FES diskurs

Matthias C. Kettemann, Felicitas Rachinger,
Meryem Vural

Menschenrechte im Digitalen

Wie wir Freiheit im digitalen Raum sichern. Handlungsoptionen für die Bundesregierung

FRIEDRICH EBERT STIFTUNG

FES diskurs
November 2022

Die Friedrich-Ebert-Stiftung
Die Friedrich-Ebert-Stiftung (FES) wurde 1925 gegründet und ist die traditionsreichste politische Stiftung Deutschlands. Dem Vermächtnis ihres Namensgebers ist sie bis heute verpflichtet und setzt sich für die Grundwerte der Sozialen Demokratie ein: Freiheit, Gerechtigkeit und Solidarität. Ideell ist sie der Sozialdemokratie und den freien Gewerkschaften verbunden.

Die FES fördert die Soziale Demokratie vor allem durch:
– politische Bildungsarbeit zur Stärkung der Zivilgesellschaft;
– Politikberatung;
– internationale Zusammenarbeit mit Auslandsbüros in über 100 Ländern;
– Begabtenförderung;
– das kollektive Gedächtnis der Sozialen Demokratie mit u. a. Archiv und Bibliothek.

Die Abteilung Analyse, Planung und Beratung der Friedrich-Ebert-Stiftung
Die Abteilung Analyse, Planung und Beratung der Friedrich-Ebert-Stiftung versteht sich als Zukunftsradar und Ideenschmiede der Sozialen Demokratie. Sie verknüpft Analyse und Diskussion. Die Abteilung bringt Expertise aus Wissenschaft, Zivilgesellschaft, Wirtschaft, Verwaltung und Politik zusammen. Ihr Ziel ist es, politische und gewerkschaftliche Entscheidungsträger_innen zu aktuellen und zukünftigen Herausforderungen zu beraten und progressive Impulse in die gesellschaftspolitische Debatte einzubringen.

FES diskurs
FES diskurse sind umfangreiche Analysen zu gesellschaftspolitischen Fragestellungen. Auf Grundlage von empirischen Erkenntnissen sprechen sie wissenschaftlich fundierte Handlungsempfehlungen für die Politik aus.

Für diese Publikation sind in der FES verantwortlich
Katrin D. Dapp, Marie von der Heydt, Medienpolitik, und Stefanie Moser, Digitalisierung.

Matthias C. Kettemann, Felicitas Rachinger, Meryem Vural

Menschenrechte im Digitalen

Wie wir Freiheit im digitalen Raum sichern. Handlungsoptionen für die Bundesregierung

INHALT

1 EINLEITUNG

Prozesse des digitalen Wandels wirken sich profund auf die Akteur_innen und Instrumente internationaler Beziehungen aus. Der Modus der Stabilisierung internationaler normativer Ordnung hat sich bereits stark verändert. Private Akteur_innen sind hervorgetreten und haben wichtige Kommunikationsräume mit flankierenden Normenordnungen geschaffen, in denen Prozesse gesellschaftlicher Selbstbestimmung ablaufen. Auch die Rolle und Machtverhältnisse der Staaten verändern sich in der digitalen Konstellation. Aus einer zunächst unipolar, dann bipolar geprägten Ordnung sind multipolare Kräfteverhältnisse gewachsen. Technologischer Wandel ändert tiefgreifend die Strukturen internationaler politischer Prozesse, die sich besonders augenscheinlich in der globalen Internet Governance beobachten lassen. Von den Herausforderungen für die Cybersicherheit im Internet of Things über den vermehrten Einsatz algorithmischer Entscheidungssysteme bis zur Nutzung digitaler Spähtools gegen Journalist_innen und Bürgerrechtler_innen: Der Schutz der Grund- und Menschenrechte als zentraler Maßstab internationaler Politik, nach innen wie außen, gerät in der digitalen Konstellation unter Druck.

Demokratische Teilhabe an diesen Kommunikationsräumen setzt Zugang voraus. Bis 2020 wollten die Vereinten Nationen (UN) alle Menschen ans Netz holen; auch die deutsche Regierung hat sich zu einem flächendeckenden Breitbandausbau (nach innen) und der prononcierten Förderung globalen Internetzugangs (nach außen) bekannt. Beide Ziele wurden deutlich verfehlt. Der Handlungsdruck, der aus menschenrechtlichen Verpflichtungen erwächst, ist ungebrochen.

Gerade in Zeiten der (post)coronabedingten Migration gesellschaftlicher Selbstbestimmungsprozesse in Online-Kommunikationsräumen ist der nachfolgenden Beschrei-

bung des Europäischen Gerichtshofs für Menschenrechte (EGMR) zuzustimmen: „Das Internet ist inzwischen zu einem der wichtigsten Mittel geworden, mit dem Einzelpersonen ihr Recht auf Freiheit des Empfangs und der Weitergabe von Informationen und Ideen ausüben, indem es [...] wesentliche Instrumente für die Teilnahme an Aktivitäten und Diskussionen über politische Fragen und Themen von allgemeinem Interesse bereitstellt."[1]

In einer 2015 von uns auf Einladung der Friedrich-Ebert-Stiftung verfassten Studie zum Völkerrecht des Netzes (Kettemann 2015) finden sich Feststellungen, die unverändert Gültigkeit haben. Unter anderem stellte die Studie heraus, dass sich die Staaten der Welt darauf geeinigt hatten, dass der Aufbau einer menschenzentrierten, entwicklungsorientierten Informationsgesellschaft nur unter Berücksichtigung der Ziele und Grundsätze der Charta der Vereinten Nationen und der Achtung des Völkerrechts und der Menschenrechte funktionieren kann.

„Das Internet ist inzwischen zu einem der wichtigsten Mittel geworden, mit dem Einzelpersonen ihr Recht auf Freiheit des Empfangs und der Weitergabe von Informationen und Ideen ausüben (...)."

Schon damals stellte die Studie fest, dass ein Internetvölkerrecht bereits besteht (in dem Sinne, dass das Völkerrecht auf das Internet anzuwenden ist und sich im geltenden Völkerrecht schon bedeutende Verpflichtungen finden, die Staaten bei der Ausgestaltung ihrer Digitalpolitik zu beachten haben). Dass der Koalitionsvertrag 2021–2025 erneut die Formulierung „Wir wollen ein Völkerrecht des Netzes" (SPD; Bündnis 90/Die Grünen; FDP 2021: 144) enthält, ohne zu präzisieren, was damit gemeint ist und wie es erreicht werden will, kann daher als erneuter Auftrag an die Wissenschaft interpretiert werden, Vorschläge zu machen, zumal der auch von Deutschland maßgeblich weiterbetriebene globale Prozess der Ausverhandlung von Cybernormen schon recht weit gediehen ist (Kettemann/Paulus 2020).

Teil zeitgerechter Menschenrechtspolitik muss der digitale Menschenrechtsschutz sein. Schon der inzwischen zwei Jahre zurückliegende 14. Bericht der Bundesregierung über ihre Menschenrechtspolitik (Auswärtiges Amt 2020) mit einem „Aktionsplan Menschenrechte" für die Jahre 2021–2022 enthielt als Priorität die Stärkung des Menschenrechtsschutzes „angesichts des digitalen Wandels". Darunter fiel beispielsweise auch der Schutz der Menschenrechte im Rahmen der Entwicklung künstlicher Intelligenz (KI). Der Koalitionsvertrag 2021–2025 erwähnt Menschenrechte nicht im Kontext der KI, während er auf die KI als „Zukunftsfeld" verweist, ein Bekenntnis zur Nutzung ihrer Potenziale festschreibt und die Bedeutung eines intensiven transatlantischen Dialogs zu Datensouveränität, Netzfreiheit und KI[2] hervorhebt (SPD; Bündnis 90/Die Grünen; FDP 2021: 19, 21, 154). Vor diesem Hintergrund – also 1. sinnvolle Festlegungen, aber 2. eine begrenzt detaillierte Ausgestaltung der operationalisierbaren Policy-Maßnahmen und 3. aktuelle Entwicklungen (Coronakrise, Russlands Angriff auf die Ukraine), die teils Umbrüche in der Politik und Praxis des digitalen Deutschlands bewirkten – will diese Studie Vorschläge für digitalmenschenrechtliche Maßnahmen für die aktuelle Legislaturperiode machen.

- Zunächst führt die Studie in die Bedeutung der Menschenrechte im Kontext der Digitalisierung ein (Kapitel 2).
- Sodann werden wichtige menschenrechtliche Themenfelder präsentiert und in den Kontext des Koalitionsvertrages sowie aktueller Herausforderungen wie der Covid-19-Pandemie und dem völkerrechtswidrigen Angriffs Russland auf die Ukraine eingeordnet (Kapitel 3).
- Empfehlungen schließen die Studie ab (Kapitel 4). ←

1 ECtHR in Cengiz and Others v. Turkey, 2015 (Übersetzung der Verfasser_innen).

2 Der Begriff der „künstlichen Intelligenz (KI)" hat sich als Referenzpunkt für die fachliche und öffentliche Diskussion darüber etabliert, wie spezifische automatisierte Prozesse die Digitalisierung vorantreiben und gesellschaftlich wirksam werden, auch wenn selbst in der Informatik kein geteiltes Verständnis von KI existiert und viele der gesellschaftlichen Fragen nicht mit bestimmten Technologien wie etwa maschinellem Lernen in neuronalen Netzen zusammenhängen.

2 MENSCHENRECHTE IN ZEITEN DER DIGITALISIERUNG

Im digitalen Zeitalter ist das Internet zu einem wichtigen Raum für die Ausübung unserer Rechte geworden; politische Diskussionen und zivilgesellschaftliches Engagement finden vermehrt online statt. Gleichzeitig stellt die zunehmende Digitalisierung eine Herausforderung dar, die entsprechenden Menschenrechtsschutz nicht nur offline, sondern auch online erfordert. Dass Menschenrechte online ebenso wie offline gelten, ist inzwischen ein Gemeinplatz. Diese Festlegung mit Leben zu erfüllen, ist indes eine an Bedeutung nicht zu unterschätzende Aufgabe der Bundesregierung.

Grundlage der Ausübung von Rechten im digitalen Raum ist das Recht auf Internetzugang. Dieses ist in Deutschland zwar nicht explizit kodifiziert, kann allerdings als eigenständiges Recht vom Grundrecht auf Gewährleistung eines menschenwürdigen Existenzminimums (Artikel 1 Abs. 1 in Verbindung mit Artikel 20 Abs. 1 Grundgesetz) abgeleitet werden. Auch aus der Funktion des Internetzugangs als Voraussetzung anderer Rechte kann abgeleitet werden, dass der Internetzugang entsprechenden rechtlichen Schutz erfordert. Daraus ergibt sich eine Verpflichtung des Staates, den Zugang zum Internet durch staatliche Infrastrukturmaßnahmen sicherzustellen (Kettemann 2020).

Darüber hinaus ist auch der Zugang zu Internetinhalten zu gewährleisten. Insbesondere die Informations- und Meinungsfreiheit wird online ausgeübt: Digitale Räume sind zu einem integralen Bestandteil einer modernen Demokratie geworden. Mit dem Schutz der Meinungsfreiheit eng verbunden ist der Schutz des Privatlebens und vor Hass und Hetze im digitalen Raum: Nur wenn dies gewährleistet ist, ist auch Sicherheit bei der Ausübung der Meinungsfreiheit gegeben.

Der Einsatz algorithmischer Entscheidungssysteme trägt zur Verstärkung von Hass und Hetze wie auch Diskriminierung in digitalen Räumen bei. Diskriminierung, die sich offline zeigt, spiegelt sich auch im digitalen Raum wider, indem sie etwa über diskriminierende Datensätze Eingang in digitale Welten findet oder in Form von digitaler Gewalt auftritt. Einer aktuellen Studie der Online-Grundrechte NGO HateAid zufolge sind 50 Prozent der jungen Erwachsenen in der EU von Hass im Internet betroffen. Vor allem Frauen ziehen sich aus Angst vor Angriffen aus den sozialen Medien zurück. 80 Prozent der Befragten sind unzufrieden mit den Schutzmaßnahmen der Plattformen (HateAid/Landecker Digital Justice Movement 2022). Hass und Hetze im Netz sind dabei immer aus einem intersektionalen Blickwinkel zu betrachten und treffen unterschiedliche Gruppen unterschiedlich stark.

Drei Dynamiken üben zurzeit besonderen Einfluss auf die Digitalisierung aus: Zunächst hat sich die Covid-19-Pandemie als Beschleuniger der Digitalisierung des Sozialen ausgewirkt. Die Folgen auch für die Menschenrechtspolitik sind beträchtlich. Seit Ausbruch der Pandemie haben sich nicht nur die Vorteile der Digitalisierung, sondern auch die Verletzlichkeit des Systems gezeigt, die sich für unterschiedliche Gruppen unterschiedlich schwer auswirkt. Die Europäische Kommission spricht in diesem Zusammenhang von einer neuen „digitalen Armut", die aktive staatliche Maßnahmen nötig mache, um die Chancen des digitalen Wandels für alle Bürger_innen zu realisieren (Europäische Kommission 2021a: 3). Desinformation ist dabei nur eines der vielen demokratie- und menschenrechtsrelevanten Themen, die durch die Covid-19-Pandemie in einen (noch) stärkeren Fokus gerückt sind (Kettemann/Fertmann 2020).

Sodann ist mit dem Ende der Ära Trump eine Wendezeit der Plattformregulierung angebrochen. Viel bewusster als zuvor nutzen Plattformen ihre Regeln und algorithmischen Empfehlungssysteme, um bestimmte Inhalte zu reduzieren (etwa impfbezogene Desinformationen im Coronakontext oder wahlbezogene Falschaussagen). Gleichzeitig versuchen Plattformen ihre internen Regeln gesellschaftlich besser abzusichern, indem sie etwa auf sogenannte Plattformräte setzen, am prominentesten Facebook mit dem Facebook Oversight Board (Kettemann/Fertmann 2021). Gleichzeitig wird der digitale Kommunikationsraum auf gesetzlicher Ebene immer weitreichender reguliert. In Deutschland ist das 2017 in Kraft getretene Netzwerkdurchsetzungsgesetz (NetzDG), dessen Novelle der Bundestag im Mai 2021 verabschiedet hat, von besonders großer Bedeutung; es wirkt sich auch über die Grenzen Deutschlands hinaus aus. Anfang 2021 trat in Österreich ein Gesetz ähnlich dem deutschen NetzDG in Kraft, auch andere Länder wie etwa Brasilien und Indonesien orientieren sich am deutschen Vorbild. Auch die EU hat zur stärkeren Regulierung der digitalen Sphäre ein Verordnungspaket bestehend aus dem Digital Services Act (DSA), dem Digital Markets Act (DMA), dem Data Governance Act (DGA) und dem Artificial Intelligence Act (AIA) vorgestellt. Der DSA und DMA wurden vom Europäischen Parlament und Rat angenommen; das Schwestergesetz Media Freedom Act ist im Entwurfsstadium; der DGA ist bereits in Kraft getreten (Europäischer Rat 2022).

Schließlich hat das deutsche Rechtssystem einen Schwenk hin zur Internationalisierung (und Extraterritorialisierung) von Verantwortung für Menschenrechte gemacht. Nicht erst seit dem BND-Beschluss des Bundesverfassungsgerichts[3], wonach deutsche Behörden Grundrechte auch jenseits der Grenze zu beachten haben, ist auch hinsichtlich der Governance des digitalen Raums der Ruf nach der verstärkten Übernahme extraterritorialer Verantwortung für digitale Menschenrechte lauter geworden. Die Bundesregierung selbst bekennt sich explizit im hier einschlägigen 14. Menschenrechtsbericht dazu, sich international verstärkt für den (digitalen) Menschenrechtsschutz einzusetzen (Auswärtiges Amt 2020: 57ff., 148ff.). Nicht zuletzt zeigt sich auch ein Trend zur Intertemporalisierung von Freiheiten, also der Sicherung nicht nur gegenwärtiger, sondern auch künftiger Freiheiten. Im März 2021 entschied das Bundesverfassungsgericht, bezogen auf Klimagerechtigkeit, dass eine objektivrechtliche Schutzverpflichtung des Staates in Bezug auf künftige Generationen begründet werden kann.[4] In analoger Anwendung dieses Urteils ist auch die Ableitung einer ähnlichen Schutzverpflichtung im Zusammenhang mit Digitalisierung denkbar. Aktuell kann auf nationaler Ebene zwar ein Recht auf Internetzugang aus unterschiedlichen Rechtsnormen abgeleitet werden, eine entsprechende Verpflichtung zur Gewährleistung der Stabilität und Sicherheit des Internets gegen-

Der Ruf nach der verstärkten Übernahme extraterritorialer Verantwortung für digitale Menschenrechte ist lauter geworden.

über künftigen Generationen wurde bisher allerdings noch nicht herausgearbeitet. Auf völkerrechtlicher Ebene besteht keine explizite vertragliche Verpflichtung zum Schutz der Infrastruktur des Internets. Die Verhandlungen um Cybernormen innerhalb der Vereinten Nationen scheinen indes trotz paralleler Prozesse und divergierender politischer Schwerpunkte bei bestimmten Regeln globalen Konsens zu verzeichnen. Um auch für künftige Generationen Zugang zum Internet zu gewährleisten, muss der Staat durch internationale Zusammenarbeit die Sicherheit und Stabilität des Internets langfristig sicherstellen. Gleichzeitig ist zu berücksichtigen, dass Digitalisierung einen wesentlichen Beitrag leisten kann, Nachhaltigkeit auch in anderen Bereichen voranzutreiben. Der Wissenschaftliche Beirat der Bundesregierung Globale Umweltveränderungen (WBGU) fordert daher folgerichtig, die „Digitalisierung in den Dienst der globalen Nachhaltigkeit" zu stellen (WBGU 2019). ←

3 BVerfG, Urteil des Ersten Senats vom 19.5.2020, 1 BvR 2835/17.
4 BVerfG, Beschluss vom 24.3.2021, 1 BvR 2656/18.

3 HANDLUNGSFELDER DES MENSCHENRECHTS-SCHUTZES IM DIGITALEN

A. ZUGANG ZU INTERNETINHALTEN

I. SCHAFFUNG UND AUFRECHTERHALTUNG ENTSPRECHENDER INFRASTRUKTUR

Als Grundlage für die Ausübung digitaler Menschenrechte ist sicherzustellen, dass der Internetzugang nachhaltig ist – in diesem Kontext sowohl als langfristig als auch ressourcenschonend verstanden. Dafür ist eine entsprechende Infrastruktur notwendig. Jüngste Untersuchungen haben gezeigt, dass es insbesondere beim Breitbandausbau aufzuholen gilt (Schulz/Kettemann 2021: 89ff.).

Während der Koalitionsvertrag 2018 vorsah, bis 2025 einen flächendeckenden Zugang zum Internet zu schaffen (Bundesregierung 2018: 38f.), findet sich im Koalitionsvertrag der neuen Bundesregierung das Ziel einer „flächendeckende[n] Versorgung mit Glasfaser und dem neuesten Mobilfunkstandard“ (SPD; Bündnis 90/Die Grünen; FDP 2021: 16). Ein entsprechendes zeitliches Ziel wird nicht angeführt. Im Bereich der Entwicklungszusammenarbeit plant die neue Bundesregierung, „am Aufbau ihrer unabhängigen digitalen Infrastruktur zur Stärkung ihrer digitalen Souveränität“ zu arbeiten (SPD; Bündnis 90/Die Grünen; FDP 2021: 144).

Wenngleich zwar ein Recht auf Internetzugang aus unterschiedlichen Rechtsnormen abgeleitet werden kann, ist die Infrastruktur des Internets durch keinen völkerrechtlichen Vertrag geschützt. Vorschläge, die Stabilität und Integrität völkerrechtlich zu schützen, wie etwa den der Global Commission for Stability in Cyberspace (2017), wurden bisher nicht völkervertragsrechtlich umgesetzt. Neuere Ansätze wie jene der „Cybernorms“, die von Arbeitsgruppen innerhalb der Vereinten Nationen entwickelt werden, deuten indes darauf hin, dass die Bedeutung eines Schutzes der Kernressourcen der Internetkonnektivität sehr wohl anerkannt wird. Völkergewohnheitsrechtlich ist jedenfalls ein verstärkter Schutz des Internets zu beobachten, etwa in der Konkretisierung der sich aus dem Kooperations- und Vorsorgeprinzip ergebenden Pflichten (Kettemann 2020: 11).

II. CYBERSICHERHEIT

Um effektiven Internetzugang langfristig sicherzustellen, ist insbesondere auch für Cybersicherheit zu sorgen. Cybersicherheit 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“ (Kettemann 2020: 9f.). Hilfreich wären entsprechende internationale Zusammenarbeit und präventive Maßnahmen (Kettemann 2020: 11f.). Die Bundesregierung sieht es als „staatliche Pflicht“, digitale Bürgerrechte und IT-Sicherheit zu gewährleisten (SPD; Bündnis 90/Die Grünen; FDP 2021: 16). Die vorgesehene Weiterentwicklung der Cybersicherheitsstrategie sowie des IT-Sicherheitsrechts und darüber hinaus ein „struktureller Umbau der IT-Sicherheitsarchitektur“ sind vor dem Hintergrund des Angriffs Russlands auf die Ukraine, in dem Desinformation und Cyberattacken (auch gegen der Ukraine positiv gegenüberstehende Staaten) eine große Rolle spielen, besonders bedeutsam.

III. BARRIEREFREIER ZUGANG ZUM INTERNET

Das Internet muss technisch wie sprachlich barrierefrei zugänglich sein. Hinsichtlich eines barrierefreien Zugangs zum Internet besteht indes noch substanzieller Aufholbedarf. Ende 2021 legte die Überwachungsstelle des Bundes für Barrierefreiheit von Informationstechnik den ersten nach der EU-Web-Accessibility-Richtlinie erforderlichen Bericht zur Barrierefreiheit digitaler Angebote öffentlicher Stellen vor, aus dem sich deutlich erkennen lässt, dass eine Vielzahl der Webauftritte und mobilen Anwendungen nach wie vor nicht den Anforderungen entspricht (BFIT 2021). Im Koalitionsvertrag 2021 wird zur digitalen Barrierefreiheit ausgeführt: „Wir prüfen Wege hin zu einer besseren digitalen Teilhabe für alle, z. B. durch Barrierefreiheit“ (SPD; Bündnis 90/Die Grünen; FDP 2021: 16). In Bezug auf Medien hält der Koalitionsvertrag fest, dass diese barrierefrei sein müssten (SPD; Bündnis 90/Die Grünen; FDP 2021: 124). Darüber hinaus soll „die Machbarkeit einer technologieoffenen, barrierefreien und europaweiten Medienplattform“(SPD; Bündnis 90/Die Grünen; FDP 2021: 124) geprüft werden. Auch der barrierefreie Zugang zu di-

Installation eines Glasfaserkabels

▸▸ Nach wie vor ist schnelles Internet in Deutschland nicht überall verfügbar. Die Bundesnetzagentur stellte im September 2022 erstmals „förmlich“ eine Unterversorgung fest. Die rechtlich vorgeschriebene Mindestversorgung werde nicht erfüllt. Was folgt auf solch eine Feststellung? Wie die Bundesnetzagentur (2022) berichtet, könnten sich nun Telekommunikationsanbieter gegenüber der Bundesnetzagentur zur Versorgung der betroffenen Haushalte verpflichten. „Sollte kein Unternehmen ein Angebot machen, wird die Bundesnetzagentur innerhalb von spätestens vier Monaten eines oder mehrere Unternehmen dazu verpflichten, die betroffenen Haushalte mit einem Telekommunikationsanschluss zu versehen und Telekommunikationsdienste anzubieten.“ Dies entfließe dem Telekommunikationsgesetz, nach dem jede Bürgerin und jeder Bürger einen Rechtsanspruch auf Versorgung mit einem Mindestangebot an Sprachkommunikation und einem schnellen Internetzugangsdienst habe – dies sei wichtig für eine angemessene soziale und wirtschaftliche Teilhabe (Bundesnetzagentur 2022).

Kritische Infrastruktur

▸▸ Der Angriff Russlands auf die Ukraine zeigte 2022 erneut die Relevanz der Cybersicherheit. Besonders Angriffe auf kritische Infrastruktur wie die Energieversorgung machen neue Bedrohungsvektoren sichtbar (Tagesschau 2022). Jüngste Angriffe auf Universitäten zeigen, wie Cyberkriminelle gestohlene Daten nutzen, um Geld zu erpressen (Futurezone 2022a).

Braillezeile

▸▸ Fehlt bei Fotos die Bildunterschrift, sind Internetinhalte für blinde und sehbeeinträchtigte Menschen nicht oder nur erschwert zugänglich. Ähnlich stellen Audioinhalte ohne Untertitel für Personen mit Hörbeeinträchtigungen Schwierigkeiten dar. Das sind nur zwei Beispiele für noch vielfach mangelnde digitale Barrierefreiheit.

Absolvent_innen-feier Uni Bonn

▸▸ Große Bedeutung hat der Schutz der Privatsphäre und dabei insbesondere der Datenschutz in der Coronapandemie erlangt. Aufgrund der Lockdowns mussten Studierende Prüfungen online ablegen, wobei von Universitäten eingesetzte Überwachungssoftware kritisch betrachtet und teilweise als rechtswidrig eingestuft wurde (Netzpolitik 2021; Gesellschaft für Freiheitsrechte 2021).

▸▸ Aktuelle Proteste im Iran zeigen die Relevanz von geschützter, anonymer Kommunikation: Aktivist_innen können Informationen aus dem Iran heraustragen und auf aktuelle Geschehnisse aufmerksam machen. Gleichzeitig wird dadurch ein gesicherter Austausch unter Menschen im Iran selbst ermöglicht (Netzpolitik/Beckedahl 2022).

Tor Browser

gitalen Finanzdienstleistungen ist vorgesehen (SPD; Bündnis 90/Die Grünen; FDP 2021: 172). Barrierefreie Internetnutzung ist vor allem deswegen so wichtig, weil das Internet gerade Menschen mit Behinderung die selbstermächtigte Teilnahme am sozialen, kulturellen und beruflichen Leben in größerem Ausmaß als bisher ermöglicht.

B. SCHUTZ DES RECHTS AUF PRIVATSPHÄRE IM DIGITALEN ZEITALTER

I. BEKENNTNIS ZUM SCHUTZ DER PRIVATSPHÄRE

Die Bundesregierung setzt sich global für das Recht auf Privatsphäre im digitalen Zeitalter ein; nicht zuletzt durch die regelmäßig miteingebrachte UNO-Resolution mit diesem Titel (United Nations 2020). Die Resolution betont die Bedeutsamkeit des Schutzes vor Eingriffen in die Privatsphäre durch die unrechtmäßige Sammlung personenbezogener Daten, durch die Verwendung von Personenprofilen, automatisierte Entscheidungsprozesse, Technologien des maschinellen Lernens und der Biometrie (United Nations 2020: para 7c) oder durch rechtswidrige oder willkürliche Überwachung (United Nations 2020: para 7d). Darüber hinaus wird eine verstärkte Rücksichtnahme auf Frauen und Kinder gefordert, wenn Eingriffe in die Privatsphäre besondere Auswirkungen auf diese Gruppen haben (United Nations 2020: para 7i). Als Instrument des „Soft Law“ ist die Bedeutung der Resolution indes nicht zu unterschätzen.

Auf völkerrechtlicher Ebene ist das Recht auf Privatsphäre von Artikel 12 der Allgemeinen Erklärung der Menschenrechte, die als Völkergewohnheitsrecht angesehen wird, Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte und Artikel 8 der Europäischen Menschenrechtskonvention geschützt.

Im Koalitionsvertrag der Bundesregierung ist in diesem Zusammenhang ausdrücklich angemerkt, dass „allgemeine Überwachungspflichten, Maßnahmen zum Scannen privater Kommunikation und eine Identifizierungspflicht“ abgelehnt werden (SPD; Bündnis 90/Die Grünen; FDP 2021: 17f.). Dass der EuGH im September 2022 die lange ausgesetzte Vorratsdatenspeicherung zu großen Teilen für unverhältnismäßig erklärt hat, ist vor diesem Hintergrund positiv zu sehen.

II. ANONYMISIERUNGS- UND VERSCHLÜSSELUNGSTECHNOLOGIEN

Eine Kriminalisierung von Anonymisierungs- und Verschlüsselungstechnologien, wie etwa durch den 2019 vorgeschlagenen „Darknetparagrafen“ (§ 126a StGB-Entwurf), erscheint wenig sinnvoll. Insgesamt hat sich gezeigt, dass Anonymisierungstechnologien die Strafverfolgung nicht erheblich gefährden, jedoch zur geschützten Kommunikation von Journalist_innen, Oppositionellen, Menschenrechtsaktivist_innen beitragen, insbesondere auch in autoritären Regimen (Kettemann 2020: 37f.). Wie bereits im

Zusammenhang mit dem NetzDG ist auch hier zu bedenken, dass Deutschland in der Digitalgesetzgebung häufig eine Vorreiterrolle einnimmt und andere Staaten Gesetze regelmäßig übernehmen. Statt einer Kriminalisierung des Darknets erscheint die Förderung des Einsatzes individuelle Freiheitsräume bewahrender Technologien (Privacy by Design, Ende-zu-Ende-Verschlüsselung, VPNs) sinnvoll. Diesem Ansatz entsprechend besagt der Koalitionsvertrag der neuen Bundesregierung, Anonymisierungstechniken fördern zu wollen. Darüber hinaus soll „rechtswidrige Deanonymisierung" unter Strafe gestellt werden (SPD; Bündnis 90/Die Grünen; FDP 2021: 17). Des Weiteren soll „anonyme und pseudonyme Online-Nutzung" gewahrt (SPD; Bündnis 90/Die Grünen; FDP 2021: 18) und das „Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet" gewährleistet werden (SPD; Bündnis 90/Die Grünen; FDP 2021: 109).

C. REGULIERUNG NEUER TECHNOLOGIEN

Die EU-Digitalgesetzgebung ist aktuell in einem „Overdrive". DSA, DMA, DGA und AI Act werden die digitale Ordnung maßgeblich beeinflussen. Der DSA und DMA wurden bereits verabschiedet und der DGA ist seit Juni 2022 in Kraft. Die neue Bundesregierung steht den europäischen Regulierungsansätzen befürwortend gegenüber (SPD; Bündnis 90/Die Grünen; FDP 2021: 18, 124). Insbesondere der risikobasierte Ansatz des AI Act wird von der Bundesregierung unterstützt. In Bezug auf DSA und DMA legt die Bundesregierung Wert auf die Abbildung von „Pluralismus und Vielfalt" sowie die Gewährleistung einer „staatsfernen Medienaufsicht und Regulierung" (SPD; Bündnis 90/Die Grünen; FDP 2021: 18, 124). Beide Werte finden sich auch als Regelungsziele im Media Freedom Act, der als Entwurf im September 2022 vorgelegt wurde.

D. ALGORITHMISCHE ENTSCHEIDUNGSSYSTEME

Eine in der Praxis wichtige Ausprägung von künstlicher Intelligenz sind algorithmische Entscheidungs- und Empfehlungssysteme (wobei diese nicht immer und nicht notwendigerweise KI-Aspekte aufweisen). In umfassenden Teilen des alltäglichen Lebens sind algorithmische Entscheidungssysteme zunehmend involviert und stellen häufig Herausforderungen für den Menschenrechtsschutz dar: Im Bereich von privaten Kommunikationsplattformen und Inhalte-Governance, aber auch in vielen weiteren Bereichen, etwa in der Risikobewertung, der Kreditvergabe, der Visavergabe und der Arbeitsplatzbewirtschaftung kommen sie regelmäßig (weltweit) zum Einsatz. Durch die in das System eingespeisten Lerndaten findet Diskriminierung aus der analogen Welt Eingang in den digitalen Raum. Ungerechtigkeiten der Vergangenheit werden so technisch kaschiert und weitergeschrieben.

Werden derartige Systeme eingesetzt, ist in einem ersten Schritt erhöhte Transparenz wünschenswert.[5] Relevant ist dabei auch die Transparenz der verwendeten Daten, deren Auswahl wesentlichen Einfluss auf die Entscheidungen des Systems hat. Nur wenn ausreichend Transparenz bezüglich dieser Daten besteht, lässt sich auch beurteilen, wie sich das System auswirkt und ob es etwa zu diskriminierenden Entscheidungen kommt (Kettemann 2020: 35; Ananny/Crawford 2018). Eine Empfehlung der UNESCO zu KI und Ethik geht hier weiter und fordert, etwa im Bereich Gender, nicht nur Maßnahmen gegen Diskriminierung durch KI-Systeme, sondern hält die Mitgliedstaaten darüber hinaus auch an, die Vielfalt in der Technologiebranche selbst zu fördern, in der unter anderem Frauen nach wie vor stark unterrepräsentiert sind (Kettemann 2022).

Der Koalitionsvertrag enthält bezüglich der Transparenz algorithmischer Entscheidungssysteme und künstlicher Intelligenz wenige Anhaltspunkte. Lediglich in Zu-

Plenartagung über den Digital Services Act im Europäischen Parlament

▸▸ Der Digital Services Act sieht vor, dass ein Koordinator für Digitale Dienste ernannt wird. Diese unabhängige Institution muss verschiedene Rollen und Kompetenzen in sich vereinen, darunter jene, die aktuell (unter anderem) von den Landesmedienanstalten, den Datenschutzbehörden, den Jugendschutzbehörden, dem Bundesamt für Justiz und den Konsumentenschützer_innen innegehabt werden. Die genaue Ausgestaltung ist noch unklar, allerdings scheint die Bundesnetzagentur eine wichtige Rolle einzunehmen. Deren Konturen müssen im Rahmen eines Regulierungsinnovationsprozesses erst gezeichnet werden.

5 An unterschiedlichen Stellen wird „Transparency" als zentrales Prinzip beim Einsatz künstlicher Intelligenz genannt, siehe etwa Europäische Kommission (2019).

Joy Buolamwini, Gründerin der Algorithmic Justice League

▸▸ Im September 2022 kündigte Microsoft an, vorerst aufgrund deren Fehleranfälligkeit keine automatisierte Gesichtserkennungssoftware anzubieten (Netzpolitik 2022). Der Einsatz von Gesichtserkennungssoftware sorgte bereits 2018 für Aufsehen, das Problem ist nach wie vor aktuell: Wissenschaftler_innen haben erkannt, dass derartige Software für weiße Männer gut funktioniert, für People of Color und vor allem Women of Color allerdings große Defizite aufweist (Buolamwini/Gebru 2018) und in den USA sogar zu fälschlichen Verhaftungen führte (Futurezone 2020). Woran liegt das? Vor allem an einseitigen Datensets, in denen bestimmte Personengruppen unterrepräsentiert sind, sowie an falschen Belohnungsstrukturen der Algorithmen (hier fehlt Diversität der Ergebnisse als Erfolgsmatrix für das Programm) sowie mangelnder Diversität der Entwickler_innenteams.

▸▸ Uploadfilter, also künstliche Filter, die bereits vor dem Hochladen von Inhalten deren Zulässigkeit beurteilen, werden aufgrund möglicher Einschränkungen der Meinungsfreiheit innerhalb der Union nach wie vor kritisch diskutiert. Erst kürzlich entschied der EuGH jedoch, dass – unter engen Bedingungen und unter Wahrung der Verhältnismäßigkeit – die Verpflichtung von Dienstanbieter_innen, zum Schutz des geistigen Eigentums eine vorherige Überprüfung hochzuladender Inhalte durchzuführen, mit dem Grundrecht auf Meinungsäußerungsfreiheit noch vereinbar sei (Etteldorf 2022).

Protest gegen Uploadfilter

sammenhang mit dem DSA wird die „Überprüfbarkeit“ algorithmischer (Empfehlungs-)Systeme als sinnhaft erwähnt (SPD; Bündnis 90/Die Grünen; FDP 2021: 17). Diese wird im DSA nun auch verpflichtend eingeführt.

Aktuell ist dieser Bereich in Deutschland noch größtenteils unreguliert. Auf europäischer Ebene sollen gemäß dem AI Act etwa KI-Systeme, die die Sicherheit, Lebensgrundlagen und Rechte der Menschen klar bedrohen, verboten werden (Europäische Kommission 2021b). Ähnlich fordert Amnesty International in einer Stellungnahme zum 14. Menschenrechtsbericht der Bundesregierung ein „Verbot der Anwendung[en] Künstlicher Intelligenz, die mit unvertretbaren Risiken für die Menschenrechte einhergehen“ (Amnesty International 2021b: 22). Beispielhaft werden Gesichtserkennungsmaßnahmen im öffentlichen Raum angeführt (Amnesty International 2021b: 22), die – ebenso wie Social-Scoring-Systeme – auch im Koalitionsvertrag der neuen Bundesregierung ausdrücklich abgelehnt werden (SPD; Bündnis 90/Die Grünen; FDP 2021: 18). Folgerichtig tritt Deutschland auch beim Entwurf des AI Acts für ein Verbot der Nutzung biometrischer Daten ein, wie sie etwa von Clearview AI – einer bildbasierten Suchmaschine auf Basis von Millionen rechtswidrig gescrapeter Daten – genutzt werden.

Die Bundesregierung führt an, Informations- und Meinungsfreiheit beim Einsatz automatisierter Entscheidungsmechanismen gewährleisten zu wollen (SPD; Bündnis 90/Die Grünen; FDP 2021: 123); dies bezieht sich insbesondere auf das Funktionieren von Empfehlungsalgorithmen. Die Logiken dieser Algorithmen offenlegen zu müssen ist als Pflicht im DSA für große Plattformen vorgesehen.

E. ONLINE-MEINUNGSFREIHEIT

Menschenrechtlich geschützt ist nicht nur die Freiheit, Meinungen zu äußern, sondern auch, Informationen zu beschaffen oder weiterzuverbreiten. Von besonderer Bedeutung sind private digitale Kommunikationsräume, in denen Meinungsaustausch vermehrt stattfindet. In ihrer Funktion als private Räume kommt den jeweiligen Plattformen grundsätzlich das Hausrecht zu, kurz gesagt also die Möglichkeit, zu bestimmen, welche Inhalte veröffentlicht werden dürfen und welche nicht. Hier braucht es Re-

gulierung, die Meinungsfreiheit schützt, gleichzeitig aber Hass im Netz und Desinformation vorbeugt. Inwieweit der Staat hier in private Räume eingreifen darf (oder soll), ist Gegenstand vielzähliger Diskussionen. Die Nichtregierungsorganisation AccessNow zeigt exemplarisch auf, welche Risiken für den Menschenrechtsschutz staatliche Regulierung birgt und wie diese menschenrechtsschützend umgesetzt werden kann: Zentral sind dabei Möglichkeiten zur effektiven Rechtsdurchsetzung von Nutzer_innen durch funktionierende Meldemechanismen sowie Transparenzverpflichtungen (AccessNow 2020).

Deutschland hat mit dem NetzDG einen Trend zu umfassender Regulierung angestoßen. Andere Staaten, etwa Brasilien und Österreich, folgten dem deutschen Beispiel, Plattformen bestimmte Transparenz- und Rechenschaftspflichten aufzuerlegen. In den nächsten Jahren wird in der EU der DSA für Veränderung sorgen, das NetzDG aber nicht gänzlich verdrängen. So verweist der DSA nicht konkret auf staatliche Strafrechtsnormen und enthält auch keine klaren Fristen. Generell werden durch den DSA – schon alleine aus Kompetenzgründen – keine neuen inhaltlichen Regeln aufgestellt. Ein Schwerpunkt liegt hingegen in der eingeforderten Transparenz, zu der private Plattformen verpflichtet werden. Welche Inhalte online bleiben oder gelöscht werden, wann User_innen gesperrt werden, wie algorithmische Entscheidungssysteme zur Moderierung der Plattform eingesetzt werden – all dies sind Fragen, zu deren Klärung verstärkte Transparenz beitragen kann. Schon das sahen Transparenzberichte über den Umgang der Plattformen mit rechtswidrigen Inhalten und Beschwerden vor.[6] Wichtig ist eine entsprechende Kontrolle der Einhaltung der Transparenzverpflichtungen.[7]

Bezüglich des NetzDG hält der Koalitionsvertrag fest, dass dieses nach Einführung des DSA überarbeitet werde (SPD; Bündnis 90/Die Grünen; FDP 2021: 17). Verpflichtende Uploadfilter lehnt die neue Bundesregierung entschieden ab (SPD; Bündnis 90/Die Grünen; FDP 2021: 110). Interessant ist auch, dass die Bundesregierung anführt, den „Aufbau von Plattformräten" fördern zu wollen (SPD; Bündnis 90/Die Grünen; FDP 2021: 17).

Gedenkveranstaltung für Ärztin Kellermayr

▸▸ Im Jahr 2022 brachte der österreichische Fall der Ärztin Lisa-Maria Kellermayr erneute Diskussionen um Hate Speech und digitale Gewalt hervor. Die Ärztin war über Monate auf sozialen Medien beleidigt, beschimpft und sogar mit dem Mord bedroht worden, was schließlich im Suizid der Ärztin mündete (Süddeutsche Zeitung 2022). Der Fall zeigt: Hate Speech und digitale Gewalt wirken sich schwerwiegend auf betroffene Personen aus.

F. EINDÄMMUNG VON HASS, HETZE UND DESINFORMATION IM NETZ

I. HATE SPEECH UND DIGITALE GEWALT

Der schwierige Ausgleich zwischen Meinungsfreiheit und Verhinderung von Hate Speech und digitaler Gewalt stellt eine große Herausforderung dar. In einer 2019 bundesweit durchgeführten Studie gaben 40 Prozent der Befragten an, Hate Speech im Internet wahrgenommen zu haben. Noch mehr (54 Prozent) gaben an, sich aufgrund von Hate Speech weniger in Diskussionen im Internet einzubringen (Geschke et al. 2019).

Von Bedeutung ist hier einerseits, den (straf- und zivil-)rechtlichen Rahmen laufend zu überprüfen und gegebenenfalls anzupassen. An dieser Stelle sei auf Forderungen hingewiesen, die zivilgesellschaftliche Akteur_innen formuliert haben (Campact 2022: HateAid 2022).

Andererseits ist eine über den individuellen Fall hinausgehende Bekämpfung von Hate Speech und Gewalt notwendig. Im Zusammenhang mit Gendered Hate Speech und der vermehrten Betroffenheit von Frauen zeigt sich vor allem, dass eine ausreichende wissenschaftliche, politische und juristische Auseinandersetzung mit diesem Thema fehlt. Sinnvoll wäre, Informationen über die Genderdimension in die vom NetzDG vorgeschriebenen Transparenzberichte aufzunehmen, um umfassendere Daten zu gewinnen.[8] Das No Hate Speech Movement weist außerdem

6 Nähere Informationen zur Umsetzung dieser Vorschrift finden sich im Bericht der Bundesregierung zur Evaluierung des NetzDG, https://www.bmjv.de/SharedDocs/Downloads/DE/News/PM/090920_Evaluierungsbericht_NetzDG.pdf;jsessionid=1AEFF5C048A9B155DF28DE79AD5D8BE6.2_cid297?__blob=publicationFile&v=3 (5.10.2022).

7 So etwa die Forderung eines Zusammenschlusses aus zivilgesellschaftlichen Organisationen, vgl. Governing Platforms Project (2020).

8 Ausführlich zu Gendered Hate Speech etwa Kettemann (2020: 38ff.).

EUvsDisinfo

▸▸ Parallel zu Russlands Angriffskrieg gegen die Ukraine wurde von vor allem russischen Akteur_innen ein „Informationskrieg" begonnen. Behauptungen, wie etwa, dass das Referendum in Donbass historisches Unrecht korrigiert hätte oder Russland in der Ukraine die NATO bekämpfen würde, wurden von einer Einheit des Europäischen Auswärtigen Dienstes (EAD) aufgedeckt und als falsche Behauptungen widerlegt. Auf der Internetseite des EAD, EUvsDisinfo, werden diese und weitere aktuelle Fälle aufgelistet (EAD, EUvsDisinfo 2022; Presse- und Informationsamt der Bundesregierung 2022).

schon 2016 darauf hin, dass „[n]eben muslimischen und geflüchteten Frauen […] vor allem Feministinnen und jene, die in der Öffentlichkeit stehen" (Geisler 2016), betroffen sind; das hat sich leider nicht geändert.

Dem aktuellen Koalitionsvertrag ist zu entnehmen, dass die neue Bundesregierung ein Gesetz gegen digitale Gewalt erlassen wird, um rechtliche Hürden für Betroffene abzubauen und Beratungsstellen einzurichten (SPD; Bündnis 90/Die Grünen; FDP 2021: 18). Bezüglich Gendered Hate Speech und queerfeindlicher Hasskriminalität wird angemerkt, dass die Polizei in Bund und Ländern die sich darauf beziehende Kriminalität separat erfassen soll (SPD; Bündnis 90/Die Grünen; FDP 2021: 119).

II. DESINFORMATION

In Zeiten der Covid-19-Pandemie, die viele Diskussionen und einen Großteil des Informationsaustausches in den digitalen Raum verlagert hat, im Zusammenhang mit der US-Wahl und dem Superwahljahr 2021 und noch einmal verstärkt durch den russischen Angriff auf die Ukraine, ist das Problem der Desinformation vermehrt in den Fokus gerückt. Ein im Mai 2021 erstelltes Gutachten zeigt auf, wo im deutschen Rechtssystem noch Lücken im Hinblick auf den Umgang mit Desinformation bestehen und wie sich diese möglicherweise schließen lassen (Dreyer et al. 2021). Daraus ergibt sich, dass die rechtlichen Möglichkeiten zur Eindämmung von Desinformation aktuell sehr eingeschränkt sind, insbesondere wenn keine individuellen Persönlichkeitsrechte betroffen sind. Vorgeschlagen werden im Gutachten etwa Regelungen, die bei unwahren Äußerungen im Zusammenhang mit Wahlen Abhilfe schaffen sollen, oder Regelungen, die dann greifen sollen, wenn mit Desinformation Gefahren für höchste individuelle Rechtsgüter wie Leben und körperliche Unversehrtheit drohen. In diesen Fällen wird auch eine vorläufige Löschung der Inhalte erwogen, die erst später eine Überprüfung erfährt (Dreyer et al. 2021: 97f.).

Im Koalitionsvertrag finden sich für den Umgang mit Desinformationen keine expliziten Commitments. Es wird lediglich erwähnt, dass man sich im Rahmen des DSA für klarere Regelungen gegen Desinformation einsetzen wolle (SPD; Bündnis 90/Die Grünen; FDP 2021: 17). Dies verwundert nicht, ist doch Desinformation notorisch schwer regulativ zu fassen. Wie eine ausführliche Studie vor Kurzem nachzeichnete, müssten im Zentrum gesetzlicher Gegenmaßnahmen die Gefährdungspotenziale von Äußerungen für individuelle Rechte und gesellschaftliche Interessen stehen: „Wo geschützte Rechte durch Äußerungen betroffen sind, öffnet sich für den Gesetzgeber grundsätzlich eine Eingriffsbefugnis" (Dreyer et al. 2021). Das für gelingende Selbstvergewisserung erforderliche Funktionieren dieses diskursiven Prozesses können staatliche Maßnahmen nur sehr begrenzt gewährleisten. So schreiben die Autor_innen: „An die Unwahrheit anknüpfende Maßnahmen kommen in Betracht, wenn mit hoher Wahrscheinlichkeit unmittelbare Gefahren für höchste individuelle Rechtsgüter wie Leben und körperliche Unversehrtheit drohen" (Dreyer et al. 2021).

G. HANDEL MIT DIGITALEN TECHNOLOGIEN

Der Handel mit digitalen Technologien ist auch aufgrund des Exports von Überwachungstechnologien immer wieder in der Diskussion.[9] Es soll verhindert werden, dass derartige Technik in Staaten mit unter Umständen niedrigen Menschenrechtsstandards exportiert und dort missbräuchlich bzw. menschenrechtsverletzend angewandt wird. Trotz Wassenaar-Abkommen oder der Dual-Use-Verordnung exportiert Deutschland nach wie vor Überwachungstechnologien (Biermann 2019).

Der UN-Sonderberichterstatter für den Schutz der Meinungsfreiheit, David Kaye, gab 2019 Empfehlungen für Menschenrechtsschutz im Zusammenhang mit digitalen Überwachungstechnologien: Als ersten Punkt forderte er ein Moratorium für den Verkauf, Transfer und die Nutzung privat entwickelter Überwachungstechnologien, das so lange bestehen bleiben sollte, bis in diesem Bereich Menschenrechte ausreichend geschützt werden können (Kaye 2019: 20). Darüber hinaus empfahl er den dem Was-

9 Die Ausführungen in diesem Abschnitt beruhen auf Überlegungen von Kettemann (2020).

senaar-Abkommen beigetretenen Staaten, die Vereinbarkeit einer Technologie mit den Menschenrechten als Voraussetzung für deren Genehmigung zu prüfen (Kaye 2019: 20).

Als Lösung werden etwa weitreichendere internationale Abkommen vorgeschlagen, insbesondere mit mehr Unterzeichnenden (so sollen etwa auch mehr Staaten dem Wassenaar-Abkommen beitreten). Auch eine externe Überprüfung der Exportgenehmigungen im Hinblick auf die Übereinstimmung mit Menschenrechtsstandards wird empfohlen. Im Sinne vermehrter Transparenz wird die Veröffentlichung aller bestätigten oder abgewiesenen Genehmigungsanträge sowie die Einbeziehung lokaler zivilgesellschaftlicher Organisationen des Staates, in die digitale Technologien exportiert werden soll, vorgeschlagen (Wagner 2021).

In ihrem Koalitionsvertrag bekräftigt die neue Bundesregierung, einen „Stopp der Weitergabe von Überwachungstechnologien an repressive Regime“ zu befürworten und insgesamt eine „Politik der Abrüstung“ zu verfolgen (SPD; Bündnis 90/Die Grünen; FDP 2021: 144).

H. DIGITALER MENSCHENRECHTSSCHUTZ IN INTERNATIONALEN FOREN

Die (frühere) deutsche Bundesregierung betonte den Einsatz für die Stärkung des digitalen Menschenrechtsschutzes in unterschiedlichen internationalen Foren und Organisationen, darunter im UN-Menschenrechtsrat, im dritten Ausschuss der UN-Vollversammlung (zuständig für soziale, humanitäre und kulturelle Fragen), im Rahmen der EU, der UNESCO und des Europarats sowie insbesondere auch im Rahmen der Freedom Online Coalition, eines Zusammenschlusses aus aktuell 32 Staaten mit dem Ziel der Stärkung digitaler Menschenrechte.

Neben inhaltlicher Beteiligung ist auch an budgetäre Beiträge zu denken. Amnesty International fordert etwa einen außerbudgetären Beitrag Deutschlands zur Schaffung einer digitalen Infrastruktur für mehr Effizienz und Transparenz in der Menschenrechtsarbeit der Vereinten Nationen (Amnesty International 2021b: 14).

Auch die neue Bundesregierung ist bestrebt, den Menschenrechtsschutz auszuweiten und zu verbessern. Im Ko-

Firmensitz FinFisher

▸▸ Obwohl der Export von Überwachungstechnologien in der EU genehmigungspflichtig ist, kommt es nach wie vor zu illegalen Exporten: Bereits 2019 wurde daher ein Strafverfahren gegen das Unternehmen FinFisher GmbH eingeleitet, das weltweit die Überwachungssoftware „FinSpy“ vertrieb, 2022 stellte das Unternehmen den Geschäftsbetrieb ein. Problematisch ist der Vertrieb der Software vor allem, wenn diese von repressiven Regimen zur Überwachung etwa von Aktivist_innen oder Journalist_innen eingesetzt wird (Gesellschaft für Freiheitsrechte 2022).

▸▸ In ihrem letzten Bericht an die Generalversammlung vom Sommer 2022 unterstrich die Sonderberichterstatterin für die Förderung und den Schutz des Rechts auf Meinungsfreiheit und freie Meinungsäußerung, Irene Khan, die Herausforderungen, die die Manipulation von Informationen für das Recht auf freie Meinungsäußerung während bewaffneten Konflikten darstellen. In ihrem Bericht stellt sie fest, dass das Informationsumfeld im digitalen Zeitalter zu einem gefährlichen Kriegsschauplatz geworden ist, auf dem staatliche und nichtstaatliche Akteure und soziale Medien Informationen als Waffe einsetzen (United Nations 2022).

Sonderberichterstatterin Irene Khan

alitionsvertrag wird dazu Folgendes angeführt: „Die Arbeit der UN-Vertragsorgane und Sonderberichterstatterinnen und -erstatter wollen wir stärken sowie die Ratifizierung weiterer Menschenrechtskonventionen anstreben.“ Von Belang für die Netzpolitik sind auch die beiden Ziele der Bundesregierung, die Rechte von Minderheiten auf internationaler Ebene zu stärken und für LGBTQI*-Rechte verstärkt einzutreten (SPD; Bündnis 90/Die Grünen; FDP 2021: 147). Diese Rechte sind auch in digitalen Räumen bedroht und müssen dort geschützt und garantiert werden.

I. DIGITALISIERUNG UND NACHHALTIGKEIT

Um auch für zukünftige Generationen individuelle Freiheitsräume zu sichern, spielt Nachhaltigkeit eine große Rolle. Einerseits ist Digitalisierung selbst klimaneutral und ressourcenschonend zu gestalten, etwa durch den Aufbau nachhaltiger Infrastruktur und den Verzicht auf stromintensive Datenzentren.

Smarter Kühlschrank

▸▸ Aktuell wird an vielen Entwicklungen gearbeitet, die Digitalisierung zugunsten der Nachhaltigkeit einsetzen: etwa ein Kühlschrank, der dank KI weniger Strom brauchen soll (Futurezone 2022). Gleichzeitig wird auch daran gearbeitet, digitale Produkte nachhaltiger zu gestalten, etwa durch die Verminderung der benötigten Rechenleistung von künstlicher Intelligenz (SustAIn-Magazin 2022).

Andererseits kann Digitalisierung selbst in unterschiedlichen Formen zu mehr Nachhaltigkeit beitragen, so durch den Einsatz digitaler Technologien in der Landwirtschaft oder der Stadtentwicklung. Das 2019 veröffentlichte Gutachten des WBGU („Unsere gemeinsame digitale Zukunft“) empfiehlt ausdrücklich, „die Digitalisierung in den Dienst der Nachhaltigkeit zu stellen“ (WBGU 2019: 369f.). Das Hauptgutachten dieses Beirats enthält ausführliche Handlungsempfehlungen. Im Bereich der Global Governance wird darin etwa vorgeschlagen, Deutschland solle sich für einen UN-Gipfel zum Thema „Digitalisierung und Nachhaltigkeit“ einsetzen, dessen Ergebnis eine UN-Charta sein könnte, die eine Digitalisierung im Sinne der Nachhaltigkeit fordert und entsprechende Ziele und Grundsätze festlegt (WBGU 2019: 398f.).

Aufgabe der Bundesregierung ist es auch, nachhaltigkeitsfördernde Forschung zu stärken.[10] Der Koalitionsvertrag der neuen Bundesregierung hat diesem Thema einen eigenen Unterpunkt gewidmet und einige einschlägige Maßnahmen formuliert. Zum einen sollen neue Rechenzentren ab 2027 klimaneutral betrieben werden und öffentliche Rechenzentren bis 2025 ein Umweltmanagementsystem nach dem EMAS (Eco Management and Audit Scheme) einführen; zum anderen soll der Verbrauch an Ressourcen durch die Förderung digitaler Zwillinge (virtuelle Modelle analoger Produkte) verringert werden (SPD; Bündnis 90/Die Grünen; FDP 2021: 18). ←

10 Für eine ausführliche Analyse, in welchen Bereichen Forschungsbedarf besteht, sei an dieser Stelle auf das Gutachten des WBGU verwiesen (WBGU 2019: 407ff.).

4 EMPFEHLUNGEN

A. RECHTLICHE SCHRITTE

— Gerade angesichts der Unwägbarkeiten des technologischen Fortschritts sind klare Foresight-Analysen nötig, die als Grundlage aller Gesetzgebungsprozesse im digitalen Bereich dienen sollten. Darüber hinaus sollte die Bundesregierung die Einführung eines verpflichtenden (Digital) Human Rights Impact Assessment forcieren. Dieses sollte auch berücksichtigen, wie sich das entsprechende Gesetz auf die Menschenrechtssituation in anderen Staaten auswirken könnte, sollten diese das Gesetz übernehmen. Die bestehende Zusammenarbeit mit den Technikfolgenabschätzer_innen beim Bundestag sollte zu diesem Zweck vertieft werden.

— Wie der DSA vorzeichnet, sollen die Transparenzerfordernisse im digitalen Raum erweitert werden. Im Bereich algorithmischer Entscheidungssysteme und künstlicher Intelligenz etwa ist eine Transparenzverpflichtung nicht nur bezüglich der verwendeten Systeme, sondern auch hinsichtlich der verwendeten Daten, der Entwickler_innenteams und der Ziele, auf die die algorithmischen Systeme optimiert werden, empfehlenswert, um die Verstärkung von benachteiligender Ungleichbehandlung zu verhindern.

— Die aktuell bereits bestehenden Rechtsnormen, die zum Menschenrechtsschutz im digitalen Raum beitragen, sollten in der Praxis effektiver überprüft werden. Dies bedingt, dass das zu schaffende Amt des Digital Services Coordinator ausreichend mit Kompetenzen und Ressourcen ausgestattet ist.

— Bei der Exportkontrolle ist die Menschenrechtssituation des Staates, in den digitale Dienste und Güter exportiert werden sollen, in besonderem Maße zu berücksichtigen. Zu diesem Zweck sollten Auswirkungen auf die dortige Menschenrechtssituation extern beurteilt werden, idealerweise unter Einbeziehung lokaler zivilgesellschaftlicher Organisationen. Eine entsprechende rechtliche Verpflichtung zur Durchführung dieser Abschätzung erscheint empfehlenswert.

— Bei der Verwendung algorithmischer Entscheidungssysteme und künstlicher Intelligenz sollte ein Human Rights Impact Assessment vor deren Einsatz rechtlich

verpflichtend sein, um die Wahrung menschenrechtlicher Standards zu gewährleisten.

— Ein Bekenntnis zum Schutz von Anonymisierungs- und Verschlüsselungstechnologien trägt u. a. zum Schutz der Presse bei. Global sollte die Bundesregierung etwa durch ein Verbot der Produktion, des Ankaufs und Exports von Spähsoftware dazu beitragen, dass Journalist_innen und Oppositionelle geschützt werden.

B. POLITISCHE SCHRITTE

— Die Bundesregierung sollte sich international verstärkt für einen völkerrechtlichen Vertrag zum Schutz der Infrastruktur des Internets einsetzen, um langfristig und grenzüberschreitend Zugang zum Internet zu gewährleisten.

— Im Bereich digitaler Nachhaltigkeit sollte die Bundesregierung die Implementierung der digitalen Dimension der völkerrechtlich verbindlichen Nachhaltigkeitsziele der Vereinten Nationen weiter unterstützen.

— Bei der Ausarbeitung rechtlicher Normen im Bereich der Digitalisierung sollte das Zusammenspiel staatlicher Normen und privater, unternehmenseigener Normen besondere Berücksichtigung finden. Als damit verbundene Schutzziele können die Wahrung individueller Freiheitsräume und die Sicherung gesellschaftlichen Zusammenhalts dienen.

— Die Bundesregierung sollte im Rahmen internationaler Kooperation stets menschenrechtsbasierte Digitalpolitik forcieren.

— Die Bundesregierung sollte bei ihrer Personalbesetzung für ein ausgeglichenes Geschlechterverhältnis sorgen, insbesondere bei im digitalen Bereich tätigen Führungspersonen, und innerhalb von Digitalunternehmen in allen Phasen des KI-Lebenszyklus für Diversität und Gendergerechtigkeit in Nutzungsplanung und Teamauswahl eintreten.

C. FAKTISCHE MASSNAHMEN

— Um langfristig Zugang zum Internet gewährleisten zu können, sollte die Infrastruktur weiter ausgebaut werden. Dabei ist der Breitbandausbau, insbesondere in ländlichen Gegenden, von besonderer Relevanz.

— Die Bundesregierung sollte sich für die Ausarbeitung und Umsetzung von Maßnahmen einsetzen, die den Zugang und die Nutzung des Internets für alle Personen erleichtern, insbesondere auch für Personen, die aktuell wenig im Internet aktiv sind.

— Bei ihren digitalen Angeboten sollte die Bundesregierung die Anforderungen an Barrierefreiheit konsequent umsetzen. Gleichzeitig ist eine Förderung des Privatsektors empfehlenswert, um auch hier Barrierefreiheit im digitalen Raum voranzutreiben.

— Die Förderung von zielgruppenspezifischen Digitalprojekten durch die Bundesregierung ist empfehlenswert. Insbesondere Projekte an der Schnittstelle von Digitalisierung und Nachhaltigkeit, im Bereich von Hate Speech gegen Frauen und marginalisierte Personengruppen und im Bereich der digitalen Verwaltung sind von großer Bedeutung.

— Digitale Kompetenzen sollten als Querschnittsmaterie und Schulfach ein wesentlicher Bestandteil der Schulbildung sein. Auch die digitale Versorgung von Schulen ist zu fördern. Die Förderung digitaler Kompetenzen ist auch bei Lehrkräften wesentlich. ←

LITERATURVERZEICHNIS

AccessNow 2020: 26 Recommendations on Content Governance – A Guide for Lawmakers, Regulators, and Company Policy Makers, https://www.accessnow.org/cms/assets/uploads/2020/03/Recommendations-On-Content-Governance-digital.pdf (3.10.2022).

Aktion Mensch e. V./die medienanstalten 2016: Forschungsbericht – Mediennutzung von Menschen mit Behinderungen, https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Weitere_Veroeffentlichungen/Studie-Mediennutzung_Menschen_mit_Behinderungen_Langfassung.pdf (5.10.2022).

Amnesty International 2021a: EUROPE: Proposed Legislation too Weak to Protect us From Dangerous AI Systems, https://www.amnesty.org/en/latest/news/2021/04/eu-legislation-to-ban-dangerous-ai-may-not-stop-law-enforcement-abuse (3.10.2022).

Amnesty International 2021b: Schriftliche Stellungnahme von Amnesty International zum „14. Bericht der Bundesregierung über ihre Menschenrechtspolitik", https://www.amnesty.de/informieren/positionspapiere/deutschland-stellungnahme-amnesty-menschenrechtsbericht-bundesregierung (3.10.2022).

Ananny, Mike; Crawford, Kate 2018: Seeing without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability, in: New Media and Society 20 (3), S. 973–989 (3.10.2022).

Auswärtiges Amt 2020: 14. Bericht der Bundesregierung über ihre Menschenrechtspolitik (Berichtszeitraum 1.10.2018–30.9.2020), https://www.auswaertiges-amt.de/blob/2422192/f01891c5efa5d6d89df7a5693eab5c9a/201202-mrb-14-download-data.pdf (3.10.2022).

BFIT 2021: Überwachungsstelle des Bundes für Barrierefreiheit von Informationstechnik (BFIT), Bericht der Bundesrepublik Deutschland an die Europäische Kommission über die periodische Überwachung der Einhaltung der Barrierefreiheitsanforderungen von Websites und mobilen Anwendungen öffentlicher Stellen gemäß Artikel 8 der Richtlinie (EU) 2016/2102 (1. Berichtszeitraum 1.1.2020 – 22.12.2021).

Biber, Sümeyye Elif 2021: Machines Learning the Rule of Law – EU Proposes the World's First Artificial Intelligence Act, Verfassungsblog, 13.7.2021, https://verfassungsblog.de/ai-rol (3.10.2022).

Biermann, Kai 2019: Exportkontrolle von Digitalwaffen funktioniert nicht, in: Zeit Online, 28.12.2019, https://www.zeit.de/digital/internet/2019-12/spionagesoftware-trojaner-finspy-finfisher-chaos-computer-club-digitalwaffen (3.10.2022).

Bundesnetzagentur 2022: Pressemitteilung vom 8.9.2022, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2022/20220908_UnterversorgungTK.html (13.10.2022).

Buolamwini, Joy; Gebru, Timnit 2018: Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81, 2018 Conference on Fairness, Accountability, and Transparency.

Campact-Kampagne 2022: Hate Speech im Netz stoppen, https://aktion.campact.de/hate-speech/appell-bundesweit/teilnehmen?utm_source=homepage&utm_medium=cms

Council of Europe 2018: Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications, Straßburg, https://ec.europa.eu/futurium/en/european-ai-alliance/study-human-rights-dimensions-automated-data-processing-techniques-particular.html (3.10.2022).

Dreyer, Stephan; Stanciu, Elena; Potthast, Keno Christopher; Schulz, Wolfgang 2021: Desinformation: Risiken, Regulierungslücken und adäquate Gegenmaßnahmen, wissenschaftliches Gutachten im Auftrag der Landesanstalt für Medien NRW, Hamburg, https://leibniz-hbi.de/uploads/media/default/cms/media/w4ru5o8_Desinformation-Rechtsgutachten.pdf (5.10.2022).

EAD EUvsDisinfo 2022: Disinfo Database, https://euvsdisinfo.eu/de/disinfo-database-de/ (13.10.2022).

Etteldorf, Christina 2022: EuGH: Zukunft der Upload-Filter und Vereinbarkeit mit der Meinungsfreiheit, MMR-Aktuell, Ausgabe 8 (2022), München.

Europäische Kommission 2019: AI HLEG, High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html (5.10.2022).

Europäische Kommission 2020a: Digital Economy and Society Index (DESI) 2020 – Digital Public Services, https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020 (5.10.2022).

Europäische Kommission 2020b: DESI Country Profile – Germany (2020), https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020 (5.10.2022).

Europäische Kommission 2020c: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, COM(2020) 825 final, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0825 (5.10.2022).

Europäische Kommission 2021a: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 2030 Digital Compass: The European Way for the Digital Decade, COM(2021) 118 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118&from=fr (5.10.2022).

Europäische Kommission 2021b: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=ES (5.10.2022).

Europäischer Rat, Gesetz über digitale Märkte 2022: Neue Vorschriften für fairen Online-Wettbewerb vom Rat endgültig gebilligt, Pressemitteilung vom 18.7.2022, https://www.consilium.europa.eu/de/press/press-releases/2022/07/18/dma-council-gives-final-approval-to-new-rules-for-fair-competition-online/pdf (5.10.2022).

Futurezone 2020: Unschuldiger wegen Gesichterkennungs-Fehler verhaftet, 24.6.2020, https://futurezone.at/netzpolitik/unschuldiger-wegen-gesichtserkennungs-fehler-verhaftet/400950371 (13.10.2022).

Futurezone 2022: Samsung-Kühlschrank soll dank KI ein Drittel weniger Strom brauchen, 1.9.2022, https://futurezone.at/produkte/samsung-smart-things-energy-energiesparen-smart-home-ifa/402130910 (13.10.2022).

Futurezone 2022a: Daten aus dem Cyberangriff auf die MedUni Innsbruck aufgetaucht, 27.6.2022, https://futurezone.at/digital-life/cyberangriff-medizinische-universitaet-innsbruck/402054436 (13.10.2022).

Geisler, Sarah 2016: Öfter im Shitstorm, in: fluter.de, 7.12.2016, https://www.fluter.de/Frauen-oefter-Opfer-von-Hate-Speech (5.10.2022).

Geschke, Daniel; Klaßen, Anja; Quent, Matthias; Richter, Christoph 2019: Forschungsbericht zu Hass im Netz: Der schleichende Angriff auf unsere Demokratie, https://www.idz-jena.de/fileadmin/user_upload/_Hass_im_Netz_-_Der_schleichende_Angriff.pdf (5.10.2022).

Gesellschaft für Freiheitsrechte 2021: Spähsoftware gegen Studierende: Online-Proctoring als Gefahr für die IT-Sicherheit und den Datenschutz, 14.7.2021, https://legacy.freiheitsrechte.org/home/wp-content/uploads/2021/07/GFF_IT-Gutachten_Proctoring-Spaehsoftware-gegen-Studierende.pdf (13.10.2022).

Gesellschaft für Freiheitsrechte 2022: Strafanzeige gegen illegalen Export von Überwachungssoftware zeigt Wirkung: Die FinFisher-Unternehmensgruppe stellt nach Kontopfändung durch Staatsanwaltschaft den Geschäftsbetrieb ein, 28.3.2022, https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-finfisher-insolvenz (14.10.2022).

Gleiß, Hanna; Laubenstein, Sina 2020: Maßnahmen und Strategien zur Bekämpfung von Hate Speech auf europäischer Ebene – ein Überblick, http://library.fes.de/pdf-files/dialog/17430.pdf (5.10.2022).

Global Commission on the Stability of Cyberspace 2017: Call to Protect the Public Core of the Internet, New Delhi.

Governing Platforms Project 2020: Putting Meaningful Transparency at the Heart of the Digital Services Act – Why Data Access for Research Matters & How We Can Make It Happen, https://algorithmwatch.org/en/wp-content/uploads/2020/10/Governing-Platforms_DSA-Recommendations.pdf (5.10.2022).

HateAid 2022: Unsere politischen Forderungen, https://hateaid.org/politische-forderungen/ (5.10.2022).

HateAid/Landecker Digital Justice Movement 2022: Grenzenloser Hass im Internet – Dramatische Lage in ganz Europa, https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021-DE.pdf (13.10.2022).

Kaye, David 2019: 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, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement (5.10.2022).

Kettemann, Matthias C. 2015: Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht, Friedrich-Ebert-Stiftung, Bonn, https://library.fes.de/pdf-files/akademie/12068.pdf (24.10.2022).

Kettemann, Matthias C. 2019: Standpunkt: Ein Internet für alle Menschen, in: Tagesspiegel Background, 5.6.2019, https://background.tagesspiegel.de/digitalisierung/ein-internet-fuer-alle-menschen (5.10.2022).

Kettemann, Matthias C. 2020: Menschenrechte und politische Teilhabe im digitalen Zeitalter: Stellungnahme als Sachverständiger auf Einladung des Ausschusses für Menschenrechte und humanitäre Hilfe des Deutschen Bundestags, Working Papers of the Hans-Bredow-Institut I Works in Progress 2/2020, Hamburg, https://www.ssoar.info/ssoar/handle/document/71723 (5.10.2022).

Kettemann, Matthias C.; Fertmann, Martin (Hrsg.) 2020: Viral Information: How States and Platforms Deal with Covid-19-related Disinformation: an Exploratory Study of 20 Countries, GDHRNet WorkingPaper #1, Hamburg, https://leibniz-hbi.de/uploads/media/default/cms/media/ry5rg42_GDHRNet_Working%20Paper1.pdf (5.10.2022).

Kettemann, Matthias C.; Fertmann, Martin 2021: Die Demokratie plattformfest machen – Social Media Councils als Werkzeug zur gesellschaftlichen Rückbindung der privaten Ordnungen digitaler Plattformen, https://leibniz-hbi.de/de/publikationen/die-demokratie-plattformfest-machen (5.10.2022).

Kettemann, Matthias C.; Paulus, Alexandra 2020: Ein Update für das Internet: Reform der globalen digitalen Zusammenarbeit 2021, Global Governance Spotlight 4/2020, Stiftung Entwicklung und Politik (sef), Bonn, https://www.sef-bonn.org/fileadmin/SEF-Dateiliste/04_Publikationen/GG-Spotlight/2020/ggs_2020-04_de.pdf (5.10.2022).

Kettemann, Matthias C.; Tiedeke, A. S. 2020: Back up: Can Users Sue Platforms to Reinstate Deleted Content?, in: Internet Policy Review 9 (2), https://doi.org/10.14763/2020.2.1484 (5.10.2022).

Kettemann, UNESCO-Empfehlung zur Ethik Künstlicher Intelligenz 2022: Bedingungen zur Implementierung in Deutschland, Bonn, https://www.unesco.de/sites/default/files/2022-03/DUK_Broschuere_KI-Empfehlung_DS_web_final.pdf (5.10.2022).

Netzpolitik 2021: Online-Prüfungsüberwachung verletzt Datenschutz und IT-Sicherheit, 14.7.2021, https://netzpolitik.org/2021/gutachten-online-pruefungsueberwachung-verletzt-datenschutz-und-it-sicherheit/ (13.10.2022).

Netzpolitik/Beckedahl 2022: Irgendwas mit Internet: Fördert endlich Anti-Zensur-Tools! 6.10.2022, https://netzpolitik.org/2022/irgendwas-mit-internet-foerdert-endlich-anti-zensur-tools/ (14.10.2022).

Netzpolitik 2022: Ethik der Biometrie: Microsoft gesteht Missbruachsgefahr von Gesichtserkennung ein, 29.6.2022, https://netzpolitik.org/2022/ethik-der-biometrie-microsoft-gesteht-missbrauchsgefahr-von-gesichtserkennung-ein/ (14.10.2022).

Presse- und Informationsamt der Bundesregierung 2022: Analyse zur russischen Desinformation: Desinformation als Waffe, 10.8.2022, https://www.bundesregierung.de/breg-de/themen/krieg-in-der-ukraine/eu-gegen-desinformation-2007442 (13.10.2022).

Rat der EU 2020: Einigung über neue Vorschriften für den Handel mit Gütern mit doppeltem Verwendungszweck, Pressemitteilung, 9.11.2020, https://www.consilium.europa.eu/de/press/press-releases/2020/11/09/new-rules-on-trade-of-dual-use-items-agreed (5.10.2022).

Schulz, Wolfgang et al. 2021: Die Lage des Internets in Deutschland – Anwendung der UNESCO-Internet-Universalitäts-Indikatoren in Deutschland und Erstellung eines Ergebnisberichts (IUI), Hans-Bredow-Institut, Hamburg, https://wiegehtsdeminternet.de (5.10.2022).

SPD; Bündnis 90/Die Grünen, FDP 2021: Mehr Fortschritt wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021–2025 zwischen SPD/Bündnis 90/Die Grünen/FDP: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (5.10.2022).

Süddeutsche Zeitung 2022: Suizid einer Ärztin entfacht Debatte um Hass im Netz, 2.8.2022, https://www.sueddeutsche.de/gesundheit/gesundheit-suizid-einer-aerztin-entfacht-debatte-um-hass-im-netz-dpa.urn-newsml-dpa-com-20090101-220802-99-246617 (13.10.2022).

SustAIn-Magazin 2022: sustain: Nachhaltige KI in der Praxis, Magazin 1, https://algorithmwatch.org/de/wp-content/uploads/2022/06/Sustain_Magazin_2022_DE.pdf (24.10.2022).

Tagesschau 2022: Nach Cyberangriff auf Ukraine: Sorge um Deutschlands IT-Sicherheit, 13.4.2022, https://www.tagesschau.de/investigativ/swr/cyberkrieg-ukraine-101.html (13.10.2022).

United Nations 2020: Resolution Resolution der UN-Vollversammlung, verabschiedet am 16.12.2020: Das Recht auf Privatheit im digitalen Zeitalter, A/RES/75/176, https://digitallibrary.un.org/record/3896430?ln=en (5.10.2022).

United Nations 2022: United Nations A/77/288: Disinformation and Freedom of Opinion and Expression During Armed Conflicts – Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 12.8.2022, https://www.ohchr.org/en/documents/thematic-reports/a77288-disinformation-and-freedom-opinion-and-expression-during-armed (20.10.2022).

Wagner, Ben 2021: Whose Politics? Whose Rights? Transparency, Capture and Dual-Use Export Controls, in: Security and Human Rights 32, S. 1–12.

Wagner, Ben et al. 2020: Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act, ACM Conference on Fairness, Accountability, and Transparency, Barcelona, https://www.researchgate.net/publication/338802975_Regulating_Transparency_Facebook_Twitter_and_the_German_Network_Enforcement_Act (5.10.2022).

Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen (WBGU) 2019: Unsere gemeinsame digitale Zukunft, Berlin, https://issuu.com/wbgu/docs/wbgu_hg2019?fr=sM2JiOTEyNzMy (5.10.2022).

AUTOR_INNEN


Foto: © HBI

Prof. Dr. Matthias C. Kettemann, LL.M. (Harvard), ist Professor für Innovation, Theorie und Philosophie des Rechts und Leiter des Instituts für Theorie und Zukunft des Rechts der Universität Innsbruck, Forschungsprogrammleiter am Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), Hamburg, und Leiter der Forschungsgruppe „Globaler Konstitutionalismus und das Internet“ am Humboldt-Institut für Internet und Gesellschaft, Berlin. Nach Studien der Rechtswissenschaften in Graz, Genf und an der Harvard School habilitierte er sich an der Goethe-Universität Frankfurt 2019 mit einer Arbeit zur normativen Ordnung des Internets. Er forscht zu den Regeln der Macht und der Macht der Regeln in digitalen Räumen und war mehrfach Sachverständiger im Bundestag, Gutachter für DAX-Unternehmen und Berater für das Außen- und Wirtschaftsministerium, die deutsche UNESCO-Kommission, die Agentur der Europäischen Union für Grundrechte, die OSZE und den Europarat für Recht und Governance in der digitalen Konstellation.


Foto: © privat

Mag.a Felicitas Rachinger ist Universitätsassistentin und Dissertantin am Institut für Theorie und Zukunft des Rechts an der Universität Innsbruck mit besonderem Fokus auf Themen wie Internet Governance, Digitalrecht und Online-Moderation. Sie entwickelte zuletzt ein Codierschema für Hassrede online für Deutschland und Österreich. Sie studierte Rechtswissenschaften an den Universitäten Wien und Turku und war als Rechtsberaterin im Bereich „Antidiskriminierung und Hass im Netz“ tätig.


Foto: © privat

Mag.a Meryem Vural, LL.B., ist Universitätsassistentin und Dissertantin am Institut für Theorie und Zukunft des Rechts an der Universität Innsbruck. Ihre Forschungsschwerpunkte liegen im Europarecht, im Völkerrecht und im Recht der Digitalisierung. Sie studierte Rechtswissenschaften und Wirtschaftsrecht an der Universität Innsbruck und war Universitätsassistentin am Institut für Europa- und Völkerrecht.

WEITERE VERÖFFENTLICHUNGEN DIESER REIHE

Bürgernahe Verwaltung digital? I-Kfz und digitaler Kombiantrag; Elternleistungen im Praxistest
→ FES diskurs, Bonn Juli/2022

Bürgernahe Verwaltung digital? Digitalisierung und Automatisierung im Praxistest
→ FES impuls, Bonn Juli/2022

Wie Medienvielfalt zukunftsfest machen? Bausteine für eine konvergente Medienregulierung
→ FES diskurs, Bonn März/2022

Regulierung digitaler Plattformen als Infrastrukturen der Daseinsvorsorge
→ WiSo diskurs, Bonn April/2022

Breaking the News? Politische Öffentlichkeit und die Regulierung von Medienintermediären
→ Bonn Februar/2021

Volltexte und weitere Publikationen der Friedrich-Ebert-Stiftung unter
www.fes.de/publikationen

Impressum

November 2022

Friedrich-Ebert-Stiftung
Herausgeberin: Abteilung Analyse, Planung und Beratung
Hiroshimastraße 17, 10785 Berlin, Deutschland
www.fes.de

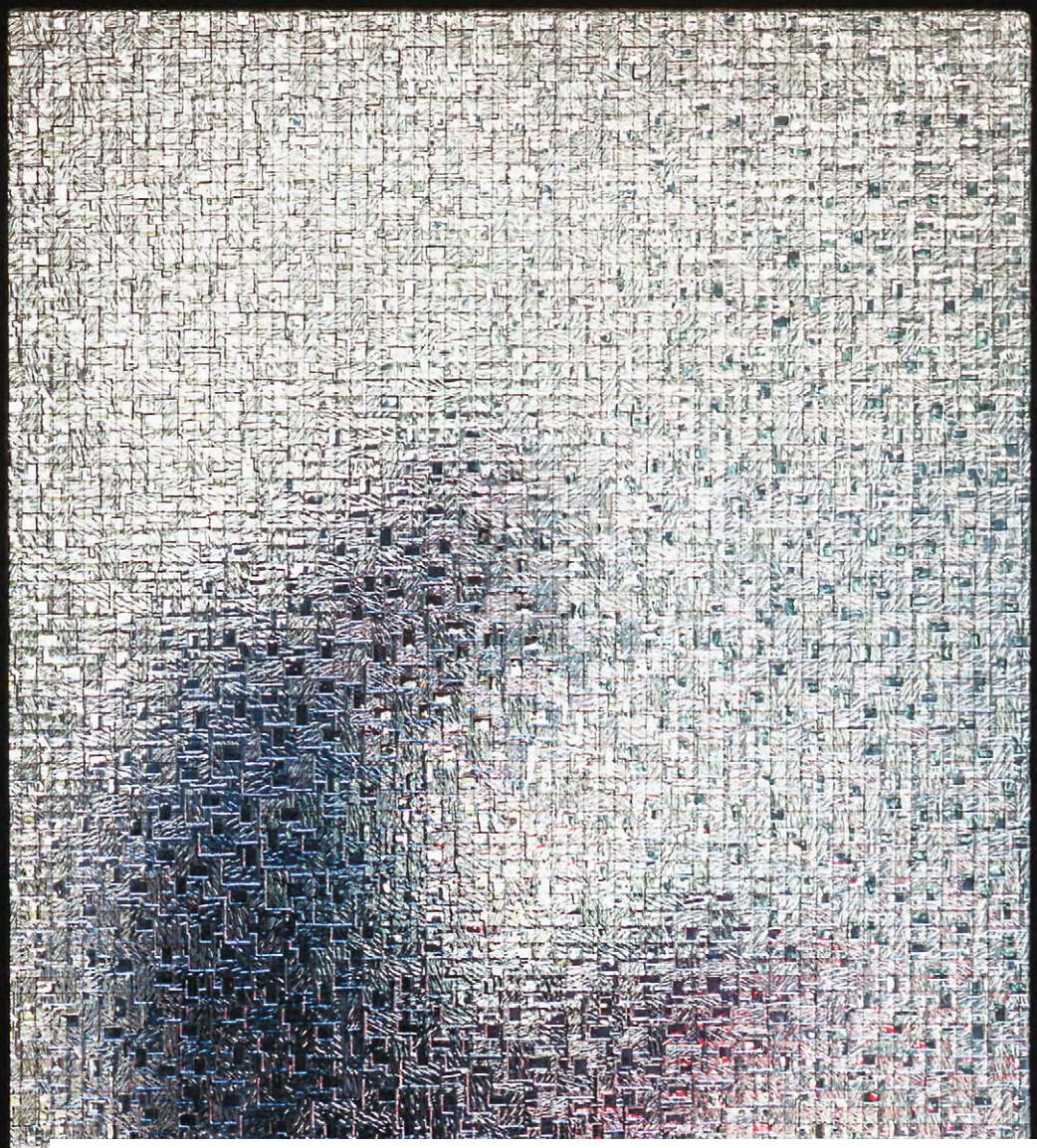
Bestellungen/Kontakt: medienpolitik@fes.de

ISBN: 978-3-98628-214-1

Titelmotiv: picture alliance/Zoonar I Ewald Fr
Fotos: picture alliance/dpa I Ole Spata (Seite 4), picture alliance/Everett Collection I Courtesy Everett Collection (Seite 6), picture alliance/dpa I Jan Woitas (Seite 8), picture alliance I Markus Scholz (Seite 9 links), picture alliance I Daniel Kubirski (Seite 9 rechts oben), picture alliance/dpa I Holger Hollemann (Seite 9 rechts unten), picture alliance/photothek I U. Grabowsky (Seite 10 links), picture alliance/ZUMAPRESS.com I Rafael Henrique (Seite 10 rechts), picture alliance/Geisler-Fotopress I Dwi Anoraganingrum (Seite 11), picture alliance/dpa I Karl-Josef Hildenbrand (Seite 12 links), picture alliance/NurPhoto I Alexander Pohl (Seite 12 rechts), picture alliance/FOTOKERSCHI.AT/APA/picturedesk.com I FOTOKERSCHI.AT (Seite 13), Screenshot https://euvsdisinfo.eu/de/ (Seite 14), picture alliance/EPA-EFE I Lukas Barth-Tuttas (Seite 15 links), picture alliance/Pacific Press I Lev Radin (Seite 15 rechts), picture alliance/Westend61 I Eva Blanco (Seite 16), picture alliance/Westend61 I Josep Suria (Seite 17)

Gestaltungskonzept: www.leitwerk.com
Umsetzung/Satz: tigerworx

Druck: Friedrich-Ebert-Stiftung, Bonn



Im digitalen Zeitalter ist das Internet zu einem wichtigen Raum für die Ausübung unserer Rechte geworden. Politische Debatten und zivilgesellschaftliches Engagement finden (nicht erst seit der Covid-19-Pandemie) vermehrt im Netz statt – wenngleich auch in Deutschland nicht alle Menschen Online-Zugang haben und noch weniger das Internet selbstermächtigt nutzen können. Zur Kehrseite der digitalisierten Kommunikation gehört unter anderem, dass Online-Hass und -Hetze zunehmen (mit Wirkungen für die Offline-Welt) und neue Macht- und Ausschlusssysteme entstehen. Algorithmische Diskriminierung und ein unterkomplexes Verständnis von Desinformation führen zu erheblichen Herausforderungen für Menschenwürde und Menschrechte. Aufgabe der Bundesregierung (und auch der EU) ist es, die Menschenrechte auch im Digitalen zu sichern und allen Bürger_innen einen diskriminierungsfreien, ermächtigenden Zugang zum Internet zu gewährleisten. Dafür bestehen einige Handlungsoptionen.

ISBN 978-3-98628-214-1

FRIEDRICH EBERT STIFTUNG