gewandelt. Das Internet ist heute zum „öffentlichen Raum des 21. Jahrhunderts geworden – der Hauptplatz der Welt, das Klassenzimmer, Marktplatz, Kaffeehaus und der Nachtklub".[234] Durch die Mobilisierung des Zugangs mittels Smartphones ist das Internet (allzu) allgegenwärtig. Während in der Frühphase des Netzes noch eine dezentrale Regulierung von Online-Verhalten funktionierte, führte die Popularisierung ab Mitte der 1990er Jahre zu verstärken normativen Interventionen von Staaten. Gleichzeitig entwickelte sich ein „Völkerrecht des Netzes" aus bestehenden, für das Internet fruchtbar gemachten Regeln aus dem allgemeinen Völkervertrags- und -gewohnheitsrecht sowie aus soft law-Regeln und privaten Rechtsregimen.

Die Aufgabe dieses Gutachtens war es zu untersuchen, ob es eines „Völkerrechts des Netzes" bedarf und wie dies ausgestaltet werden müsste, um die geltenden Grund- und Freiheitsrechte und die Chancen für eine demokratische Teilhabe am weltweiten Kommunikationsnetz zu verstärken;

und ob zwischen nationalem, europäischem und internationalem Recht Regelungs- oder Umsetzungsdefizite im Internet bestünden.

Hauptziel des Gutachtens war es, begriffliche Klarheit zu schaffen und die Bedeutung des Völkerrechts für die Entwicklung einer menschenrechtssensiblen und entwicklungsorientierten Informationsgesellschaft herauszuarbeiten. Es war ein glücklicher Zufall, dass die Hauptphase der Bearbeitung dieser Fragen in die Zeit der UNO-Vollversammlung im September 2015 fiel. Dort einigten sich die Staaten der Welt auf Nachhaltige Entwicklungsziele, darunter jenes, bis 2020 allen Menschen Internetzugang zu verschaffen. Dieses Bekenntnis schlägt eine normative Schneise durch Völkerrecht, Europarecht und Staatsrecht und zeigt – als soft law Norm mit viel Umsetzungsspielraum, aber gleichzeitig mir starkem moralischen Gewicht und hoher Effektuierungswahrscheinlichkeit – zugleich auf, vor welchen Herausforderungen das Recht in der Informationsgesellschaft steht.

Das Völkerrecht des Netzes findet Erwähnung sowohl im Koalitionsvertrag als auch in der Digitalen Agenda. Ich habe eingangs versucht, die „Funktionalisierung", die das Völkerrecht des Netzes in beiden Dokumenten erfährt, zu problematisieren. Wir brauchen kein neues Völkerrecht des Netzes, *um* Menschenrechte zu schützen und Teilhabechancen zu erhöhen. Wir *haben* ein Völkerrecht des Netzes, das – unvollkommen – Menschenrechte schützt und Teilhabechancen realisieren lässt. Bestehendes Völkerrecht muss lediglich im Lichte der Finalität der Informationsgesellschaft, in einem responsiven normativen Prozess, in dem Staatsrecht und Europarecht sowie private Rechtsregime und Regelungsarrangements relevant sind, adaptiert werden.

Die Anwendbarkeit des Völkerrechts auf das Internet wird bekräftigt in den Berichten der *Group of Governmental Experts*. Zuletzt bestätigte der „Zero Draft" des Outcome Documents für das WSIS+10-Treffen, den Review-Gipfel der Ergebnisse des Weltgipfel-Prozesses von 2003 und 2005,[235] die Anwendbarkeit dessen Völkerrechts und dessen zentraler Prinzipien auf das Internet. Der (schon weitgehend akkordierte) Zero

Draft legt ein besonderes Augenmerk auf die Bedeutung des Internets für die Entwicklung und die Rolle des Völkerrechts im Zusammenhang mit der Realisierung der „Vision von WSIS“ – diese korrespondiert ja mit der Finalität der Internetregulierung.

Die internationale Gemeinschaft bedarf jedenfalls eines Völkerrechts des Netzes – im Sinne eines auf staatliche und nichtstaatliche Aktivitäten mit Bezug zum Internet anwendbaren internationalen Normenbestandes. Nur mit diesem lassen sich Freiheit und Sicherheit im Internet effektiv schützen; nur mit Völkerrecht lassen sich etwa die global commons sichern; das Völkerrecht ist das *ius necessarium* der internationalen Gemeinschaft. Die Staaten der Welt haben sich darauf geeinigt, eine menschenzentrierte, einschließende, entwicklungsorientierte Informationsgesellschaft anzustreben – gestützt auf die Ziele und Grundsätze der Charta der Vereinten Nationen, des Völkerrechts und der Menschenrechte.

Das setzt allerdings voraus, dass der Zugang zum Internet (der durch Infrastrukturmaßnahmen sicherzustellen ist) und der Zugang zu Internet-Inhalten (der vor Zensur zu schützen ist) garantiert ist. Nur dann kann das wichtige Prinzip, dass nämlich alle Menschenrechte, die offline gelten, auch online gelten, umfassend und ganzheitlich umgesetzt werden. Zwar sind alle Menschenrechte im Internet zu schützen (und geschützt), bedingen sich wechselseitig und bekräftigen einander; doch kann dem Schutz des Privatlebens als *Gateway* für die Meinungsäußerungsfreiheit eine besondere Funktion eingeschrieben werden. Die Meinungsäußerungsfreiheit wiederum kann als katalysierendes Recht für alle anderen Rechte gelten.

Eine zentrale Erkenntnis des Gutachtens ist, dass nicht das Völkerrecht des Netzes an sich lückenhaft ist. Vielmehr sind es völkerrechtswidrige Handlungen durch die USA und die anderen „Five Eyes“-Staaten sowie europäische Staaten, die eng mit diesen kooperiert haben, die das Recht auf Privatsphäre im Internetzeitalter und den Charakter des Internets als Vertrauensraum gefährden. Die Verletzung einer Norm bekräftig aber zugleich deren Gültigkeit, besonders wenn die Auslegung des Völkerrechts durch den Verletzerstaat nicht von der überwiegenden Mehrheit der

Staaten gedeckt wird – hier bezogen auf die Verweigerung der USA, dem Zivilpakt extraterritoriale Wirkung zuzuerkennen und den Schutz der Privatsphäre diskriminierungsfrei auch *non-US persons* angedeihen zu lassen.

Das Internet dynamisiert demokratische Teilhabeprozesse. Individuell kann die demokratische Legitimation der normativen Ordnung des Internets inkrementell dadurch gefördert werden, dass Einzelne verstärkt an globalen Prozessen der Internet Governance teilnehmen. Systemisch wird dies durch den Multistakeholder-Ansatz durchgesetzt, der seine Verwirklichung findet in der Entwicklung und Anwendung durch Regierungen (Staaten), den Privatsektor (Unternehmen) und die Zivilgesellschaft (Individuen) in ihren jeweiligen Rollen von Instrumenten und Prozessen zur Regelung des Internets.

Die demokratische Legitimation von Internetpolitik-Prozessen ist unvollständig. Prinzipien wie Rechtstaatlichkeit sind nur schwer in internationale Kontexte mit unsteten Regelungsgeographien und changierenden Akteurskonstellationen zu übersetzen. *Checks and Balances* ist mangels akkordierter Regeln für die „Checks“ und konkurrierender Gewalten für die „Balances“ nur in Ansätzen implementierbar. Aber Rule of Law – nicht im Sinne von Rechts*staat*lichkeit, sondern eher einer Institutionalisierung eines Rechtfertigungszwangs für Entscheidungsstrukturen wie Entscheidungen durch deren Legitimierung unter Beteiligung aller Stakeholder – verbleibt ein wichtiges Prinzip für jede Formation, die international-öffentliche Gewalt im weitesten Sinne ausübt. Accountability oder Rechenschaftspflicht ist auszugestalten als das Recht aller Stakeholder der normativen Ordnung, andere Akteure und Prozesse auf die Rechtfertigung ihres Bestehens, Handelns und ihrer Normenproduktion zu befragen. Sämtliche formalen und informellen Institutionen, die relevant sind für die Entwicklung und Anwendung von Normen und Praktiken mit Bezug zum Internet sehen sich gegenüber der in Multistakeholderstrukturen organisierten internationalen Gemeinschaft zunehmend einem Rechtfertigungsdruck ausgesetzt. Das Beispiel der ICANN-Reform und der Transition der IANA-Funktionen spricht hier eine deutliche Sprache.

Uneindeutig zu beantworten verbleibt hingegen oft die Frage nach dem anwendbaren Recht in Fällen mit Internetbezug. In der Gemengelange von Völkerrecht, Europarecht, Staatsrecht, privaten Rechtsregimen und transnationalen Regelungsarrangements stellt es eine Herausforderung dar, für Rechtsschutz zu sorgen; aus ihrer entsprechenden Pflicht entlassen werden Staaten dennoch nicht.

Die normative Ordnung des Internets ist zwar keine klassische Rechtsordnung, doch weist sie wie auch ihre Teilordnungen aus einschlägigen Normen der drei erwähnten Ebenen global, regional und national Defizite dergestalt auf, als sie die angestrebten Ziele der internationalen Gemeinschaft für die Informationsgesellschaft, nämlich deren entwicklungsorientierte, einschließende, menschenrechtssensible Ausgestaltung auf Grundlage der Charta der Vereinten Nationen, des Völkerrechts und der Allgemeinen Erklärung der Menschenrechte nicht ohne Änderungen erreichen kann. Das ist aber kein fundamentaler Einwand. Jede Rechtsordnung muss sich wandeln, um zeitgemäß zu sein; kein Normenbestand kann angesichts des sozialen Wandelns versteinern.

Ein Grundproblem im Schutz der Grundrechte hat das Gutachten im Auseinanderdriften der faktischen Schutzmöglichkeiten des Staates und der Schutzerwartung des Einzelnen identifiziert. Nutzer sind sich oft nicht bewusst, dass sie zwar vor ihrem Computer (oder Smartphone) verbleiben, sich ihre Daten beim Zugriff auf Clouds und Online-Spiele aber außerhalb der Reichweite des deutschen Staates befinden mögen. Das schafft faktische Rechtsschutzhindernisse. Doch diese bestehen selbst dort, wo der Staat unstrittig handeln könnte, nämlich auf seinem Territorium – hier müssen Grundrechtspositionen auch gegenüber Geheimdiensten gesichert werden. Neuer Grundrechte bedarf es nicht; es dürfte ausreichen, wenn die Schutzpflichtdimension der Grundrechte in Lehre und Rechtsprechung weiterentwickelt wird, wobei auch verstärkt über das Recht der AGBs Grenzen für die Autonomie sozialer Räume und ihre Betreiber aufgezeigt werden können. Weitere Maßnahmen zur Förderung des Vertrauens in das Internet können im Aufbau von eigenen Diensten, der Förderung von Zertifizierungen und von Verschlüsselungstechnologien liegen.

Die EU hat sich explizit zur Multistakeholderstruktur und zur Förderung der Menschenrechte in der Internet Governance bekannt. Damit baut sie eine starke Gegenmachtposition gegenüber den USA (im Bereich Schutz des Privatlebens) und gegenüber Russland und China (Internet als Instrument zur Förderung der Menschenrechte, nicht deren Einschränkung) auf. Die normative Ausgestaltung internationaler Kooperationsbeziehungen darf europäisches Recht nicht verletzen; das gilt etwa für das ‚Umbrella Agreement' zu transatlantischem Datenverkehr ebenso wie für TTIP und TISA. Für die beiden letztgenannten Verträge ist der Fall Schrems einschlägig, der es dem EuGH erlaubt hat, die in Google Spain and Google (Recht auf Deindexierung) begonnene Judikatur zum Schutz des Privatlebens online zu expandieren und mittels der Forderung des der EU „gleichwertigen Schutzes" von Daten im Zielland des Datentransfers dem europäischen Datenschutzrecht eine bedeutende extraterritoriale Wirkung zu verleihen.

Die EU hat auch Kompetenzen im Bereich des Wettbewerbsrechts, die sie nutzen kann, um eine missbräuchliche Ausnutzung einer marktbeherrschenden Stellung durch einzelne IT-Unternehmen zu inkriminieren. Nach fünf Jahren Vorbereitungen hat sie nun Beschwerdepunkte gegen Google bekannt gegeben.

Das Völkerrecht ist Grundlage der Informationsgesellschaft. Ausweislich des Berichts von 2015 der GGE ist es vollumfänglich auf das Internet anzuwenden. Seine zentralen Prinzipien – souveräne Gleichheit, Nichtintervention, friedliche Streitbeilegung, völkerrechtliche Verantwortlichkeit, Schutz der Menschenrechte – gestalten maßgeblich die Internet Governance. Diese Grundsätze nehmen regelmäßig den Rang von Gewohnheitsrecht ein, teilweise sind sie sogar ius cogens Normen. Es ist daher nicht sinnvoll, nach neuen Verträgen – z.B. zu Datenschutz oder globaler Cyber-Sicherheit – zu rufen. Ganz unabhängig von inhaltlichen Fragen würden Vertragsverhandlungen zwischen Staaten einen normativen Rückgriff auf das klassische Normenvokabular des Völkerrechts bedeuten, das den Multistakeholderstrukturen der Internet Governance schwerlich gerecht wird. Aktuelle Proteste gegen TTIP zeigen, dass sich engagierte zivilgesellschaftliche Koalitionen bilden, wenn bestimmte

funktionellen Regelungsregime – und die Internetregulierung qua Cyber-Sicherheitsvertrag wäre ohne Zweifel einschlägig – betroffen sind.

Weit zielführender ist es, bestehendes Recht internetsensibel anzuwenden und den langsamen Prozess der Kristallisierung neuer gewohnheitsrechtlicher Normen beobachtend und kritisierend zu begleiten. Für die Habitualisierung der internationalen Gemeinschaft an die soft law-basierte Entwicklung von großer Bedeutung (wenn schon mangels Bindungswillen nicht als Hinweis auf entsprechende Staatenpraxis) ist der Bestand an Berichten von Experten, Expertengremien und Einrichtungen von Internationalen Organisationen.

Große Internet-Unternehmen sind wenig formal bindenden Normen des Völkerrechts unterworfen. Allerdings wächst der Bestand an soft law-Normen und Selbstverpflichtungen, im Prozess der Umsetzung des UN Guiding Principles on Business and Human Rights zur Implementierung des „Protect, Respect and Remedy"-Frameworks. Dies betrifft auch ICANN, deren Bindung an Menschenrechte in allen Tätigkeitsbereichen nun nicht mehr in Frage gestellt wird.

Von Unternehmen sollte im verstärkten Maße die Durchführung von Impact Assessments im Bereich der Menschenrechte gefordert werden, um sicherzustellen, dass neue Produkte und neue Technologien nicht Menschenrechte gefährden. Algorithmen sind auf Menschenrechtssensibilität und ungewollte Negativfolgen – auch empirisch – zu prüfen und ggf. zu korrigieren. Auch in der Einführung des Internets der vernetzten Dinge und der verstärkten Nutzung von Big Data zur Lenkung von staatlichen Entscheidungen und Finanzflüssen müssen die Menschenrechte eine zentrale Rolle spielen.

Ein vom Auswärtigen Amt und dem Humboldt-Institut für Internet und Gesellschaft 2014 in Berlin organisierter Workshop zum „Völkerrecht des Netzes" kam zu dem Schluss, dass sämtliche Stakeholder mit dem Status Quo unzufrieden seien:

> „Staaten sind frustriert, dass sie Recht im Internet nicht durchsetzen können. Mangels eindeutiger und geltender Regelungen wissen Unternehmen nicht, wie sie mit (staatlichen und privaten) Anfragen umgehen sollen; sie sind quasi gezwungen, Recht zu sprechen. Nutzer haben Angst um ihre Daten und vor Verletzungen ihrer Grundrechte."[236]

Dem Friedensnobelpreisträger und Juristen Aristide Briand wird der Aphorismus zugeschrieben, dass eine Entscheidung dann gut sei, wenn alle gleich unzufrieden seien. Demnach bestünde also kein Änderungsdruck für die normative Ordnung des Internets. Dem ist natürlich nicht so. Wie ich in diesem Gutachten gezeigt habe, ist die kontinuierliche Weiterentwicklung eines responsiven und reflexiven Rechtsbestandes auf allen Ebenen nötig, um eine menschenzentrierte und entwicklungsorientierte Informationsgesellschaft ebenso nachhaltig zu sichern wie Internetzugang für alle bis 2020.

232 IGH, Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion of 11 April 1949, ICJ Reports (1949), 174 (178).

233 Vgl. ibid. Allerdings im Gutachten nur bezogen auf die Rechtssubjekte: „The subjects of law in any legal system are not necessarily identical in their nature or in the extent of their rights, and their nature depends upon the needs of the community".

234 Secretary of State Hillary Clinton, Internet Rights and Wrong: Choices and Challenges in a Networked World, George Washington University, Washington, D.C., 15.2.2011, http://www.state.gov/secretary/rm/2011/02/156 619.htm (Übersetzung des Verf.).

235 United Nations General Assembly's Overall Review of the Implementation of WSIS Outcomes – Zero Draft, Oktober 2015, http://digitalwatch.giplatform.org/instruments/wsis-10-resolution-zero-draft (Abs. 5. „We also recognize the need for respect for political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states, as well as applicable international law, in the realization of the WSIS vision"), Abs. 48 („We recognize the central importance of the principles of international law enshrined in the UN Charter in building confidence and security in the use of ICT, particularly the political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states and respect for human rights and fundamental freedoms"), Abs. 42 („We reaffirm the principle, recognised in General Assembly resolution 68/167, that the same rights that people have offline must also be protected online". Dies betrifft auch Völkerrecht im allgemeinen Sinne)).

236 Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG), Workshop zu „Völkerrecht des Netzes, 8.9.2014, Protokoll, http://www.hiig.de/wp-content/uploads/2014/12/Vo--lkerrecht-des-Netzes.pdf, 7.

Annex: German Government Proposal on Global Internet Principles (2014)[237]

"(1) The global, open and free nature of the Internet as a single commons has to be ensured. It is a driving force for progress towards development in its various forms including economic growth, encouraging innovation and allowing for creativity. [*adjusted from UN, OECD: open, distributed, interconnected, CoE and G8 similar, also similar ROAM, COMPACT*]

(2) The same rights that people have offline must also be protected online. [*UN*] Consistency and effectiveness in privacy protection have to be strengthened at a global level. Although concerns about public security may justify gathering and protection of certain sensitive information, unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, may violate the rights to privacy, freedom of expression and access to information. [*adopted from UN, OECD, similar also UK paper on roles for governments in ITU*]

(3) Access to the Internet should respect the principles of non-discrimination, transparency and openness. [*adjusted from OECD, similar G8; CGI.br, CoE; OECD*]

(4) All stakeholders working together, cooperating in policy development processes and on internet governance arrangements, each in their respective roles and with specific responsibilities, respect these principles and refrain from any measure which may violate human rights, undermine equal and democratic participation, disrespect the rule of law or compromise the global and open nature of the internet. [*adjusted from CoE, similar G8, CGI.br, COMPACT*]

(5) The rule of law must be the foundation for legislation and normative development online. States must ensure full compliance with their obligations under international law.

(6) Cultural and linguistic diversity can foster the development of local content, regardless of language or script, notwithstanding the universality of human rights. [*adjusted from CoE, similar CGI.br, also UK paper on roles for governments in ITU*]

(7) Individual empowerment is a key resource and further efforts to strengthen it have to be undertaken, not only with regard to education, knowledge, health and infrastructure, but also with regard to an accessible, affordable, stable, reliable and secure digital environment. [*adjusted from OECD, CoE and G8, similar also UK paper on roles for governments in ITU*] To this end, technically advanced states should endeavor to support appropriate capacity building in digitally less advanced states where needed and ensure that exchange is based on locally appropriate approaches. [*adopted among others from G8*]

(8) Decision-taking processes in the realm of Internet Governance need to be transparent and fair and include all stakeholders in their respective role ensuring that decision-makers are held accountable for their decisions. [*adjusted from OECD, similar G8, COMPACT*]

(9) The security, stability, robustness and resilience of the Internet as well as its ability to evolve should be a key objective of internet governance. [*adjusted from CoE, similar CGI.br*]

(10) The technical community as well as the private sector should retain their leading role in the day-to-day management of technical and operational matters in the management of the internet, decentralised in character. [*adjusted from CoE*]"

237 Germany, Federal Foreign Office, Commissioner for International Cyber Policy, German Government Proposal on Global Internet Principles (February 2014), http://content.netmundial.br/contribution/german-government-proposal-on-global-internet-principles/32.

Zum Autor

Dr. Matthias C. Kettemann, LL.M. (Harvard)

Matthias C. Kettemann (*1983) studierte Rechtswissenschaften in Graz und Genf und war Fulbright und Boas Scholar an der Harvard Law School (LL.M. 2010). 2012 promovierte er an der Karl-Franzens-Universität Graz mit einer Arbeit zur Zukunft des Individuums im Völkerrecht. 2006 bis 2013 war er Universitätsassistent und Lektor am Institut für Völkerrecht und Internationale Beziehungen der Universität Graz. Seit Oktober 2013 forscht er als Post-Doc Fellow am Exzellenzcluster „Die Herausbildung normativer Ordnungen" der Goethe-Universität Frankfurt am Main, wo er sich zur normativen Ordnung des Internets habilitiert.

Er war Co-Chair der Internet Rights & Principles Coalition, hat für den Europarat, das Europäische Parlament und das Internet&Society Co:llaboratory geforscht und publiziert regelmäßig zu Rechtsfragen des Internets in Online- und Offlinemedien. Er ist unter anderem Ständiger Redakteur bei *jusIT – Zeitschrift für Informationsrecht, Redakteur des juridikum. Zeitschrift für Recht, Kritik, Gesellschaft,* Reviewer für Zeitschriften wie First Monday, Global Communication und Global Governance, Affiliate des Network of Excellence in Internet Science und nationaler Experte des Internet & Jurisdiction Observatory. Dr. Kettemann ist Reviewer für Rechtsfragen des Internets für die Czech Science Foundation und als Experte Mitglied im EU Fundamental Rights Agency (FRANET) Consortium. 2014 wurde er von Vertretern der internationalen Internetforschung als Vertreter

der Wissenschaft in das Exekutivkomitee des Global Multistakeholder Meeting on the Future of the Internet (NETmundial Meeting) gewählt.

In letzter Zeit erschienen von ihm *European Yearbook on Human Rights 2015* (jährlich, Mitherausgeber), *The Common Interest in International Law* (2014, Mitherausgeber), *Bestand und Wandel im Völkerrecht* (2014, Mitherausgeber), Freedom of Expression on the Internet (2014 (engl.), 2015 (franz.), Mitautor), *Grenzen im Völkerrecht* (2013, Herausgeber), *Netzpolitik in Österreich. Internet. Macht. Menschenrechte* (2013, Mitherausgeber) und *The Future of Individuals in International Law* (2013).

Kontakt:
Dr. Matthias C. Kettemann, LL.M. (Harvard)
Exzellenzcluster Normative Ordnungen
Goethe-Universität Frankfurt am Main
Max-Horkheimer-Straße 2
60629 Frankfurt am Main

matthias.kettemann@normativeorders.net
kettemann@jur.uni-frankfurt.de
internationallawandtheinternet.blogspot.de

ISBN 978-3-95861-328-7