Deutscher Bundestag

Ausschuss für Menschenrechte
und humanitäre Hilfe

Ausschussdrucksache
19(17)96

LEIBNIZ-INSTITUT
FÜR MEDIENFORSCHUNG
HANS-BREDOW-INSTITUT

Stellungnahme als Sachverständiger zur öffentlichen Anhörung auf Einladung des Ausschusses für Menschenrechte und humanitäre Hilfe des Deutschen Bundestags zum Thema „Menschenrechte und politische Teilhabe im digitalen Zeitalter“, 17. Juni 2020

von Priv.-Doz. Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard)
Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI) [1]

Inhaltsverzeichnis

[1] PD Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard), Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), Rothenbaumchaussee 36, 20148 Hamburg; Vertretungsprofessor für Internationales Recht, Friedrich-Schiller-Universität Jena; Privatdozent für Völkerrecht, Internetrecht, Rechtstheorie, Institut für Öffentliches Recht, Goethe-Universität Frankfurt am Main; Projektleiter, Völkerrecht des Netzes, Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG), Berlin; Forschungsgruppenleiter, Content and Platform Governance, Sustainable Computing Lab, WU Wien; Lektor, Institut für Völkerrecht und Internationale Beziehungen, Karl-Franzens-Universität Graz. Der Verfasser dankt Stephan Dreyer, Katharina Mosene, Felix Victor Münch, Thorian Schmied, Johannes Schmees, Wolfgang Schulz, Carlotta Siegel, Anna Sophia Tiedeke und Florian Wittner (Hamburg), Julia Pohle (Berlin), Martha Routen (Jena), Wolfgang Benedek, Gregor Fischer und Ilse Kettemann (Graz) und Felicitas Rachinger und Marie-Therese Sekwenz (Wien) für Unterstützung bei der Recherche bzw. für hilfreiche Kommentare.

1. Gegenstand der Anhörung und der Stellungnahme

Gegenstand der öffentlichen Anhörung des Ausschusses für Menschenrechte und humanitäre Hilfe des Deutschen Bundestags am 17. Juni 2020 ist das Thema „Menschenrechte und politische Teilhabe im digitalen Zeitalter". Den Sachverständigen wurde eine Liste von zwölf Fragen der Fraktionen übermittelt, auf die ich in dieser Stellungnahme mit (angesichts der Breite der angesprochenen Themen) unterschiedlichem Auflösungsgrad eingehen werde.

Die folgenden Ausführungen nehmen mithin *ausgewählte* Rechtsfragen in den Blick,[2] die sich im Zusammenhang mit dem Einfluss der Digitalisierung auf Achtung, Schutz und Gewährleistung von Menschenrechten, darunter politischen Teilhaberechten, ergeben.[3]

Meiner Stellungnahme voranstellten möchte ich zwei Erkenntnisse. Zunächst fußen meine Ausführungen mit Berg, Rakoswki und Thiel auf der Erkenntnis, dass auch in der digitalen Konstellation demokratische Politik Gestaltungsmöglichkeiten hat: „Die Annahme einer relativen Gestaltungsfähigkeit kollektiver Handlungsformen bildet dabei die Voraussetzung politischer Reflexion und erst unter dieser Bedingung kann eine politikwissenschaftlich

[2] Ich habe meine Antworten unterschiedlich detailliert gestaltet. Zu vielen der angesprochenen Themen habe ich weiterführende Lektüre angegeben.

[3] Ich befasse mich seit 15 Jahren mit dem Schutz der Menschenrechte im Internet. Der Beitrag greift daher auf Überlegungen und Texte zurück, die bereits veröffentlicht sind, darunter: Kettemann, The Normative Order of the Internet. A Theory of Online Rule and Regulation (Oxford: Oxford University Press, 2020); Benedek/Kettemann, Freedom of Expression on the Internet (Straßburg: Europarat, 2014, 2. Aufl. 2020 i.E.) (französische Übersetzung: 2015, 2. Aufl.: 2021, ukrainische Übersetzung: 2015; türkische Übersetzung: 2016); Kettemann/Schulz, Setting Rules for 2.7 Billion. A (First) Look into Facebook's Norm-Making System: Results of a Pilot Study (Hamburg: Working Papers of the Hans-Bredow-Institut, Works in Progress # 1, January 2020); Schulz/Kettemann/Heldt (Hrsg.), Probleme und Potenziale des NetzDG – ein Reader mit fünf HBI-Expertisen / Problems and Potentials of the NetzDG – a Reader with five HBI Expert Opinions (Hamburg: Verlag Hans-Bredow-Institut, November 2019 (Arbeitspapiere des HBI Nr. 48); Kettemann, Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Stiftung, 2015); Kettemann/Mosene, Hassrede und Katzenbilder: Ausgewählte menschenrechtliche Aspekte der Governance von Meinungsäußerungen im Internet, Elisabeth Greif und Silvia Ulrich (Hrsg.), Hass im Netz – Grenzen digitaler Freiheit (Linz: Böhlau, 2019), 92-122; Kettemann/Benedek, Freedom of expression online, in Mart Susi (Hrsg.), Human Rights, Digital Society and the Law. A Research Companion (London: Routledge, 2019), 58-74; Kettemann, "This is Not a Drill": International Law and Protection of Cybersecurity, in Wagner/Kettemann/Vieth (Hrsg.), Research Handbook of Human Rights and Digital Technology (Cheltenham: Edward Elgar, 2019), 113-128; Kettemann, Grundrechte im Internet: Die Rolle der Justiz in der Entwicklung der "Internetverfassung", in Bundesministerium für Justiz, Die Medienlandschaft 2015 – Herausforderungen für die Justiz (2016), 73-84; Kettemann, Die Weltordnung des Digitalen, Vereinte Nationen. Zeitschrift für die Vereinten Nationen und ihre Sonderorganisationen/German Review on the United Nations 5/2019, 195-200; Kettemann, Internationale Regeln für soziale Medien. Menschenrechte wahren und Desinformation bekämpfen, Global Governance Spotlight 2/2019, Stiftung Entwicklung und Politik (sef.) (Bonn, 2019); Kettemann, Zwischen Hassrede und Katzenbildern, in Jaume-Palasí/Pohle/Spielkamp (Hrsg.), Digitalpolitik. Eine Einführung (Berlin: ICANN, Wikimedia, iRights, 2017), 48-57; Kettemann, Menschenrechte im Multistakeholder-Zeitalter: Mehr Demokratie für das Internet, ZFMR 1, 2016, 24-36; sowie weitere im Einzelnen zitierte Texte. Teils wurden Textstellen übernommen und aktualisiert.

reflektierte Betrachtung der Digitalisierung [...] erfolgreich formuliert werden."[4] Gekoppelt mit der Erkenntnis, dass Technik und Technologie durch Normen formbar sind,[5] ermöglicht das dem Bundestag, in politische Prozesse einzutreten, an deren Ende konkrete, im Internet menschenrechtswahrende und politische Teilhabe im Digitalen fördernde Maßnahmen und Gesetze stehen. Diesen Prozess mit meinen Ausführungen zu unterlegen, ist Ziel dieser Stellungnahme.

2. Vorgelegte Fragen

Die vorgelegten Fragen decken wichtige Aspekte der Rolle der Menschenrechte und der Sicherstellung politischer Teilhabe im digitalen Zeitalter ab.

A. Bedrohung von Menschenrechten durch den Einsatz digitaler Kontroll- und Überwachungssysteme

1. Welche mittelfristigen und langfristigen Auswirkungen hat die dynamisch steigende Instrumentalisierung digitaler Technologien durch autoritäre Akteure für die praktische Durchsetzung der Menschenrechte national wie international, und welche Akteure können Menschenrechte dagegen in digitalen Räumen mit welchen Strategien verteidigen? (CDU/CSU)

2. Die kommunistische Führung Chinas versucht in enger Koordination von staatlichen und Partei-Strukturen sowie privaten und dennoch vom Staat abhängigen Unternehmen eine Totalüberwachung und Kontrolle der gesamten Bevölkerung in allen öffentlichen und privaten Bereichen durchzusetzen, insbesondere von ethnischen und religiösen Minderheiten. Welche Strategie nutzt die kommunistische Führung unter Xi Jinping nicht nur national, sondern auch regional und immer stärker global, um die neue Rolle Chinas als ökonomische und digitale Supermacht auch dafür einzusetzen, die universellen Menschenrechte im Sinne der autoritären Ideologie der KP Chinas umzudefinieren? (CDU/CSU)

3. Wie wirken die Werte Transparenz und Datenschutz im digitalen Zeitalter zusammen, und was sind Ihrer Ansicht nach die größten Bedrohungen für die Menschenrechte und die politische Beteiligung im digitalen Zeitalter, insbesondere in Hinblick auf Menschenrechtsverteidiger, Whistleblower und andere Gruppen, die moderne

[4] Berg, S., Rakowski, N. & Thiel, T. Die digitale Konstellation. Eine Positionsbestimmung, Zeitschrift für Politikwissenschaft (2020).

[5] Vgl. Kettemann, The Normative Order of the Internet (Oxford: OUP, 2020).

Informationstechnologien nicht nur nutzen, sondern mit deren Hilfe auch besonders drangsaliert werden? (DIE LINKE.)

4. Was kann Gesichtserkennung (Facial Recognition Technology), und welche Auswirkungen hat diese Form der Künstlichen Intelligenz auf den Schutz, die Respektierung und Gewährleistung von Menschenrechten im nationalen sowie internationalen Kontext? (BÜNDNIS 90/DIE GRÜNEN)

B. Digitale Optionen und Strategien für den Schutz von Menschenrechten

5. Können Sie konkrete Beispiele nennen, in denen das Darknet – genauer: die helle Seite des Darknets – Journalisten und Menschenrechtlern unter dem Schutz der Anonymität Austausch, Recherche und das Aufdecken von Missständen in Autokratien und Diktaturen erst ermöglicht, also Voraussetzung für jede regimekritische Tätigkeit ist, und wie bewerten Sie in diesem Zusammenhang den vom BMI geforderten Darknetparagraphen? (SPD)

6. In welchen Bereichen identifizieren Sie die größten Chancen und Herausforderungen digitaler Technologien in Bezug auf Gendergerechtigkeit, Frauenrechte und politische Teilhabe von Frauen? (FDP)

7. Wie können die Rechte von MenschenrechtsverteidigerInnen, AktivistInnen, JournalistInnen und politischen Oppositionellen weltweit in Zukunft besser im digitalen Raum geschützt werden? (FDP)

8. Wie können wir die politische Beteiligung im digitalen Zeitalter fördern und gleichzeitig Menschenrechte schützen, und welche neuen Möglichkeiten bieten digitale Technologien für den Schutz der Menschenrechte und die Stärkung politischer Beteiligung, ohne die am meisten benachteiligten Menschen zurückzulassen? (DIE LINKE.)

C. Soziale Medien und Meinungsfreiheit

9. Welche Bedeutung haben die Begriffe Hass und Hetze im Internet angesichts der mit [dem von der AfD nominierten Sachverständigen] erstrittenen Gerichtsurteile, also taugen sie als prozessverwertbare Vorwürfe? (AfD)

10. Manipulieren Plattformen wie Google, Facebook und Twitter in Deutschland das politische Klima ebenso, wie es Whistleblower in den USA („unconscious bias“, wie beschrieben von Dr. Robert Epstein) aufdecken konnten? (AfD)

D. Regulierung des internationalen Handels mit digitalen Technologien

11. Autokratien und Diktaturen nutzen u. a. aus europäischen Ländern stammende Überwachungssoftware, um Journalisten, Bürgerrechtler, Menschenrechtsverteidiger u. a. zu „durchleuchten“ und zu überwachen – oft mit gravierenden persönlichen Folgen für die Betroffenen. Bedarf es hier weiterer Vorgaben für den Export von Überwachungssoftware? (SPD)

12. Welche Notwendigkeit einer Regulierung von Gesichtserkennung bei ihrer (Weiter-)Entwicklung, Anwendung und Exportkontrolle sehen Sie, und wie könnte eine solche Regulierung auf nationalstaatlicher, supranationaler und internationaler Ebene oder unter Akteuren der Privatwirtschaft aussehen? (BÜNDNIS 90/DIE GRÜNEN)

3. Zusammenfassung und Empfehlungen

2020 ist für Deutschland ein Jahr, in dem es international effektiv für den Schutz der Menschenrechte und der politischen Teilhabe im digitalen Zeitalter eintreten kann. In diesem Jahr ist Deutschland Mitglied sowohl im Menschenrechtsrat als auch im Sicherheitsrat der Vereinten Nationen und damit in zwei bedeutenden Gremien des Menschenrechtsschutzes (Menschenrechtsrat) und der multilateralen Ordnung und internationalen Zusammenarbeit (Sicherheitsrat).

Es erscheint wünschenswert, dass Deutschland im Menschenrechtsrat der Vereinten Nationen und im Sicherheitsrat weiterhin für die Universalität, Unteilbarkeit und Interdependenz der Menschenrechte eintritt und Versuchen anderer Staaten, die Fundamente des Multilateralismus und des globalen Menschenrechtsschutzes zu untergraben, bewusst entgegentritt – grundsätzlich und unter besonderer Berücksichtigung des Schutzes der Menschenrechte und der Verwirklichung politischer Teilhabe im und durch das Internet in enger Zusammenarbeit mit anderen Staaten und nichtstaatlichen Stakeholdern in Anerkennung der Multistakeholderstruktur der Internet Governance.

Als „Co-Champion“ für zwei Empfehlungen des Berichts des High-Level Panel des UNO-Generalsekretärs über digitale Kooperation steht Deutschland in der Verantwortung, Optionen für eine menschenzentrierte und politische Teilhabe fördernde Reform der digitalen

Kooperationsarchitektur vorzulegen. Fußen muss der Prozess auf der schon vor fast zwanzig Jahren erzielten Einigung der Staatengemeinschaft auf das Ziel des Aufbaus einer menschenzentrierten, entwicklungsorientierten Informationsgesellschaft unter Berücksichtigung der Ziele und Grundsätze der Charta der Vereinten Nationen und der Achtung des Völkerrechts und der Menschenrechte.

Bemerkenswert sind die von zwei Ministerien im Kontext der Reform der globalen digitalen Kooperationsarchitektur aktuell durchgeführten Multistakeholderbefragungen und globale Bürger*innendialoge als Mittel der Hebung deliberativer Demokratiepotenziale. Diese können ein Modell für eine Verstärkung der deliberativen Dimension demokratischer Entscheidungsfindungsprozesse werden und Teilhabemöglichkeiten aller Stakeholder an der Entwicklung neuer Normen und Institutionen mit Internetbezug befördern.

Darüber hinaus hat Deutschland im Rahmen der EU-Ratspräsidentschaft (Juli-Dezember 2020) die Möglichkeit, auf europäischer Ebene für menschenrechtsbasierte und technologiesensible Politiken hinzuwirken und in der europäischen Außenpolitik die Werte europäischer Digitalpolitik zu verfechten. Insbesondere die digitale Außenpolitik in Hinblick auf Afrika sollte getragen sein von einem bewussten Eintreten für die Bedeutung des Menschenrechtsschutzes im Internet. Ein erster Schritt wäre etwa die Entwicklung von Modellgesetzen für den Einsatz von Überwachungstechnologien und die verstärkte Integration von digitalrechtlichen Gefährdungen in die Menschenrechtskonditionalitäten der Entwicklungszusammenarbeit.

Die Entwicklung des Internets beeinflusst privates und öffentliches Kommunikationsverhalten. Wie der Europäische Gerichtshof für Menschenrechte im Jahr 2015 feststellte, ist das Internet eines der wichtigsten Mittel geworden, mit dem wir unsere Rechte ausüben, insbesondere die Informations- und Meinungsäußerungsfreiheit. Das Internet stellt unverzichtbare Instrumente zur Teilhabe an Aktivitäten und Diskussionen von politischen Themen und Angelegenheiten allgemeinen Interesses zur Verfügung.

Alle Menschenrechte, die offline gelten, gelten online. Voraussetzung für die Ausübung der Menschenrechte im Internet sind der Zugang zum Internet (der durch staatliche Infrastrukturmaßnahmen sicherzustellen ist) und der Zugang zu Internet-Inhalten (der vor überschießender Zensur zu schützen ist).

Während in manchen Staaten bereits ein Recht auf Internetzugang gesetzlich festgeschrieben ist oder sich aus dem Recht dogmatisch ableiten lässt, ist eine explizite Kodifizierung weder national noch international Voraussetzung für das Bestehen des Rechts. Für den deutschen Rechtsraum lässt sich ein Recht auf Zugang dogmatisch als objektiv-rechtliche Grundrechtswirkung sowohl als eigenständiges Recht, umfasst vom Grundrecht auf Gewähr-

leistung eines menschenwürdigen Existenzminimums (Art 1 Abs 1 iVm Art 20 Abs 1 GG), aber auch als rechtlich geschützte Vorbedingung der Ausübung anderer Rechte konstruieren. Angesichts der zentralen Rolle, die das Internet inzwischen einnimmt, entspricht diese Grundrechtswirkung einer positiven Leistungspflicht des Staates: ein unmittelbar verfassungsrechtlicher Leistungsanspruch auf Gewährleistung eines menschenwürdigen Existenzminimums, der auch die Sicherung der Möglichkeit zur Pflege zwischenmenschlicher Beziehungen und zu einem Mindestmaß an Teilhabe am gesellschaftlichen, kulturellen und politischen Leben umfasst. Um dieses Recht zu verwirklich ist eine flächendeckende Versorgung aller Menschen in Deutschland mit möglichst schnellem, stabilem Internet zu einem möglichst geringen Preis sinnvoll; in diesem Zusammenhang ist ernsthaft in Erwägung zu ziehen, welche gesellschaftlichen Potenziale eine Betrachtung von Internetzugang als Dienstleistung der Daseinsvorsorge hat.

Aktuell wird auf Grundlage der Internet-Universalitäts-Indikatoren der UNESCO ein Lagebild zum Internet in Deutschland erhoben. Dabei werden erstmals Daten zu allen wichtigen Kategorien der Internetnutzung in Deutschland zusammengestellt. Im Dezember 2020 wird ein Endbericht vorgelegt.

Ein *Zugang* zum Internet alleine reicht allerdings nicht aus, um Grund- und Menschenrechte in der Digitalität zu sichern. Das Recht auf *Internet*zugang umfasst auch den Schutz legaler Inhalte im Internet. Hier erfüllen sowohl der Staat als auch der Privatsektor eine wichtige Rolle. Die primäre Verantwortung für Achtung, Schutz und Gewährleistung der Grund- und Menschenrechte verbleibt bei den Staaten, insbesondere erstreckt sie sich auf staatliche Kernkompetenzen, wie etwa im Bereich der Strafrechtspflege, die nicht auf private Akteure übertragen werden kann. Bei der Aufteilung der Verantwortlichkeiten zwischen Staaten und Intermediären (Plattformen) kann die Empfehlung des Ministerkomitees des Europarates an die Mitgliedsstaaten über die Rollen und Verantwortlichkeiten von Internet-Intermediären (2018) in Betracht gezogen werden.

Im Lichte der Bedeutung des Internets für Staat, Wirtschaft und Gesellschaft ist Cyber-Sicherheit als Vorbedingungen eines funktionierenden und sicheren Internets zu einem Schutzgut im globalen Gemeinschaftsinteresse geworden. Cyber-Sicherheit ist umfassend zu verstehen als Bemühen aller Akteure um ein stabiles, sicheres, resilientes, funktionsfähiges, offenes und freies Internet. Cyber-Sicherheit umfasst innen- wie außenpolitische Dimensionen und spricht menschliche Sicherheit, nationale Sicherheit und internationale Sicherheit an.

Der Schutz des Privatlebens – auch im Internet – ist ein „gateway“ für die Meinungsäußerungsfreiheit. 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 die Realisierung der Menschenrechte online. Vor diesem Hintergrund erscheint ein Darknetparagrafen als problematisch. Sinnvoll erscheint vielmehr, die Entwicklung von Anonymisierungssoftware als Mittel der Kommunikation von Menschenrechtsverteidiger*innen zu fördern.

Positiven Beispielen zum Trotz (darunter die Stärkung von Hashtag-Bewegungen, die Möglichkeit für schnelle und globale Mobilisierungs- und Aufklärungskampagnen, die Destabilisierung von hegemonialen Wissenshierarchien und die Raumnahme von feministischen informierten antihegemonialen Narrativen), stärkt das Internet auch bestehende und tradierte Macht- und Ausgrenzungssysteme.

Die Qualifikation einer Äußerung als „Hassrede“ ist insofern ein „prozessverwertbarer Vorwurf“ im Sinne einer der vorgelegten Fragen, als er es sozialen Netzwerken ermöglicht, den Inhalt zu löschen (bzw. diese dazu sogar nach NetzDG verpflichtet sein können, wenn ein entsprechender Tatbestand erfüllt ist). Das Verbot und die Definition der „Hassrede“ im Gemeinschaftsstandard halten der rechtlichen Überprüfung als allgemeine Geschäftsbedingungen stand.

Während nicht empirisch belegbar ist, dass Plattformen das politische Klima „manipulieren“, ist mehr Forschung zum Einfluss von Plattformen und Suchmaschinen auf Meinungsbildungsprozesse in einer demokratischen Gesellschaft notwendig. Diese muss allerdings erkenntnisgeleitet, replizierbar und methodisch belastbar sein und einer Peer Review standhalten.

Die Prozesse der Exportkontrolle hinsichtlich Digitalwaffen und Überwachungssoftware scheinen optimierbar. Lange Genehmigungsdauern verleiten Unternehmen zu Umgehungsgeschäften. Jedenfalls sollte besonderes Augenmerk auf die Transparenz gelegt werden. Der UN-Sonderberichterstatter für Meinungsäußerungsfreiheit hat ein Moratorium für die Ausfuhr, den Verkauf, die Weitergabe, die Verwendung oder die Wartung privat entwickelter Überwachungsinstrumente vorgeschlagen.

4. Herausforderungen des Menschenrechtsschutzes „im digitalen Zeitalter“

Vor sechs Jahren kam ein unter Beteiligung des Auswärtigen Amts in Berlin organisierter Workshop zum „Völkerrecht des Netzes“ zu dem Schluss, dass sämtliche digitalpolitische Akteure 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.“[6]

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 dieser Stellungahme zeige, ist die kontinuierliche Weiterentwicklung eines responsiven und reflexiven Rechtsbestandes auf allen Ebenen notwendig, um eine menschenzentrierte und entwicklungsorientierte Informationsgesellschaft ebenso nachhaltig zu sichern wie den Internetzugang für alle.

Wie ist um das Internet weltweit bestellt?[7] 4,4 Milliarden Menschen haben Internetzugang. Das heißt aber auch: 3,3 Milliarden noch nicht. Marginalisierungen werden durch das Internet nicht nur überwunden, sondern zum Teil auch fortgeschrieben. Gerade die Vereinten Nationen haben schon früh erkannt, dass das Internet der menschlichen Entwicklung dienen muss. Im Rahmen des UN-Weltgipfels zur Informationsgesellschaft (WSIS) (2003, 2005) bekannten sich die Staaten der Welt zu einer „den Menschen in den Mittelpunkt stellenden, inklusiven und entwicklungsorientierten Informationsgesellschaft“. Diese ist gestützt auf die Ziele und Grundsätze der Charta der Vereinten Nationen, das Völkerrecht und den Multilateralismus sowie die „volle Achtung und Einhaltung der Allgemeinen Erklärung der Menschenrechte“.

Während inzwischen bei allen in der Politik angekommen sein sollte, dass der Klimawandel eine Gefahr für die Welt darstellt, ist die zentrale Infrastruktur des Internets formal noch großteils ungeschützt. Kein völkerrechtlicher Vertrag schützt den öffentlichen Kern des Internets. Dabei schlug schon 2017 die Global Commission for Stability in Cyberpace vor, universell geltende

[6] Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG), Workshop zu „Völkerrecht des Netzes", 8.9.2014, 7.

[7] Kettemann, Die normative Ordnung der Cyber-Sicherheit. Zum Potenzial von Cyber-Sicherheitsnormen, Normative Orders Working Paper 01/2019; Kettemann, Ein Internet für alle Menschen, Tagesspiegel Background Digitalisierung und KI, 5.6.2019, https://background.tagesspiegel.de/ein-internet-fuer-alle-menschen.

Normen zum Schutz der Stabilität und Integrität des Internets zu verabschieden: Staatliche und nicht-staatliche Akteure sollten keine Maßnahmen – selbst Gesetze – mehr setzen dürfen, die technische Essentialien des Internets (IP-Adressen, Router, Internetknotenpunkte, Unterseekabel) gefährden. 2018 haben sich in Paris 64 Staaten und fast 700 nicht-staatliche Akteure im „Paris Call" zu mehr Vertrauen und Sicherheit im Cyberspace bekannt. Auch der zunehmend erstarkende völkergewohnheitsrechtliche Schutz des Internets, besonders die Konkretisierung der Pflichten, die aus dem Kooperationsprinzip und dem Vorsorgeprinzip fließen, macht Hoffnung. So müssen Staaten etwa in Anwendung des Grundsatzes der guten Nachbarschaft (und des Nichteingriffsprinzips) dafür sorgen, dass ihr Territorium nicht missbraucht wird, um anderen Staaten Schäden zuzufügen. Dies bedeutet auch, dass sie dem Präventionsprinzip folgend Schutzmaßnahmen ergreifen müssen, die für mehr Stabilität und Sicherheit im Internet sorgen.

Das Internet alleine führt nicht zu mehr Demokratie, auch wenn Rechtstaatlichkeit und hohe Internetzugangsraten positiv korrelieren. Das Internet kann jedoch als effektives Mittel zur Erstarkung zivilgesellschaftlichen Engagements eingesetzt werden. Gleichzeitig müssen wir neben den Schutz individueller Freiheitsräume auch die gesellschaftlichen Voraussetzungen sozialen Zusammenhalts sichern, was angesichts der Privatisierung von Plattformen und der Destabilisierung von geteilten Informationsbeständen, Kommunikationspraktiken und Medien-portfolios eine große Herausforderung darstellt.

Freie Internetkommunikation ist so voraussetzungsreich wie entscheidend für eine offene, einer funktionierenden Demokratie vorausgesetzte Debatte. Neben dem Staat ist auch das Internet von Voraussetzungen abhängig, die es selbst nicht hervorbringen kann: Wir brauchen das Recht, gerade das Völkerrecht, um die technischen Grundvoraussetzungen des Internets abzusichern und zu stabilisieren und – auf die Online-Inhalte blickend – die Potenziale des Internets für die Menschen zu realisieren.

Während mache Staaten unter dem Deckmantel der „Sicherheit" das Internet autoritär umstrukturieren und Menschenrechtsverteidiger*innen virtuell und physisch bekämpfen, ist richtig (menschenzentriert) verstandene Cybersicherheit als zentrales Schlagwort der Internetpolitik eng verknüpft mit der Stabilität, Robustheit, Resilienz und Funktionalität des Internets. Cyber-Sicherheit kann bedroht werden durch Cyber-Kriminalität und Cyber-Terrorismus, aber auch durch mangelnde rechtliche und technische Kooperation zwischen Staaten und fehlende präventive Maßnahmen, wie die Entwicklung von Kriseninterventionszentren und -teams, sowie mangelhaft erprobte transnationale Krisen-kommunikationsstrukturen für Cyber-Vorfälle. Auch falsch ausgestattete oder unerfahrene Cybereinheiten sind als Instrumente der Landesverteidigung eher eine Gefahr mit Eskalationspotenzial als ein klarer Sicherheitsfaktor, besonders wenn ihre Kompetenzen im

Verhältnis zu polizeilichen und nachrichtendienstlichen Cybersicherheitsaktivitäten unklar sind und solange die Frage der Grenzen zwischen präventiver und reaktiver Cyberabwehr ungeklärt ist. Die Förderung und die Gewährleistung von Cybersicherheit sind Voraussetzung für den ruhigen Lauf nationaler volkswirtschaftlicher Prozesse und des internationalen Wirtschafts- und Finanzsystems, transnationaler Kommunikationsflüsse, für das Funktionieren von Energienetzen, die Leistungsfähigkeit nationaler, regionaler und internationaler Verteidigungsinfrastrukturen und schließlich Voraussetzung für die volle Realisierung aller Menschenrechte.

Zu oft wird (Cyber)Sicherheit als Gegenstück von (Internet)Freiheit konzipiert. Dieser Ansatz ist verfehlt. Gerade die Gewährleistung von Freiheit und Sicherheit zählt zu den Kernaufgaben des Staates – offline wie online. Auch wenn die Definitionen von Cybersicherheit auseinanderdriften, liegt diese im Gemeinschaftsinteresse aller Staaten. Dieses Gemeinschaftsinteresse ist mehr als die simple Summe aller Einzelinteressen; sie ist vielmehr ihre sich potenzierende Querschnittmenge.

Das Völkerrecht ist vollumfänglich auf das Internet anzuwenden und konturiert daher auch die Cybersicherheit. Vor allem das Völkergewohnheitsrecht und die Allgemeinen Rechtsprinzipien des Völkerrechts beschränken (und befähigen) nationale Internetpolitik. Insbesondere bestehen dem Völkergewohnheitsrecht entfließende Schutzpflichten eines die Cyber-Sicherheit beeinträchtigenden Staates gegenüber der internationalen Gemeinschaft, Gefahren für die Stabilität, Integrität und Funktionalität des Internets abzuwenden und den globalen, unbeschränkten, grenzübergreifenden Internetverkehr nicht negativ zu beeinflussen. Dem Vorsorgeprinzip (due diligence-Prinzip) sowie den Grundsätzen der guten Nachbarschaft sind neben Informations- und Kommunikationspflichten nach Vorfällen auch präventive Pflichten zu entnehmen.

5. Stellungnahme zu den vorgelegten Fragen

A. Bedrohung von Menschenrechten durch den Einsatz digitaler Kontroll- und Überwachungssysteme

Frage 1. a) Welche mittelfristigen und langfristigen Auswirkungen hat die dynamisch steigende Instrumentalisierung digitaler Technologien durch autoritäre Akteure für die praktische Durchsetzung der Menschenrechte national wie international? (CDU/CSU)

Diese Frage ist differenziert zu beantworten.[8] Während national keine *autoritären* Akteure digitale Technologien nutzen, sondern eher staatliche und nichtstaatliche Akteure Technologien auf (teils) menschenrechtsverletzende und zumindest -insensible Weise nutzen, lässt sich international zweifellos (und seit vielen Jahren) die steigende Nutzung digitaler Anwendungen für autoritäre Zwecke des Machterhalts feststellen.

Die steigende Nutzung digitaler Technologien in allen Lebensbereichen ist prägendes Moment der „Digitalisierung". Diese Stellungnahme fokussiert auch auf den Menschenrechtsschutz und die politische Teilhabe „im digitalen Zeitalter". Eingangs ist gleich festzuhalten, dass es zunehmend schwerfällt, zwischen „online" und „offline" zu unterscheiden. Zum Glück ist das auch müßig. Mireille Hildebrandt hat *onlife* als Begriff geprägt, um zu zeigen, dass unser Leben selbst dann, wenn wir nicht online sind, von digitalen Normativitäten, Strukturen, Produkten geprägt wird.[9] Autoritäre Regime werden nicht nur „im Internet" autoritär. Menschenrechtsverletzungen durch digitale Technologien gehen stets einher mit solchen offline. Regimekritische Blogger*innen werden nicht nur Opfer von staatlichen Onlinekampagnen, sondern auch verhaftet; die Mobilfunkkommunikation von Demonstrierenden wird unterbrochen, aber sie werden auch mit Wasserwerfern und Tränengas bekämpft und verhaftet.

Menschenrechtsschutz muss daher stets ganzheitlich begriffen werden. Es macht auch wenig Sinn, von einem „digitalen Zeitalter" zu sprechen. Die Digitalisierung, hier verstanden als die durch digitale Technologien beförderte Entwicklung von Menschen und Maschinen, hat in allen Bereichen der Lebenswirklichkeit Einflüsse gezeitigt. Technologien (und auch digitale Technologien) sind stets eingebettet in voraussetzungsreiche politische, soziökonomische und kulturelle Kontexte. Ihre Produktion und ihr Einsatz (Hardware, Software, Dienste, Anwendungen) und ihre praktische Nutzung sowie ihr Einfluss auf Individuum und Gesellschaft lassen sich eher im Begriff Digitalität[10] fassen. Diese wiederum ist charakterisiert unter anderem durch die starke Sammlung und Ökonomisierung von Daten, den zunehmenden Einsatz von automatisierten Entscheidungssystemen (unscharf unter dem Signum „AI" debattiert), die Flexibilisierung der Instrumente normativer Lenkung und das Hinzutreten neuer relevanter, unsere sozialen Interaktionen und die Verteilung von Gütern und Rechten in Gesellschaften beeinflussender Akteure. Diese – man denke an ein Unternehmen wie Clearview, das vorgibt, drei Millionen Bilder von Menschen unter Umgehung der Nutzungsbedingungen sozialer Netzwerke gesammelt zu haben – haben *autoritäre* Auswirkungen dergestalt, dass sie – ohne unter einem entsprechenden Rechtfertigungsdruck zu stehen – die Menschenrechte eines

[8] Dieser Abschnitt geht zurück auf: Kettemann, Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Stiftung, 2015).
[9] Mireille Hildebrandt, Smart Technologies and the End(s) of Law (Cheltenham: Edward Elgar, 2015).
[10] Felix Stalder, Kultur der Digitalität (Frankfurt am Main: Suhrkamp, 2016).

großen Teils der Weltbevölkerung zumindest berühren können. Wissen Sie, ob Ihr Bild von Clearview zum Trainieren seiner Künstlichen Intelligenzen verwendet wird? Wenn ja, würde Sie das stören? Welcher Akteur sollte etwas dagegen tun? Deutschland? Die USA als Sitzland des Unternehmens? Facebook, dessen Bilder verarbeitet wurden? Dieses Beispiel alleine zeigt eine Dimension der Komplexität des Menschenrechtsschutzes im Internet, noch ohne dass traditionell als autoritär bezeichnete Akteure involviert wären.

Entwicklung des Politikfelds Internet als antiautoritäres Projekt

Der heutige Stand der digitalen Durchdringung deutscher Politiken ist Ergebnis eines inzwischen mehrere Jahrzehnte andauernden Prozesses der Etablierung des Politikfelds Internet aufgrund dreier Entwicklungen: einer beständigen Politisierung internet-bezogener Themen, einer nachhaltigen Institutionalisierung in Staat (zB.: Verwaltung[11]), Wirtschaft und Zivilgesellschaft und der breiten Anerkennung, dass das Internet sich zu etwas „Schützenswertem“ entwickelt hat, für das es sich lohnt, sich politisch zu engagieren.[12] Diese drei Entwicklungslinien haben dazu geführt, dass Internet- (oder Digital)politik inzwischen von allen Ministerien betrieben wird, was – divide et impera – für die Beherrschung des Politikfeldes positiv ist. (Zugleich ist die Monopolisierung der Kontrolle über das Internet oder des Zugangs zum Internet, etwa durch Aufbau einer staatlichen Firewall oder durch direkte Kontrolle über die Telekommunikationsanbieter ein Zeichen für eine drohende autoritäre Gefährdung der Internetfreiheit).

Wir befinden uns mithin mitten in der Digitalität. In dieser Situation über Menschenrechte und politische Teilhabe zu sprechen, besonders auf Ebene der Politik, ist von besonderer Bedeutung. Die Menschen- und Grundrechte sind ihrem Wesen nach online wie offline dieselben,[13] doch unterscheidet sich der Schutzauftrag des Staates (und der gesetzgeberische Auftrag für den Bundestag) in privaten, hybriden und öffentlichen Räumen, die regulativ in unterschiedlichen Kräfteverhältnissen von Staaten, Unternehmen und User*innen geprägt sind.

Generell ist hier auch hervorzuheben, dass das Konzept der „digitalen Welt“ eine neue Lebensrealität jenseits des staatlichen Territoriums impliziert, in der Recht bzw. Menschenrechte nicht gälten – beides ist falsch. Der „Cyberspace“ ist keine rechtliche terra nullius.[14] Natürlich entstehen mit den neuen „Territorialitäten“[15] neue normative

[11] Hösl, Maximilian/Kniep, Ronja (2020): "Auf den Spuren eines Politikfeldes. Die Institutionalisierung von Internetpolitik in der Ministerialverwaltung", Berliner Journal für Soziologie (2020) (advanced online access).
[12] Pohle Julia/Hösl, Maximilian/Kniep, Ronja (2016): "Analysing Internet Policy as a Field of Struggle, Internet Policy Review - Journal on Internet Regulation, Vol. 5, No. 3, S. 1-21.
[13] Siehe dazu gleich 2.2.
[14] Stephan Hobe, Cyberspace – der virtuelle Raum, in: Isensee/Kirchof (Hrsg.), HStR XI, 2013, 3. Auflage, § 231.

Herausforderungen, aber die Normativität des Rechts wird nicht vor grundlegende neue Herausforderungen gestellt. Recht gilt online wie offline. Menschenrechte gelten online wie offline.[16]

Zur Geltung der Menschenrechte online wie offline (am Beispiel der Meinungsäußerungsfreiheit)[17]

Das größte Versprechen des Internets liegt in den neuen Formen und Foren freier Meinungsäußerung. Schon in den Abschlussdokumenten des Weltgipfels zur Informationsgesellschaft bekräftigten die Staaten ihr Bekenntnis zur Bedeutung der Meinungs(äußerungs)freiheit, die gemäß Artikel 19 der Allgemeinen Erklärung der Menschenrechte von 1948 die Freiheit beinhaltet, „Informationen und Ideen über alle Medien und ohne Grenzen zu suchen, zu empfangen und weiterzugeben".

Neben der AEMR schützt auch Art 19 Abs 2 des UN-Paktes über bürgerliche und politische Rechte (IPBPR) „das Recht [jedes Menschen] auf freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, ohne Rücksicht auf Staatsgrenzen Informationen und Gedankengut jeder Art in Wort, Schrift oder Druck, durch Kunstwerke oder andere Mittel eigener Wahl sich zu beschaffen, zu empfangen und weiterzugeben."

In der jüngsten Resolution von 2018 zu Menschenrechten im Internet (die seit 2012 regelmäßig verabschiedet werden) bekräftigte der Menschenrechtsrat unter Bezugnahme auf Artikel 19 der AEMR und IPBPR den gleichen Schutz der Rechte offline wie online: "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 [...].[18]

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

[15] Saskia Sassen, Territory, Authority, Rights. From Medieval to Global Assemblages (Princeton: Princeton University Press, 2006), 346: "[T]erritorialities […] entail specific political, operational, or subjective encasements, including some that might be formalized and some that might remain informal." Die Formalisierung dieser ‚Encasements' ist ein normativer Prozess. Vgl. auch instruktiv: Daniel Lambach, The Territorialization of Cyberspace, International Studies Review, viz022, https://doi.org/10.1093/isr/viz022.

[16] Siehe Kettemann, Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Stiftung, 2015), http://library.fes.de/pdf-files/akademie/12068.pdf.

[17] Dieser Abschnitt greift zurück auf Kettemann/Benedek, Freedom of expression online, in Mart Susi (Hrsg.), Human Rights, Digital Society and the Law. A Research Companion (London: Routledge, 2019), 58-74 und Kettemann/Mosene, Hassrede und Katzenbilder: Ausgewählte menschenrechtliche Aspekte der Governance von Meinungsäußerungen im Internet, Elisabeth Greif und Silvia Ulrich (Hrsg.), Hass im Netz – Grenzen digitaler Freiheit (Linz: Böhlau, 2019), 92-122.

[18] UN Human Rights Council Resolution 38/7, The promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/RES/38/7 vom 05.07.2018.

privacy."[19] 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."[20]

Der regionale Schutz der Meinungsfreiheit ist textlich ähnlich verankert. Art 10 Abs 1 der EMRK garantiert das Recht auf freie Meinungsäußerung. Dieses Recht umfasst die Freiheit, Meinungen zu äußern und Informationen und Ideen zu empfangen und weiterzugeben, ohne dass die Behörden eingreifen und ohne Rücksicht auf (Landes-)Grenzen. Besondere Beachtung sollte an dieser Stelle dem Hinweis auf die Eingriffe „durch die öffentliche Hand" geschenkt werden: Die Staaten sind dazu verpflichtet, die Meinungsfreiheit sowohl als alleinstehendes Recht als auch als wesentliches „enabling right" (also als wesentliche Grundlage) für andere Rechte *im* Internet zu schützen. Wie der ehemalige UN-Sonderberichterstatter für Meinungsfreiheit *Frank La Rue* schrieb, "by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realisation of a range of other human rights".[21]

Dieses klare Bekenntnis zur technologischen Neutralität des Menschenrechtsschutzes, das schon der AEMR zugrunde gelegt ist, wurde vom Europäischen Gerichtshof für Menschenrechte in seiner *Yildirim*-Entscheidung nachvollzogen.[22] 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.[23] Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte hilft zu verstehen, wie die in der EMRK verankerte Meinungsfreiheit als indirekter Schutz der Integrität des Internets angesehen werden kann (als "modern means of imparting information"[24]). Aufgrund der Reichweite des Internets ist jedoch besondere Vorsicht geboten, da das Internet auch sozial korrosiv wirkende Kommunikationsinhalte (laut-)verstärkt. Besonders Faktoren wie Einfluss einer Meinungsäußerung, Zugang, Dauer und Asynchronizität der Informationen sind Teile der

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

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

[21] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/17/27 vom 16.05.2011, Abs 22 und 23.

[22] 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.

[23] 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.

[24] EGMR, Research Division (2015), Internet: case-law of the European Court of Human Rights, June 2015.

‚Spezifizität' von internetbezogenen Äußerungen online. Dementsprechend stellte der EGMR fest, dass die Wirkung von Informationen vervielfacht wird[25] und auch die Privatsphäre besonders gefährdet werden kann.[26]

Zur Garantie des Rechts auf Internetzugang (als Grund- und Menschenrechte) als Abwehr gegen autoritäre Instrumentalisierung des Internets und als Vorbedingung politischer Teilhabe

Im privaten und öffentlichen Umgang mit der Corona-Krise hat sich zumindest eine Einsicht abgeklärt: Die Bedeutung digitaler Technologien und eines funktionierenden Internetzugangs über verlässliche Endgeräte bei einem ausreichend großen und leistbaren Datenvolumens für ein funktionierendes Miteinander ist groß. Schon 2015 habe ich argumentiert,[27] dass sich aus Völker-, Europa- und Staatsrecht ein grund- wie menschenrechtlicher, verfassungsrechtlich abgesicherter Leistungsanspruch auf Internetzugang ableiten lässt. Die Corona-Krise hat die Konturen dieses Anspruchs noch einmal geschärft.

Ohne Zugang zum Internet und zu Internetinhalten können Menschen nicht am Möglichkeitsraum des Internets teilnehmen. Wer seine Menschenrechte und die Meinungsäußerungsfreiheit auch online ausüben möchte, benötigt Zugang zum Internet, das als technische Einrichtung selbst eine katalysierende Funktion für die Ausübung der Menschenrechte hat.

Es lässt sich mit guten Gründen argumentieren, dass ein Recht auf Internetzugang im Völkerrecht besteht. Artikel 19 Absatz 2 des Zivilpaktes kann in diesem Sinne ausgelegt werden. Er schützt die Verbindungstechnologien, indem er Meinungsäußerung durch „Mittel eigener Wahl" absichert. Der Menschenrechtsausschuss bestätigt in seiner Kommentierung zwar die abwehrrechtliche Dimension[28] des Artikels, zeigt aber auch gegenüber einer Leistungsdimension offen: „Staaten sollten alle notwendigen Schritten unternehmen, um die Unabhängigkeit dieser neuen Medien zu fördern und den individuellen Zugang zu gewährleisten".[29]

Das Völkerrecht schützt den Zugang zum Internet als Menschenrecht. Die abwehrrechtliche Dimension des Zugangs zu Internet-Inhalten wirft wenig elementare Fragen auf. Schwieriger ist es, die positivrechtliche Dimension des Zugangs im Bereich der Infrastruktur auszubuch-

[25] EGMR 13.01.2011, No 16354/06, Mouvement Raëlien Suisse vs Switzerland, Abs 54.
[26] EGMR 05.05.2011, No 33014/05, Editorial Board of Pravoye Delo and Shteckel vs Ukraine, Abs 63.
[27] Dieser Abschnitt beruht auf Veröffentlichungen des Verfassers, die auf iRights.info erschienen sind. Eine längere Fassung ist in drei Teilen auf dem Völkerrechtsblog erschienen.
[28] Human Rights Committee, General Comment Nr. 34, http://www.humanrights.ch/upload/pdf/111201_CCPR-C-GC-34.pdf.
[29] Ibid., Abs. 15.

stabieren. Dennoch kann im Lichte der herausragenden Bedeutung des Internets für die Realisierung aller Menschenrechte der physische Zugang zum Internet nur als völkerrechtlich geschützt gedeutet werden: ohne Zugang keine Meinungsäußerung bei freier Wahl des Kommunikationsmediums. Ein Recht auf Internetzugang ist demnach Vorbedingung der Realisierung aller anderen Menschenrechte über das Internet. Es setzt jedoch zumindest eine grundlegende staatlich garantierte Kommunikationsinfrastruktur voraus. Nationales Verfassungsrecht, Völkerrecht und auch Europarecht spielen hier ineinander.

Im Fall *Yıldırım v. Türkei* bestätigte der Europäische Menschenrechtsgerichtshof, dass ein Recht auf Internetzugang dem Recht auf Zugang zu Informationen und Kommunikation, das durch nationale Verfassungen geschützt wird, eingeschrieben ist.[30] Darüber hinaus ist ein Recht auf Internetzugang in einigen Staaten explizit festgeschrieben oder lässt sich dogmatisch ableiten.

Die völkerrechtlichen und europarechtlichen Verpflichtungen stecken den Rahmen ab, innerhalb dessen auch Deutschland die Sicherung des Internetzugangs garantierten muss. Das Grundgesetz schützt zwar primär subjektive Rechte, aber diesen sind grundrechtsdogmatisch entwickelte Gewährleistungspflichten eingeschrieben: objektiv-rechtliche Aufträge also, eine Infrastruktur als Vorbedingung zur Ausübung der Kommunikationsrechte zur Verfügung zu stellen. Dem Status der Grundrechte als Abwehrrechte – es besteht ein Recht auf „unbehinderten" Zugang, wie im Fall *Yıldırım* – kann also ein Anspruch auf Gewährleistung eines Zugangs zur Seite gestellt werden.

Die völkerrechtlichen (und europarechtlichen) Verpflichtungen stecken den Rahmen ab, innerhalb dessen Deutschland die Sicherung des Internetzugangs garantierten muss. Verantwortliche Staatsorgane sind aufgerufen, nicht nur passiv auf Entwicklungen des Völkerrechts zu warten und diese dann zu rezipieren, sondern aktiv an deren Bewältigung mitzuwirken.[31] Das bestätigt auch das Bundesverfassungsgericht: „Dem Gesetzgeber steht ein Gestaltungsspielraum zu […]; [dabei] ist er auch durch völkerrechtliche Verpflichtungen gebunden."[32] Was dem Völkerrecht über Internetzugang zu entnehmen ist, ist also relevant für die staatsrechtliche Ausgestaltung des Rechts auf Internet.

Das Grundgesetz schützt primär subjektive Rechte, aber diesen sind grundrechtsdogmatisch entwickelte Gewährleistungspflichten eingeschrieben: objektiv-rechtliche Aufträge also, eine Infrastruktur als Vorbedingung zur Ausübung der Kommunikationsrechte zur Verfügung zu stellen. Dem *status negativus* der Grundrechte – es besteht ein Recht auf „unbehinderten" Zugang, wie im Fall *Yıldırım* – kann also ein Anspruch auf Gewährleistung eines Zugangs zur Seite

[30] EGMR, Yıldırım v. Türkei.
[31] Tomuschat in HStR XI, 2013[3], § 226 Rz 4.
[32] BVerfG, 1 BvL 10/12 vom 23.7.2014, Rn. 74; aber auch schon in 1 BvL 10/10, 1 BvL 2/11 vom 18.7.2012, Rn. 94.

gestellt werden. Konturen dieser Gewährleistungsgarantie lassen sich aber aus mehreren Entscheidungen Karlsruhes ableiten, die zusammengelesen werden können.

Das Bundesverfassungsgericht hat 2008 geurteilt, dass das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einschließt.[33] Der Fokus lag zunächst auf dem *status negativus* der Grundrechtswirkung: „Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet."[34] Der Staat muss „achten", darf also nicht ungerechtfertigt eingreifen: die Achtung von Grundrechten ist dem *status negativus* klassisch eingeschrieben. Aber im Urteil geht es um mehr – eben um die *Gewährleistung* der Vertraulichkeit und Integrität informationstechnischer Systeme. Der Einzelne ist zu seiner Persönlichkeitsentfaltung angewiesen auf die Nutzung informationstechnischer Systeme.[35] Er hat ein Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit solcher Systeme, wenn im Gesetz Eingriffsermächtigungen bestehen, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten".[36] Das muss der Staat *gewährleisten.* Entsprechende Gesetze müssen unter anderem den Geboten der Normenklarheit und Normenbestimmtheit und dem Grundsatz der Verhältnismäßigkeit genügen.

Diese Gewährleistung muss lückenlos sein. Daher entwickelte das BVerfG auch das *neue* Grundrecht: „Einer solchen lückenschließenden Gewährleistung bedarf es insbesondere, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann."[37] Wie permanent der Wandel ist, lässt sich zum jetzigen Zeitpunkt nicht abschätzen. Aber die Schneisen, die die Corona-Krise im Wald der sozial-kommunikationen Gewissheiten hinterlassen wird, werden jeden Tag klarer. Mit der Technologie muss sich auch die Interpretation von Normen wandeln. Wie schon das Bundesverfassungsgericht 2008 mit leicht anderer Terminologie („zentrale Bedeutung" der Informationstechnik für die „Lebensführung" vieler Bürger*innen[38]) hat der Bundesgerichtshof 2013 bestätigt, wie wichtig das Internet ist: Der „überwiegende Teil der Einwohner

[33] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07.
[34] Ibid., Rn 181.
[35] Ibid., Rn. 200.
[36] Ibid., Rn. 203.
[37] Ibid., Rn. 169.
[38] Ibid., Rn 171.

Deutschlands“ bediene sich täglich des Internets. Das Internet ist ein für die Lebensgestaltung prägendes Medium, dessen „Ausfall sich signifikant im Alltag bemerkbar macht“.[39]

Ein Recht auf Zugang lässt sich dogmatisch 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), als auch als rechtlich geschützte Vorbedingung der Ausübung anderer Rechte konstruieren (dies umfasst auch den Systemschutz[40]). Dies zeigt sich besonders eindrücklich während der jetzigen Krise. Wieviele Aspekte unseres Lebens sind nun mediatisiert: Schule und Ausbildung, Beruf und Konferenzteilnahme, Gesundheitskommunikation und Staat-Bürger*inneninteraktion?

Angesichts der zentralen Rolle, die das Internet inzwischen einnimmt, entspricht diese Grundrechtswirkung einer positiven Leistungspflicht des Staates: ein unmittelbar verfassungsrechtlicher Leistungsanspruch auf Gewährleistung eines menschenwürdigen Existenzminimums aus Art. 1 Abs. 1 GG in Verbindung mit dem Sozialstaatsprinzip des Art. 20 Abs. 1 GG. Das Existenzminimum, so das BVerfG im *Hartz IV*-Urteil, umfasst die „Sicherung der Möglichkeit zur Pflege zwischenmenschlicher Beziehungen und zu einem Mindestmaß an Teilhabe am gesellschaftlichen, kulturellen und politischen Leben“[41]. Wie Karlsruhe so schön schreibt: „Die verfassungsrechtliche Gewährleistung eines menschenwürdigen Existenzminimums muss durch ein Parlamentsgesetz erfolgen, das einen konkreten Leistungsanspruch des Bürgers gegenüber dem zuständigen Leistungsträger enthält.“[42] 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.“[43] Erst 2014 führte Karlsruhe dann erneut aus, dass das Grundrecht auf ein menschenwürdiges Existenzminimum der „Konkretisierung und stetigen Aktualisierung durch den Gesetzgeber“ bedarf.[44]

Diese müsse orientiert sein „an dem jeweiligen Entwicklungsstand des Gemeinwesens und den bestehenden Lebensbedingungen im Hinblick auf die konkreten Bedarfe der Betroffenen“[45]. Und wer könnte leugnen, dass die Kommunikationsbedürfnisse zu den Bedingungen der

[39] BGH, Urteil des III. Zivilsenats vom 24.1.2013 - III ZR 98/12.
[40] Hoffmann-Riem, JZ 2/2014, 53.
[41] BVerfG, Urteil des Ersten Senats vom 09. Februar 2010, 1 BvL 1/09, Rn 135.
[42] Ibid., Rn. 136.
[43] Ibid., Rn. 138.
[44] BVerfG, Beschluss des Ersten Senats vom 23. Juli 2014, 1 BvL 10/12.
[45] Ibid., Rn. 74.

Informationsgesellschaft nur mittels des Internets erfüllt werden können? Es besteht also ein individuelles Recht auf Internetzugang, um am kommunikativen Leben teilhaben zu können, das mittels konkretem Leistungsanspruch durchgesetzt werden kann.

Den in *Hartz IV* gewählten Ansatz bestätigte das Bundesverfassungsgericht ganz konkret in Hinblick auf Leistungen für Asylbewerber*innen 2012 in einer Entscheidung zum Asylbewerberleistungsgesetz: Auch Aslybewerber*innen haben ein Recht auf ein menschenwürdiges Existenzminimum, das Artikel 1 Absatz 1 GG „als Menschenrecht" (zweiter Leitsatz) begründet.[46] Mit identischen Worten wie in *Hartz IV* bestätigt Karlsruhe, dass das Existenzminimum die „Sicherung der Möglichkeit zur Pflege zwischenmenschlicher Beziehungen" umfasse und zu einem „Mindestmaß an Teilhabe am gesellschaftlichen, kulturellen und politischen Leben" befähigen müsse, denn „der Mensch als Person existiert notwendig in sozialen Bezügen" – der *Mensch*, nicht nur der Staatsbürger. Wiederum bestätigt das Bundesverfassungsgericht, dass dieser objektiven Verpflichtung aus Art. 1 Abs. 1 GG ein individueller unmittelbarer verfassungsrechtlicher Leistungsanspruch entspricht, der – wieder – von den „jeweiligen wirtschaftlichen und technischen Gegebenheiten" abhänge.

Hauptverantwortung des Staates für die Menschenrechte

Die Staaten haben die Hauptverantwortung, die Grund- und Menschenrechte im digitalen Umfeld zu schützen. Alle von ihnen eingeführten Regulierungsrahmen, einschließlich Selbst- oder Ko-Regulierungsansätze, müssen wirksame Aufsichtsmechanismen enthalten und mit geeigneten Möglichkeiten zur Rechtsdurchsetzung einhergehen. Staaten haben nicht nur die negative Verpflichtung, das Recht auf freie Meinungsäußerung und andere Menschenrechte im digitalen Umfeld nicht zu verletzen, sondern auch eine positive Verpflichtung, die Menschenrechte zu achten, zu schützen und zu gewährleisten – und ein regulatives Umfeld für alle zu schaffen, um diese Rechte auch auszuüben.

In Anbetracht der Drittwirkung der Grundrechte schließt diese positive Verpflichtung – funktional gradiert – den Schutz von Einzelpersonen vor den Handlungen privater Parteien ein, besonders wenn sich die zwei Vertragsparteien nicht auf Augenhöhe begegnen (können). Staaten müssen sicherstellen, dass Unternehmen rechtlich und in der Praxis alle einschlägigen gesetzlichen und regulatorischen Rahmenbedingungen einhalten. Dabei müssen Staaten insbesondere die Bedeutung von Medien-, Steuer-, Kartell- und Datenschutzrecht erwägen, um ggf. mächtigen privaten Internetakteuren besondere Verpflichtungen aufzuerlegen.

Dem Privatsektor kommt eine besondere Rolle bei der Realisierung der Menschenrechte im Internet zu. Die weitaus meisten kommunikativen Räume im Internet befinden sich in privater

[46] Ibid.

Hand. Intermediäre, einschließlich Social-Media-Unternehmen, sind zu wichtigen normativen Akteuren geworden. Netzwerkeffekte und Fusionen haben dazu geführt, dass eine relativ kleine Anzahl wichtiger Intermediäre den Markt dominiert. Diese Unternehmen haben Pflichten nach internationalem und nationalem Recht. Im Einklang mit den UN-Leitprinzipien für Wirtschaft und Menschenrechte und dem Rahmen „Schutz, Achtung und Abhilfe" („Ruggie-Prinzipien")[47] sollen Intermediäre die Menschenrechte ihrer Nutzer*innen (und anderer Betroffener) bei allen ihren Handlungen (einschließlich der Formulierung und Anwendung von Nutzungsbedingungen) respektieren und Abhilfe schaffen im Falle von negativen Auswirkungen auf die Menschenrechte, die in direktem Zusammenhang mit ihren wirtschaftlichen Tätigkeiten stehen.

Wie ich in meiner Stellungnahme als Sachverständiger für die öffentliche Anhörung zum Netzwerkdurchsetzungsgesetz am 15. Mai 2019 ausgeführt habe,[48] ist für das Austarieren des Verhältnisses von Staaten und Intermediären (Plattformen) von zentraler Bedeutung namentlich die von Deutschland verabschiedete Empfehlung CM/Rec(2018)2 des Ministerkomitees des Europarates an Mitgliedstaaten zu der Rolle und Verantwortung von Internet-Intermediären.[49]

> (in Bezug auf Staaten)
>
> 1.3.7. States should ensure, in law and in practice, that intermediaries are not held liable for third-party content which they merely give access to or which they transmit or store. State authorities may hold intermediaries co-responsible with respect to content that they store if they do not act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature, including through notice-based procedures. **State authorities should ensure that notice-based procedures are not designed in a manner that incentivises the take-down of legal content, for example due to inappropriately short timeframes.** Notices should contain sufficient information for intermediaries to take appropriate measures. Notices submitted by States should be based on their own assessment of the illegality of the notified content, in accordance with international standards. Content restrictions should provide for notice of such restriction being given to the content producer/issuer as early as possible, unless this interferes with ongoing law-enforcement activities. Information should also be made available to users seeking access to the content, in accordance with applicable data protection laws.

[47] Siehe 'Ruggie Principles': 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, UN Doc A/HRC/17/31 vom 21.03.2011 (deutsche Fassung).

[48] Kettemann, „Stellungnahme als Sachverständiger für die öffentliche Anhörung zum Netzwerkdurchsetzungsgesetz auf Einladung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestags" in Schulz/Kettemann/Heldt (Hrsg.), Probleme und Potenziale des NetzDG – ein Reader mit fünf HBI-Expertisen / Problems and Potentials of the NetzDG – a Reader with five HBI Expert Opinions (Hamburg: Verlag Hans-Bredow-Institut, November 2019 (Arbeitspapiere des HBI Nr. 48).

[49] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries.

1.2.1. Any legislation applicable to internet intermediaries and to their relations with States and users should be accessible and foreseeable. **All laws should be clear and sufficiently precise to enable intermediaries, users and affected parties to regulate their conduct.** The laws should create a safe and enabling online environment for private communications and public debate and should comply with relevant international standards.

1.3.2. **State authorities should obtain an order by a judicial authority or other independent administrative authority, whose decisions are subject to judicial review, when demanding intermediaries to restrict access to content.** This does not apply in cases concerning content that is illegal irrespective of context, such as content involving child sexual abuse material, or in cases where expedited measures are required in accordance with the conditions prescribed in Article 10 of the Convention.

1.1.2. **Laws**, regulations and policies **applicable to internet intermediaries**, regardless of their objective or scope of application, including commercial and non-commercial activities, **should effectively safeguard human rights and fundamental freedoms, as enshrined in the European Convention on Human Rights, and should maintain adequate guarantees against arbitrary application in practice**.

1.1.3. **States have the ultimate obligation to protect human rights and fundamental freedoms in the digital environment.** All regulatory frameworks, including self- or co-regulatory approaches, should include **effective oversight mechanisms** to comply with that obligation and be accompanied by appropriate redress opportunities.

1.1.4. The process of enacting legislation or regulations applicable to internet intermediaries should be transparent and inclusive. **States should regularly consult with all relevant stakeholders** with a view to ensuring that an appropriate balance is struck between the public interest, the interests of the users and affected parties, and the interests of the intermediary. **Before adopting legislation or regulations, States should conduct human rights impact assessments** to understand and prevent or mitigate any potential negative impact on human rights.

(in Bezug auf Unternehmen)

2.1.2. **The responsibility of intermediaries to respect human rights and to employ adequate measures applies regardless of their size, sector, operational context, ownership structure or nature.** The scale and complexity of the means through which intermediaries meet their responsibilities may vary, however, taking into account the severity of impact on human rights that their services may have. **The greater the impact and the potential damage to the objects of legal protection and the higher the value of the services for the exercise of human rights, the greater the precautions that the intermediary should employ** when developing and applying

their terms and conditions of service, community standards and codes of ethics aiming, notably, to prevent the spread of abusive language and imagery, of hatred and of incitement to violence.

2.2.1. Internet intermediaries should ensure that **all terms of service agreements** and policies specifying the rights of users and all other standards and practices for content moderation and the processing and disclosure of user data **are publicly available in clear, plain language and accessible formats**. [...]

2.3.3. Any **restriction of content** should be **limited in scope to the precise remit of the order or request and should be accompanied by information to the public, explaining which content has been restricted and on what legal basis**. Notice should also be given to the user and other affected parties, unless this interferes with ongoing law-enforcement activities, including information on procedural safeguards, opportunities for adversarial procedures for both parties as appropriate and available redress mechanisms.

2.3.4. All members of staff of intermediaries who are engaged in content moderation should be given **adequate initial and ongoing training on the applicable laws and international human rights standards, their relationship with the intermediaries' terms of service and their internal standards, as well as on the action to be taken in case of conflict**. Such training may be provided internally or externally, including through associations of intermediaries, and its scope should correspond to the importance of the intermediaries' role and the impact that their actions may have on the ability of users to exercise their freedom of expression. Staff should also be provided with appropriate working conditions. This includes the allocation of sufficient time for assessing content and opportunities to seek professional support and qualified legal advice where necessary.

2.3.5. Automated means of content identification are useful to prevent the reappearance of specific items of previously restricted content. Due to the current limited ability of automated means to assess context, intermediaries should carefully assess the human rights impact of automated content management and should ensure human review where appropriate. They should take into account the risk of an overrestrictive or too lenient approach resulting from inexact algorithmic systems, and the effect these algorithms may have on the services that they provide for public debate. Restrictions of access to identical content should not prevent the legitimate use of such content in other contexts. [...]

2.5. Access to an effective remedy

2.5.1. **Internet intermediaries should make available – online and offline – effective remedies and dispute resolution systems that provide prompt and direct redress in cases of user, content provider and affected party grievances**. While the complaint mechanisms and their procedural implementation may vary with the size, impact and role of the internet intermediary, all remedies should allow for an impartial and independent review of the alleged violation. These

should – depending on the violation in question – result in inquiry, explanation, reply, correction, apology, deletion, reconnection or compensation.

2.5.2. **Complaint mechanisms, including notice-based procedures, should comply with applicable procedural safeguards and should be accessible, equitable, compatible with rights, transparent and affordable**. They should also include built-in safeguards to avoid conflicts of interest when the company is directly administering the mechanism, for example, by involving oversight structures. Complaints should be handled without unwarranted delays and the relevant mechanisms should not negatively impact the opportunities for complainants to seek recourse through independent national, including judicial, review mechanisms.

2.5.3. Intermediaries should ensure that all users and other parties affected by their actions have full and easy access to transparent information in clear and easily understandable language about applicable complaint mechanisms, the various stages of the procedure, indicative time frames and expected outcomes.

[...]

2.5.5. Intermediaries should seek to provide access to alternative review mechanisms that can facilitate the resolution of disputes that may arise between users. Intermediaries should not, however, make alternative dispute mechanisms obligatory as the only means of dispute resolution.

2.5.6. **Intermediaries should engage in dialogue with consumer associations, human rights advocates and other organisations representing the interests of users and affected parties, as well as with data protection and other independent administrative or regulatory authorities, to ensure that their complaint mechanisms are designed, implemented, evaluated and improved through participatory processes**. They should also regularly analyse the frequency, patterns and causes of complaints received in order to learn lessons to improve their policies, procedures and practices and prevent future grievances.

Politische Teilhabe im „digitalen Zeitalter“[50]

Ein wichtiger Aspekt der politischen Teilhabe im digitalen Zeitalter ist nicht nur die Beteiligung an nationalen Prozessen zur Gestaltung des Internets, sondern auch die Reform globaler Prozesse der Internet Governance.[51] 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,

[50] Dieser Abschnitt ist mit kleineren Aktualisierungen entnommen Kettemann, Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Stiftung, 2015).
[51] Kettemann, Internet Governance, in Jahnel et al. (Hrsg.), Internetrecht, 4. Auflage (Wien: Springer, 2020), 47-73.

Regeln, Entscheidungsfindungsprozessen und Programmen, die die Weiterentwicklung und Verwendung des Internets gestalten".[52] Die Bedeutung der Teilhabe aller Stakeholdergruppen (Staaten, Privatsektor, Zivilgesellschaft) wird schon in der Definition deutlich.

Demokratie ist ein höchst umstrittener Begriff. Politisch oszilliert der Begriff zwischen „Lebensform"[53] und leerer Bekenntnisformel[54]. Völkerrechtlich ist inzwischen[55] allerdings weitgehend anerkannt, dass sie als „teleologisches Prinzip"[56] 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 dem gemeinsamen Artikel 1 Zivil- und Sozialpakt, Artikel 21 der Allgemeinen Erklärung der Menschenrechte sowie Artikel 25 des Zivilpaktes in seiner Auslegung und nachfolgender Praxis,[57] und den regionalen Verbriefungen (Artikel 10 Abs. 2 EMRK; Artikel 13, 15, 16 AMRK, Artikel 10, 11 AfrMRK) abgeleitet werden kann.[58]

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,

[52] Arbeitsgruppe über Internet Governance (WGIG), Bericht der Arbeitsgruppe (2005), Abs. 10.
[53] 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.
[54] Wendy Brown, We Are All Democrats Now, The Kettering Review (2011) 29, 44-52.
[55] 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).
[56] Niels Petersen, Demokratie als teleologisches Prinzip: Zur Legitimität von Staatsgewalt im Völkerrecht (Frankfurt am Main: Springer, 2009).
[57] 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.
[58] Thomas Franck, The Emerging Right to Democratic Governance, AJIL 1992, 46-91.

dessen Operationalisierung – 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. [59]

Der Multistakeholderprozess als inklusiver Ansatz der Internet Governance Policy-Gestaltung ist mit wenigen Ausnahmen (ordnungspolitische 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).[60] Die Regelungsergebnisse von Internet Governance-Prozessen sind aufgrund ihrer Legitimität auch im Großen und Ganzen effektiv, was wiederum ihre Legitimität befördert.

Recht auf Privatsphäre als Schutz vor autoritären Eingriffen[61]

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). 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).[62] Staaten müssen also nicht nur

[59] 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).

[60] 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).

[61] Dieser Abschnitt ist entnommen: Kettemann, Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Stiftung, 2015).

[62] Christoph Grabenwarter, Katharina Pabel, Europäische Menschenrechtskonvention, 5. Aufl. (München: Beck, 2012), 226 (mit weiteren Nachweisen).

von Eingriffen in die Privatsphäre Abstand nehmen, sondern auch gewährleisten, dass andere soziale Akteure (und andere Staaten) die Privatsphäre Einzelner nicht verletzen.[63]

Artikel 17 IPbpR in seiner Auslegung durch den Menschenrechtsausschuss hat eine ähnliche Wirkung. 1988 hat der Ausschuss festgehalten,[64] dass Überwachungsmaßnahmen („whether electronic or otherwise") von allen Arten von Kommunikationen mit den üblichen Ausnahmen verboten seien.[65] Staaten müssten einen Rechtsrahmen schaffen, um Eingriffe „by natural or legal persons" zu verbieten.[66] Rückblickend auf die Massenüberwachung durch die NSA ging es 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[67]), sondern vielmehr um die Umsetzung dieser Verpflichtungen in der Praxis.[68]

Auch der Menschenrechtsrat der Vereinten Nationen zeigte sich in seiner von Deutschland und Brasilien eingebrachten 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."[69]

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

---

[63] Siehe die exzellente Zusammenfassung bei Helmut Philipp Aust, Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014, 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages.

[64] Menschenrechtskomitee, Allgemeiner Kommentar No. 16 (1994), Abs. 21.

[65] Ibid., Abs. 8.

[66] Ibid., Abs. 9.

[67] 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.

[68] 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.

[69] Menschenrechtsrat, Resolution 28/16, The Right to Privacy in the Digital Age, A/HRC/RES/28/16 vom 1.4.2015.

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 .[70]

Der Schutz des Privatlebens – auch im Internet – ist ein „gateway" für die Meinungs-äußerungsfreiheit.[71] 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.[72]

Um den Schutz der Privatsphäre im Internet zu verstärken, müssen Staaten im Lichte dieser Ausführungen ihre nationalen Gesetze und Politiken auf Übereinstimmung mit ihren menschen-rechtlichen 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 Definition 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).

[70] Generalversammlung, The Right to Privacy in the Digital Age, Resolution 68/167, A/RES/68/167 vom 21.1.2014.
[71] 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.
[72] Ibid., Abs. 17.

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.[73] Ähnliche Forderungen stellt die Venedig-Kommission des Europarates auf.[74]

Im Mai 2020 hat das Bundesverfassungsgericht in einem wichtigen Urteil[75] zur rechtstaatlichen Kontrolle von Nachrichtendiensten festgehalten, dass sich der Schutz des Art. 10 Abs. 1 und des Art. 5 Abs. 1 Satz 2 GG als Abwehrrechte gegenüber einer Telekommunikationsüberwachung auch auf Ausländer*innen im Ausland erstreckt. Regelungen zur Kooperation mit ausländischen Nachrichtendiensten genügten grundrechtlichen Anforderungen nur dann, wenn sichergestellt sei, das „rechtsstaatliche Grenzen durch den gegenseitigen Austausch nicht überspielt werden und die Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen und ausgewerteten Daten im Kern gewahrt bleibt". Dies wird eine Überarbeitung der Regeln zur Ausland-Ausland-Telekommunikationsüberwachung mit sich ziehen und ist eine wichtige Wegmarke hin zur Geltung rechtstaatlicher Grundsätze auch bei der Durchführung von Überwachungsmaßnahmen und der Analyse von Telekommunikationsdaten über das Internet.

Internetabschaltungen als Mittel autoritärer Internetpolitik[76]

Die Beispiele Iran, China, Myanmar, Ägypten, Libyen, Syrien und zuletzt Indien haben gezeigt, dass repressive Regierungen (oder zumindest Regierungen, die in Teilen repressive und autoritäre Politiken verfolgen) Internet-(Teil)Abschaltungen als Mittel der Unterdrückung der Mobilisierung und Artikulation von Dissens nach innen und als Versuch der Unterbindung der Überwachung von außen verwenden. Internetabschaltungen werden regelmäßig gegen menschenrechtliche Mindestgarantien verstoßen. Der Schutz vor Internetabschaltungen wird durch die informations- und kommunikationsbezogenen Menschenrechte geleistet, die auf Art. 19 IPbürgR und den entsprechenden regionalen Menschenrechtsschutzsystemen fußen; der Schutz ist in seinem Kerngehalt gewohnheitsrechtlich abgesichert.

---

[73] Council of Europe Commissioner for Human Rights, Democratic and effective oversight of national security services (Mai 2015), Abs. 18.

[74] 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), Study No. 719/2013, CDL-AD(2015)006.

[75] BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17.

[76] Dieser Abschnitt geht zurück auf *Kettemann*, Grotius goes Google: Der Einfluss der Internet Governance auf das Völkergewohnheitsrecht, in *Vedder* (Hrsg.), Tagungsband 37. Österreichischer Völkerrechtstag 2012, 89-104, Wien 2013; und *Kettemann,* Nationale Sicherheit und Informationsfreiheit. Zur Völkerrechtmäßigkeit von Internetabschaltungen, in *Schmalenbach* (Hrsg.), Aktuelle Herausforderungen des Völkerrechts. Beiträge zum 36. Österreichischen Völkerrechtstag 2011, Peter Lang, Wien 2012, 41-62.

In menschenrechtlicher Hinsicht ist eine Internet-Abschaltung aufgrund ihrer Zielrichtung jedenfalls als Eingriff in die Informations- und Kommunikationsfreiheit zu qualifizieren. Zwar kann ein Eingriff gerechtfertigt werden, dazu muss er aber der menschenrechtlichen Schrankentrias genügen. Eine staatenweite Internetabschaltung ist ein schwerer Eingriff in die Informations- und Kommunikationsfreiheit. Oft wird mangels Gesetz die Überprüfung der Rechtmäßigkeit schon eingangs scheitern. Der Verweis auf den an sich legitimen Zweck der nationalen Sicherheit als Begründung einer Ausnahme von der Informations- und Kommunikationsfreiheit wird regelmäßig in die Leere gehen, da die nationale Sicherheit nicht zur Unterdrückung legitimer demokratischer Bestrebungen geltend gemacht werden kann. Schlussendlich fehlt es einer globalen Abschaltung in fast allen Fällen an der Verhältnismäßigkeit, während die gesetzlich gedeckte Abschaltung einzelner Server durchaus Deckung in der Abwägungstrias finden könnte. Ein öffentlicher Notstand kann zwar zu Einschränkungen der Menschenrechte führen, doch ist das Überleben eines bestimmen Regimes nicht mit dem Überleben der Nationen, das notstandstauglich wäre, gleichzusetzen.

Es bestehen den Menschenrechten entfließende Schutzpflichten des das Internet abschaltenden Staates gegenüber der internationalen Gemeinschaft, Gefahren für die Stabilität, Integrität und Funktionalität des Internets abzuwenden und den globalen, unbeschränkten, grenzenübergreifenden Internetverkehr nicht negativ zu beeinflussen. Gleichzeitig bestehen globale Schutzpflichten der internationalen Gemeinschaft hinsichtlich des Internets, die sich unter anderem aus der Pflicht der Staaten zur Gewährleistung der Vorbedingungen der Ausübung der Kommunikations- und Informationsrechte nach Art. 19 IPBürgR ergeben.

b) Welche Akteure können Menschenrechte dagegen in digitalen Räumen mit welchen Strategien verteidigen? (CDU/CSU)

Kurz: Wir alle. Jede*r Internetuser*in kann menschenverachtende Kommentare melden. Jede Plattform kann sich menschenrechtssensible Moderationsstandards geben. Jeder Staat kann eine menschenrechtssensible Cyberaußenpolitik pflegen. Eine Vielzahl an hochspezialisierten Nichtregierungsorganisationen im Digitalbereich wie Access Now[77], Amnesty International[78] und Algorithm Watch[79] zeigen am Beispiel des Monitorings von Algorithmen und des Datenschutzes bei der Verwendung von Corona-(Tracing)-Apps, wie man effektiv in digitalen Konstellationen für Menschenrechte eintreten kann. Datenschutzbehörden spielen ebenso eine

[77] 'Experts Are Finished, Politicians to Deliver - the Council of Europe Publishes Expert Recommendations on the Human Rights Impacts of Algorithmic Systems, Access Now, 2019.

[78] Amnesty International, Schütze deine Daten und deine Menschenrechte: Drei Schritte zum Datenschutz.

[79] States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights, AlgorithmWatch, 2020.

wichtige Rolle. International sind auch Ombudspersonen[80] von Bedeutung. Gute Praxen in Bereich konkreter Aktivitäten sind etwa Human Rights Hackathons (EqualiTECH 2019),[81] der Kompetenzaufbau im Bildungsbereich (zu Menschenrechtsverteidiger*innen[82]; zu internationalem Menschenrechtsschutz[83]); und universitäre Kurse in Kooperation mit Menschenrechtsorganisationen.[84] Auf Ebene von normativen Instrumenten ist zu nennen die Entwicklung von freiwilligen Standards von Plattformen (International Standards wie zB. 'Code of Practice on Disinformation'[85]), die bewusste Konsultation von Expert*innen im Kontext von Rechtssetzungsverfahren,[86] verpflichtende Algorithmenfolgenabschätzungen (Kanada[87]) sowie Modelle verstärkter Transparenz im Kampf gegen Hate Speech.[88]

Hinsichtlich der verbesserten Teilhabe aller Akteure an der globalen digitalen Kooperationsinfrastruktur hat sich in letzten Jahren ein gewisser Änderungsdruck aufgebaut. Eine zentrale Frage ist jene nach der institutionellen Gestaltung der neuen Kooperationsordnung.[89] Zuletzt legte ein im Auftrag des UNO-Generalsekretärs tätiges Panel 2019 einen Bericht zur Neugestaltung digitaler Kooperationsarchitekturen vor.[90] Ein an anderer Stelle geäußertes Bekenntnis des UNO-Generalsekretärs vorwegnehmend („[w]e cannot leave our fate in the digital era to the invisible hand of the market force" [91]), fordert der Bericht eine Neuaufstellung der globalen Internet Governance, wobei nichttraditionelle „multilateral and multi-stakeholder cooperation" entscheidend sein wird: sowohl zwischen Staaten als auch unter Integration aller Stakeholdergruppen (Staaten, Zivilgesellschaft, Privatsektor, internationale Organisationen). Dies ist seit 15 Jahren konsentiert: Der klare Staatenwillen, den Menschen in den Mittelpunkt der Internet Governance zu rücken und die Informationsgesellschaft inklusiv und entwicklung-

[80] E.g. Australian Competition and Consumer Commission, 'Digital Platforms Inquiry - Final Report', Australian Competition and Consumer Commission, 2019.
[81] 'EqualiTECH 2019 Human Rights Hackathon to Launch in Kosovo', Civil Rights Defenders, 2019.
[82] 'Human Rights Defenders', My Mooc < >.
[83] 'ILIA Online - Education in International Human Rights Law', Human Rights House Foundation.
[84] 'University Course with Social Innovation and Human Rights at the Centre', Civil Rights Defenders, 2020.
[85] European Commission, 'Code of Practice on Disinformation', Shaping Europe's Digital Future - European Commission, 2018.
[86] 'Assessment for German Parliament's Commission on Artificial Intelligence: Technology-Driven Disinformation by Bots', Botswatch Technologies, 2020.
[87] Treasury Board of Canada Secretariat Government of Canada, Algorithmic Impact Assessment (Archived) - Government of Canada Digital Playbook (Draft).
[88] Ben Wagner and others, 'Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act', in Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, FAT* '20 (Barcelona, Spain: Association for Computing Machinery, 2020), pp. 261–271.
[89] Vorschläge dazu etwa bei Kettemann/Kleinwächter/Senges/Schweiger, Comments on Recommendation 5A/B of the UN High Level Panel on Digital Cooperation, How to Build an Enhanced Mechanism for Digital Cooperation. A Multistakeholder Statement from Germany, 27.4.2020.
[90] The Age of Digital Interdependence, Report of the UN Secretary-General's High-level Panel on Digital Cooperation (2019).
[91] António Guterres, Preface, in Wolfgang Kleinwächter, Matthias C. Kettemann and Max Senges (Hrsg.), Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s (Hamburg: HBI, 2019), 10.

sorientiert auszugestalten, wird schon 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[92]) 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."[93]

Im Tunis Commitment von 2005 wird dies wiederholt. Ausweislich des Tunis Commitments ist Regelungsziel der Internet Governance der Aufbau einer menschenzentrierten, einschließenden, entwicklungsorientierten Informationsgesellschaft, gestützt auf die „Ziele und Grundsätze der Charta der Vereinten Nationen, das Völkerrecht und den Multilateralismus sowie unter voller Achtung und Einhaltung der Allgemeinen Erklärung der Menschenrechte". [94]

Als Follow-up zum Bericht wurde Deutschland vom UNO-Generalsekretär gemeinsam mit den Vereinigten Arabischen Emirate als „Co-Champions" designiert, um Konsultationen mit anderen Staaten, Unternehmen, zivilgesellschaftlichen Akteuren, der Wissenschaft, der Internetgemeinschaft und technischen Expert*innen durchzuführen.[95] Diesen Auftrag zur Sicherstellung gelebter Teilhabe führt BMWi über globale Stakeholderkonsultationen mit dem Internet & Jurisdiction Policy Network[96] sowie das Auswärtige Amt mit Missions Publiques[97] als Kooperationspartner durch. Ziel von Deutschland ist es dabei, Wege zur Umsetzung der Ideen des Panels zu finden, die von einer möglichst breiten Koalition der Stakeholder*innen

[92] WSIS, Tunis Commitment, WSIS-05/TUNIS/DOC/7-E (2005), Abs. 2.
[93] WSIS, Geneva Declaration of Principles, WSIS-03/GENEVA/DOC/4 (2003), Abs. 1.
[94] WSIS, Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, 18 November 2005, para. 2.
[95] Vgl. Kettemann/Kleinwächter/Senges/Schweiger, Comments on Recommendation 5A/B of the UN High Level Panel on Digital Cooperation, How to Build an Enhanced Mechanism for Digital Cooperation. A Multistakeholder Statement from Germany, 27.4.2020.
[96] Vgl. African Union Commission and Internet & Jurisdiction Policy Network Regional Conference 2020, Outcomes of the UN ECLAC and Internet & Jurisdiction Policy Network Regional Conference 2020.
[97] Vgl. Missions Publiques, Global Citizens' and Stakeholders' Dialogue: "We, the Internet": "On June 5th and 6th [2020], we are inviting stakeholders worldwide to discuss the future of Internet governance. How should we shape the future of digital cooperation? Who should decide how to leverage the opportunities brought by the use of digital technologies and mitigate the risks they involve? The Stakeholders' Dialogue aims to evaluate the three scenarios for the future of Internet governance [...]." Im Oktober 2020 wird ein globaler Bürger*innendialog stattfinden: "groups of hundreds of ordinary citizens will meet, get informed, discuss, and deliver a collective view on the core stakes of digitalization. Participants will be selected to represent the diversity of their regions and countries and will come from all walks of life. Those dialogues will help provide quantitative and qualitative data at global, national, and regional levels. They will articulate the needs and visions of citizens worldwide, and provide smart new insights."

befürwortet werden. Diese werden dann im Laufe des Frühsommers 2020 im Rahmen eines Optionenpapiers dem UNO-Generalsekretär vorgelegt werden und in den Reformprozess einfließen.[98] Die hier auf Grundlage von Beschlüssen des Bundestags zur Verfügung gestellten Mittel sind ein sehr sinnvolles Investment in eine menschenzentrierte Internet Governance-Politik und stellen ein wichtiges Experiment für politische Teilhabe in transnationalen Kontexten dar. Die Kooperation der beiden Ministerien mit erfahrenen Organisationen der Internet Governance und Stakeholderbefragung ist begrüßenswert.[99]

Daten sind entscheidend: Ein Lagebild zum Internet in Deutschland

Disaggregierte unter Wahrung von Datenschutz und dem Recht auf Privatsphäre gesammelte, sinnvoll aufbereitete und offenen Daten zur Nutzung des Internets sind entscheidend als Grundlage für eine Optimierung staatlicher Internetpolitik. So empfiehlt etwa das Panel des UNO-Generalsekretärs 2019 „eine Plattform für die gemeinsame Nutzung digitaler öffentlicher Güter“ zu schaffen, die „Datensätze in Bereichen, die mit der Erreichung der [nachhaltigen Entwicklungsziele] zusammenhängen, [...] zusammenführt.“ Insbesondere fordert das Panel, dass „dringend eine Reihe von Metriken für die digitale Inklusivität vereinbart [werden sollten], weltweit gemessen und mit nach Geschlecht disaggregierten Daten in den Jahresberichten von Institutionen wie der UNO, dem Internationalen Währungsfonds, der Weltbank, anderen multilateralen Entwicklungsbanken und der OECD detailliert aufgeführt werden sollten. „[100]

Für Deutschland läuft ein entsprechender Prozess gerade. Im Mai 2020 wurde das Leibniz-Institut für Medienforschung von der Deutschen UNESCO-Kommission beauftragt, ein indikatorenbasiertes Lagebild zum Internet in Deutschland zu erstellen. Die 130 anzuwendenden Indikatoren[101] werden eine bisher so noch nicht vorhandene Übersicht der Zugänge, der Nutzung, der Regulierung und Gestaltung des Internets in Deutschland ermöglichen. Diese Übersicht zusammen mit Empfehlungen des Forschungsteams werden Ende 2020 vorgelegt werden und können dann als Grundlage für zukünftige Regelungsansätze im Hinblick auf die Weiterentwicklung der Digitalstrategie Deutschlands fungieren. Mit der Anwendung der Indikatoren als eines der ersten Länder innerhalb der Europäischen Union (in Frankreich läuft der Prozess aktuell) hat Deutschland die Gelegenheit, Vorbildwirkung zu

[98] BMWI, Following up on HLPDC Recommendations 5A/B, Follow-up on Digital Cooperation Architecture (2019).
[99] Transparenzhinweis: Der Sachverständige war in beiden Prozessen als wissenschaftlicher Berater involviert.
[100] The Age of Digital Interdependence, Report of the UN Secretary-General’s High-level Panel on Digital Cooperation (2019), Empfehlungen 1B und 1D.
[101] UNESCO (David Souter, Anri van der Spuy), UNESCO’s Internet Universality Indicators: A Framework for Assessing Internet Development (2019). Die 303 Indikatoren befassen sich mit Fragen von Internetzugang, Offenheit, mit Fragen der Geschlechtergleichstellung und den Bedürfnissen von Kindern und Jugendlichen, der nachhaltigen Entwicklung, des Vertrauens und der Sicherheit sowie mit rechtlichen und ethischen Aspekten des Internets. Dazu kommen kontextbezogene Indikatoren zu Wirtschaft, Demographie, Entwicklung, Gleichberechtigung, Regierungshandeln sowie Indikatoren zur Entwicklung von Informations- und Kommunikationstechnologie (IKT).

entfalten. Die Anwendung der Indikatoren kann die transformative Kraft des Internets stärken und trägt zur Verwirklichung der Agenda für nachhaltige Entwicklung von 2030 bei.[102]

Frage 2: Die kommunistische Führung Chinas versucht in enger Koordination von staatlichen und Partei-Strukturen sowie privaten und dennoch vom Staat abhängigen Unternehmen eine Totalüberwachung und Kontrolle der gesamten Bevölkerung in allen öffentlichen und privaten Bereichen durchzusetzen, insbesondere von ethnischen und religiösen Minderheiten. Welche Strategie nutzt die kommunistische Führung unter Xi Jinping nicht nur national, sondern auch regional und immer stärker global, um die neue Rolle Chinas als ökonomische und digitale Supermacht auch dafür einzusetzen, die universellen Menschenrechte im Sinne der autoritären Ideologie der KP Chinas umzudefinieren? (CDU/CSU)

Ich fokussiere auf die regionale und globale Dimension chinesischer Menschenrechtspolitik. Zu nationalen Aspekten des Einsatzes von Informationstechnologie sei hier gesagt, dass dieser, soweit medial bekannt, aufgrund der Eingriffstiefe in die Lebensführung von Menschen in einzelnen Regionen (wie Xinjiang[103]) jedenfalls nicht mit den menschenrechtlichen Verpflichtungen Chinas konform geht.

China verfolgt wie andere im Selbstverständnis sozialistische Regimes ein Menschenrechtskonzept mit Schwergewicht auf den wirtschaftlichen, sozialen und kulturellen Rechten. Hier ist gleich eingangs festzuhalten, dass die Priorisierung von einzelnen Menschenrechten bzw. einzelner Menschrechtsgenerationen oder -bilder im Licht klarer internationaler Bekenntnisse problematisch ist. Wie schon in den Schlussdokumenten zur Wiener Weltmenschenrechtskonferenz 1993 der UNO bekräftigt,[104] sind Achtung, Schutz und Gewährleistung *aller* Menschenrechte für *alle* Menschen das Ziel der Staatengemeinschaft. Wirtschaftliche, soziale und kulturelle Rechte und bürgerliche und politische Rechte sind allgemein gültig, unteilbar, bedingen sich wechselseitig und sind miteinander verknüpft. Nur wenn wirtschaftliche, soziale und kulturelle Rechte in der Praxis geschützt sind, können Bürger*innen ihre bürgerlichen und politischen Rechte wahrnehmen. Deren Einhaltung ist wiederum Vorbedingung zur Umsetzung der wirtschaftlichen, sozialen und kulturellen Rechte. Übergreifend ist in allem die Menschen-

[102] Insbes. Ziel 16.10, Zugang der Öffentlichkeit zu Informationen und Grundfreiheiten.
[103] Cave, Danielle; Hoffmann, Samantha; Joske, Alex; Ryan, Fergus; Thomas Elise: „Mapping China's technology giants", ASPI International Cyber Policy Centre, Report no. 15/2019, p. 16.
[104] DGVN, Dokumente zur Wiener Weltmenschenrechtskonferenz (1993).

würde zu wahren, in der auch die nichtdiskriminierende Garantie aller Menschenrechte begründet liegt.

Narrativen, denen zufolge die chinesische Bevölkerung bereit sei, auf „etwas Freiheit" zu verzichten, um „etwas (soziale) Sicherheit" und Wachstum zu erlangen, ist mit Vorsicht zu begegnen. Wie eine jüngst erschiene Studie des Mercator-Instituts für China-Studien zeigt, sind die Ansichten junger Menschen in China zu sozialen Bonitätssystemen (Social Scoring/Sozialkreditsystem) einigermaßen komplex.[105] Nachdem sie von Forscher*innen über mögliche positive und negative Auswirkungen informiert worden waren, korrigierten chinesische Befragte ihre Zustimmung zu Sozialkreditsystemen von 53 Prozent auf nur 29 Prozent.[106]

Die chinesische Regierung hat in den letzten 10-15 Jahren, insbesondere in den letzten fünf, bewusst versucht, auf globaler Ebene Gegenentwürfe zur als westlich dominiert wahrgenommenen Menschenrechtspolitik zu entwickeln. Zwar kann China nicht universelle Menschenrechte „umdefinieren", aber es lässt sich nicht leugnen, dass sich chinesische Menschenrechtsdiplomatie, gerade im Menschenrechtsrat der Vereinten Nationen, von einer passiven Rolle hin zu einem aktiven Selbstverständnis verschoben hat. Einerseits versucht China, durch eine stärkere Präsenz in internationalen Institutionen und durch Einflussnahme auf das Design der Menschenrechtsschutzarchitektur Kritik von der eigenen Menschenrechtspolitik abzuwenden. Andererseits tritt China offen für eine traditionelle, staatenorientiere Interpretation der Menschenrechte und des Völkerrechts ein, in deren Zentrum die staatliche Souveränität und die Nichteinmischung anderer Staaten in „innere Angelegenheiten"[107] stehen. Chinas Ziel ist es dabei, die globale Ordnung so zu gestalten, dass sie national verstandene Interessen stärker berücksichtigt.[108]

In seiner Menschenrechtsaußenpolitik wird neben der Perspektivenverschiebung auf wirtschaftliche, soziale und kulturelle Rechte auch ein relativistisches Menschenrechtsverständnis eingefordert. Schon jetzt ist anerkannt, dass Menschenrechte aus historischen, kulturellen und religiösen Gründen in einzelnen Staaten unterschiedliche Beschränkungen erfahren, während weiterhin *alle* Menschenrechte *für alle* gelten. Die aktuelle Sicht der chinesischen Regierung qualifiziert dies allerdings dergestalt, dass die Menschenrechte auf der Geschichte, der Kultur und den Werten, dem politischen System und dem Entwicklungsstand jedes einzelnen Landes

[105] Marc Oliver Rieger, Mei Wang, Mareike Ohlberg, What do Young Chinese Think about Social Credit? It's Complicated, Mercator Institute for China Studies, China Monitor, 26.3.2020
[106] Ibid.
[107] Piccone, Ted: „China's Long Game on Human Rights at the United Nations", Foreign Policy at Brookings, September 2018, p. 1.
[108] Lagon, M. P., & Lou, T.: The Dragon in Turtle Bay: The Impact of China's Rise in the UN on the United States and Global Governance, World Affairs, 181(3) (2018), 241.

basieren müssen.[109] Teil der Menschenrechtsdiplomatie Chinas ist auch der Fokus auf staatlich gelenkte Entwicklung, basierend auf nationale Souveränität.[110] Präventiver Menschenrechtsschutz und die Rolle der Zivilgesellschaft sowie internationaler Organisationen im Menschenrechtsschutz werden indes eher kritisch gesehen.[111] Berichten zufolge fordert China auch Staaten, die es im Rahmen der "Belt and Road"-Initiative unterstützt, auf, positive Bewertungen der chinesischen Menschenrechtspolitik im Rahmen von globalen Überwachungsmechanismen abzugeben.[112]

Die externe Technologiepolitik Chinas ist im Kontext von "Made in China 2025" zu sehen, einer Initiative des Staatsrates vom Mai 2015 mit dem bewussten Ziel, China perspektivisch in Führungsposition unter den Industrienationen zu bringen.[113] Dazu wurde zunächst intern versucht, technologische Hard- und Softwarekompetenz in Unabhängigkeit von den USA zu erlangen (ein Prozess, der nicht zuletzt durch die Sanktionen von US-Präsident Trump katalysiert wurde) und sodann die eigene Technologie weltweit zu verbreiten.[114] Dies war erfolgreich. Chinas Kommunikationstechnologiefirmen ZTE und Huawei gehören zu den erfolgreichsten Zugangsanbietern in Afrika.[115] Huawei und chinesische Plattformen, wie TikTok, sind inzwischen auch in Europa am Markt präsent.

Nach einem Bericht der NGO Freedom House von 2018 haben chinesische IT-Unternehmen in mindestens 38 Ländern Internet- und Mobilfunknetzeinrichtungen installiert.[116] Sowohl privatwirtschaftliche Unternehmen, die als „national champions" auf strategische Ziele der chinesischen Regierung verpflichtet sind, als auch staatliche Unternehmen wie China Telecom, China Unicom und China Mobile sind an der „ digitalen Seidenstraße" beteiligt.[117] Besonders stark präsent sind chinesische Unternehmen im Infrastrukturaufbau für Netze: Huawei verantwortet in Mexiko das größte öffentliche WLAN-Netz Lateinamerikas, in Bangladesch das 5G-Mobilfunknetz und in Kambodscha den 4,5G-Dienst und berät die kenianische Regierung beim Aufbau von WLAN-Netzen.

---

[109] Taylor, I.: "China and Political Governance in Africa", Oxford Research Encyclopedia of Politics, Januar 2019,
[110] Maizland, Lindsay: "Is China Undermining Human Rights at the United Nations?", Council on Foreign Relations, 9. Juli 2019,.
[111] Lagon, M. P., & Lou, T.: The Dragon in Turtle Bay: The Impact of China's Rise in the UN on the United States and Global Governance, World Affairs, 181(3) (2018), 245.
[112] Maizland, Lindsay: "Is China Undermining Human Rights at the United Nations?", Council on Foreign Relations, 9. Juli 2019.
[113] Peter, Rudolf: „Der amerikanisch-chinesische Weltkonflikt", SWP-Studie 23, Oktober 2019, p. 29.
[114] Schulze, Matthias & Voelsen, Daniel: „Einflussspähren der Digitalisierung" in Lippert und Berthes (Hrsg.), „Strategische Rivalität zwischen USA und China: worum es geht, was es für Europa (und andere) bedeutet" p. 32.
[115] Umejei, Emeka, „The Imitation Game: Will China's Investments Reshape Africa's Internet?", Power 3.0 Blog – International Forum For Democratic Studies, 6. Dezember 2018.
[116] Shahbaz, Adrian, "Freedom on the Net 2018 - The Rise of Digital Authoritarianism" (Freedom House, 2018).
[117] Ibid.

Problematisch erscheint auch, dass chinesische Unternehmen in etlichen Staaten Asiens und Afrikas Regierungsstellen Überwachungssoftware zur Verfügung stellen. [118] In 18 der 65 von Freedom House untersuchten Ländern verwenden Unternehmen wie Yitu, Hikvision und CloudWalk AI-basierte Gesichtserkennungssoftware.[119] Ein aktueller Bericht australischer Expert*innen bezeichnet den Export von chinesischer Überwachungssoftware als „wichtigen und wenig beachteten Teil der globalen Expansion chinesischer Technologieunternehmen". Huawei sei in diesem Bereich besonders dominant. Zu diesen „'Safe City'-Projekten" gehören die Bereitstellung von Überwachungskameras, Kommando- und Kontrollzentren, Gesichts- und Kennzeichenerkennungstechnologien, Datenlabors und tragbare Systeme für den schnellen Einsatz in Notfällen. Die australischen Forscher*innen bezeichnen das Wachstum von Huaweis "Public Security Solution"-Projekten als „rasant": 230 Städte hätten diese schon eingesetzt (Stand 2018).[120]

Neben dem Einsatz der Technologie ist auch die Vorbildfunktion des chinesischen Modells (Nutzung von Überwachungstechnologie zur gesellschaftlichen Lenkung) eine Herausforderung für eine nachhaltig-demokratie Entwicklung afrikanischer Staaten zu stabilen Rechtsstaaten. Besonders Staaten mit sich erst stabilisierenden demokratischen, zivilgesellschaftlichen und rechtstaatlichen Strukturen wie Kenia, Mali, Ägypten, Tansania, Uganda, Tschad, Kamerun und Sambia würde durch das chinesische Vorbild gezeigt, dass ein „freies und offenes Internet für die Entwicklung weder notwendig noch wünschenswert" sei.[121]

Hier ist es auch Rolle Deutschlands als Partnerland in der Entwicklungszusammenarbeit (auch via Projekte der GTZ, der Konrad-Adenauer- und der Friedrich-Ebert-Stiftung) sowie im Rahmen der EU-Ratspräsidentschaft Akzente zu setzen. Zum Beispiel könnte durch rechtspolitische Beratung bei Interesse an einer Umsetzung eines Gesetzes nach dem Modell des Netzwerkdurchsetzungsgesetzes die Sicherung rechtsstaatlicher Standards gesichert werden. Auch Modellgesetze für den Einsatz von Überwachungstechnologien und die verstärkte Integration von digitalrechtlichen Gefährdungen in die Menschenrechtskonditionalitäten der Entwicklungszusammenarbeit erscheinen möglich und sinnvoll. Insbesondere die digitale Außenpolitik in Hinblick auf Afrika sollte getragen sein von einem bewussten Eintreten für die Bedeutung des Menschenrechtsschutzes im Internet. Erste Schritte wären etwa die Entwicklung von Modellgesetzen für den Einsatz von Überwachungstechnologien und die verstärkte Integration von digitalrechtlichen Gefährdungen in die Menschenrechtskonditionalitäten der Entwicklungszusammenarbeit.

---

[118] Kliman, Daniel; Doshi, Rush; Lee, Kristine; Cooper, Zack: „Grading China's Belt and Road", CNAS Report April 2019, p. 24-25,

[119] Shahbaz, Adrian, "Freedom on the Net 2018 - The Rise of Digital Authoritarianism" (Freedom House, 2018).

[120] Cave, Danielle; Hoffmann, Samantha; Joske, Alex; Ryan, Fergus; Thomas Elise: „Mapping China's technology giants", ASPI International Cyber Policy Centre, Report no. 15/2019, p. 9-10.

[121] Ibid., p. 11.

Frage 3: Wie wirken die Werte Transparenz und Datenschutz im digitalen Zeitalter zusammen, und was sind Ihrer Ansicht nach die größten Bedrohungen für die Menschenrechte und die politische Beteiligung im digitalen Zeitalter, insbesondere in Hinblick auf Menschenrechtsverteidiger, Whistleblower und andere Gruppen, die moderne Informationstechnologien nicht nur nutzen, sondern mit deren Hilfe auch besonders drangsaliert werden? (DIE LINKE.)

Zu Gefährdungspotenzialen von digitalen Technologien, gerade vor dem Hintergrund intersektionaler Diskriminierung, verweise ich auf meine Ausführungen zu Fragen 6 und 7; die Rolle von Anonymisierungstechnologien spreche ich im Kontext meiner Beantwortung von Frage 5 an. Im Folgenden gehe ich auf die Rolle von Transparenz und Datenschutz ein.

Transparenz hat keinen inhärenten Wert, stellt aber ein wichtiges Prinzip dar, um normative Werte zu effektuieren.[122] Transparenz kann aus verschiedenen Perspektiven wichtig sein und dann auch unterschiedliche Bedeutungen haben: Geht es um gesamtgesellschaftliche Kontrolle der Verteilungsprozesse für Rechte und Güter? Um die Art und Weise, wie Entscheidungen gefällt werden? Sowohl in dem Whitepaper der EU-Kommission als auch in den Ethical Guidelines der High-Level Expert Group on Trustworthy AI wird „Transparency" als ein zentrales Prinzip beim Einsatz von Künstlicher Intelligenz genannt; genauso in zahlreichen Prinzipienerklärungen zur KI.[123]

Transparenz hat notwendigerweise einen Zusammenhang mit den von automatisierten Entscheidungssystemen verwendeten und generierten Daten: Wenn ein algorithmisches Entscheidungssystem durch Verwendung von Machine Learning (ML) anhand von Trainingsdaten trainiert wird, um eigene Regeln und Korrelationen zwischen Merkmalen zu deduzieren, ist deren Auswahl essenziell für den Output, den dieses System liefert. Werden diese Daten aber nicht transparent gemacht und ausgewählt, können sich dort verschiedenste Vorurteile und Diskriminierungen (Stichwort: *machine bias*) verbergen, die sich durch einen flächendeckenden Einsatz der Systeme skalieren lassen. Dabei kommt es selten auf den Code/Algorithmus selbst an, sondern auf das Verhältnis von Daten und Algorithmen spwie den verschiedenen Gewichtungen und Werten.[124] Alleine eine Veröffentlichung des Codes würde keine Transparenz schaffen.[125]

---

[122] Ball, C. (2009). What is transparency? Public Integrity, 11(4), 293-308.

[123] Europäische Kommission, AI HLEG, High-Level Expert Group on Artificial Intelligence (2019), Ethics Guidelines for Trustworthy AI.

[124] Ananny, M., & K. Crawford (2018) Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. New Media and Society, 20(3), 973–989.

[125] Vgl. Larsson, S. & Heintz, F. (2020). Transparency in artificial intelligence. Internet Policy Review, 9(2). DOI: 10.14763/2020.2.1469.

Versteht man unter Transparenz auch die Erklärbarkeit eines automatisierten Entscheidungsfindungssystems, das Methoden des maschinellen Lernens benutzt, als engeren Begriff, kann nachgeprüft werden, ob das System und seine Vorhersagen mit den einschlägigen Rechtsnormen im Einklang stehen. Somit kann auch das Vertrauen der beteiligten Akteure und Betroffenen in das System und seine Entscheidung(en) verbessert werden.

Zum Verhältnis von Transparenz und Datenschutz ist zu sagen, dass (Verarbeitungs-)Transparenz als instrumentelles Mittel zur Durchsetzung wirksamen Datenschutzes hilfreich sein kann. Datenschutz als stark mit (informationeller) Selbstbestimmung zusammenhängendes (aber nicht identisches!) Rechtsgebiet setzt auf den Selbstschutz von sowie die Kontrolle durch betroffene Individuen (die Einwilligungen erteilen und widerrufen können, ihre Ansprüche aus dem Recht auf Vergessen realisieren können, Auskunftsrechte, Widerspruchsrechte in Anspruch nehmen können etc.).

Dagegen ist Transparenz hinsichtlich der verarbeiteten Daten und ihre Zwecke über den Verantwortlichen und über etwaige Empfänger der Daten eine Rechtspflicht (vgl. Art. 12-15 DSGVO).[126] Transparenz hinsichtlich der Datenverarbeitung ist außerdem unabdingbar für Aufsichtsbehörden, die zur wirksamen Kontrolle von datenschutzrechtlichen Verantwortlichen Einblick in deren interne Abläufe benötigen. Als eigenständiger Grundsatz wird er festgehalten in Art. 5 Abs. 1 lit. a Var. 3 DSGVO, eng verknüpft mit dem Grundsatz der Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO.[127]

Transparenz allein ermächtigt Individuen nicht zu wirksamer Kontrolle, es muss auch dafür gesorgt werden, dass diese Gebrauch von ihren Rechten machen, also z. B. hinreichend sensibilisiert für Datenschutzrisiken sind und die ihnen zur Verfügung stehenden Rechte ohne Rechtsberatung ausüben können. Kurz: Die transparent gemachten Informationen müssen für das Individuum verständlich und nachvollziehbar, gleichzeitig aber auch vollständig sein.[128]

Transparenz darf aber nicht verabsolutiert werden. Nicht zuletzt Whistleblower und andere vulnerable Gruppen sind auf pseudonyme bzw. anonyme Nutzung digitaler Dienste, aber auch auf die Möglichkeit zur Verschlüsselung digitaler Kommunikation angewiesen, sodass hier staatlich verordnete Transparenz (etwa in Form einer Klarnamenpflicht) eine große Gefahr darstellen kann.[129]

---

[126] Art. 29-Arbeitsgruppe, Leitlinien der Art. 29-Datenschutzgruppe für Transparenz.

[127] Siehe Stellungnahme der Art. 29 Datenschutzgruppe, Opinion on the Principle of Accountability.

[128] Vgl. Robrecht, B. (2015). EU-Datenschutzgrundverordnung: Transparenzgewinn oder Information-Overkill. Oldenburger Verlag für Wirtschaft, Informatik und Recht.

[129] Schwander, Das digitale Vermummungsverbot – eine irreführende Analogie, in: ZRP 2019, 207.

4. Was kann Gesichtserkennung (Facial Recognition Technology), und welche Auswirkungen hat diese Form der Künstlichen Intelligenz auf den Schutz, die Respektierung und Gewährleistung von Menschenrechten im nationalen sowie internationalen Kontext? (BÜNDNIS 90/DIE GRÜNEN)

Spätestens seit dem Einsatz von Gesichtserkennungssoftware[130] am Berliner Bahnhof Südkreuz sowie durch das Unternehmen Clearview, das Berichten zufolge drei Milliarden Bilder gespeichert hat (wobei auch Duplikate dabei sein werden),[131] ist Gesichtserkennungstechnologie im Zentrum der Debatten über die Grenzen der Nutzung von Überwachungstechnologie angekommen. Wie bei jeder Technologie gibt es Potenziale[132] und Risiken.[133] Ich gehe hier noch sehr kurz darauf ein.

In der DSGVO findet sich angesichts des sehr hohen Eingriffsniveaus des Sammelns von biometrischen Daten zwar ein grundsätzliches Verbot, dieses gilt aber nicht bei Zustimmung der Betroffenen oder der Notwendigkeit der biometrischen Identifizierung aus Gründen eines erheblichen öffentlichen Interesses (z. B. bei der Verfolgung schwerer Straftaten), wobei auch hier die Rechte und Interessen von Nichtbetroffenen in das Abwägungsmodell einzugliedern sind.[134] Angesichts der Erheblichkeit des Grundrechtseingriffs ist eine analoge Anwendung der Vorschriften zur Videoüberwachung nicht vertretbar. Auch müssten in jedem Fall überzeugende Belege beigebracht werden, dass schon durchgeführte Überwachungen auf Grundlage von Gesichtserkennung zur Erreichung gesamtgesellschaftlicher Ziele in einem Maß beigetragen haben, das die Eingriffstiefe in individuelle Rechtspositionen rechtfertigt.

B. Digitale Optionen und Strategien für den Schutz von Menschenrechten

Frage 5: Können Sie konkrete Beispiele nennen, in denen das Darknet – genauer: die helle Seite des Darknets – Journalisten und Menschenrechtlern unter dem Schutz der Anonymität Austausch, Recherche und das Aufdecken von Missständen in Autokratien und Diktaturen erst ermöglicht, also Voraussetzung

[130] Vgl. BSI, Gesichtserkennung.
[131] ZEIT (Lisa Hegemann), Die Firma, die uns alle identifizieren will.
[132] Thales Group, Facial recognition: top 7 trends.
[133] Electronic Frontier Foundation, Face Recognition; ACLU, Face Recognition Technology.
[134] Berlin: Biometrische Gesichtserkennung – Technik mit Zukunft?
ZD-Aktuell 2017, 05522

für jede regimekritische Tätigkeit ist, und wie bewerten Sie in diesem Zusammenhang den vom BMI geforderten Darknetparagraphen? (SPD)

Das Darknet als solches zu kriminalisieren ist wenig sinnvoll. Streng genommen gibt es auch nicht „das Darknet", sondern viele Darknets. „Darknet" steht für anonymisierte Kommunikation im Internet, zum Beispiel über einen Tor-Browser. Anders als im ‚normalen' Internet werden Verbindungen zwischen User*innen gezielt und manuell hergestellt. Dieses sehr kleine Netz kann dann erweitert werden. Die Darknets bieten aus architektonischen Gründen mehr Anonymität als die übliche Internutzung, was *auch* Menschen mit kriminellen Absichten anlockt, es ist aber empirisch nicht nachweisbar, dass sich substanzielle Rechtsschutzdefizite ergeben oder dass die staatliche Pflicht zur effektiven Strafverfolgung aufgrund von Anonymisierungstechnologien in erheblichem Maße gefährdet wäre. Hier besteht keine Rechtsschutzlücke. Regelmäßig wird über die Zerschlagung von Darknet-Marktplätzen (AlphaBay, Hansa,[135] Wall Street Market[136]) berichtet, über die illegale Erzeugnisse verkauft worden waren.[137] Nur als Beispiel: Wer in einem verschlüsselten Forum Waffen kauft, kann sich ebenso strafbar machen[138] wie jener, der sie verkauft; letzterer wegen Beihilfe zum vorsätzlichen unerlaubten Handeltreiben mit Waffen und Munition.[139] Anstelle neuer Gesetze ist die Förderung cyberforensischer Kapazitäten bei den Strafverfolgungsbehörden zu fordern.

Mit dem 2019 vorgeschlagenen „Darknetparagraf" (§ 126a StGB-Entwurf) kann jedes Engagement für Anonymität im Internet kriminalisiert werden, was einen abschreckenden Effekt für Betreiber*innen von Anonymisierungsdiensten und für Nutzer*innen von Anonymisierungssoftware hätte. Eine Analyse für Reporter ohne Grenzen zitiert einen Betroffenen: „Selbst wenn der Staat Dein Verhalten nicht direkt kriminalisiert, fragst Du Dich ständig: Mache ich mich verdächtig, nur weil ich jetzt gerade einen VPN oder Tor nutze? Es gibt einen Chilling Effect, der schleichend Dein Verhalten verändert."[140]

Deutschland muss sich hier auch der Vorbildwirkung seiner Internetgesetzgebung auf Grundlage der freiheitlich-demokratischen Grundordnung bewusst sein. Wie das Beispiel des NetzDG zeigt, kopieren andere Staaten deutsche Gesetze, ohne aber die im deutschen Recht verankerten Verhältnismäßigkeitserwägung oder den Rechtsschutz mit zu übernehmen.

---

[135] Spiegel Online, Ermittler zerschlagen zwei der größten Darknet-Marktplätze, 20.07.2017.
[136] Sonja Peteranderl, Ermittler nehmen Betreiber von "Wall Street Market" fest, Spiegel Online, 3.5.2020.
[137] Max Hoppenstedt, BKA nimmt mutmaßliche Betreiber von Online-Drogenshop fest, Spiegel Online, 3.6.2020.
[138] WabnitzJanovsky WirtschaftsStrafR-HdB, 15. Kapitel. Computer- und Internetkriminalität, Rn. 200.
[139] LG Karlsruhe, Urteil vom 19.12.2018 – 4 KLs 608 Js 19580/17 = MMR 2019, 632.
[140] Moritz Bartl/Daniel Moßbrucker/Christian Rückert (Reporter ohne Grenzen), Angriff auf die Anonymität im Internet. Folgen des sogenannten "Darknet-Paragraphen" als § 126a Strafgesetzbuch für die rechtliche Praxis – und Kollateralschäden seines Einsatzes für die Presse-, Meinungs- und Telekommunikationsfreiheiten (2019), 18.

Berichten von Nichtregierungsorganisationen und Medien kann man positive Beispiele für die Nutzung von Anonymisierungssoftware entnehmen. Darknets werden als „wichtiges Werkzeug für Oppositionelle und Aktivisten in autoritären Regimen, für Whistleblower, für Journalisten und für Menschen, die sich überwacht fühlen, wenn sie ihren normalen Browser öffnen" beschrieben.[141] Etablierte Medien (wie die New York Times und die taz) haben Whistleblower-Briefkästen eingerichtet, die verschlüsselte Einsendungen ermöglichen. Oppositionelle autoritären Staaten nutzen das Darknet als „einzige Chance, sich anonym zu äußern".[142]

Systemli.org (in Deutschland) und Riseup.net (in den USA) bieten E-Mail-, Cloud- und Hosting-Dienste unter Nutzung von .onion-Adressen an. Auch diese anonymisierte Kommunikation kann von Menschenrechtsverteidiger*innen genutzt werden.[143] Der dezentrale Messenger-Dienst FireChat macht einzelne Smartphones zu Kommunikationsknoten und ermöglicht damit Kommunikation auch nach Abschaltung von Handynetzen.[144] Auch wenn in Staaten das Internet zunehmend zensiert wird, können Darknets zur Kommunikation mit der Außenwelt genutzt werden. In einem Deutschlandfunk-Bericht wird Syrien als Beispiel genannt: „Aktivisten [...] haben dort ihr Material hochgeladen – Videos, Fotos – und haben dann diese Links an westliche Redaktionen geschickt. Das Darknet war das Nadelöhr, dann konnten westliche Medien über die wahren Zustände in Syrien berichten." [145]

Das AG Mannheim führt in einem Beschluss von 2018 aus, dass das Darknet auch „schlicht zur verschlüsselten Kommunikation" genutzt werden kann. Die bloße Nutzung des TOR-Browsers sei legal und könne richtigerweise nicht zu der Vermutung führen, dass Nutzer*innen Straftaten begehe: „Jede andere Sichtweise hätte zur Folge, dass sämtliche Nutzer von frei zugänglicher und legaler Software durch deren bloße Verwendung unter Generalverdacht gestellt würden."[146] Angesichts der steigenden Nutzungszahlen privatssphäreschonender Kommunikationsdienste wie Signal ist es mit ein Zeichen der Zeit, dass das individuelle und gesellschaftliche Bewusstsein für die Bedeutung von Anonymität im Internet gestiegen ist. Wie Michael Thiesen schreibt: „Die weitestgehend unerkannte Nutzung des Internet wird mehr und mehr zum Ideal für den mündigen Bürger. Für Whistleblower und Journalisten ist sie eine über den presserechtlichen Quellenschutz hinausgehende Sicherheitsvorkehrung. Für Regimekritiker aus aller Welt steigert sie sich zur schlichtweg unverzichtbaren und lebensrettenden Grundvoraussetzung."[147]

[141] SPIEGEL Online, Das Darknet ist besser als sein Ruf.
[142] mdr.de, Das Darknet – mehr als ein Ort für Pädophile und Waffenhändler.
[143] Daniel Wendorf/Benedikt Plass-Fleßenkämper, Darknet – Fünf Beispiele, warum der schlechte Ruf nicht gerechtfertigt ist (Goethe-Institut).
[144] Ibid.
[145] Deutschlandfunk, Die helle Seite des Darknet.
[146] AG Mannheim, Beschluss vom 25.04.2018 - 1 Ls 805 Js 21014/15, BeckRS 2018; FD-StrafR 2018, 40777.
[147] Thiesen, Wie hoch ist der Preis der Anonymität? - Haftungsrisiken beim Betrieb eines TOR-Servers, MMR 2014, 80.

Frage 6: In welchen Bereichen identifizieren Sie die größten Chancen und Herausforderungen digitaler Technologien in Bezug auf Gendergerechtigkeit, Frauenrechte und politische Teilhabe von Frauen? (FDP)

Gerade für marginalisierte Gruppen galt das Internet lange als *das* emanzipatorische Instrument zur Überwindung aller Arten von Ausgrenzung.[148] Auch wenn das Internet für viele marginalisierte soziale Gruppen der Gesellschaft Raum für kommunikative Selbstverwirklichung bietet (zB: #metoo, #metwo, #schauhin, #ThingsDisabledPeopleKnow), sind diese Gruppen auch in der digitalen Welt nach wie vor in besonderem Maß von Diskriminierung betroffen.[149]

Amnesty International bestätigte 2018, dass

> „Frauen mit dunkler Hautfarbe, Frauen religiöser oder ethnischer Minderheiten, lesbische, bisexuelle, transsexuelle oder intersexuelle (LBTI) Frauen, Frauen mit Behinderungen oder nichtbinäre Personen, die den traditionellen Geschlechternormen von Männern und Frauen nicht entsprechen, [im Internet] oft Formen von digitaler Gewalt ausgesetzt sind, die sie auf einzigartige oder besondere Weise betrifft."[150]

An selber Stelle weist Amnesty darauf hin, dass Frauen wie Feministinnen, die sich gezielt für Frauenrechte einsetzen, und Frauen, die in der Öffentlichkeit stehen, wie Journalistinnen und Politikerinnen, besonders von Hate Speech betroffen sind.[151] Diese Verquickung von Vulnerabilitäts-Faktoren bestätigt auch das, was das vom Europarat gegründete No-Hate Speech-Movement festhält: „Wenn man sich anschaut, welche Frauen von Hate Speech betroffen sind, fällt auf: Neben muslimischen und geflüchteten Frauen betrifft dieses Phänomen vor allem Feministinnen und jene, die in der Öffentlichkeit stehen."[152]

Legt man einen besonderen Fokus auf den Komplex Sexist oder Gendered Hate Speech, so wird schnell deutlich, dass Hate Speech Frauen unterschiedlich stark betrifft, sie aber vor allem *in ihrer Unterschiedlichkeit* betrifft und dass das Thema daher nie aus dem intersektionalen Kontext gehoben werden darf. Eine Studie aus 2019 zu Erfahrungen deutscher Internetnutzer*innen mit Hate Speech im Internet zeigt deutlich, dass Menschen, die Hate

[148] Dieser Abschnitt beruht insbesondere auf Forschungen von Katharina Mosene sowie auf unserem Beitrag: Kettemann/Mosene, Hassrede und Katzenbilder: Ausgewählte menschenrechtliche Aspekte der Governance von Meinungsäußerungen im Internet, Elisabeth Greif und Silvia Ulrich (Hrsg.), Hass im Netz – Grenzen digitaler Freiheit (Linz: Böhlau, 2019), 92-122.

[149] Drüeke, R., & Klaus, E. (2014). Öffentlichkeiten im Internet: zwischen Feminismus und Antifeminismus. Femina Politica - Zeitschrift für feministische Politikwissenschaft, 23(2), 59-71.

[150] „In the case of online violence and abuse, women of colour, religious or ethnic minority women, lesbian, bisexual, transgender or intersex (LBTI) women, women with disabilities, or non-binary individuals who do not conform to traditional gender norms of male and female, will often experience abuse that targets them in a unique or compounded way" (Amnesty International, Online Violence against Women (2018), Kap 2).

[151] Ibid.

[152] Sara Geisler, Öfter im Shitstorm, fluter.de, 2016.

Speech erfahren, sich nicht selten aus dem Internet zurückziehen. Sogenanntes durch Hate Speech hervorgerufenes *Silencing* wird oftmals gezielt eingesetzt, um gegen bestimmte (marginalisierte) Gruppen vorzugehen. Fast immer zieht dies mit Blick auf die Verursachenden keine rechtlichen Konsequenzen nach sich. Fast die Hälfte (länderabhängig zwischen 42 % und 57 %) der Betroffenen von Hate Speech bestätigten gegenüber den Studienautor*innen die Aussage: „Ich selbst beteilige mich wegen Hassrede seltener an Diskussionen im Netz." Dies führt nicht zuletzt zu einer (gefährlichen) Verkleinerung der Räume für Betroffene, ihre Meinungsäußerungsfreiheit auszuüben und somit zu einer verzerrten Mehrheitswahrnehmung im "öffentlichen Raum" des Internets.[153]

Ebenso macht die Studie deutlich, gegen welche Gruppen in Deutschland Hate Speech überproportional beobachtet wird: Dazu gehören mehrheitlich Menschen mit Migrationshintergrund, muslimische und jüdische Menschen, Geflüchtete, Frauen, Menschen, die nicht dem aktuellen Schönheitsideal entsprechen, homo- und transsexuelle Menschen, arme Menschen und Menschen mit Behinderung.[154] In der oben genannten Aufzählung finden sich alle Gruppen von *verwundbaren* Minderheiten wieder; es spiegeln sich die etablierten Ausschlusssysteme von *sex* und *gender; class, race* und *ethnicity; language, age; ability* und *lookism*.

2018 weist die UN-Sonderberichterstatterin zu Gewalt gegen Frauen, bezugnehmend auf eine Studie der Europäischen Grundrechteagentur über Gewalt gegen Frauen darauf hin, dass 23% alle Frauen berichten, Opfer von "online abuse" oder "harassment" geworden zu sein.[155] Das Pew Research Center bestätigt dies 2017 mit einem höheren Prozentsatz: „37 % of women have experienced at least one of the six behaviors this study uses to define online harassment."[156] Deutlich wird hier auch, dass Frauen auch von sexualisierter internetvermittelter Gewalt wesentlich stärker betroffen sind als Männer: „women – and especially young women – encounter sexualized forms of abuse at much higher rates than men. Some 21 % of women aged 18 to 29 report being sexually harassed online, a figure that is more than double the share among men in the same age group (9 %)."[157] Wie gravierend die Bedrohung empfunden wird, unterstreicht eine Studie von Amnesty aus dem Jahr 2017: „Alarmingly, 41 % of women who had experienced online abuse or harassment said that on at least one occasion these online experiences made them feel that their physical safety was threatened."[158]

---

[153] Daniel Geschke/Anja Klaßen/Matthias Quent/Christoph Richter, Hass im Netz – Der schleichende Angriff auf unsere Demokratie, IDZ Jena (2019), 28.
[154] Ibid 20.
[155] Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, Report for 2018, 5; die genannte Studie findet sich hier: European Union Agency for Fundamental Rights, Violence against women: an EU-wide survey, 2014.
[156] Pew Research Center, Online Harassment 2017.
[157] Ibid.
[158] Amnesty International, Amnesty reveals alarming impact of online abuse against women, 2017.

Das Thema Hate Speech hat politisch zuletzt am Fall *Lübke*[159] Fahrt aufgenommen. Betrachtet man aber das Thema Gendered Hate Speech und die Betroffenheit von Frauen, verbleibt der politische Diskurs bislang diffus. Der gesamte Kontext *Digitale Gewalt* findet bisher weder wissenschaftlich (was den Mangel an validen Daten, Zahlen und Statistiken erklärt) noch politisch und juristisch ausreichend Beachtung. Als Fortschreibung des Diskurses um Gewalt gegen Frauen sollte er aber zunehmend ins Bewusstsein gerückt werden: „Cyber violence and hate speech online against women constitute gender-based violence and are part of a continuum of violence against women starting offline and reverberating online and vice versa."[160] Digitale Gewalt kennt neben Hate Speech noch eine Vielzahl weiterer Varianten: Dazu gehören die Nutzung von Überwachungstechnologien durch (Ex-)Partner*innen ebenso wie das Doxing, Stalking und Revenge Porn.[161]

Auf europäischer Ebene wird das Thema bereits stärker in den Fokus gerückt: Das Policy Department for Citizens' Rights and Constitutional Affairs des Europäischen Parlamentes hat 2018 eine Studie zu *Cyber violence and hate speech online against women* veröffentlicht, die die wenigen validen Zahlen, Analysen und Studien über die Ausmaße von Sexist Hate Speach, über Opfer (mehrheitlich Frauen) und Verursachende (mehrheitlich Männer) zusammenführt. Im Ergebnis wird deutlich, dass es sowohl aufseiten der Datenerhebung wie der Positionierung des Themas im öffentlichen Diskurs und in der anhängenden Rechtsprechung noch deutlichen Nachholbedarf gibt.

In der Erklärung des Europarates zu den Rechten von Internetnutzer*innen betonte dieser seine besondere Verantwortung, „gender equality on the Internet" zu fördern und Genderstereotype in den Medien zu bekämpfen. Normativ geschieht dies unter anderem durch die Istanbul-Konvention, die sich auch der Rolle des kommunikationstechnologischen Sektors widmet. Auch der EGMR ist sich seiner Verantwortung, gegen Gendered Hate Speech im Netz vorzugehen, zumindest im Prinzip bewusst: In seiner Judikatur verweigert er Gendered Hate Speech als Ausdruck des Verbots des Missbrauchs der Konventionsrechte (Art 17) den Schutz oder schließt diese – in weniger offensichtlichen Fällen – nach Art 10 Abs 2 vom Schutzbereich der Konvention aus.[162]

---

[159] Der Kasseler Regierungspräsident wurde im Sommer 2019 durch einen Kopfschuss ermordet, im Nachgang stellte sich heraus, dass der Politiker aufgrund seiner positiven Haltung zur Flüchtlingspolitik der Bundesregierung schon zu Lebzeiten im Internet von Hate Speech und Doxing betroffen war. Sie ZDF, Fall Lübke.

[160] Policy Department for Citizens' Rights and Constitutional Affairs des Europäischen Parlamentes: Cyber violence and hate speech online against women, 2018, 63 ff; in eine ähnliche Richtung stoßen die Background Note on Sexist Hate Speech der Gender Equality Unit des Europarates von 2016, sowie die Studie Europarat, Combating Sexist Hate Speech.

[161] Vgl Anne Roth, CCC Congress, Dezember 2018, und beim CCC Camp im August 2019, Was tun gegen digitale Gewalt gegen Frauen?

[162] EGMR, Informationsblatt Hate Speech, 2019, 1.

Das NetzDG ist im Umgang mit Sexist Hate Speech wenig wirksam; die Transparenzberichte der Plattformanbieter sagen nichts über eine mögliche Genderdimension der gemeldeten Äußerungsdelikte aus. Vielmehr müsste das bestehende deutsche Strafrecht gefährdungssensibel nachjustiert werden. So auch der Deutsche Juristinnenbund in seiner Analyse des NetzDG: „Der djb hält zum Schutz der Persönlichkeitsrechte von Frauen im Netz und zur Bekämpfung digitaler Gewalt gegen Frauen ein Gesamtpaket von Maßnahmen für dringend erforderlich. Das NetzDG ist dabei nur ein Baustein.“[163]

Positiv zu bewerten sind bewusste Versuche, die Sichtbarkeit von Frauen zu erhöhen und feministisch informierten Diskursen mehr Raum zu geben.[164] Feministische Blogs bieten Resonanzräume für progressive feministische Diskurse, Räume zum Austausch, zur Unterstützung und Vernetzung. Feministische Archive leisten ebenfalls einen großen Beitrag zu Sichtbarkeit und Pluralisierung von (weiblicher) Geschichte. Aktivismen via feministischen Hashtags auf Online-Medien stehen in der Tradition feministischer Praktiken der Sensibilisierung für Fragen von Ungleichheit und Diskriminierung: Berichte von sexueller und rassistisch motivierter Gewalt zwingen dem digitalen Raum durch die öffentliche Erzählung der eigenen Erlebnisse ihre offenkundige Realität auf und schaffen sich so Sichtbarkeit. Diese neuen politischen, transnationalen Öffentlichkeiten bieten mannigfaltige Möglichkeiten zum Sichtbar-Machen und Speichern von marginalisiertem Wissen. Dabei wird nicht nur neues Wissen produziert, vielmehr werden hegemoniale Wissenshierarchien in Frage gestellt.

Positiven Beispielen zum Trotz (darunter die Stärkung von Hashtag-Bewegungen, Möglichkeit für schnelle und globale Mobilisierungs- und Aufklärungskampagnen, die Destabilisierung von hegemonialen Wissenshierarchien und die Raumnahme von feministischen informierten antihegemonialen Narrativen), stärkt das Internet auch bestehende und tradierte Macht- und Ausgrenzungssysteme.

[163] Pressemitteilung des Deutschen Juristinnenbundes vom 15.05.2019: Hate speech und digitale Gewalt haben eine Geschlechterdimension.

[164] Neue Allianzen, die vor allem um Sichtbarkeit von Frauen*themen und Frauen* bemüht sind: zB die Speakerinnenliste oder das Womens Experts' Network, D64 verweisen in ihren Veranstaltungsankündigungen längst auf die Verteilung von Sprecher*innenrollen. Vgl. auch zur verstärkten Sichtbarkeit von Aktivistinnen zB re:publica 2019: Opening Keynote von Nanjira Sambuli (intersektionale Perspektive für einen gleichberechtigten Zugang zum Internet); ebenda Caroline Sinders und ihr ''Feminist Data Set". Auch netzpolitk.org hat unlängst eine Feminismus-Sparte um Chris Köver etabliert.

7. Wie können die Rechte von MenschenrechtsverteidigerInnen, AktivistInnen, JournalistInnen und politischen Oppositionellen weltweit in Zukunft besser im digitalen Raum geschützt werden? (FDP)

Hierzu verweise ich auf meine Empfehlungen zu Fragen 1-6 und pointiere noch einmal, dass es von besonderer Bedeutung ist,

- in allen Stellen der Bildungs- und Erwerbsbiographien den umfassenden Schutz der Grund- und Menschenrechte auch in der digitalen Sphäre zu verankern,
- regierungsseitig international für den Schutz von Menschenrechten aller und eine teilhabeorientierte Reform der globalen Internet Governance-Infrastrukturen einzutreten,
- auf Ebene der Gesetzgebung Menschenrechtsverträglichkeitsprüfungen aller Gesetze mit Internetbezug vorzusehen, Verschlüsselungs- und Anonymisierungssoftware nicht zu verbieten oder zu kriminalisieren, digitale Gewalt und intersektionelle Diskriminierung stärker zu berücksichtigen;
- Unternehmen verstärkt in die Verantwortung zu nehmen, ihre zunächst privaten Hausrecht unterliegenden Räume einer menschenrechtssensiblen Governance von Meinungsäußerungen zu unterwerfen, die auf Regeln beruht, die so offen wie möglich entstehen und in Verfahren einheitlich und erklärbar angewandt werden, die Rechtsschutzmöglichkeiten für Betroffene vorsehen;
- Plattformen im Hinblick auf ihre Zusammenarbeit mit autoritären Regimen rechenschaftspflichtig zu machen; und
- die Zivilgesellschaft und die Opferverbände zu stärken.

8. Wie können wir die politische Beteiligung im digitalen Zeitalter fördern und gleichzeitig Menschenrechte schützen, und welche neuen Möglichkeiten bieten digitale Technologien für den Schutz der Menschenrechte und die Stärkung politischer Beteiligung, ohne die am meisten benachteiligten Menschen zurückzulassen? (DIE LINKE.)

Zu den Möglichkeiten der verstärken Teilhabe am Internet verweise auf meine Ausführungen zu Frage 1. Zur Genderdimension verweise ich auf meine Ausführungen zu Frage 6.

Insbesondere zur Förderung von besonders benachteiligten Menschen sei noch ergänzt, dass schon der Zugang zum Internet eng verknüpft ist mit der Frage des Zugangs zu materiellen wie immateriellen Ressourcen. Diese sind ungleich verteilt, darauf machen u.a. feministische und anti-rassistische Bewegungen schon lange aufmerksam: Frauen, BIPoC (Black, Indigenous, and

People of Colour) und LGBTIQA+-Rechteverteidiger*innen kritisieren sowohl begrenzte Zugangschancen und Teilhabemöglichkeiten, schlechtere Chancen auf Bildung sowie die geringere Beteiligung an Entscheidungsprozessen und Machtpositionen. Diese ungleiche Verteilung der Ressourcen wird durch die Digitalisierung zunehmend sichtbar und verschärft.

Am Beispiel Digitale Gewalt und Hate Speech wird deutlich, dass der öffentliche digitale Raum für Frauen, BIPoC und LGBTIQA+-Personen ein weitaus gefährlicherer Ort ist als für andere Gruppen. Sich überlappende Formen der Diskriminierung aufgrund von Geschlecht, ethnischer Zugehörigkeit, Hautfarbe oder sexueller Identität sind in sozialen Medien vielfach festzustellen. Digitale Gewalt betrifft insbesondere marginalisierte Gruppen: Sexismus, Rassismus, Antisemitismus, Ableismus, Islamophobie, Antiseminitismus, Trans- und Homophobie prägen diesen Komplex. Intersektional betrachtet wird schnell deutlich, dass mehrfache „Unterschiedlichkeiten" das Diskriminierungspotenzial noch erhöhen. Amnesty International hat für das Internet festgestellt, dass schwarze Frauen zum Beispiel deutlich häufiger von Hate Speech auf Twitter betroffen sind als weiße Frauen.[165] Dies schließt digital wie analog Betroffene aus diskursiven Räumen aus, hindert sie daran, ihre Meinungsäußerungsfreiheit auszuüben, und führt letztlich zu einer verzerrten Mehrheitswahrnehmung. Sozioökonomische Benachteiligungen, Brüche in der Bildungs- und Erwerbsbiographie, Pflege- und Careverantwortung sind auch für die Nutzung der internetvermittelten Kommunikation entscheidende Diskriminierungsfaktoren, die bei Politiken zur Bekämpfung von Diskriminierung in allen Planungsstufen mitgedacht werden müssen.

Dies betrifft nicht nur die Formulierung von Politiken und den Beschluss von Gesetzen. Gerade in Hinblick auf alltagsweltliche Diskriminierungserfahrungen üben die Affordanzen von Computerprogrammen eine normative Wirkung aus. Diskriminierende Stereotype manifestieren sich im Code.[166] Es ist hinlänglich bekannt, dass biometrische Gesichtserkennung lange nicht in der Lage war, People of Colour zu identifizieren, da sie sich überwiegend auf Trainingsdatensätze weißer Personen stützte. Gebündelt als Big Data werden tradierte Ausschlusssysteme so implizit in den Code eingeschrieben. Ähnlich verhält es sich mit KI-Trainingsdatensätzen für autonome Fahrzeuge, die Trainingsdaten von nicht-normierten Körpern wie Rollstuhlfahrer*innen nicht berücksichtigen.[167]

[165] "In the case of online violence and abuse, women of colour, religious or ethnic minority women, lesbian, bisexual, transgender or intersex (LBTI) women, women with disabilities, or non-binary individuals who do not conform to traditional gender norms of male and female, will often experience abuse that targets them in a unique or compounded way" (Amnesty International, Online Violence against Women (2018), Kap. 2).

[166] Vgl. zB Nicole Shepard, Was hat Überwachung mit Sex und Gender zu tun?, 2017. In: Denknetz-Jahrbuch 2017 - Technisierte Gesellschaft, 108-116.

[167] Vgl. Nicole Shephard, 5 reasons why surveillance is a feminist issue, 2016.

C. Soziale Medien und Meinungsfreiheit

Frage 9: Zur Bedeutung von „Hass“ und „Hetze“ im Internet und zur Frage, ob diese als prozessverwertbare Vorwürfe eingesetzt werden können (AfD)

Bei den Begriffen „Hass“ und „Hetze“ handelt es sich um Begriffe, die keinen direkten Anknüpfungspunkt zu Straftatbeständen aufweisen. Allerdings wurde das NetzDG erlassen, um „Hasskriminalität“ im Netz zu bekämpfen. In § 1 III NetzDG wird auf Straftatbestände verwiesen, die konkretisieren, was „Rechtswidrigkeit“ im Sinne des NetzDG bedeutet. Darunter finden sich keine mit Hass und Hetze direkt äquivalenten Tatbestände. Äußerungen, die sich als „Hassrede“ charakterisieren lassen, sind in Deutschland u.a. als Volksverhetzung nach § 130 StGB strafbar.[20] Auch Straftatbestände wie die öffentliche Aufforderung zu Straftaten (§ 111 StGB), die Beleidigung (§ 185 StGB) und die Bedrohung (§ 241 StGB) sind je nach Sachverhaltskonstellation möglich.[168] Schutzgut der § 185 ff StGB ist das allgemeine Persönlichkeitsrecht, das auch durch Artikel 1 I und 2 I GG geschützt wird.

Zur Illustration: Am 4.6.2020 berichte Heise Online über den Mordfall Walter Lübcke unter der Überschrift: „Bundesweite Durchsuchungen wegen Internet-*Hetze*“, präzisiert dann aber: „40 Personen werden Aufforderung und Billigung von Straftaten sowie Verunglimpfen des Andenkens Verstorbener vorgeworfen.“ Insbesondere werde gegen 40 Personen bundesweit wegen der öffentlichen Aufforderung zu Straftaten (§ 111 StGB), der Billigung von Straftaten (§ 140 StGB) und des Verunglimpfens des Andenkens Verstorbener (§ 189 StGB) ermittelt.[169]

Im Einzelnen schützt § 185 StGB schützt vor Angriffen auf die Ehre durch Kundgabe von rechtswidrigen Meinungen in Form der Nicht-, Gering- oder Missachtung. § 186 StGB schützt vor übler Nachrede. Während § 185 StGB vor Beeinträchtigungen der Meinungsäußerung schützt, knüpft § 186 StGB an Tatsachenbehauptungen an. Sanktioniert wird hier das Behaupten oder Verbreiten ehrenrühriger, nicht beweisbarer Tatsachen über den Betroffenen. Strafschärfend gem. § 187 StGB ist die Verbreitung unwahrer Tatsachen wider besseres Wissen. Ebenso strafschärfend gem. § 188 StGB ist, wenn „Personen des politischen Lebens“ unter besonderen Voraussetzungen betroffen sind. Diese müssten jedoch im Rahmen des § 185 StGB im Vergleich zu normalen Bürgern ein besonders hohes Maß an kritischen Äußerungen ertragen.

Eine als „Hass“ oder „Hetze“ beschreibbare Äußerung muss sich an den strafrechtlichen Grenzen der Äußerungsdelikte der § 185 ff. StGB messen lassen. Insofern ändern die

[168] Ausarbeitung des Wissenschaftlichen Dienstes des Bundestags, Behandlung von „Hate Speech“ vor 2015 YouTube, Facebook und Twitter, WD 10 – 3000 – 045/19 (2019).
[169] Andreas Wilkens, Mordfall Walter Lübcke: Bundesweite Durchsuchungen wegen Internet-Hetze, Heise Online, 4.6.2020.

Begrifflichkeiten nichts an der strafrechtlichen Bewertung und damit nichts an der Möglichkeit, diese vor Gericht gelten zu machen.

Verletzungen des allgemeinen Persönlichkeitsrechts werden zivilrechtlich über den quasi-negatorischen Unterlassungsanspruch nach §§, 823, 1004 analog geltend gemacht. Andere heute ebenso geladene Sachverständige haben in der Vergangenheit erreicht, dass soziale Medien Meinungsäußerungen wiederherstellen müssen, die keinen Straftatbestand erfüllen, aber möglicherweise gegen Gemeinschaftsstandards (Community Standards/Nutzungs-bedingungen) der sozialen Medien verstoßen. Mittlerweile habt sich eine Vielzahl an Gerichten mit der Frage der Wiederherstellung von Inhalten oder der Entsperrung von Nutzer*innenkonten beschäftigt.

Beispielhaft seien zwei Entscheidungen gegenübergestellt (LG Frankfurt, Beschluss vom 14. Mai 2018 und OLG Karlsruhe, Beschluss vom 28.2.2019). Das LG Frankfurt hält fest, dass ein Betreiber eines sozialen Netzwerks seine Verhaltensregeln grundsätzlich auch durch Entfernung eines rechtswidrigen Inhalts oder durch Sperrung eines Nutzer*innenaccounts durchsetzen könne. Der Vertrag zwischen Nutzer*in und Plattformbetreiber beinhaltete jedoch Schutzpflichten des Plattformbetreibers gemäß § 241 Abs. 2 BGB, in deren Rahmen - im Wege der mittelbaren Drittwirkung - die Grundrechte der Betroffenen berücksichtigt werden müssten. Voraussetzung einer Sperre sei daher, dass diese sachlich gerechtfertigt und nicht willkürlich sei. Eine Sperre und Löschung wegen einer Äußerung sind dann nicht gerechtfertigt, wenn die Äußerung von der Meinungsfreiheit gedeckt sei. Solange eine Meinungsäußerung keine „Hassrede“ ist, muss sie nicht gelöscht werden. Das OLG Karlsruhe hält fest, dass das Grundrecht der Meinungsfreiheit der Nutzer*innen soziale Netzwerke nicht unmittelbar verpflichte, aber Ausstrahlungswirkung habe und im Rahmen zivilrechtlicher Generalklauseln und unbestimmter Rechtsbegriffe bei der Auslegung zur Geltung zu bringen sei. Daher dürfe Facebook den Beitrag von Nutzer*innen nur löschen, wenn „die (strafrechtlichen) Grenzen zulässiger Meinungsäußerung“ überschritten seien. Dazu gehöre auch, wenn die „Äußerung als „Hassrede“ zu qualifizieren sei“ (dies nach den Gemeinschaftsstandards). Facebook müsse für „Hassrede“ seine Plattform auch unter Berücksichtigung der Meinungsfreiheit des Nutzers nicht zur Verfügung stellen.

Die Qualifikation einer Äußerung als „Hassrede“ ist also ein „prozessverwertbarer Vorwurf“ im Sinne der Frage, als er es sozialen Netzwerken ermöglicht, den Inhalt zu löschen (bzw. diese dazu sogar nach NetzDG verpflichtet sein können). Das Verbot und die Definition der „Hassrede“ im Gemeinschaftsstandard halten, so auch das OLG Karlsruhe, der rechtlichen Überprüfung als allgemeine Geschäftsbedingungen stand.[170]

[170] Kettemann/Tiedeke, Back up: can users sue platforms to reinstate deleted content?. Internet Policy Review 9 (2020) 2, DOI: 10.14763/2020.2.1484.

Frage 10: Manipulieren Plattformen wie Google, Facebook und Twitter in Deutschland das politische Klima ebenso, wie es Whistleblower in den USA („unconscious bias“, wie beschrieben von Dr. Robert Epstein) aufdecken konnten? (AfD)

Nein. Diese Frage beruht auf falschen Annahmen, sie ist tendenziös und verwendet Begriffe sinnwidrig. Das „politische Klima“ ist als Begriff diffus. Der Vorwurf der Manipulation setzt voraus, dass es ein natürliches politisches Klima gebe. Jede Zeitung trifft herausgeberische Entscheidungen, für die sie sich medienethisch und ggf. medienrechtlich verantworten muss. Wenn eine große Boulevard-Zeitung eine Kampagne gegen Christian Drosten startet, liegt darin eine „Manipulation“ bzw. der Versuch, „das politische Klima“ zu manipulieren?

Fest steht, dass Social-Media-Plattformen wie z.B. Facebook, Twitter, YouTube oder TikTok als User-Generated-Content-Unternehmen (UGC-Unternehmen) stark von menschlichen wie algorithmischen Inhaltsmoderationssystemen abhängig sind.[171] Algorithmen im Allgemeinen und ACM-Systeme im Besonderen werden als hocheffektives Steuerungsinstrument angesehen, da sie die Kosten senken.[172]

Soziale Plattformen haben eigenständige normative (rechtliche) Ordnungen entwickelt.[173] Sie dürfen (innerhalb des rechtlichen Rahmens) eigene Normen setzen (hierzu schon oben bei Frage 9). Sie können die Inhalte auf ihren Plattformen beeinflussen, so sie ihre Nutzer*innen gleichbehandeln, und diese nicht willkürlich löschen (in Deutschland,[174] anders aber in den USA, wo das “Hausrecht” noch breiter verstanden wird[175]). Ob dies angesichts der wachsenden Rolle von Plattformen für die öffentliche Kommunikation ein Problem darstellt, auf das das Recht reagieren sollte, wurde auch im Zusammenhang mit dem neuen Medienstaatsvertrag, der gewisse vielfaltsbezogene Vorschriften für Intermediäre enthält, kontrovers diskutiert.

[171] Gorwa, Robert; Binns, Reuben, Katzenbach, Christian, ‘Algorithmic content moderation: Technical and political challenges in the automation of platform governance’ Big Data & Society, 2020 p. 3, DOI: 10.1177/2053951719897945

[172] Schwarz, Ori, ‘Facebook rules: structures of governance in digital capitalism and the control of generalized social capital’, Theory, Culture & Society, p. 7.

[173] Kettemann/Schulz, Setting Rules for 2.7 Billion. A (First) Look into Facebook’s Norm-Making System: Results of a Pilot Study (Hamburg: Working Papers of the Hans-Bredow-Institut, Works in Progress # 1, January 2020).

[174] Kettemann/Tiedeke, Back up: can users sue platforms to reinstate deleted content?. Internet Policy Review 9 (2020) 2.

[175] Ibid.

Die angesprochene „Studie“[176] ist methodisch so fehlerhaft, dass sie nicht erstgenommen werden kann. Sie ist eine nicht peer-reviewte, in keiner wissenschaftlichen Zeitschrift erschiene Eigenveröffentlichung von Robert Epstein und Ronald E. Robertson. Die beiden Autoren behaupten, dass durch Manipulation der Suchmaschinenergebnisse bei Google bis zu 2.6 Mio Menschen in ihrer Wahlentscheidung beeinflusst worden seien. Sowohl Journatlist*innen[177] als auch Wissenschaftler*innen[178] haben auf die methodischen Defizite der Studie hingewiesen, die sie nicht replizierbar machen. Ihre Ergebnisse sind nicht belastbar. Insbesondere[179] hatte die Studie keinerlei Zugriff auf die „Entscheidungsgrundlage“ von Googles Suchalgorithmus, was z.B. durch eine Rekonstruktion von PageRank Werten durch einen extensiven Crawl relevanter Websites und deren Verlinkungen oder die Erhebung von Klickzahlen in experimentellen Settings möglich gewesen wäre. Damit kann die Studie keinen „Bias“ bei Google feststellen. Ein Vergleich mit anderen Suchmaschinen erlaubt nur die Feststellung von Unterschieden, die z.B. durch das Verhalten von Google-Nutzer*innen oder den Fokus von Suchmaschinen-optimierungstechnologien (SEO) auf Google erklärt werden können. Dazu blendet die Studie den Einfluss von SEO vollkommen aus: Wenn jemand aktiv versucht, Suchergebnisse zu manipulieren, dann sind dies wohl zunächst die Seitenbetreiber selbst. Die Teilnehmer*innen wurden durch eine „crowdsourcing website“ gewonnen. Die Autoren machen keine Angaben dazu, wie sie dort möglichen Bias kontrolliert haben (z.B. Demographie, politische Präferenzen, Persönlichkeitstest, etc.). Sehr problematisch ist auch der Ausschluss aller Teilnehmer*innen, die Gmail benutzen. In der Studie finden sich keine Angaben, wieviele Daten dadurch ausgeschlossen wurden. Schon das macht das Ergebnis bestenfalls zur Grundlage für weitere Studien.

Aktuelle Studien zeigen darüber hinaus, dass die Rolle, die soziale Medien bei Wahlentscheidungen und Wahlen spielen, tendenziell überschätzt wird.[180] Viele Sortierungs-Algorithmen führen sogar dazu, dass sozial-homophile (sich ähnelnde) Minderheitenmeinungen von sich selbst und von sozial-heterophilen (ideenpluralistischeren) Mehrheiten in der Größe eher überschätzt werden. Die Homophilie kann Minderheitengruppen benachteiligen, indem sie ihre Fähigkeit einschränkt, Verbindungen zu einer Mehrheitsgruppe herzustellen oder Zugang zu

[176] Robert Epstein und Ronald E. Robertson, A Method for Detecting Bias in Search Rankings, with Evidence of Systematic Bias Related to the 2016 Presidential Election, White Paper of the American Institute for Behavioral Research and Technology, 1.6.2017.
[177] Qiu in New York Times, 2019.
[178] Algorithmwatch, Working Paper 2017.
[179] Dieser Abschnitt hat von Hinweisen von Felix Victor Münch profitiert.
[180] Vgl. Richard Fletcher, Nic Newman and Anne Schulz, A Mile Wide, an Inch Deep: Online News and Media Use in the 2019 UK General Election, Digital News Project 2020. Reuters Institute for the Study of Journalism at Oxford University; A.W. Geiger, Key findings about the online news landscape in America, Pew Research Centre, 2019 .

neuartigen Informationen zu erhalten.[181] Suchalgorithmen können daher eher zu einer positiv zu bewertenden Diversifizierung des Informationsangebots beitragen.[182] Diese Diversifizierung scheint von User*innen auch gewünscht zu werden.[183]

Der Begriff „unconscious bias" wird von Robert Epstein in der Studie nicht erwähnt. Überhaupt scheint der Begriff in den vorgelegten Fragen falsch gebraucht zu werden. Unter „unconscious bias" versteht man eine unbewusste Voreingenommenheit, eine verzerrte Sicht auf die Welt, die unser Urteilsvermögen durch *Biases* reduziert und uns in unseren Interaktionen mit anderen Menschen beeinflusst. Wie die Harvard Business Review in einer Analyse von Facebooks „Unconcious Bias Training"[184] ihrer Mitarbeiter*innen schreibt:

> „Jahrzehntelange Forschung zeigt uns, dass systematische Fehler unser Urteilsvermögen und unsere Entscheidungen bei der Arbeit sowie die Art und Weise, wie wir mit anderen interagieren, beeinflussen. Und einige dieser Voreingenommenheiten sind unbewusst, einschließlich der Diskriminierung aufgrund von Rasse, Geschlecht und Einkommen. Die Folgen solcher tückischen Voreingenommenheiten können für eine Organisation recht kostspielig sein, von der Veranlassung, die falschen Kandidaten einzustellen oder zu befördern, bis hin zur Investition in weniger innovative Ideen, nur weil derjenige, der sie vorgeschlagen hat, ethische Grenzen überschritten hat."[185]

Ein charakteristischer *Bias* etwa ist der *Performance Bias*, der dann Wirkung entfaltet, wenn Personen, die zu gesellschaftlich dominanten Gruppen gehören, nach ihrem Potenzial beurteilt werden, während Personen, die zu weniger dominanten Gruppen gehören, nach ihren erbrachten Leistungen beurteilt werden. Dies gilt auch für die Leistungszuschreibung (hat jemand aus *Glück* oder wegen *Talents* Erfolg) und den Sympathie-Bias: Wahrnehmung von Erfolg und gefühlte Sympathie korrelieren bei Männern positiv, bei Frauen häufig negativ.

Wir müssen – in Schulen, am Arbeitsplatz, im Bundestag – sicherstellen, dass *Biases* aufgedeckt, benannt und bekämpft werden, um ihre negativen Folgen abzufedern. Zunächst muss das Bewusstsein für die Existenz von *Biases* erhöht werden. Dies geht gut über Schulungsprogramme, die auf einer vorgeschalteten Testung der eigenen Voreingenommenheit basieren.[186] Als erfolgreiche Strategien gegen „unconscious bias" haben sich in der Forschung die Perspektivenübernahme (Übernahme der Perspektive eines Mitglieds einer stigmatisierten

[181] Fariba Karimi, Mathieu Génois, Claudia Wagner, Philipp Singer & Markus Strohmaier, Homophily influences ranking of minorities in social networks, Nature, Scientific Reports (2018) 8:11077 | DOI:10.1038/s41598-018-29405-7.

[182] Fabrizio Germano, Vicenç Gómez, and Gaël Le Mens. 2019. The few-get-richer: a surprising consequence of popularity-based rankings. In Proceedings of the 2019 World Wide Web Conference (WWW '19), May 13–17, 2019, San Francisco.

[183] Camille Roth, Algorithmic Distortion of Informational Landscapes, Intellectica (2019).

[184] Facebook, Managing Unconscious Bias (2015).

[185] Francesca Gino, What Facebook's Anti-Bias Training Program Gets Right, Harvard Business Review, 24.8.2015 (eigene Übersetzung).

[186] Harvard University, Project Implicit, Implicit Association Test (2011)

Gruppe), die Kontaktaufnahme (durch persönliches Gespräch) und die Individualisierung (bewusste Behandlung/Bewertung anderer nach ihren persönlichen Eigenschaften statt nach stereotypen Merkmalen) erwiesen. Biases können bewusst *verlernt* werden. Francesca Ginon (Harvard University) berichtet, dass in einer Studie die vorurteilsbehafteten Einstellungen „mindestens zwei Monate lang gering" blieben: "So können unbewusste Vorurteile, wie eine schlechte Angewohnheit, verlernt werden, aber es bedarf einiger bewusster Anstrengungen."[187]

Während nicht empirisch belegbar ist, dass Plattformen das politische Klima „manipulieren", ist mehr Forschung zum Einfluss von Plattformen und Suchmaschinen auf Meinungsbildungsprozesse in einer demokratischen Gesellschaft notwendig. Diese muss allerding erkenntnisgeleitet, replizierbar und methodisch belastbar sein und einer Peer Review standhalten. Darüber hinaus sind Biases in jedem sozialen Setting zu bekämpfen. Ein erster Schritt dazu ist es, deren Bestehen wahrzunehmen. Als effektive Ansätze gegen unbewusste Voreingenommenheit („unconscious bias") haben sich in der Forschung entstereotypsierende Interventionen erwiesen, wie die Perspektivenübernahme und die Individualisierung.

D. Regulierung des internationalen Handels mit digitalen Technologien

11. Autokratien und Diktaturen nutzen u. a. aus europäischen Ländern stammende Überwachungssoftware, um Journalisten, Bürgerrechtler, Menschenrechtsverteidiger u. a. zu „durchleuchten" und zu überwachen – oft mit gravierenden persönlichen Folgen für die Betroffenen. Bedarf es hier weiterer Vorgaben für den Export von Überwachungssoftware? (SPD)

12. Welche Notwendigkeit einer Regulierung von Gesichtserkennung bei ihrer (Weiter-)Entwicklung, Anwendung und Exportkontrolle sehen Sie, und wie könnte eine solche Regulierung auf nationalstaatlicher, supranationaler und internationaler Ebene oder unter Akteuren der Privatwirtschaft aussehen? (BÜNDNIS 90/DIE GRÜNEN)

Ich beantworte diese Fragen gemeinsam mit einem Schwerpunkt auf Exportkontrolle, ohne in die Tiefe gehen zu können. Wie medialen Berichten zu entnehmen ist, scheint die deutsche Exportkontrolle für Digitalwaffen nicht vollumfänglich wirksam zu sein.[188] Zwar kontrolliert das

[187] Francesca Gino, What Facebook's Anti-Bias Training Program Gets Right, Harvard Business Review, 24.8.2015 (eigene Übersetzung).
[188] ZEIT ONLINE, Exportkontrolle von Digitalwaffen funktioniert nicht.

Bundeswirtschaftsministerium die Ausfuhr von Technik zur Überwachung von digitalen Endgeräten und wendet über die Kontrollen im Wassenaar-Abkommen und in der Dual-Use-Verordnung hinaus nationale Kontrollen an, die sich auch auf Dienstleistungen in Zusammenhang mit genehmigungspflichtiger Überwachungstechnik beziehen,[189] doch finden immer noch Exporte statt. Ein Grund dafür kann in der langen Bearbeitungsdauer liegen.

Ende 2019 kritisierte die Gesellschaf für Freiheitsrechte die mangelnde effiziente Strafverfolgung, die auch auf „komplizierte transnationale Firmenstrukturen" zurückzuführen sei, und erstattete Anzeige bei der Staatsanwaltschaft München gegen die Geschäftsführer der Unternehmensgruppe FinFisher wegen Verkaufs von Überwachungssoftware an die Türkei unter Umgehung des Außenwirtschaftsgesetzes.[190]

Auch auf europäischer Ebene erscheint die Rechtslage nicht befriedigend. Ein positiver Ansatz, die Nutzung europäischer Software zu stoppen, um Menschenrechtsverteidiger*innen im Ausland auszuspähen, wurde durch die *Strategie für digitale Freiheit in der EU-Außenpolitik* vorgesehen, die vom Europäischen Parlament bereits im Dezember 2012 verabschiedet wurde.[191] Die Strategie "bedauert die Tatsache, dass von der EU hergestellte Technologien und Dienste manchmal in Drittländern genutzt werden, um die Menschenrechte zu verletzen, und zwar durch Zensur von Informationen, Massenüberwachung, Monitoring und das Aufspüren und Verfolgen von Bürgern und ihren Aktivitäten in (Mobil-)Telefonnetzen und im Internet".[192] Die Kommission wird aufgefordert, diesen „digitalen Waffenhandel" zu unterbinden.

Langjährige Versuche, auf EU-Ebene eine zufriedenstellende Lösung zu erreichen, sind indes zuletzt 2019 gescheitert. Während Kommission und Parlament stärkere Kontrollen und mehr Transparenz vorsehen wollten, lehnten dies die Mitgliedstaaten – darunter Deutschland[193] – ab.[194] Eine menschenrechtsorientierte Beobachtung des weiteren Rechtsetzungsprozesses, besonders der Einflussmöglichkeiten des Europäischen Parlamentes im Trilog, ist hier besonders wichtig.

---

[189] Bundesministerium für Wirtschaft und Energie, Außenwirtschaftsrecht – Kontrolle des Exports von Waffentechnik.

[190] Gesellschaft für Freiheitsrechte, Export von Überwachungssoftware (Luisa Podsadny, 4. September 2019), GFF und Partner erstatten Anzeige gegen Münchener Firmen wegen illegaler Exporte von Überwachungssoftware an die Türkei.

[191] European Parliament (11 December 2012), Resolution on a digital freedom strategy in EU foreign policy, 2012/2094(INI).

[192] Ibid., p. 22.

[193] Daniel Moßbrucker, Überwachungsexporte: Bundesregierung stellt Industrie vor Menschenrechte, Netzpolitik.org, 29.10.2018.

[194] Daniel Moßbrucker, EU-Staaten lehnen einstimmig schärfere Exportkontrollen für Spähsoftware ab, Netzpolitik.org, 16.7.2019.

Positiv zu bewerten ist, dass im Sommer 2019 die Bundesregierung erstmals auf Frage der Vorsitzenden dieses Ausschusses Zahlen zu den nach dem Außenwirtschaftsgesetz genehmigten Exporten genannt hat.[195] So wurden seit 2015 Einzelausfuhrgenehmigungen für Dual-Use-Güter aus dem Bereich der Überwachungstechnologie nach der Güternummer 5A001.f EU Dual-Use-Verordnung („Telekommunikationsüberwachung“) wie folgt genehmigt:[196]

Jahr	Endbestimmungsland	Anzahl	Wert in Euro
2015	Algerien	1	1.500.000
	Libanon	2	2.361.734
	Marokko	1	310.000
	Vereinigte Arabische Emirate	1	699.206
2016	Dänemark	1	135.000
	Saudi-Arabien	1	1.142
2017	Indien	1	7.628.670
	Jordanien	1	5.361.929
	Libanon	1	365.700
	Tunesien	1	1.335.970
2018	Indien	1	0*
2019 (bis 11.06.)	Israel	1	1*

* Systembedingte Buchungswerte

Weiters wurden nach Güterlistenposition 5A902 AWV (Überwachungszentren und Vorratsdatenspeicherungssysteme oder -geräte für Ereignisdaten) genehmigt[197]:

Jahr	Endbestimmungsland	Anzahl	Wert in Euro
2015	Ägypten	1	1.764.388
	Katar*	1	178.882
	Kosovo	1	460.000
2016	Brunei Darussalam	1	1.125.772
	Katar*	1	536.646
	Montenegro	1	76.100
	Oman*	1	341.130
2017	Indonesien	3	1.606.043
2018	Indonesien	2	22.256
	Katar*	1	563.196
2019 (bis 1.06.)	Ägypten*	1	124.000
	Brunei Darussalam*	1	153.321

* Genehmigung steht in Zusammenhang mit früheren Vorgängen und zum Teil sich daraus ergebenden Folgeverpflichtungen der Unternehmen (insbesondere rechtliche z. B. Gewährleistung).

Es ist festzustellen, dass die Anzahl der genehmigten Einzelausfuhrgenehmigungen abnimmt. Darüber hinaus weist die Bundesregierung in ihrer Antwort darauf hin, dass die

[195] Schriftliche Fragen mit den in der Woche vom 17. Juni 2019 eingegangenen Antworten der Bundesregierung, Deutscher Bundestag – 19. Wahlperiode – 19 – Drucksache 19/11017, Fragen von Abgeordnete Gyde Jensen (FDP), Fragen 33-35.
[196] Ibid., S. 20.
[197] Ibid., S. 21.

Güterlistenposition „Überwachungszentren und Vorratsdatenspeicherungssysteme oder -geräte für Ereignisdaten“ 2015 als „zusätzliche nationale Maßnahme eingeführt“ worden sei, weltweit einzigartig sei und die Bundesregierung damit über europa- und völkerrechtliche Vorgaben zur Kontrolle der Ausfuhr von Gütern der Telekommunikationsüberwachung hinausgehe. 2019 wurde – soweit ersichtlich – keine neue Genehmigung erteilt. Allerdings ist darauf hinzuweisen, dass auch „Folgeverpflichtungen“ von Unternehmen aus genehmigten Exporten nicht die Verantwortung einer Kontrolle ersetzen, zumal sich Rechtslage wie politische Umstände wandeln können.

Der UN-Sonderberichterstatter für Meinungsäußerungsfreiheit, David Kaye, rief 2019 zu einem Moratorium für den Verkauf, Transfer und die Nutzung von Überwachungstechnologie auf, bis ein menschenrechtlich abgesicherter Rahmen national und international konsentiert sei.[198] Ich gebe seine Empfehlungen[199], denen ich mich anschließe, wieder:

> “66. For States:
>
> (a) States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place;
>
> (b) States that purchase or use surveillance technologies (“purchasing States”) should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity and legitimacy of objectives, and establish legal mechanisms of redress consistent with their obligation to provide victims of surveillance-related abuses with an effective remedy;
>
> (c) Purchasing States should also establish mechanisms that ensure public or community approval, oversight and control of the purchase of surveillance technologies;
>
> (d) States that export or permit the export of surveillance technologies (“exporting States”) should ensure that the relevant government agencies solicit public input and conduct multi-stakeholder consultations when they are processing applications for export licences. All records pertaining to export licences should be stored and made available to the greatest extent possible. They should also establish safe harbours for security research and exempt encryption items from export control restrictions;

[198] UN, UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools, 28.5.2019.
[199] David Kaye, Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 28.5.2019, UN Doc. A/HRC/41/35.

(e) Exporting States should join the Wassenaar Arrangement and abide by its rules and standards to the extent that these are consistent with international human rights law;

(f) States participating in the Wassenaar Arrangement should develop a framework by which the licensing of any technology would be conditional upon a national human rights review and companies' compliance with the Guiding Principles on Business and Human Rights. Such a framework could be developed through a specially established human rights working group. Additionally, they should set clear and enforceable guidelines on transparency and accountability with respect to licensing decisions, surveillance-related human rights abuses and the treatment of digital vulnerabilities.

67. For companies:

(a) Private surveillance companies should publicly affirm their responsibility to respect freedom of expression, privacy and related human rights, and integrate human rights due diligence processes from the earliest stages of product development and throughout their operations. These processes should establish human rights by design, regular consultations with civil society (particularly groups at risk of surveillance), and robust transparency reporting on business activities that have an impact on human rights;

(b) Companies should also put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. These safeguards include contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law, technical design features to flag, prevent or mitigate misuse, and human rights audits and verification processes;

(c) When companies detect misuses of their products and services to commit human rights abuses, they should promptly report them to the relevant domestic, regional or international oversight bodies. They should also establish effective grievance and remedial mechanisms that enable victims of surveillance-related human rights abuses to submit complaints and seek redress.

…

69. For all stakeholders: States, the private sector, civil society and other relevant stakeholders should establish co-regulatory initiatives that develop rights-based standards of conduct for the private surveillance

> industry and implement these standards through independent audits, and learning and policy initiatives."

Die Prozesse der Exportkontrolle hinsichtlich Digitalwaffen und Überwachungssoftware scheinen optimierbar. Lange Genehmigungsdauern verleiten Unternehmen zu Umgehungsgeschäften. Jedenfalls sollte besonderes Augenmerk auf die Transparenz gelegt werden.

Annex

Die UNESCO Internet Universalitäts-Indikatoren

Ein Rahmen zur Bewertung der Entwicklung des Internets[200]

Kontextbezogene Indikatoren

Wirtschaftliche Indikatoren

1. **A. Bruttonationaleinkommen (BNE) (Kaufkraftparität) pro Kopf**

Die Hauptquelle für diesen Indikator ist der von der Weltbank gepflegte Datensatz über das BNE.

2. **B. Wachstumsrate des BNE in den letzten zehn Jahren**

Die Hauptquelle für diesen Indikator ist der von der Weltbank gepflegte Datensatz über das BNE.

3. C. Anteil der Dienstleistungen am BIP

Die Hauptquelle für diesen Indikator ist der Datensatz zur sektoralen Verteilung des BIP, der von der Weltbank gepflegt wird.

Demographische Indikatoren

4. A. Gesamtbevölkerungsgröße und Wachstumstrend

Die Hauptquelle für diesen Indikator ist der Datensatz zu Bevölkerungsgröße und Wachstumstrend, der von der Bevölkerungsabteilung der UN-Abteilung für wirtschaftliche und soziale Angelegenheiten gepflegt wird.

5. B. Durchschnittliche Lebenserwartung bei der Geburt, disaggregiert nach Geschlecht

Die Hauptquelle für diesen Indikator ist der von der Weltgesundheitsorganisation (WHO) gepflegte Datensatz zur Lebenserwartung bei der Geburt. Daten zur Lebenserwartung bei der Geburt sind auch im Index der menschlichen Entwicklung (HDI) enthalten.

6. C. Anteile von Kindern, Jugendlichen, Personen im erwerbsfähigen Alter und älteren Menschen

Die Hauptquelle für diesen Indikator ist der Datensatz über die Bevölkerung nach Altersgruppen, der von der Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten der Vereinten Nationen verwaltet wird.

7. D. Sprachliche Vielfalt

Die Hauptquelle für diesen Indikator ist der von Ethnologue geführte Index der sprachlichen Vielfalt (mit Länderzusammenfassungen).

[200] Übersetzung und Dokumentation: Matthias C. Kettemann, Katharina Mosene, Maximilian Piet, Felicitas Rachinger, Johanna Friederike Stelling, (Leibniz-Institut für Medienforschung | Hans-Bredow-Institut), Andreas Salz (Deutsche UNESCO-Kommission).

8. E. Grad der Verstädterung

Die Hauptquelle für diesen Indikator ist der Datensatz über die städtische und ländliche Bevölkerungsgröße, der von der Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten der Vereinten Nationen verwaltet wird.

Entwicklungs-Indikatoren

9. A. UNDP-Index der menschlichen Entwicklung (HDI)

Als Hauptquelle für diesen Indikator wird der HDI vorgeschlagen, der vom UNDP erstellt und in dessen Jahresbericht über die menschliche Entwicklung veröffentlicht wird.

10. B. Durchschnittliche Schuljahre und Anteile der entsprechenden Altersgruppen in der Primar-, Sekundar- und Tertiärbildung, aufgeschlüsselt nach Geschlecht

Die Hauptquelle für diesen Indikator sind Datensätze, die vom UNESCO-Institut für Statistik erhoben werden. Daten zu den durchschnittlichen Schuljahren sind ebenfalls im HDI enthalten.

11. C. Alphabetisierungsrate bei Erwachsenen, disaggregiert nach Geschlecht (und ggf. Sprache)

Die Hauptquelle für diesen Indikator besteht aus Daten, die von der Weltbank gesammelt wurden.

12. D. Anteil der von der Stromversorgung erfassten Bevölkerung

Die Hauptquelle für diesen Indikator ist die Datenbank "Nachhaltige Energie für alle" der Weltbank.

Gleichheits-Indikatoren

13. A. GINI-Koeffizient

Die Hauptquelle für diesen Indikator ist der von der Weltbank erstellte Gini-Index.

14. B. Index der geschlechtsspezifischen Ungleichheit

Die Hauptquelle für diesen Indikator ist der vom Entwicklungsprogramm der Vereinten Nationen erstellte Index der Ungleichheit zwischen den Geschlechtern.

Governance-Indikatoren

15. A. Weltweite Governance-Indikatoren

Die Hauptquelle für diesen Indikator sind die sechs aggregierten World Governance Indicators, die von der Weltbank entwickelt wurden.

16. B. Rechtsstaatlichkeits-Index

Die Hauptquelle für diesen Indikator ist der vom World Justice Project entwickelte Rechtsstaatlichkeitsindex.

17. C. Doing Business Index

Die Hauptquelle für diesen Indikator ist der von der Weltbank erstellte Doing-Business-Index.

IKT-Entwicklungs-Indikatoren

18. A. IKT-Entwicklungsindex

Die Hauptquelle für diesen Indikator ist der von der Internationalen Fernmeldeunion (ITU) erstellte IKT-Entwicklungsindex. (Einige der in diesem Index enthaltenen Indikatoren sind in Kategorie A dieses Indikatorrahmens enthalten).

19. B. Index der mobilen Konnektivität

Die Hauptquelle für diesen Indikator ist der von der GSMA Association erstellte Mobile Connectivity Index. (Einige der, in diesem Index enthaltenen Indikatoren sind in Kategorie A dieses Indikatorrahmens enthalten).

20. C. Weltwirtschaftsforum Networked Readiness Index

Als Hauptquelle für diesen Indikator wird der, vom Weltwirtschaftsforum erstellte Networked Readiness Index vorgeschlagen. (Einige der, in diesem Index enthaltenen Indikatoren sind in Kategorie A enthalten).

21. D. UNCTAD-E-Commerce-Index

Die wichtigste für diesen Indikator vorgeschlagene Quelle ist der, von der UNCTAD erstellte B2C (business to consumer) E-Commerce-Index.

Kern-Indikatoren zur Internet-Universalität

Kategorie R - Rechte

A.1 Gibt es einen rechtlichen Rahmen für den Geltung und Durchsetzung der Menschenrechte, der mit internationalen und regionalen Vereinbarungen, Gesetzen und Standards sowie mit der Rechtsstaatlichkeit vereinbar ist?

Indikator:

22. Bestehen eines verfassungsrechtlichen oder gesetzlichen Rahmens, einschließlich Kontrollverfahren, der mit internationalen und regionalen Vereinbarungen, Gesetzen und Standards im Bereich der Menschenrechte in Einklang steht, und Nachweis, dass dieser von der Regierung und anderen zuständigen Behörden respektiert und durchgesetzt wird.

A.2 Gibt es einen rechtlichen Rahmen, der anerkennt, dass die gleichen Rechte, die Menschen offline haben, auch online geschützt werden müssen?

Indikator:

23. Beweise dafür, dass das Prinzip der Online-/Offline-Äquivalenz in Recht und Praxis akzeptiert und umgesetzt wird.

B.2 Sind Einschränkungen der Meinungsfreiheit eng definiert, transparent, und werden sie in Übereinstimmung mit internationalen Vereinbarungen, Gesetzen und Normen umgesetzt?

Indikator:

24. Rechtliche Einschränkungen der Meinungsfreiheit, die mit internationalen und regionalen Vereinbarungen, Gesetzen und Standards in Einklang stehen, und Nachweise, dass diese von der Regierung und anderen zuständigen Behörden eingehalten werden.

B.4 Unter welchen Bedingungen macht das Gesetz Plattformen und andere Anbieter von Online-Diensten für Inhalte haftbar, die von den Benutzerinnen und Benutzern auf diesen veröffentlicht oder geteilt werden?

Indikator:

25. Der rechtliche Rahmen für die Vermittlerhaftung und die Regulierung von Inhalten steht im Einklang mit internationalen und regionalen Vereinbarungen, Gesetzen und Standards sowie dem Nachweis der Verhältnismäßigkeit der Umsetzung.

C.2 Blockiert oder filtert die Regierung den Zugang zum Internet insgesamt oder zu bestimmten Online-Diensten, Anwendungen oder Websites, und aus welchen Gründen und mit welchem Grad an Transparenz wird dies ausgeübt?

Die Indikatoren:

26. Rechtlicher Rahmen für die Sperrung oder Filterung des Internetzugangs, einschließlich Transparenz- und Aufsichtsregelungen.
27. Beweise in Regierungs- und Gerichtsentscheidungen sowie aus anderen glaubwürdigen und maßgeblichen Quellen bezüglich der Sperrung oder Filterung des Zugangs.
28. Vorkommen, Art und Grundlage für Abschaltungen oder andere Einschränkungen der Internet-Konnektivität.
29. Anzahl und Trend der Zugangsbeschränkungen zu Inhalten, der Zurücknahme von Domänennamen und anderer Interventionen in den letzten drei Jahren.

C.4 Werden Einzelpersonen, Journalistinnen und Journalisten oder andere Online-/Medienakteure willkürlich festgenommen, strafrechtlich verfolgt oder eingeschüchtert, weil sie online auf Informationen zugreifen?

Indikatoren:

30. Umfang und Art der gesetzlichen Bestimmungen und der Praxis.
31. Anzahl willkürlicher Festnahmen und Strafverfolgungen wegen des Zugangs zu Inhalten, die unter internationalen Vereinbarungen über die Umstände und Kriterien für zulässige Beschränkungen nicht unrechtmäßig sind.

D.2 Können sich Nichtregierungsorganisationen frei online organisieren?

Indikator:

32. Nachweis einer Online-Organisation und keine unzulässige Einmischung in eine solche Organisation.

D.3 Gibt es Regierungsrichtlinien für E-Government und/oder E-Partizipation, die die Teilnahme an Regierungs- und öffentlichen Prozessen fördern?

Indikatoren:

33. Vorhandensein von Regierungspolitiken für E-Government und E-Partizipation, einschließlich der Nutzung des Internets für öffentliche Konsultationen.
34. Werte/Rankings im Index der E-Partizipation der UNDESA.

E.2 Ist der Schutz personenbezogener Daten gegenüber Regierungen, Unternehmen und anderen Organisationen gesetzlich garantiert und in der Praxis durchgesetzt, einschließlich des Rechts auf Zugang zu den vorhandenen Informationen und auf Rechtsbehelfe?

Indikatoren:

35. Rechtlicher Rahmen für den Datenschutz, einschließlich Überwachungsmechanismen und Rechtsbehelfe, und Nachweis, dass er von der Regierung und anderen zuständigen Behörden respektiert und durchgesetzt wird.
36. Rechtsrahmen für die kommerzielle Nutzung personenbezogener Daten und die internationale Datenübertragung/Sicherheit, einschließlich Überwachungsmechanismen und Rechtsmittel.
37. Existenz und Befugnisse einer unabhängigen Datenschutzbehörde oder einer ähnlichen Einrichtung.

E.3 Sind die Befugnisse der Strafverfolgungs- und anderer Behörden für das rechtmäßige Abfangen von Daten von Benutzerinnen und Benutzern notwendig, verhältnismäßig und auf Umstände beschränkt, die mit internationalen und regionalen Vereinbarungen, Gesetzen und Normen vereinbar sind?

Indikator:

38. Rechtsrahmen für das rechtmäßige Abfangen von Daten, einschließlich unabhängiger Aufsicht und Transparenz, sowie Nachweise für die Umsetzung durch die Regierung und andere zuständige Behörden.

F.1 Bezieht die Regierungspolitik das Internet in Strategien ein, die sich mit Beschäftigung, Gesundheit und Bildung befassen, unter besonderer Berücksichtigung der Rechte des Internationalen Paktes über wirtschaftliche, soziale und kulturelle Rechte (IPWSKR)?

Indikatoren:

39. Belege für die Einbeziehung a) des Internets und b) der Achtung der IPWSK-Rechte in sektorspezifischen Strategien für Beschäftigung, Gesundheit und Bildung.
40. Belege für eine Analyse der Auswirkungen des Internets auf Beschäftigung, Gesundheit und Bildung durch die Regierung.

F.2 Sind alle Bürgerinnen und Bürger und andere Einzelpersonen gleichermaßen in der Lage, das Internet zur Teilnahme an kulturellen Aktivitäten zu nutzen?

Indikatoren:

41. Ausmaß und Art der Unterschiede beim Internetzugang und der Internetnutzung zwischen verschiedenen Gemeinschaften/Ethnien.
42. Existenz einer Regierungspolitik bezüglich des Kulturerbes online.
43. Verfassungsmäßige oder gesetzliche Garantie der Freiheit des künstlerischen Ausdrucks.

Kategorie O - Offenheit

A.2 Erleichtert der rechtliche und ordnungspolitische Rahmen für Wirtschaft, Wissenschaft und Zivilgesellschaft die Innovation im Internet?

Die Indikatoren:

44. Belege für die Eignung des rechtlichen und ordnungspolitischen Rahmens für die Gründung neuer Unternehmen und die Innovation durch Wissenschaft und Zivilgesellschaft.
45. Wahrnehmung der Erfahrungen der Unternehmen mit dem ordnungspolitischen Umfeld für Unternehmen und IKT, einschließlich internetgestützter Unternehmen.

B.3 Fördert die Regierung die Vielfalt der Lizenzierungsoptionen für geistiges Eigentum, einschließlich freier und quelloffener Software (FOSS)?

Indikatoren:

46. Regierungspolitik gegenüber FOSS und anderen Lizenzoptionen.
47. Umfang, in dem Software mit verschiedenen Lizenzoptionen in Behörden eingesetzt wird.

B.4 Fördert und verabschiedet die Regierung Standards, um Menschen mit Behinderungen den Zugang zum Internet und zu E-Government-Diensten zu erleichtern?

Indikatoren:

48. Politik und Praxis der Regierung zur Gewährleistung der Zugänglichkeit für Menschen mit Behinderungen.
49. Wahrnehmungen von Menschen mit Behinderungen in Bezug auf Politik und Praxis der Zugänglichkeit.

C.1 Gibt es eine unabhängige Regulierung der Kommunikationsmärkte, die in Übereinstimmung mit internationalen Normen und Standards erfolgt?

Indikatoren:

50. Vorhandensein einer unabhängigen Regulierungsbehörde.
51. Belege für die Regulierungsleistung, einschließlich der Wahrnehmung der Qualität der Regulierung durch Kommunikationsunternehmen, Verbraucherverbände und andere Organisationen.

C.4 Gibt es einen ausreichend wirksamen Wettbewerb in Kommunikationszugangsnetzen, um die Interessen der Verbaucherinnen und Verbraucher zu schützen?

Indikatoren:

52. Anzahl der stationären und mobilen Breitbandanbieter.
53. Marktanteile der stationären und mobilen Breitbandanbieter.

D.4 Fördert die Regierung die Nutzung offener Bildungsressourcen (OER) und erleichtert den offenen Zugang zu akademischen und wissenschaftlichen Ressourcen?

Indikatoren:

54. Bildungspolitischer Rahmen bezüglich OER.
55. Regelungen für den Zugang zu akademischen und wissenschaftlichen Ressourcen für Hochschuleinrichtungen und Studierende.

D.5 Verlangt die Regierung von Internetdienstanbietern, den Netzverkehr transparent, unparteiisch und neutral zu verwalten, ohne bestimmte Arten von Inhalten oder Inhalte aus bestimmten Quellen zu diskriminieren?

Indikator:

56. Regulierungsvereinbarungen und -praxis bezüglich Netzneutralität und Wettbewerb für Online- und Netzdienste.

E.1 Wurden Gesetze erlassen, die einen offenen Zugang zu öffentlichen und öffentlich finanzierten Daten mit angemessenem Schutz der Privatsphäre vorschreiben, und werden diese Gesetze umgesetzt?

Indikatoren:

57. Vorhandensein eines rechtlichen Rahmens für den Zugang zu offenen Daten, der mit internationalen Normen und Anforderungen an den Schutz der Privatsphäre in Einklang steht.
58. Belege dafür, inwieweit offene Datenquellen online verfügbar sind und genutzt werden.

E.2 Verfügen Regierungsabteilungen und lokale Regierungsbehörden über Websites, die in allen offiziellen Sprachen und mit allen gängigen Browsern verfügbar sind?

Indikatoren:

59. Regierungspolitik zur Gewährleistung der Bereitstellung von Websites in geeigneter Sprache und mit geeignetem Browser-Zugang sowie Nachweise über die effektive Umsetzung.
60. Anteil der Regierungsdienste mit Websites (Wert/Ranking im Index der Online-Dienste der UNDESA).

Kategorie A - Zugänglichkeit für alle

A.1 Werden statistische Informationen über Zugang und Nutzung des Internets regelmäßig von den nationalen statistischen Systemen und/oder anderen zuständigen Behörden auf systematischer Basis gesammelt?

Indikatoren:

61. Vorkehrungen für die Erhebung aggregierter und disaggregierter statistischer Informationen aus verschiedenen Quellen, einschließlich der Einbeziehung relevanter Fragen in Haushaltserhebungen.
62. Verfügbarkeit von unabhängigen Haushaltsbefragungen und anderen Nachweisen über den aggregierten Internetzugang und die Internetnutzung.

A.4 Verfügt die Regierung über eine Politik und ein Programm zur Umsetzung des universellen Zugangs zu zuverlässigem, erschwinglichem Breitband, und wird dies effektiv umgesetzt?

Indikatoren:

63. Verabschiedung einer Strategie für den universellen Zugang und Nachweis eines wirksamen Einsatzes der Ressourcen.

64. Statistischer Nachweis der Fortschritte auf dem Weg zum universellen Zugang, aggregiert und disaggregiert unter besonderer Berücksichtigung z.B. von Geschlecht, Alter, Wohnort, ethnischer Zugehörigkeit und Behinderung.

B.1 Welcher Anteil der Bevölkerung nutzt das Internet, mit welcher Häufigkeit, und wächst dieser Anteil?

Die Indikatoren:

65. Anteil der Personen, die jemals Zugang zum Internet hatten, aggregiert und disaggregiert.

66. Anteil der Haushalte mit Internetzugang.

67. Anzahl der Internetnutzerinnen und -nutzer pro hundert Einwohnerinnen und Einwohnern, aggregiert und disaggregiert, nach Nutzungshäufigkeit.

68. Anzahl der sozialen Medien (soziale Netzwerke, Mikroblogs, Messaging, Nutzerinnen und Nutzer generiertes Videostreaming) Nutzerinnen und Nutzer pro hundert Einwohnerinnen und Einwohnern, aggregiert und disaggregiert.

69. Anzahl der Besuche von Social-Media-Websites (wie oben definiert) pro hundert Einwohnerinnen und Einwohnern.

B.3 Welcher Anteil der Bevölkerung abonniert Kommunikations-/Breitbanddienste, und nimmt dieser Anteil zu?

Die Indikatoren:

70. Prozentualer Anteil der Personen, die ein Mobiltelefon besitzen, aggregiert und disaggregiert.

71. Anzahl der stationären Breitbandabonnements pro hundert Einwohnerinnen und Einwohnern, aggregiert und disaggregiert.

72. Anzahl der einzelnen aktiven mobilen Breitband-Abonnentinnen und Abonnenten pro hundert Einwohnerinnen und Einwohnern, nach Bandbreite, aggregiert und disaggregiert.

B.4 Welche Zugangsbarrieren werden von Nuzerinnen und Nutzern und Nicht-Nutzerinnen und Nutzern des Internets identifiziert?

Indikator:

73. Wahrnehmungen (von Nutzerinnen und Nutzern und Nicht-Nutzerinnen und Nutzern) von Barrieren für ihren Internetzugang und ihre Internetnutzung, aggregiert und disaggregiert, aus Haushaltsbefragungen und/oder anderen Quellen.

C.1 Sind Mobiltelefone mit Internet-Anschlussmöglichkeit für alle Bevölkerungsgruppen erschwinglich?

Indikatoren:

74. Kosten für a) Mobiltelefone der Einstiegsklasse und b) Smartphones in Prozent des monatlichen BNE pro Kopf.

75. Wahrnehmung der Erschwinglichkeit durch Nutzerinnen und Nutzer und Nicht-Nutzerinnen und Nutzer, aggregiert und disaggregiert.

C.2 Sind der Zugang und die Nutzung von Breitband für alle Bevölkerungsgruppen erschwinglich?
Indikatoren:

76. Monatliche Kosten für einen stationären Breitbandanschluss der Einstiegsklasse und die Nutzung als Prozentsatz des monatlichen BNE pro Kopf.
77. Monatliche Kosten für eine mobile Breitbandverbindung der Einstiegsklasse und deren Nutzung in Prozent des monatlichen BNE pro Kopf.
78. Verfügbarkeit oder Nichtverfügbarkeit eines Nulltarif- oder kostengünstigen Zugangs.

D.1 Gibt es signifikante Unterschiede beim Breitbandzugang und der Breitbandnutzung zwischen Regionen sowie zwischen städtischen und ländlichen Gebieten?
Die Indikatoren:

79. Geografische Abdeckung von Breitbandnetzen in städtischen und ländlichen Gebieten, nach Bandbreitenniveau.
80. Anzahl der mobilen Breitbandabonnentinnen und -abonennten und der Internetnutzerinnen und -nutzer, aggregiert und wenn möglich aufgeschlüsselt nach städtischen und ländlichen Gebieten und in verschiedenen Regionen.

D.5 Nutzen Erwachsene in allen Altersgruppen das Internet in gleichem Maße?
Indikatoren:

81. Anteil der Erwachsenen in verschiedenen Altersgruppen, die das Internet nutzen, sowie Häufigkeit und Art der Nutzung, einschließlich einer Aufschlüsselung nach Geschlecht.
82. Wahrnehmung der Barrieren für den Internetzugang und die Internetnutzung sowie des Wertes des Internetzugangs und der Internetnutzung für Nutzerinnen und -Nutzer (sofern verfügbar), aufgeschlüsselt nach Alter und Geschlecht.

E.1 Wie viele Internet-Domains und Server gibt es im Land?
Indikatoren:

83. Anzahl der registrierten Domains (einschließlich ccTLDs. gTLDs und IDNccTLDs) pro tausend Einwohnerinnen und Einwohnern und, soweit verfügbar, Trend
84. Anzahl der sicheren Webserver pro Million Einwohnerinnen und Einwohnern und Trend, soweit verfügbar.

E.4 Gibt es ein beträchtliches und wachsendes Volumen von Internet-Inhalten in verschiedenen lokalen und indigenen Sprachen, einschließlich lokal erzeugter Inhalte?
Indikatoren:

85. Anteil der Bevölkerung, deren Hauptsprache und Schrift auf führenden Online-Diensten verfügbar sind.
86. Verfügbarkeit von Inhalten auf Regierungs-Websites in allen Sprachen mit bedeutenden Nutzerinnen- und Nutzergruppen innerhalb der Bevölkerung.

F.1 Enthalten die Lehrpläne von Schulen und Hochschulen eine Ausbildung in IKT sowie Medien- und Informationskompetenz, die auf eine effektive und sichere Nutzung ausgerichtet ist, und werden diese Lehrpläne in der Praxis umgesetzt?

Indikatoren:

87. Politik in Bezug auf Schullehrpläne, einschließlich Medien- und Informationskompetenz, interkultureller Dialog und Ausbildung in IKT-Fertigkeiten.
88. Nachweis geeigneter Bildungscurricula auf Primar-, Sekundar- und Tertiärstufe.
89. Anteil der Lehrerinnen und Lehrer in Primar- und Sekundarschulen mit einer Ausbildung in IKT oder der Nutzung von IKT im Unterricht.
90. Anteil der Schulen mit Internetzugang.
91. Anteil der Lernenden, die in der Schule Zugang zum Internet haben.

F.3 Welcher Anteil der Bevölkerung und der Arbeitskräfte ist im Umgang mit IKT qualifiziert?

Indikatoren:

92. Anteil der Internetnutzerinnen und -nutzer mit besonderen Internetkenntnissen, nach Art der Qualifikation (Grundkenntnisse, mittlere und fortgeschrittene Kenntnisse), aggregiert und disaggregiert.
93. Anteil der Arbeitskräfte, die IKT am Arbeitsplatz nutzen, nach Art der Qualifikation (Grundqualifikation, mittlere Qualifikation, fortgeschrittene Qualifikation), aggregiert und disaggregiert.
94. Anteil der Studierenden des Tertiärbereichs, die an MINT- und IKT-Kursen teilgenommen haben, aufgeschlüsselt nach Geschlecht, im Vergleich zu den globalen Durchschnittswerten.

Kategorie M - Multistakeholder-Beteiligung

A.1 Gibt es einen allgemeinen politischen, rechtlichen und ordnungspolitischen Rahmen für die Entwicklung des Internets und die Politikgestaltung, der mit internationalen Normen im Einklang steht?

Indikatoren:

95. Vorhandensein eines Gesamtrahmens, der mit den einschlägigen internationalen Normen in Einklang steht.
96. Vorhandensein rechtlicher und regulatorischer Rahmenbedingungen, die elektronischen Handel, digitale Signaturen, Cybersicherheit, Datenschutz und Verbraucherschutz ermöglichen.

B.2 Bezieht die Regierung andere Interessengruppen aktiv in die Entwicklung nationaler Internet-Richtlinien und -Gesetze ein?

Indikatoren:

97. Vorhandensein von Vorkehrungen für die Konsultation und Beteiligung mehrerer Interessengruppen an nationalen Institutionen und Prozessen der Politikgestaltung, die sich mit der Entwicklung und Nutzung des Internet befassen.
98. Anzahl der aktiv teilnehmenden nichtstaatlichen Stakeholder, nach Stakeholdergruppe, aufgeschlüsselt nach Geschlecht.

B.3 Gibt es ein nationales Internet Governance Forum und/oder ein anderes Multi-Stakeholder-Forum, das allen Stakeholdern offen steht und an dem verschiedene Stakeholder-Gruppen aktiv teilnehmen?
Indikatoren:

99. Vorhandensein eines nationalen IGF und/oder eines anderen Multi-Stakeholder-Forums, das sich mit der Internet-Verwaltung befasst.
100. Beteiligungsdaten für nationale IGF oder andere Foren, aggregiert und disaggregiert nach Geschlecht und Stakeholdergruppe, unter besonderer Berücksichtigung der Beteiligung ausgewählter Gruppen (z.B. Bildungsministerien, KMU, NGOs, die sich mit Kindern befassen, Gewerkschaften), einschließlich Vorkehrungen für die Fernteilnahme.

C.2 Nehmen die Regierung und andere Interessensvertretungen aus dem Land aktiv an wichtigen internationalen Foren teil, die sich mit IKT und dem Internet befassen?
Indikatoren:

101. Anzahl der Teilnehmerinnen und Teilnehmern aus verschiedenen Stakeholder-Gruppen, die an globalen und regionalen IGFs teilnehmen, pro Million Einwohnerinnen und Einwohnern, aggregiert und disaggregiert nach Stakeholder-Gruppe und Geschlecht.
102. Teilnahme nichtstaatlicher Akteure an offiziellen Delegationen der ITU, aggregiert und aufgeschlüsselt nach Interessengruppen und Geschlecht.

C.3 Beteiligen sich die Regierung und andere Beteiligte aktiv an der ICANN?
Indikatoren:

103. Mitgliedschaft und aktive Beteiligung im ICANN-Beratungsausschuss für Regierungsangelegenheiten (GAC).
104. Mitgliedschaft in und aktive Teilnahme an ICANN-Wahlkreisen, Arbeitsgruppen und anderen Foren.

Kategorie X - Querschnittsindikatoren

A.1 Werden die Interessen und Bedürfnisse von Frauen und Mädchen in den nationalen Strategien und Richtlinien für die Entwicklung des Internets ausdrücklich berücksichtigt und wirksam überwacht?
Indikatoren:

105. Die nationalen Strategien berücksichtigen ausdrücklich a) die Bedürfnisse von Frauen im Zusammenhang mit dem Internet und b) das Potenzial des Internets zur Unterstützung der Selbstbestimmung von Frauen und der Gleichstellung der Geschlechter.
106. Anzahl von Frauen und Männern in Führungspositionen in der Regierung, die sich mit IKT/Internet befassen.
107. Umfang der Disaggregation der verfügbaren Daten über IKT-Zugang und -Nutzung nach Geschlecht.
108. Vorhandensein nationaler Mechanismen zur Überwachung der Einbeziehung von Frauen in Strategien für den Internetzugang und die Internetnutzung.

A.2 Gibt es eine digitale Kluft zwischen den Geschlechtern beim Internetzugang und bei der Internetnutzung, und wenn ja, wächst, stabilisiert oder verringert sich diese Kluft zwischen den Geschlechtern?

Indikatoren:

109. Anteil der Personen, die das Internet nutzen, aufgeschlüsselt nach Geschlecht, im Vergleich zu den geschlechtsspezifischen Unterschieden bei Einkommen und Bildungsniveau.

110. Anteile erwachsener Frauen und Männer mit mobilen Breitbandabonnements, aufgeschlüsselt nach Geschlecht, im Vergleich zu den geschlechtsspezifischen Unterschieden bei Einkommen und Bildungsniveau.

111. Erhebungsdaten zum Internet-Bewusstsein und zu Mustern der Internet-Nutzung, disaggregiert nach Geschlecht.

112. Wahrnehmung der Barrieren für den Zugang zum Internet und dessen Nutzung sowie des Wertes des Internetzugangs und der Internetnutzung, aufgeschlüsselt nach Geschlecht.

A.5 Schützen das Gesetz, die Strafverfolgung und die Gerichtsverfahren Frauen und Mädchen vor geschlechtsspezifischer Belästigung und Gewalt im Internet?

Die Indikatoren:

113. Vorhandensein eines einschlägigen Rechtsrahmens und von Gerichtsverfahren.

114. Inzidenz von geschlechtsspezifischer Belästigung und Gewalt im Internet, die Frauen und Mädchen erfahren.

115. Belege für Maßnahmen der Regierung, der Strafverfolgung und der Justiz zum Schutz von Frauen vor geschlechtsspezifischer Belästigung und Gewalt im Internet.

116. Vorhandensein von Online-Diensten, die Frauen vor geschlechtsspezifischer Online-Belästigung schützen oder die Betroffene unterstützen sollen.

B.3 Wie nehmen Kinder das Internet wahr, und wie nutzen sie es?

Indikatoren:

117. Aus Umfragen abgeleitete Wahrnehmungen des Internets bei Kindern, einschließlich Nutzungsbarrieren, Nutzungswert und Nutzungsängste, aggregiert und disaggregiert.

118. Daten über die Nutzung des Internet durch Kinder, aggregiert und disaggregiert, im Vergleich zu anderen Altersgruppen (z.B. Daten über Ort, Häufigkeit und Art der Nutzung).

B.4 Gibt es einen rechtlichen und politischen Rahmen zur Förderung und zum Schutz der Interessen von Kindern im Internet, und wird dieser wirksam umgesetzt?

Indikator:

119. Vorhandensein eines politischen Rahmens und rechtlicher Schutzmaßnahmen, die mit der UN-Kinderrechtskonvention (KRK) vereinbar sind, und Nachweis, dass diese von der Regierung und anderen zuständigen Behörden umgesetzt werden.

C.1 Beziehen nationale und sektorale Entwicklungspolitiken und -strategien für nachhaltige Entwicklung IKT, Breitband und das Internet wirksam ein?

Indikator:

120. Vorhandensein einer neueren, umfassenden Politik für die Entwicklung der IKT, des Breitbands und des Internets, die auch Überlegungen zu den voraussichtlichen künftigen Entwicklungen in diesen Bereichen einschließt.

C.7 Welcher Anteil der Unternehmen, einschließlich kleiner und mittlerer Unternehmen, nutzt das Internet und den elektronischen Handel?

Indikatoren:

121. Anteil der KMU, die das Internet nutzen, nach Art des Zugangs.

122. Wahrnehmung des Wertes der Internetnutzung durch KMU.

D.1 Gibt es eine nationale Cybersicherheitsstrategie, die sich an den internationalen Menschenrechtsstandards orientiert, einschließlich eines nationalen Computer-Notfallreaktionsteams (CERT) oder einer gleichwertigen Einrichtung?

Indikatoren:

123. Vorhandensein einer Cybersicherheitsstrategie mit Beteiligung mehrerer Interessengruppen, die mit internationalen Rechten und Normen im Einklang steht.

124. Einrichtung eines nationalen CERT oder eines gleichwertigen Systems und Nachweis über dessen Wirksamkeit.

D.4 Gab es in den letzten drei Jahren erhebliche Verstöße gegen die Cybersicherheit im Land?

Indikatoren:

125. Häufigkeit und Art der gemeldeten Verstöße sowie Anzahl der betroffenen Einzelpersonen und Unternehmen.

126. Wahrnehmung der Internetsicherheit bei Nutzerinnen und Nutzern, Unternehmen und anderen Interessengruppen.

127. Daten zu Phishing, Spam und Bots in Domänen auf nationaler Ebene.

E.3 Wie nehmen Einzelpersonen die Vorteile, Risiken und Auswirkungen des Internets innerhalb des Landes wahr?

Indikator:

128. Wahrnehmungen von Nutzen, Risiken und Auswirkungen des Internets, abgeleitet aus Haushalts- oder Meinungsumfragen, aufgeschlüsselt nach Geschlecht.

E.4 Geben Internetnutzerinnen und -nutzer an, dass sie von anderen Internetnutzerinnen und -nutzern in erheblichem Maße belästigt oder missbraucht werden, was sie davon abhält, das Internet in vollem Umfang zu nutzen?

Indikatoren:

129. Verfügbarkeit von Meldemechanismen für Online-Belästigung oder -Missbrauch, einschließlich Meldevorkehrungen von Online-Diensteanbietern.

130. Daten über das Ausmaß, in dem Internetnutzerinnen und -nutzer Belästigung oder Missbrauch melden, unter besonderer Berücksichtigung bestimmter demographischer und sozialer Gruppen (einschließlich Frauen, ethnischer und anderer Minderheiten sowie Bürgerrechtlerinnen und Bürgerrechtlern).