Frankfurter Studien zum Datenschutz 64

Spiecker gen. Döhmann | Westland | Campos (Hrsg.)

Demokratie und Öffentlichkeit im 21. Jahrhundert – zur Macht des Digitalen

Nomos

Frankfurter Studien zum Datenschutz

Veröffentlichungen der Forschungsstelle
für Datenschutz an der Goethe-Universität
Frankfurt am Main

Herausgegeben von
Prof. Dr. Dr. h.c. Spiros Simitis
Prof. Dr. Indra Spiecker genannt Döhmann, LL.M.

Band 64

Indra Spiecker gen. Döhmann
Michael Westland | Ricardo Campos (Hrsg.)

Demokratie und Öffentlichkeit im 21. Jahrhundert – zur Macht des Digitalen

Nomos

Bei diesem Band handelt es sich um eine Gemeinschaftsproduktion zwischen dem Lehrstuhl von Prof. Dr. Indra Spiecker genannt Döhmann und der Democratic Futures Foundation, sowie deren Geschäftsführer Dr. Michael Westland.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2022

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-8487-7483-8
ISBN (ePDF): 978-3-7489-3274-1

DOI: https://doi.org/10.5771/9783748932741

Onlineversion
Nomos eLibrary

Vorwort

‚Big Data', 'Fake News', „Bots", Filterblasen, ‚Micro-Targeting' - dies sind nur einige der Schlagwörter, die in der Debatte über die politischen Begleiterscheinungen der Digitalisierung omnipräsent sind. Spätestens seit 2016 mit Donald Trump in den USA und 2018 mit Jair Bolsonaro in Brasilien scheinbar vollkommene Außenseiter, u.a. mit Hilfe von ausgefeilten, datenbasierten Social-Media-Kampagnen, zu Präsidenten bedeutender und vermeintlich stabiler Demokratien gewählt wurden, scheint die transformative Kraft des Digitalen auch auf der großen politische Bühne nachgewiesen worden zu sein – Cambridge Analytics wurde fassbar, real und, spätestens mit dem Sturm auf das Kapitol nach der Abwahl existenziell bedrohlich. Entsprechend laut sind die Rufe nach Regulierung des digitalen Raumes, nach staatlichen Gestaltungsmodellen. Kaum ein Staat, kaum ein Ministerium, welches nicht Digitalisierungsbeauftragte einsetzt. Kaum ein Parlament, welches nicht über den Einfluss der großen Social Media Plattformen, die Gefahren russischer Hacker, chinesischer Socialscores oder über die wirtschaftlichen Konsequenzen einer datengetriebenen Welt diskutiert. Umgekehrt wird aber auch immer wieder hochgehalten, dass die Digitalisierung und damit unauflösbar verbunden das Internet zur Selbstermächtigung der Bürger/innen beitragen, dass der Kontakt zwischen Wahlvolk und Abgeordneten näher, direkter, konkreter geworden sei.

Die große Komplexität des Phänomens „Digitalisierung" mit seinen technologischen, soziologischen, politischen, wirtschaftlichen und rechtlichen Komponenten geht einher mit einer Vielzahl nebeneinander stehender Debatten in den diversen Disziplinen und der Öffentlichkeit. Diese Kakophonie verlangsamt und erschwert die Beantwortung der beiden, unserer Auffassung nach für die liberale Demokratie zentralen Fragestellungen: Welche tatsächlichen und potentiellen Auswirkungen hat die Digitalisierung auf die Demokratie? Wie kann die rechtliche und ggf. politische Struktur liberaler Demokratien angepasst werden, um die großen Chancen online- und datengetriebener Kommunikation und Entscheidungsfindung zu realisieren, ein demokratisches „level-playing field" zu bewahren und gleichzeitig zu verhindern, dass dieser neue digitale öffentliche Raume für Desinformation, Manipulation und Repression genutzt wird - innerhalb des Nationalstaates und darüber hinaus?

Der vorliegende Band zielt darauf ab, mit allen notwendigen Beschränkungen, einen interdisziplinären Überblick über Problemstellung und mögliche Lösungsansätze zu liefern.

Liberale Demokratie fußt im Kern auf dem Konzept einer Bevölkerung, die in freier öffentlicher Debatte mit sich selbst politische Lösungen entwickelt und immer wieder aufs Neue hinterfragt und anpasst - alles unter der Maßgabe des Schutzes individueller Bürger- und Freiheitsrechte. Kompromiss und die Verheißung auf stete Einflussnahmemöglichkeit gehören zwangsläufig dazu, ebenso wie Minderheitenschutz und Toleranz. Dreh- und Angelpunkt dieses Demokratieverständnisses ist ein Konzept von Öffentlichkeit, das auf der freien öffentlichen Meinungsbildung basiert.

Im ersten Abschnitt des vorliegenden Bandes beschreiben der Informatiker Johannes Buchmann, der Politikwissenschaftler Thorsten Thiel und der Soziologe Carsten Ochs aus unterschiedlichen Blickwinkeln, wie sich das etablierte Konzept der Öffentlichkeit im Lichte der Digitalisierung wandelt und wie hierdurch unser Verständnis von Demokratie herausgefordert wird.

Der zweite Abschnitt dient dazu, einige wesentliche, aber außerhalb der jeweiligen Disziplinen meist nur unzureichend verstandene Teilaspekte der Funktionsweise von Digitalisierung vertieft zu erörtern. Nach einer Beschreibung der Funktion und Verantwortung von Plattformen als Informations-Intermediäre durch den Juristen Gerald Spindler erläutern die Datenwissenschaftler Frauke Kreuter und Rubens Bach, wie der Einsatz von (Online)daten im wirtschaftlichen und politischen Prozess konkret funktioniert. Wie können welche Daten erhoben und verknüpft werden, welche Rückschlüsse auf persönliche und politische Vorlieben Einzelner lassen sich dadurch gewinnen (oder eben nicht) und wie kann dies zur Ausspielung von politischem Messaging genutzt werden? Im darauffolgenden Beitrag analysieren der Bundesdatenschutzbeauftragte Ulrich Kelber und Nils Leopold aus datenschutzrechtlicher Sicht, welche Personalisierung durch Profiling, Scoring und Microtargeting möglich ist, wie diese Verfahren funktionieren und was dies für die Demokratie bedeuten kann, beispielsweise die Möglichkeit der „gezielten Manipulation der öffentlichen Meinung, ohne dass dies von den nicht adressierten Teilen der Öffentlichkeit wahrgenommen werden kann“.

Da die Entscheidung darüber, welche/r Social-MediaNutzer/in welche Inhalte und damit welchen Teilausschnitt der digitalen öffentlichen Debatte angezeigt bekommt, in wesentlichem Umfang von Algorithmen der Künstlichen Intelligenz (KI) entschieden wird, widmet sich diesem Thema, der KI-getriebenen Kuratierung von Inhalten in Sozialen Medien sowie regulativen Antworten, der Jurist und KI-Spezialist Christian Djefall,.

Den rechtlichen Schwerpunkt des Bandes bildet der dritte Abschnitt. Wie kann es aus verfassungsrechtlicher Sicht gelingen eine Konkordanz zwischen Meinungsfreiheit, dem Schutz persönlicher Daten, der Vermeidung von Hate Speech und Desinformation und schließlich der effektiven Datennutzung im Sinne einer effizienten, wettbewerbsfähigen Wirtschaft und Verwaltung zu ermöglichen (Astrid Epiney)? Sollte unser Modell von Rundfunkfreiheit und -regulierung - geschaffen für eine Konzeption öffentlicher Meinungsbildung primär durch Großorganisationen (Parteien, Presse, Rundfunk) in der stärker in Großgruppen strukturierten Industriegesellschaft (organisationsbasierte Öffentlichkeit) - auf die gänzlich andere und individualistischere Form der Meinungsbildung mit Hilfe von Computernetzwerken angewandt oder doch grundsätzlich neu gedacht werden (Thomas Vesting)?

Wie kam es zur Entwicklung eines der wesentlichen innovativen Regulierungsansätze, des Netzwerkdurchsetzungsgesetzes, und was sind seine Auswirkungen und seine Zukunft (Alexander Peukert)? Es folgt eine Vorstellung und Kritik des Kommissionsentwurfs des europäischen Digital Services Act (Johannes Buchheim), bevor der Landesdatenschutzbeauftragte von Baden-Württemberg, Stefan Brink mit Kira Vogt, hinterfragt, inwieweit die Datenschutzgrundverordnung ein demokratisches „Level Playing Field" zu schaffen vermag.

Den vierten Abschnitt bildet eine Case Study zu Brasilien. Aufgrund der sehr hohen Social-Media Nutzung des 210 Millionen-Einwohner-Landes bei einer minimalen Regulierung war Brasilien sehr früh ein Labor für das Potential des Digitalen in der öffentlichen Meinungsbildung. Im ersten Beitrag des Abschnitts beschreiben die Sozialwissenschaftler Marco Aurelio Ruediger und Amaro Grassi von der FGV Rio de Janeiro die Mechanismen, mit denen es Rechtspopulisten Jair Bolsonaro, der jahrzehntelang unscheinbar gewesen war, 2018 gelang, ohne etablierte Partei den Wahlsieg in der größten Demokratie Lateinamerikas zu erringen. Nach dieser politikwissenschaftlich-empirischen Betrachtung, analysiert der Jurist Ricardo Campos von der Universität Frankfurt a.M./LGI den regulativen Rahmen Brasiliens, welcher die zuvor beschriebenen Entwicklungen in dieser Form erst ermöglich hat, anhand der Haftung der Intermediäre und erörtert sodann die diversen, zum Erscheinungszeitpunkt nach andauernden Reformdebatten.

Der abschließende fünfte Abschnitt weitet den Blick. Sollte die digitale Transformation von Wirtschaft und Gesellschaft weiter auf internationaler Ebene voranschreiten, ohne dass sich einzelne Gesellschaften wieder stärker hinter nationale Firewalls zurückziehen - was die Herausgeber dieses Bandes nicht als wünschenswert erachten - , so stellen sich gewichtige

Fragen für die Zukunft der Demokratie. Wie kann das demokratische level playing field unter Wahrung von individuellen Rechten geschützt werden, wenn die technologische Architektur des digitalen öffentlichen Raumes nicht zuvörderst nationalstaatlich verankert ist - und somit nicht auf der Ebene angesiedelt ist, auf der politische Teilhabe weiterhin primär organisiert wird? Wie gehen Demokratien mit den Einflußnahmeversuchen autoritärer Staaten um, sei es durch digitale Eingriffe in Wahlkämpfe und öffentliche Meinungsbildung, sei es durch den Export autoritärer Regulierungskonzepte?

In ihrem Beitrag widmen sich Marco Almada, Andrea Loreggia, Juliano Maranhao und Giovanni Sartor aus Florence, Brescia, Bologna und Sao Paulo der supranationalen *governance* der Informationsgesellschaft vor allem am Beispiel der KI-gestützten Content Moderation und Haftung Sozialer Netzwerke zwischen eCommerce Directive und Digital Service Act, auf dem Weg zu einem europäischen *digital constitutionalism*.

Doch das Neudenken der Demokratie unter Bedingungen der Digitalisierung steht noch vor einer weiteren Herausforderung. Autoritäre Staaten exportieren ihr Model der Nutzung und Regulierung des Digitalen, teils durch Technologie-Export, teils durch Bestrebungen, die Setzung neuer internationaler Standards in ihrem Sinne zu fördern. Der Beitrag der Freiburger Politikwissenschaftlerin und China-Expertin Julia Gurol skizziert hierzu exemplarisch den chinesischen Vorstoß in den digitalen Raum im Bereich Technologieexport und Internetregulierung und stellt die Herausforderungen für liberale Demokratien dar, diesen Tendenzen stärker eigene Modelle entgegenzusetzen.

Diese Aufgabe, für die demokratischen Staaten, eine gemeinsame, an den individuellen Menschenrechten westlicher Prägung orientierte Gestaltung des digitalen Raumes zu schaffen und im Wettbewerb mit autoritären Staaten die Ausbreitung ihres, an Überwachung und Repression orientierten, anti-individualistischen Modells zu verhindern, stellt eine der grundlegenden internationalen Herausforderungen zum Schutz der Demokratie dar. Dieses bedarf eines weiteren Bandes.

Zum Abschluss skizziert Matthias Kettemann Perspektiven übernationaler Plattform- und KI-Regulierung am Beispiel der UNESCO-Empfehlungen zur Governance künstlicher Intelligenz.

Dieser Sammelband ist ein Kooperationsprojekt von Ricardo Campos, Goethe Universität Frankfurt a.M./Legal Grounds Institute, Sao Paulo, Prof. Dr. Indra Spiecker gen. Döhmann LL.M., Professorin für Öffentliches Recht, Informations-, Umweltrecht und Verwaltungswissenschaft, Goethe Universität Frankfurt am Main, und Dr. Michael Westland, Gründer und Geschäftsführer des Think Tanks Democratic Futures Foundation.

Die Gründung dieses Thinktanks im Jahr 2021 gab – auf der Basis in Brasilien erfolgten intensiven Austauschs – einen wesentlichen Anstoß, diesen Band zu entwickeln.

Der Dank der Herausgeber gilt zunächst den Autor/innen, die sich neben ihren vielfältigen Verpflichtungen innerhalb ihrer Disziplinen auf diesen interdisziplinären Band eingelassen haben.

Herzlich bedanken möchten wir uns zudem bei KASTEL, Institut für Informationssicherheit und Verlässlichkeit am Karlsruher Institut für Technologie, und der Forschungsinitiative Contrust - Vertrauen im Konflikt, für deren großzügige Förderung und Unterstützung, ebenso wie dem Open Access Publikationsfonds der Goethe Universität Frankfurt a.M., auf dessen Hilfe wir unbürokratisch und schnell zugreifen durften. Schließlich ist auch der Nomos-Verlag für uns ein immer offener, flexibler und unterstützender Medienpartner. So konnten wir – ganz im Zeichen der Digitalisierung und des Erhalts eines möglichst breiten öffentlichen Raums mit Zugänglichkeit für jeden– auf dem Wege des Open Access publizieren.

Indra Spiecker gen. Döhmann
Michael Westland
Ricardo Campos

Inhalt

Demokratie und Öffentlichkeit im Digitalen Zeitalter

Johannes Buchmann

1. Einleitung

30 Jahre nach Einführung des Internets ist offensichtlich, dass sich die demokratische Öffentlichkeit durch die Digitalisierung grundlegend verändert hat. Neben Presse und Rundfunk ist eine Kommunikationsinfrastruktur getreten, die durch eine Vielzahl von digitalen Plattformen, Onlinemedien, sozialen Netzwerken, Messenger-Diensten und Suchmaschinen gekennzeichnet ist. Durch die neuen Bedingungen der öffentlichen Kommunikation sind die Institutionen und Prozesse des Informationserwerbs, der Meinungsbildung und der Partizipation in der repräsentativen Demokratie in ihren Formen und Funktionen herausgefordert. Einerseits werden Hoffnungen auf eine Weiterentwicklung der Demokratie im Sinne stärkerer Beteiligungschancen für die Zivilgesellschaft und leichter zugänglicher Informationen geweckt. Andererseits verweisen zahlreiche Fälle von Falschinformation, Manipulation und Hassrede darauf, dass die Vielfalt der verfügbaren Informationen im Web 2.0 oft gerade nicht zu fairen, tatsachenbasierten und respektvoll geführten politischen Debatten führt. In Zivilgesellschaft und Politik wächst daher die Befürchtung, dass mit der Digitalisierung Gefahren für die Demokratie und besonders für die demokratische Öffentlichkeit verbunden sind. In dieser Situation haben die Deutsche Nationalakademie der Wissenschaften Leopoldina und die Deutsche Akademie der Technikwissenschaften und die Union der Deutschen Akademien der Wissenschaften 2021 eine Stellungnahme zum Thema Digitalisierung und Demokratie vorgelegt, welche dieser Beitrag zusammenfasst.

Funktionierende Demokratien sind darauf angewiesen, dass sich die Bürgerinnen und Bürger umfassend informieren und miteinander austauschen können. Infolge der Digitalisierung ist Öffentlichkeit durch einen Zuwachs an Kommunikationsangeboten und eine Pluralisierung vernehmbarer Stimmen, aber auch durch die Struktur- und Zusammenhanglosigkeit gewaltiger Informationsmengen sowie Tendenzen der Polarisierung geprägt. Digitale Plattformen sind durch die Logik des digitalen Kapitalismus, technisch determinierte Informationsarchitekturen und al-

gorithmische Kuratierung gekennzeichnet und zwingen klassische Massenmedien wie Presse und Rundfunk zum Überdenken ihrer etablierten Geschäftsmodelle und ihrer publizistischen Funktionen. Die Digitalisierung verändert die Rahmenbedingungen der demokratischen Öffentlichkeit in Bezug auf die Beteiligungschancen der Bürgerinnen und Bürger sowie deren informationelle Selbstbestimmung. In dieser Situation bedarf es einer aktuellen Zustandsbeschreibung und Analyse. Diese muss einerseits auf dem empirisch gesicherten Wissen über Mechanismen des digitalen Wandels wie z. B. die Beschaffenheiten und Dynamiken politischer Informationsflüsse aufbauen. Andererseits soll der Blick auf die Chancen wie die Problemlagen gerichtet werden, welche das demokratische Gespräch zwischen Bürgerinnen und Bürgern untereinander und mit der Politik in Presse und Rundfunk wie in digitalen Öffentlichkeiten bestimmen. In diesem Beitrag werden der Stand der wissenschaftlichen Evidenz des Zusammenspiels von Digitalisierung und Demokratie analysiert und darauf aufbauend Handlungsempfehlungen formuliert, welche zur aktiven Gestaltung künftiger Entwicklungen durch Politik und Zivilgesellschaft beitragen können.

Ein zentraler Begriff im Kontext dieses Beitrags ist Öffentlichkeit, die in sozialwissenschaftlichen Studien als Maßstab demokratischer Kommunikation verwendet wird. In westlichen Demokratien bezeichnet der Begriff Öffentlichkeit zudem ein Kommunikations- und Vermittlungssystem, das den Austausch von Bürgerinnen und Bürgern untereinander sowie zwischen Bevölkerung und politischen Institutionen nachvollziehbar organisiert. Dieses System soll für Themen und Meinungen aller gesellschaftlichen Gruppen offen sein und deren Stimmen transparent darstellen; zudem soll es die Auseinandersetzung mit den hier artikulierten Meinungen ermöglichen, die kritische Selbstreflexion einer Gesellschaft fördern und öffentliche Meinungen hervorbringen, die in einer Demokratie politisch wirksame Orientierung leisten. Öffentlichkeit ist somit das Herzstück der Demokratie – ein Raum für die Entwicklung von Ideen, von politischen Handlungsoptionen und kollektiven Identitäten, aber auch für die Legitimierung politischer Akteurinnen und Akteure zwischen den Wahlen.

Der demokratische Wert von Öffentlichkeiten lässt sich danach beurteilen, inwieweit sie Offenheit und Transparenz, Ausgewogenheit, Inklusion, Zivilität und Diskursivität ermöglichen. Diese Normen bildeten schon die Grundlage der Bewertung der massenmedialen Öffentlichkeit des 20. Jahrhunderts. Die Auswirkungen der Digitalisierung auf die Demokratie wurden anfänglich fast ausschließlich in Bezug auf die demokratieförderlichen Potenziale der Netzkommunikation diskutiert. Angesichts der ökonomischen und politischen Strukturen digitaler Öffentlichkeiten zeigt sich

indessen, dass diese die „multiplen Differenzierungslogiken" moderner Gesellschaften abbilden. Das bedeutet, dass nicht nur vielfältige Meinungen, sondern teils gegensätzliche Interessen, Positionen und Werte in digitalen Öffentlichkeiten sichtbar sind, ohne dass es aber zu einer demokratischen Auflösung der vorhandenen Widersprüche und einer entsprechend geregelten Austragung von Konflikten käme. In dieser Situation scheint es sinnvoll zu sein, die normativen Anforderungen an die demokratische Öffentlichkeit des 20. Jahrhunderts auch als Maßstab für die demokratische Qualität digitaler Öffentlichkeiten im 21. Jahrhundert heranzuziehen.

Im Zuge der Digitalisierung ist die Infrastruktur der öffentlichen Meinungsbildung unter anderem geprägt durch die technischen Architekturen und Features der entsprechenden Plattformen sowie deren Verbindungen (z. B. Hyperlinks, Tweets, Hash- tags) und Vernetzungen. Sie umfasst damit nicht nur viele verschiedene Kanäle, Foren und Netzwerke mit ihren jeweiligen Rückkopplungen, sondern unterliegt auch einer schwer abzusehenden Dynamik aufgrund kontinuierlicher technischer Weiterentwicklung durch Algorithmen im Allgemeinen und selbstlernenden Systemen im Besonderen. Denn diese technischen Bedingungen beeinflussen sowohl die Themensetzung im öffentlichen Raum und die Qualität der verfügbaren Informationen als auch die Tonlagen der Meinungsbildung. Dies alles prägt zudem die Art und Weise, wie Nutzerinnen und Nutzer mit Informationen und auch miteinander umgehen und wie sie ihre demokratischen Teilhabechancen wahrnehmen.

Dieser Beitrag diskutiert den Wandel der Demokratie im Zuge von Digitalisierung und mit Blick auf vier kritische Aspekte demokratischer Öffentlichkeit: (a) die Digitalisierung der Infrastruktur von Öffentlichkeit; (b) die Veränderung von Information und Kommunikation durch digitale Medien; (c) die Erweiterung demokratischer Partizipation durch neue digitale Formate; (d) den Wandel politischer Selbstbestimmung.

Bei der Erarbeitung des vorliegenden Beitrags wurde deutlich, dass sich die Frage nach dem Zusammenhang zwischen Demokratie und Digitalisierung einfachen Antworten entzieht. Erst seit wenigen Jahren wird systematisch geforscht, und der Wissensstand entwickelt sich Monat für Monat weiter. Die Aufschlüsselung komplexer Wirkungszusammenhänge erfordert neue, anspruchsvolle Forschungsdesigns und -methoden sowie umfangreiche Daten. Letztere sind allerdings nicht ohne Weiteres zugänglich, weil die kommerziellen Informations- und Kommunikationsplattformen dies bislang nicht im erforderlichen Umfang zulassen. Nichtsdestotrotz gibt es mittlerweile zahlreiche aussagekräftige Untersuchungen zu den politischen Folgen der Digitalisierung, die mittels verschiedener empirischer und theoretischer Zugänge weitreichende Veränderungen der demokrati-

schen Öffentlichkeit diagnostizieren. Viele dieser Studien stammen aus den USA, weshalb die Übertragung ihrer Ergebnisse auf die deutsche oder die europäische Situation angesichts der kulturellen Unterschiede nicht unproblematisch ist. Die Arbeitsgruppe ist sich dieser Problematik bewusst und hat sie bei der Formulierung dieser Stellungnahme und ihrer Empfehlungen berücksichtigt.

2. Analyse

2.1. Plattformen als Infrastrukturen

Damit Bürgerinnen und Bürger in einer Demokratie politische Meinungen bilden, politische Anliegen artikulieren und sich ihren politischen Präfenzen entsprechend für die Wahl von Repräsentantinnen und Repräsentanten im Parlament entscheiden können, sind sie auf lebendige demokratische Öffentlichkeiten angewiesen. Sie wurden bereits in der Einleitung charakterisiert. Demokratische Öffentlichkeiten beruhen auf medialen Infrastrukturen, die eine weite Verbreitung von Informationen und Verständigung über große räumliche Distanzen hinweg ermöglichen. Nach wie vor bilden zwar die klassischen Massenmedien Presse und Rundfunk die wichtigste Infrastruktur für demokratische Öffentlichkeiten, neue Infrastrukturen spielen hier aber eine zunehmend wichtige Rolle. In erster Linie sind das digitale Informations- und Kommunikationsplattformen[1] wie die US-amerikanischen sozialen Netzwerke *Facebook*, *Twitter* und *Instagram*, aber auch Videoportale wie *YouTube* oder das chinesische *TikTok*. Auch Messenger-Dienste wie *WhatsApp* und *Telegram*, Webauftritte von klassischen Massenmedien, staatlichen und privaten Institutionen, Blogs und insbesondere Suchmaschinen wie *Google* tragen zur Herstellung und Gestaltung digitaler demokratischer Öffentlichkeiten bei.

Angesichts des gewaltigen Bedeutungszuwachses dieser digitalen Plattformen, Portale, Dienste und Angebote ist ihre Neubewertung im Kontext demokratischer Öffentlichkeit dringend geboten. Der Fokus des vorliegenden Beitrags richtet sich auf Plattformen, weil Plattformbetreiber mit ihren Kuratierungsaktivitäten (Auswahl und Priorisierung von Inhalten) erhebliche Gestaltungsmacht besitzen. An diese Feststellung schließt sich die Frage an, ob, wie und in welchem Ausmaß solche Aktivitäten selbst an demokratische Verfahren und Kontrollen rückgebunden werden können.

1 Im Folgenden werden diese kurz als „Plattformen" bezeichnet.

2.1.1. Die Erweiterung der Infrastrukturen demokratischer Öffentlichkeiten

Presse und Rundfunk sind in sich heterogen: Öffentlich-rechtlicher und privater Rundfunk, aber auch Qualitäts- und Boulevardpresse unterscheiden sich hinsichtlich ihrer Arbeitsweise, ihrer Ziele und ihrer Finanzierungsgrundlagen zum Teil erheblich voneinander. Das Spektrum der jeweiligen Geschäftsmodelle und der damit verbundenen Abhängigkeiten reicht von der Beitragsfinanzierung im öffentlich-rechtlichen Mediensektor über Mischkonzepte privater Medien, die sich durch Verkaufserlöse, Nutzungsgebühren und Werbeeinnahmen finanzieren, bis hin zu spendenbasierten Lösungen. Presse- und Rundfunkangeboten ist jedoch gemeinsam, dass sie überwiegend eigene Inhalte erstellen und diese der Öffentlichkeit verfügbar machen. Die Inhalte werden von professionellen Redaktionen kuratiert, die als „Gatekeeper" bezeichnet werden: Die Redaktionen produzieren, sortieren, priorisieren und selektieren Nachrichten und Informationen auf Basis professionell normierter Kriterien wie der Aktualität, der politischen Bedeutung oder der räumlichen Nähe eines bestimmten Ereignisses, aber auch im Hinblick auf die Interessen potenzieller Adressatinnen und Adressaten oder von Werbekundinnen und -kunden.

Im Gegensatz dazu produzieren Plattformen Nachrichten und Informationen nicht selbst. Stattdessen präsentieren sie Inhalte von Dritten wie Nutzerinnen und Nutzern, traditionellen Massenmedien oder Werbetreibenden. Damit wirken sie auf den ersten Blick wie neutrale Infrastrukturen. Tatsächlich aber wählen viele Plattformen Inhalte mithilfe komplexer Algorithmen individuell für ihre Nutzerinnen und Nutzer aus. Sie betreiben also im Gegensatz zu herkömmlichen Massenmedien personalisierte Kuratierung von Inhalten Dritter. Diese Kuratierung der Plattformen orientiert sich hauptsächlich an der erwarteten Popularität der Inhalte. Sie zielt darauf, sowohl die Interaktionszeit von Nutzerinnen und Nutzern als auch die Wahrscheinlichkeit, dass diese auf individuell zugeschnittene Werbung reagieren, zu maximieren (Zuboff 2018).

Zu diesem Zweck machen sich die Plattformbetreiber auch verschiedene psychologische Mechanismen zunutze. Ungeklärt ist allerdings, wie effektiv und leistungsfähig personalisierte Werbung tatsächlich ist – auch im Vergleich zu klassischer, nichtpersonalisierter Werbung (Karpf 2019).

Personalisierte Kuratierung ist möglich, weil Nutzerinnen und Nutzer mit ihrer Wahl von Inhalten eine individuelle Datenspur hinterlassen und weil Plattformen dieses Datenprofil – beispielsweise inhaltliche Präferenzen, Kommunikationsinhalte und Kontaktpflege – detailliert erfassen und analysieren, wodurch sich Inhalte wiederum individuell zuschneiden

und präsentieren lassen. Diese Analyse vollzieht sich für Nutzerinnen und Nutzer weitgehend im Verborgenen. Mithilfe der Nutzungsdaten können die Plattformen ihre digitale Architektur immer weiter optimieren und das Interesse, die Aufmerksamkeit und teilweise auch das Verhalten von Nutzerinnen und Nutzern beeinflussen oder sogar lenken, beispielsweise durch gezielte, aber kaum merkliche „Schubser" („Nudging", „Gamification" usw.). Solche Methoden der datenbasierten Aufmerksamkeitslenkung, Verhaltensvorhersage und -beeinflussung bilden die Basis des Geschäftsmodells zahlreicher Plattformen. Datenbasierte Geschäftsmodelle sind in demokratischen Öffentlichkeiten allerdings nicht nur auf Plattformen beschränkt. Auch Suchmaschinen präsentieren und kuratieren Inhalte Dritter und orientieren sich dabei am Prinzip algorithmischer Optimierung.

Messenger-Dienste verzichten dagegen auf eine Kuratierung von Informationsströmen. Sie stellen zwar ebenfalls Infrastrukturen für den politischen Diskurs bereit, aber es handelt sich dabei in der Regel um Teilöffentlichkeiten mit beschränktem Zugang. Ihr politischer Einfluss ist ein neues Phänomen, das bisher noch nicht hinreichend erforscht ist.

2.1.2. Koexistenz von Presse, Rundfunk und Plattformen

Trotz dieser Befunde ist es keineswegs so, dass demokratische Öffentlichkeiten heute vollständig von Plattformen beherrscht würden. Presse und Rundfunk spielen nach wie vor eine wichtige Rolle. Ihre Koexistenz mit Plattformen ist allerdings durch konkurrierende Geschäftsmodelle, verschiedene Professionsstandards und erhebliche Unterschiede in der Gewinngenerierung geprägt. Weil Plattformen große Zuwächse in der Nutzung und einen hohen Anteil der Werbeeinnahmen für sich verbuchen können, bestimmen sie derzeit die Bedingungen der Kooperation mit Presse und Rundfunk – etwa bei der Einbindung von redaktionellen Inhalten in die Angebote der Plattformen. Die Plattformen bieten ihnen dabei die Möglichkeit, die Popularität der Beiträge über die laufenden Zugriffe zu verfolgen und diese mit Links zu weiterführenden Inhalten zu versehen. Individualisierte Analyse erlaubt es, Massentauglichkeit von Inhalten besser zu bestimmen und das mediale Angebot entsprechend zielgerichtet auszurichten. Die neuen Geschäftsmodelle haben also eine große Wirkung über die Plattformen hinaus auch auf Presse und Rundfunk. Plattformen gewinnen vor allem für die junge Generation immer weiter an Bedeutung. Die Rezeptionskanäle für massenmediale Inhalte verschieben sich so nach und nach zu den Plattformen. Politik und Teile der Gesellschaft befürchten, dass dies eine zunehmende Fragmentierung der

Öffentlichkeit, wachsenden Populismus und einen politischen Rechtsruck fördert. Welche wissenschaftlichen Erkenntnisse zu diesen Vermutungen und Befürchtungen vorliegen, wird in den nachfolgenden Abschnitten zu erörtern sein.

2.1.3. Die Macht von Plattformen

Plattformen sind also keineswegs neutrale Vermittler, sondern mächtige Akteure, die eine aktive Rolle in der Gestaltung demokratischer Öffentlichkeiten einnehmen. Die infrastrukturelle Macht von Plattformen beruht auf der steigenden Abhängigkeit der Nutzerinnen und Nutzer sowie der traditionellen Massenmedien von den Vermittlungsleistungen der Plattformen. Sie wird durch sogenannte ökonomische Netzwerkeffekte verstärkt, die zur Marktbeherrschung durch wenige dominante Anbieter führt. Sie äußern sich in selbst verstärkenden Konzentrationsdynamiken. Diese beruhen darauf, dass der Wert einer Plattform für potenzielle Nutzerinnen und Nutzer mit ihrem Marktanteil steigt. Netzwerkeffekte führen zu einer hohen Konzentration von Nutzerdaten bei wenigen Plattformen und zu Lock-in-Effekte, die Plattformwechsel erschweren: auf Plattformen entsteht eine Historie geteilter Inhalte. Sie kann mangels Interoperabilität nicht auf andere Plattformen übertragen werden, was die Möglichkeit eines Anbieterwechsels stark einschränkt. Allerdings entstehen immer wieder neue Plattformen, die in den jüngeren Altersgruppen starke Zuwächse verzeichnen können. Wann und warum es neuen Plattformen gelingt, sich zu etablieren, ist bislang jedoch noch nicht hinreichend geklärt. Bisher haben etablierte Plattformen auf mögliche Konkurrenten oft damit reagiert, diese aufzukaufen (beispielsweise die Übernahmen von *WhatsApp* und *Instagram* durch *Facebook*). Begünstigt wird diese Machtposition von Plattformen durch die Intransparenz ihrer Kuratierungskriterien (Dolata 2019). Sie erschwert es Dritten, Kuratierungsentscheidungen belastbar zu kritisieren oder darauf Einfluss auf sie zu nehmen. *Facebook* hat auf diese Grundsatzkritik mittlerweile reagiert und ein – allerdings demokratisch nicht legitimiertes – „Oversight Board" eingerichtet, dessen Aufgabe darin besteht, ausgewählte kontroverse Kuratierungsentscheidungen für *Facebook* verbindlich zu entscheiden. Deutlich mehr Transparenz und Nachvollziehbarkeit bleiben für die Erforschung des tatsächlichen Einflusses digitaler Infrastrukturen auf demokratische Öffentlichkeiten sowie die Entwicklung und Bewertung von Regulierungsvorschlägen aber auch weiterhin essenzielle Bedingungen.

2.1.4. Gegenwärtiger Stand der Plattformregulierung

Jede Form von Machtausübung muss in freiheitlich verfassten Demokratien auf rechtsstaatlichen Prinzipien beruhen. Liegen wesentliche für das demokratische System relevante Infrastrukturen in privater Hand, beispielsweise bei Unternehmen, müssen Zustand und Entwicklung dieser Infrastrukturen zumindest fortlaufend beobachtet werden. Zeigen sich dabei schwerwiegende Störungen, die die demokratische Funktion dieser Infrastrukturen beeinträchtigen können, so ist der Staat gehalten, sie durch entsprechende rechtliche Rahmensetzung einzuhegen. Dies geschieht bereits.

Eine Herausforderung für die Durchsetzung nationaler und europäischer Rechtsstandards besteht darin, dass die wichtigen Plattformanbietern ihre Hauptsitze im außereuropäischen Ausland und ihren Nutzerinnen und Nutzern pseudonyme oder anonyme Kommunikation ermöglichen. Eine regulatorische Gegenstrategie besteht darin, dass die territorialen Anwendungsbereiche wichtiger Regelungswerke erheblich auszudehnen. Dies wendet etwa die seit 2018 gültige Datenschutz-Grundverordnung (DSGVO) an und bindet auch rein außereuropäische Akteurinnen und Akteure dann an das europäische Datenschutzrecht, wenn auf dem europäischen Markt tätig sind. Neben der DSGVO unterliegen Plattformen umfangreichen Prüf- und Löschpflichten hinsichtlich der von Nutzerinnen und Nutzern verbreiteten unzulässigen Inhalte, die sich aus zivilrechtlichen, aber auch aus daten- und jugendschutzrechtlichen Vorschriften ergeben. Zu den unzulässigen Inhalten zählen beispielsweise Beleidigungen, Verleumdungen, Volksverhetzungen, öffentliche Aufforderungen zu Straftaten sowie die Verbreitung von Kennzeichen oder Propagandamitteln verfassungsfeindlicher Organisationen. Zudem verpflichtet das Netzwerkdurchsetzungsgesetz Plattformen, ein Verfahren, das es Nutzerinnen und Nutzer die Meldung strafbarer Inhalte zu melden und solche Inhalte innerhalb festgelegter Fristen zu sperren oder löschen. Bis jetzt sind diese Meldeverfahren noch sehr aufwändig. Auch verleitet das Gesetz die Betreiber dazu, auch rechtmäßige Inhalte vorsorglich zu löschen, und gibt Nutzerinnen und Nutzer kein hinreichend wirksames Beschwerderecht gegen ungerechtfertigte Löschungen (Ladeur und Gostomzyk 2017). Daher erlaubt es ein jüngst vom Bundestag verabschiedetes Gesetz Nutzerinnen und Nutzer gegen ungerechtfertigte Löschung vorzugehen. Darüber hinaus sind die Plattformbetreiber ab Februar 2022 verpflichtet, bestimmte rechtswidrige Inhalte an das Bundeskriminalamt zu melden. Der Entwurf eines Ende 2020 vorgestellten Gesetzentwurfs (EC 2020) enthält ebenfalls ein Meldeverfahren für illegale Plattforminhalte, eine Beschwerdemöglichkeit gegen ungerechtfertigte Löschungen oder Sperrungen vorgehen und

die Plicht für Plattformen, strafbare Inhalte an Strafverfolgungsbehörden zu melden.

Deutlich weniger klar konturierte und weitreichende Vorgaben bestehen gegenwärtig für die inhaltliche Kuratierung durch die Plattformbetreiber. Einerseits beruhen sie auf Kommunikations-, Sperr- und Löschregeln, die auf Verträgen der Plattformen mit Nutzerinnen und Nutzern beruhen. Sie sind aber möglicherweise vertragsrechtlich unzulässig, weil sie die Meinungsfreiheit übermäßig beschränken (Raue 2018). Zum anderen unterliegen zumindest manche Kuratierungsentscheidungen einer medienrechtlichen Regulierung. So enthält der im November 2020 in Kraft getretene Medienstaatsvertrag (MedStV) Regelungen für sogenannte Medienintermediäre mit mehr als einer Million Nutzerinnen und Nutzern monatlich im Bundesgebiet, die journalistisch-redaktionelle Angebote Dritter zusammenführen, auswählen und allgemein zugänglich präsentieren, ohne daraus ein Gesamtangebot zu erstellen. Sie müssen die Kriterien für die Inhaltspräsentation und die Funktionsweise der zugrunde liegenden Algorithmen transparent machen und dürfen journalistische Inhalte Dritter nicht ohne sachlichen Grund bei der Auswahl benachteiligen. Das geltende Recht enthält hingegen keine Standards für die Kuratierung von Inhalten, die Plattformnutzerinnen und -nutzer produzieren. Ebenso wenig gibt es Vorgaben für eine zivilgesellschaftliche Beteiligung bei der Formulierung und Kontrolle von Kuratierungskriterien.

2.1.5. Herausforderungen

Kommerzielle Plattformen stellen der demokratischen Öffentlichkeit Infrastrukturen bereit und haben dadurch eine erhebliche Macht. Unsere Analyse zeigt, dass der an herkömmlichen Verhältnissen ausgerichtete regulatorische Rahmen deutlich ergänzungsbedürftig ist. Plattformen sollten stärker als bislang auf demokratische und rechtsstaatliche Ziele verpflichtet werden. Dies kann durch prozedurale, inhaltliche und organisationale Bindungen geschehen, welche den privatwirtschaftlichen Status von Plattformen respektieren. Außerdem ist zu erwägen, ob und wie nicht-kommerzielle demokratieförderliche digitale Angebote für die demokratische Öffentlichkeit gefördert werden könnten, etwa der öffentlich-rechtliche Rundfunk, der durch einen demokratischen Informationsauftrag verpflichtet ist. Gegenwärtige Regulierung schränkt seine digitalen Handlungsmöglichkeiten stark ein, etwa das Verbot presseähnlicher Online-Angebote (§ 30 Abs. 7 MedStV).

2.2. Information und Kommunikation

Information und Kommunikation sind essenziell für demokratische Öffentlichkeiten. Alle Beteiligten müssen Zugang zu genügend und das Meinungsspektrum hinreichend divers abbildenden Informationen haben und sie auswählen, bewerten und einordnen können. Außerdem benötigen sie die Möglichkeit zu freiem und fairem Austausch mit anderen Beteiligten. Aber auch Information und Kommunikation wandeln sich unter den Bedingungen der Digitalisierung.

Umfang und Zugänglichkeit von Information und Kommunikation wachsen im Zuge der Digitalisierung, was aus demokratiepolitischer Sicht grundsätzlich wünschenswert ist. Gleichzeitig ist die Digitalisierung mit erheblichen Risiken verbunden. Es stellen sich zunehmend folgende Fragen: Können Akteurinnen und Akteure, beispielsweise Individuen, Gruppen oder Parteien, aus dem unüberschaubar komplexen Angebot die für sie jeweils relevanten Informationen noch immer ausreichend herausfiltern, bewerten und einordnen? Ermöglichen die reichweitenstarken digitalen Kommunikationsdienste einen Dialog zwischen unterschiedlichen politischen Gruppen und Strömungen oder tragen sie stattdessen zu einer Fragmentierung und Polarisierung der politischen Landschaft bei? Und erschweren Phänomene wie „Hate Speech“ und „Online Harassment“ (Internet Mobbing) nicht zunehmend eine zivilisierte digitale Kommunikation, wie sie für funktionierende demokratische Öffentlichkeiten unabdingbar ist?

2.2.1. Chancen für die demokratische Öffentlichkeit

Die im Zuge der Digitalisierung enorm gewachsenen Informationsmöglichkeiten sind für die demokratische Meinungs- und Willensbildung von beträchtlicher Bedeutung. Dies zeigen etwa die enorm leistungsfähige Online-Enzyklopädie Wikipedia, und die Möglichkeit detaillierter, politisch relevanter Informationen in Echtzeit durch Fortschritte in der Sensortechnik und Datenanalyse. Gleichzeitig eröffnen die vielen digitalen Kommunikationsdienste große Möglichkeiten für die demokratische Öffentlichkeit, weil sie globale Vernetzung und weitreichende Interaktion erlauben. Politische Gruppen können vergleichsweise einfach und schnell neue internationale Öffentlichkeiten schaffen, wie etwa *Fridays for Future* und *Black Lives Matter* verdeutlichen.

2.2.2. Informationsauswahl

Das enorme Informationsangebot kann aber die kognitive Kapazität der Akteurinnen und Akteure überfordern und damit die Möglichkeit einschränken, Informationen für eigene Meinungsbildung relevante Informationen auszuwählen (Lorenz-Spreen u. a. 2020). Außerdem erfordert die Nutzung der neuen Informationsquellen digitale Kompetenz, die nicht bei jedem Individuum gleich stark ausgebildet ist. Ein weiteres Hindernis für eine adäquate Informationsauswahl besteht darin, dass demokratische Öffentlichkeiten zunehmend fragmentiert und polarisiert sind, also durch unauflösbar scheinende Widersprüche geprägt und darin Konsensfindung so zunehmend zur Herausforderung wird (Pfetsch 2020). Schließlich sind Bürgerinnen und Bürger bei der Nutzung der enormen Informationsmengen und Kommunikationsmöglichkeiten auch auf eine Kuratierung durch Diensteanbieter angewiesen. Diese Kuratierung hat aber, wie bereits dargelegt, meistens das Ziel, die Aufmerksamkeit auf gewinnbringende Werbeinhalte zu lenken; das aber steht oft im Widerspruch zu einer sachgerechten und umfangreichen Informationsvermittlung, es begünstigt die Verbreitung von emotionalen und moralisierenden Inhalten.

Um solchen und nachfolgend beschriebenen Hindernissen erfolgreich zu begegnen, gibt es bereits erste vielversprechende Initiativen von zivilgesellschaftlicher Seite, um Nutzerinnen und Nutzer durch digitale Werkzeuge zu unterstützen, etwa durch Browser-Add-Ons, die die Vertrauenswürdigkeit von Nachrichtenseiten durch Symbole kennzeichnen. Allerdings scheitern solche Versuche oft noch an der sehr beschränkten Datenfreigabe durch die Plattformen, die für Entwicklung und Betrieb entsprechender Programme erforderlich wären.

2.2.3. Informationsbewertung

Bürgerinnen und Bürger müssen in der Lage sein, die Informationen, die ihnen präsentiert werden, zu bewerten. Einerseits geht es darum, einschätzen zu können, ob eine Tatsachenbehauptung korrekt ist (Faktizität). Inwieweit das möglich ist hängt von der epistemischen Qualität der Information ab (welche Evidenz wird zitiert? sind die Quellen vertrauenswürdig?) Auf der anderen Seite geht es aber auch um die Bewertung normativer Aussagen. Dafür ist es wichtig, die relevanten Prämissen zu verstehen, also zu wissen, ob der fraglichen Praxis oder Idee anerkannte Normen wie das Grundgesetz oder aber eine extremistische Ideologie zugrunde liegt. Auch die Kenntnis des relevanten Meinungsspektrums spielt hier eine wichtige

Rolle. Wie bereits unter 2.1 dargestellt, sollen bei herkömmlichen Massenmedien Journalistinnen und Journalisten Bewertbarkeit sicherstellen, wenngleich das abhängig vom einzelnen Medium in der Praxis mal mehr, mal weniger gut umgesetzt wird. Auch einige digitale Angebote sorgen für eine entsprechende Qualitätssicherung. Wie bereits unter 2.1 dargestellt, bieten viele kommerzielle digitale Dienste und besonders Plattformen eine solche Qualitätskontrolle allerdings nur in sehr eingeschränktem Maße, weil diese ihre Inhalte nach dem Prinzip der Aufmerksamkeitsbindung auswählen.

Ein weiteres zentrales Problem stellen sogenannte Fake News dar, also falsche oder aus dem Kontext gerissene, irreführende Informationen, die bewusst oder aus Unwissenheit geteilt werden. In der digitalen Öffentlichkeit finden Falschnachrichten deutlich weitreichendere und schnellere Verbreitung als korrekte Informationen – vermutlich als Folge des aufmerksamkeitsbasierten Geschäftsmodells (Mocanu u. a. 2015). Besonders problematisch sind Deepfakes, also mit künstlicher Intelligenz hergestellte Fake-Videos. Falschnachrichten können sich viral verbreiten und somit eine sachliche politische Debatte erschweren. Sie werden auch strategisch eingesetzt, beispielsweise durch den ehemaligen US-Präsidenten Donald Trump. Der Konsum von solchen Falschnachrichten scheint sich aber bis jetzt eher auf kleine, politisch extreme Gruppen zu konzentrieren (Grinberg u. a. 2019). Die Verbreitung von Falschnachrichten und deren Auswirkungen werden gegenwärtig aktiv erforscht.

2.2.4. Pluralität

Für demokratische Öffentlichkeiten ist die Pluralität der Perspektiven von herausragender Bedeutung: alle relevanten Perspektiven sollen eingebracht werden können und alle Akteurinnen und Akteure sollen Zugang zu hinreichend vielfältiger Information und Kommunikation haben. Das ist eine entscheidende Voraussetzung dafür, Informationen und Kommunikation einordnen, bewerten und auf der Basis von Alternativen kritisieren zu können. Nur so sind eine fundierte politische Meinungsbildung und sachlich begründete politische Entscheidungen möglich. Hier stellt sich nun die Frage, inwieweit die Digitalisierung solche Pluralität begünstigt oder behindert.

Zunächst kann ein positiver Effekt der digitalen Medien konstatiert werden. Die Möglichkeiten zur Mitwirkung und Artikulation sowie zur Informationserhebung erweitern sich unter den Bedingungen der Digitalisierung nämlich stetig. Andererseits gibt es aber auch digitalisierungsbe-

dingte negative Effekte sowohl individuell als auch auf gesellschaftlicher Ebene.

Auf individueller Ebene werden vor allem Echokammern diskutiert. Damit ist einerseits gemeint, dass Nutzerinnen und Nutzer digitaler Dienste hauptsächlich Quellen auswählen, die ihre eigene Meinung und Weltanschauung zu bestätigen scheinen. Das führt zu einem höchst einseitigen Konsum von Inhalten. Das betrifft vor allem Konsumentinnen und Konsumenten mit extremen politischen Ansichten (Stier u. a. 2020). Für andere Nutzerinnen und Nutzer lässt sich sogar eine Verbreiterung der Wahrnehmung feststellen. Andererseits bezeichnet der Begriff Echokammer die Herausbildung von Gruppen, die ein homogenes Meinungsbild haben und sich in ihrer Meinung gegenseitig verstärken. Das kann Mechanismen der Gruppenpolarisierung verstärken, bei denen positives soziales Feedback auch extreme politische Überzeugungen verhärtet (Sunstein, Cass 2018).

Auf gesellschaftlicher Ebene ist für die Pluralität besonders die Modularisierung problematisch, also die Gliederung in unterschiedliche Gruppen (Teilöffentlichkeiten). Sie wird durch die Digitalisierung verstärkt, weil es möglich ist, Gleichgesinnte aus einem großen Pool möglicher Kontaktpartnerinnen und -partner auszuwählen. Aus Modularität wird die für Pluralität problematische Fragmentierung, wenn sich nicht mehr nur zu Spezialthemen, sondern auch zu den großen Fragen der Gesellschaft nur noch Teilöffentlichkeiten herausbilden, die sich nicht vernetzen, einander kaum wahrnehmen oder sich gar ablehnend gegenüberstehen. Feldexperimente zeigen, dass digitale Fragmentierung zudem dadurch begünstigt wird, dass Plattformen die Auffindbarkeit von Gruppen wiederum nach Kriterien eines aufmerksamkeitsbasierten Geschäftsmodells steuern (Shmargad und Klar 2020). Problematisch ist die Fragmentierung der öffentlichen Debatte also auch deshalb, weil sie zu einer Radikalisierung der Positionen und zu einer Verschärfung der Tonlage in der politischen Auseinandersetzung beitragen kann. In den angelsächsischen Mehrheitsdemokratien ist bereits ein deutlicher Trend zur Polarisierung festzustellen. In demokratischen Systemen mit Proportionalwahlrecht entsteht vor allem eine neue Konfliktlinie zwischen autoritärem Populismus und liberalem Kosmopolitismus. Gerade im rechten politischen Spektrum tragen diese Phänomene zu Radikalisierung und Hassreden bei und können zudem politisch motivierte Gewalttaten begünstigen (Müller und Schwarz 2020).

2.2.5. Zivilität

Schließlich ist auch die Möglichkeit zu freiem und fairem Austausch zentral für eine funktionierende demokratische Öffentlichkeit. Besonders problematisch sind in diesem Zusammenhang Zivilitätsbrüche, insbesondere „Hate Speech" und „Online Harassment".

„Hate Speech" würdigt Personen oder Gruppen gezielt herab oder ruft sogar zu Straftaten gegen diese auf. Prominente Beispiele sind antisemitische, rassistische und sexistische Äußerungen. „Online Harassment" soll einzelne Personen bedrohen oder einschüchtern. Bestimmte Arten von „Hate Speech" (insbesondere mit rassistischer und homophober Zielrichtung) werden häufiger als andere anonym verbreitet. Gezieltes „Online Harassment" geht meistens von persönlich Bekannten der Opfer aus. Es ist empirisch gesichert, dass „Hate Speech" und „Online Harassment" ein großes Problem darstellen(Geschke u. a. 2019). Hate Speech führte sogar bereits direkt zu Straftaten. Solche Phänomene behindern Teilhabebereitschaft und aktive Beteiligung am öffentlichen Diskurs.

Viele Formen von „Hate Speech" und „Online Harassment sind Straftaten. Zur effektiven, Rechtsdurchsetzung müssen strafbare von zugespitzten, aber rechtlich zulässigen Äußerungen zunächst klar abgegrenzt werden. Außerdem müssen bei Straftaten die entsprechenden Urheberinnen und Urheber ermittelt und der Strafverfolgung zugeführt werden. Angesichts der großen Anzahl potenziell strafbarer Äußerungen kann das zu einer der Durchsetzungsmacht des Rechtsstaats führen.

Die beschriebenen Tendenzen können dazu führen, dass sich die moderate politische Mehrheit, aber auch vulnerable Gruppen und Personen, davon abgeschreckt werden, sich politisch zu beteiligen oder sogar ein politisches Amt zu übernehmen. Das stärkt politische Fragmentierung und politisch extreme Positionen.

2.2.6. Herausforderungen

Die erste Herausforderung besteht darin, Bürgerinnen und Bürger, die sich an digitalen demokratischen Öffentlichkeiten beteiligen, zu unterstützen. Von zentraler Bedeutung ist dabei die Förderung von Digitalkompetenz in allen Bevölkerungsgruppen. Eine zweite Herausforderung resultiert aus den problematischen Auswirkungen der Aufmerksamkeitsökonomie, was insbesondere Auswahl, Bewertung und Pluralität von Information und Kommunikation beeinträchtigen kann. Hier müssen regulatorische Maßnahmen, die bereits unter 2.1 erörtert wurden, für Transparenz und

eine stärker relevanz- und sachorientierte Kuratierung sorgen. Die dritte Herausforderung im Kontext der Informations- und Kommunikationsökologie besteht darin, negativen Veränderungen der Informations- und Kommunikationskultur z.B. in Form von „Hate Speech" und „Fake News" konsequent entgegenzuwirken. Dafür muss der bereits bestehende rechtliche Rahmen weiterentwickelt und insbesondere die Rechtsdurchsetzung gestärkt werden. Alle hier genannten Maßnahmen erfordern eine Begleitung durch entsprechende Forschung. Diese kommt ohne Zugriff auf Daten der Plattform- und Dienstanbieter allerdings nicht zu gesicherten Erkenntnissen und generalisierbaren Aussagen. Daher muss auch die Pflicht zur Bereitstellung der entsprechenden Daten Bestandteil der Regulierung sein.

2.3. Partizipation

In der digitalen Welt hat sich ein breiter Partizipationsbegriff durchgesetzt, der sich auf eine möglichst umfassende aktive Teilhabe von Bürgerinnen und Bürgern in allen gesellschaftlichen Feldern erstreckt. Das schließt beispielsweise das Engagement in Bürgerinitiativen ebenso ein wie die betriebliche Mitbestimmung oder die Mitgestaltung des öffentlichen Raums.

Im Hinblick auf solche Partizipation wurde die Etablierung der digitalen Medien und ihrer Infrastrukturen – allen voran die des Internets und der Mobilkommunikation – anfangs von hohen Erwartungen begleitet. Mit der unter 2.1 beschriebenen fortschreitenden Kommerzialisierung des Internets und der Durchsetzung eines Anbieteroligopols haben sich die Partizipationsmöglichkeiten im digitalen Raum jedoch bereits wieder verändert. Während sich einzelne Hoffnungen auf mehr Möglichkeiten zur Partizipation erfüllt haben, andere hingegen enttäuscht wurden, kam noch eine neue Problematik hinzu: Die zugrunde liegenden Infrastrukturen werden nicht demokratisch, sondern von einigen wenigen kommerziellen Plattformunternehmen verwaltet, wobei deren Motiv nicht die Förderung der Partizipation, sondern Gewinnmaximierung ist.

2.3.1. Vielstimmigkeit der Partizipationsmöglichkeiten

Ein wesentlicher Wandel, der sich in den letzten Jahren vollzogen hat, betrifft die zunehmende Vielstimmigkeit der Partizipationsmöglichkeiten durch digitale Medien. Dies betrifft zum einen die Positionen, die über die verschiedenen digitalen Medien Teil des öffentlichen Diskurses werden

und zum anderen die Möglichkeit, ganze Artikulationskampagnen rein digital zu organisieren. Eine niedrigschwellige Form der Beteiligung sind Kommentare und Feedbacks, die zahlreiche Online-Medien als Funktion standardmäßig ermöglichen. Nutzerinnen und Nutzer können fortlaufend mit Journalistinnen und Journalisten kommunizieren. Das führt sowohl zu einer stärkeren Orientierung von Journalistinnen und Journalisten am Publikum als auch zu einer größeren Irritation durch das Publikum(Loosen und Dohle 2014). Auch die Position des Journalismus im Hinblick auf den öffentlichen Diskurs hat sich verändert hat, seitdem zivilgesellschaftliche Akteurinnen und Akteure ihre Aktivitäten als Online-Kommunikationskampagnen realisieren.

Heute können Menschen, die bisher keinen Zugang zu öffentlicher Kommunikation hatten, sich mithilfe von Plattformen wie *Instagram*, *Facebook* und *Twitter* äußern und mittels Messenger-Diensten wie *WhatsApp* oder *Telegram* Gruppenöffentlichkeiten schaffen. Das hat neue Partizipationskanäle geöffnet. Die unter 2.2.4 bereits erwähnten Influencer bzw. „YouTube Stars" verdeutlichen den Wandel besonders prägnant. Die Voraussetzung dafür, über solche digitalen Kanäle massenhaft Gehör zu finden, ist typischerweise sowohl ein entsprechendes kulturelles und soziales Kapital als auch eine entsprechende Medienkompetenz (Media Literacy). Aktuell zeigt die Forschung erhebliche Ungleichheiten unter Akteurinnen und Akteuren, was die Beteiligungsmöglichkeiten betrifft (Helsper 2021). Menschen aus bildungsfernen und einkommensschwachen Schichten sind im Nachteil, ihre politischen Positionen daher oft unterrepräsentiert. Das gilt wegen mangelnder Barrierefreiheit auch für Menschen mit körperlichen oder geistigen Einschränkungen, die viele digitale Partizipationsangebote nicht nutzen können. Dennoch erlangen durch Plattformen und andere digitalen Medien viel mehr Individuen und Gruppen öffentliche Aufmerksamkeit. Das bietet einerseits die Chance, politische Diskurse über geografische Distanzen hinweg sowie schicht- und milieuübergreifend zu gestalten, aber auch interkulturelle Dialoge zu führen. Andererseits bedeutet dies jedoch, dass nun auch verstärkt demokratiekritische oder -feindliche Positionen in öffentlichen Diskursen sichtbar werden. Besonders problematisch in diesem Zusammenhang ist, dass die Kuratierungsalgorithmen der Plattformen radikalen Positionen in ihren Empfehlungen sogar bevorzugt berücksichtigen (siehe auch 2.2).

2.3.2. Rolle zivilgesellschaftlicher Organisationen und Bewegungen

Mit der fortschreitenden Verbreitung digitaler Medien und deren technischer Infrastrukturen avancierten diese selbst zum Gegenstand zivilgesellschaftlicher Partizipation: Eine zunehmende Zahl zivilgesellschaftlicher Organisationen und Bewegungen setzt sich dafür ein, sie aktiv mitzugestalten und alternative Angebots- und Nutzungsformate zu etablieren. Wichtige Impulse setzen hier beispielsweise die *Open-Data-* und die *Civic-Tech*-Bewegung. Erstere setzt sich für den freien Zugang aller Bürgerinnen und Bürger zu mit staatlichen Mittel erhobenen Daten ein. Letztere nutzt solche Daten, um digitale Dienste einzurichten, welche die Zivilgesellschaft stärken. Einige dieser Initiativen gehen so weit, dass sie neue Plattformen für öffentliche Kommunikation und gesellschaftliche Interaktion einfordern, die nicht nach den kommerziellen Prinzipien des von ihnen sogenannten Überwachungskapitalismus organisiert sind, sondern eine Partizipation nach kooperativen Prinzipien ermöglichen (Scholz und Schneider 2017). Auch im Bereich des Journalismus beginnen sich unter der Bezeichnung „Pionierjournalismus" Initiativen zu bilden, die darauf ausgerichtet sind, neue Strukturen und Praktiken journalistischer Produktion und Verbreitung zu etablieren. Bekannte Beispiele in Deutschland sind *Correctiv*, *Riffreporter* oder *Rums*. Solche Formen eröffnen Potenziale für eine weitere Demokratisierung.

2.3.3. Partizipationsmöglichkeiten durch Daten

Eine weitere partizipationsrelevante Neuerung im Zuge der fortschreitenden Digitalisierung betrifft die explizite Freigabe von Daten zur Nutzung durch Dritte. Die Nutzung digitaler Endgeräte – allen voran Smartphones – führt zu fortlaufenden Datenspuren. Aus wissenschaftlicher Sicht wurde dies bislang im Zusammenhang mit einer allgemeinen Verbreitung von Selbstvermessung und Quantifizierung kritisch diskutiert(Bolin und Velkova 2020). Solche Datenspuren können aber auch auf konstruktiv genutzt und beispielsweise sie zur Etablierung von Anwendungen mit Gemeinwohlinteresse eingesetzt werden. Eine wichtige Möglichkeit sind freiwillige, sogenannte Datenspenden. Kurzfristig können Nutzerinnen und Nutzer ihre Daten so etwa Organisationen zur Verfügung stellen, damit diese die Funktionsweise von kommerziell eingesetzten Algorithmen rekonstruieren und offenlegen können. Langfristig könnten freiwillig zur Verfügung gestellte Daten wie Bewegungs- oder andere Nutzungsdaten außerdem dazu beitragen, Gemeinwohlprojekte und öffentliche Infrastruktu-

ren im Interesse von Bürgerinnen und Bürgern zu optimieren, beispielsweise Verkehrsflüsse. Das kann zur Reduzierung des Energieverbrauchs oder von Abgasen führen und damitund zur Erhöhung der Lebensqualität beitragen.

2.3.4. Herausforderungen

Eine wesentliche Herausforderung besteht darin, Partizipation unter den Bedingungen der Digitalisierung so zu gestalten, dass sie demokratische Öffentlichkeiten und Diskurse stärkt und das Gemeinwesen fördert. Da partizipative Akte über digitale Medien und Infrastrukturen immer auch protokollier- und verwertbare Daten generieren, ist es notwendig, die Etablierung von Infrastrukturen zu fördern, die stärker auf die Demokratie und das Gemeinwohl hin orientiert sind.

2.4. Selbstbestimmung

Freie politische Willensbildung und individuelle Selbstbestimmung sind notwendige Bedingungen für die Funktionsfähigkeit repräsentativer Demokratien. Um aber besser nachvollziehen zu können, wie sich die Digitalisierung auf Prozesse individueller Selbstbestimmung in Demokratien auswirkt, muss analysiert werden, wie sich die Praktiken digitaler Plattformen, Dienste und Portale auf das individuelle Verhalten und die Einstellungen von Nutzerinnen und Nutzern genau auswirken. Dabei ist zu bedenken, dass menschliche durch viele innere und äußere Faktoren wie Rationalität, Emotionalität, soziale Prägung und äußere Gegebenheiten beeinflusst werden.

2.4.1. Selbstbestimmte Entfaltung in digitalen Öffentlichkeiten

Digitale Öffentlichkeiten erlauben es dem Individuum, sich in vielfältiger Weise zu äußern, seine Meinung zu artikulieren oder einen bestimmten Lebensstil zu präsentieren. Diese Räume nutzen etwa Influencer auf Plattformen. Aber auch private Posts Einzelner können sehr relevant sein (Everyday Politics). So entstehen neue Formen demokratischer Partizipation (siehe 2.3) welche die Selbstbestimmungsmöglichkeiten von Nutzerinnen und Nutzern erweitern.

Zugleich steigt aber durch die große Öffentlichkeit, die Individuen im digitalen Raum erreichen können, die Gefahr von sozialem Anpassungsdruck und Mobbing. So werden „Online Harassment" und „Hate Speech" mittlerweile verstärkt gegen bestimmte Personengruppen eingesetzt, um diese einzuschüchtern (siehe 2.2). Zudem wurde die Existenz sogenannter Chilling Effects nachgewiesen: Allein die Erwartung einer digitalen Verhaltensüberwachung hält viele Bürgerinnen und Bürger davon ab, ihre Freiheit zu nutzen(Penney 2016). Schließlich ist digitale Teilhabe aus technischen und praktischen Gründen nicht allen Bürgerinnen und Bürgern möglich (siehe 2.2). Das schränkt die selbstbestimmte Entfaltung in der digitalen Öffentlichkeit erheblich ein.

2.4.2. Beeinflussung in digitalen Öffentlichkeiten

In demokratischen Öffentlichkeiten versuchen verschiedenste Akteurinnen und Akteure die politische Meinungs- und Willensbildung zu beeinflussen. Manche Beeinflussungsversuche sind legitim wie Wahlwerbung oder sogar erwünscht, etwa politische Diskussion und Aufklärung. Beeinflussungsversuche können aber problematisch sein, insbesondere, wenn sie intransparent sind und verdeckt geschehen. Sie schränken selbstbestimmtes erheblich ein und führen bei Entdeckung bei den Adressaten zur Empfindung von Kontrollverlust (Pew Research Centre 2014). In digitalen Öffentlichkeiten gibt es eine neue bzw. stark intensivierte Form des Beeinflussungsversuchs: das sogenannte Microtargeting. Dabei sammeln digitale Dienste Informationen über ihre Nutzerinnen und Nutzer und werten diese algorithmisch aus mit dem Ziel, diese durch individuell zugeschnittene Maßnahmen möglichst effizient zu beeinflussen. Der Handel mit personengebundenen Nutzungsdaten hat sich zu einem prosperierenden Wirtschaftszweig entwickelt. In der Öffentlichkeit weitgehend unbekannte Unternehmen besitzen international eine enorme Daten- und Marktmacht. So soll allein *Acxiom* im Jahr 2018 beispielsweise über Datensätze von 44 Millionen Deutschen verfügt haben, die von Dritten zu kommerziellen Zwecken erworben werden können. Im wirtschaftlichen Bereich wird Microtargeting für personalisierte Werbung, für dynamisierte und individualisierte Preisbildung oder sogenannte Recommender-Systeme verwendet. In politischen Bereichen wird die solche Adressierung aber klar abgelehnt (Kozyreva u. a. o. J.). Dennoch gab und gibt es auch hier datenbasierte und algorithmisch gesteuerte Versuche zur Beeinflussung; so beispielsweise im US Präsidentschaftswahlkampf 2016. Auch in Deutschland gibt es Wahlwerbung über digitale Medien, politische Beeinflussungs-

versuche über individuell zugeschnittenes Microtargeting scheinen aber in bisherigen Wahlkämpfen kaum eine Rolle gespielt zu haben(Kurz und Dachwitz 2019). Allerdings sind auch in Deutschland und Europa die technischen Voraussetzungen für effektives Mikrotargeting bereits gegeben. Mittlerweile bemühen sich digitale Plattformen und Dienste zunehmend, politische Beeinflussungsversuche einzuschränken. Inwieweit solche datenbasierten Beeinflussungsversuche tatsächlich erfolgreich sind, ist wissenschaftlich schwer zu ermitteln und konnte bis jetzt nicht geklärt werden. Die fehlende Evidenz in diesem Fall ist aber keinesfalls als Evidenz einer geringen Wirksamkeit solcher datenbasierter Beeinflussung misszuverstehen. Es gibt also keinen Grund zur Entwarnung. Selbst wenn digitale Manipulationsversuche kurzfristig nur wenig bewirken sollten, könnten auch kleine Veränderungen langfristig weitreichende Folgen haben, weil sie sehr viele Menschen erreichen. Dies gilt insbesondere in Situationen, in denen eine sehr knappe Wahl- oder Abstimmungsentscheidung erwartet wird. Zudem verändern bereits Manipulationsversuche und entsprechende Befürchtungen den öffentlichen Diskurs. Und schließlich ist die Vermutung plausibel, dass die Wirkung von datenbasierten Beeinflussungsversuchen aufgrund technologischer Weiterentwicklung und angetrieben durch den wirtschaftlichen Wettbewerb künftig weiter steigen wird.

2.4.3. Herausforderungen

Digitalisierung kann die demokratische Selbstbestimmung erheblich unterstützen, indem sie Bürgerinnen und Bürgern viele Möglichkeiten eröffnet, sich politisch zu äußern, sich zu beteiligen und eigene Lebensvorstellungen zu präsentieren. Zugleich ist diese Selbstbestimmung aber durch mangelnde Zivilität in der digitalen Kommunikation und datenbasierte Beeinflussungsversuche gefährdet. In dieser Situation kommt es darauf an, neue Partizipationsmöglichkeiten und die individuelle, lebenslange Aneignung von Kompetenzen im Umgang mit digitalen Diensten wie oben dargestellt finanziell und politisch zu fördern. Die Begrenzung der Gefahren erfordert auch regulatorische und technische Maßnahmen. Sie beziehen sich einerseits auf die Stärkung ziviler Kommunikation; andererseits sollen sie die Möglichkeiten datenbasierter, personalisierter Manipulation begrenzen. Die technische Entwicklung richtet sich besonders auf Transparenz, Nachvollziehbarkeit und Fairness algorithmischer Systeme. Schließlich ist auch in diesem Zusammenhang der Zugang zu den Datenbeständen der Plattform- und Dienstebetreiber nötig, um eine sys-

tematische Erforschung der Wechselwirkungen von Digitalisierung und politischer Selbstbestimmung zu gewährleisten.

3. Handlungsempfehlungen

Vor dem hier skizzierten Hintergrund empfehlen die Nationale Akademie der Wissenschaften Leopoldina, die Deutsche Akademie der Technikwissenschaften – acatech und die Union der deutschen Akademien der Wissenschaften unter anderem folgende Maßnahmen:

Kuratierungspraxis digitaler Informations- und Kommunikationsplattformen regulieren

Die Plattformbetreiber sollten verpflichtet werden, an den Entscheidungen über Prinzipien und Verfahren der Kuratierung von Inhalten ein von ihnen finanziertes, jedoch unabhängiges und pluralistisch besetztes Gremium mit verbindlicher Entscheidungsbefugnis zu beteiligen, das aus Vertreterinnen und Vertretern staatlicher und zivilgesellschaftlicher Stellen sowie aus Nutzerinnen und Nutzern besteht. Das Gremium sollte dazu beitragen, dass sich die Vielfalt öffentlich bedeutsamer Themen und Positionen auf den Plattformen angemessen abbildet. Die Plattformbetreiber sollten auch dazu verpflichtet werden, Informationen über die Gestaltung ihrer Plattform und die Prinzipien der Kuratierung zu veröffentlichen, um Transparenz herzustellen und deren öffentliche Diskussion zu ermöglichen. Nutzerinnen und Nutzern sollten die Möglichkeit erhalten, einzelne Kuratierungsentscheidungen (wie die Löschung oder Kommentierung bestimmter Beiträge) überprüfen zu lassen.

Internetangebote des öffentlich-rechtlichen Rundfunks stärken

Der Beitrag des öffentlich-rechtlichen Rundfunks zur digitalen Öffentlichkeit sollte weiter ausgebaut werden. Außerdem sollten die Rundfunkanstalten Beiträge verstärkt unter offenen Lizenzen veröffentlichen, insbesondere bildungsrelevante Inhalte wie Dokumentationen, Erklärfilme und Beiträge zur Zeitgeschichte.

Forschung auf den Datenbeständen von Plattformen erleichtern

Plattformbetreiber sollten verpflichtet werden, ihre Datenbestände für nichtkommerzielle Forschungsprojekte bereitzustellen, die wissenschaftlichen Standards genügen. Dabei dürfen berechtigte Geheimhaltungsinteressen der Plattformbetreiber nicht verletzt werden. Um Geschäftsgeheimnisse und personenbezogene Daten wirksam zu schützen, sollte ein unabhängiges Gremium geschaffen werden, das über Zugangsbegehren entscheidet. Außerdem sollten die bestehenden rechtlichen Vorgaben für die weitere Verarbeitung erhobener Forschungsdaten überprüft werden, weil sie bis jetzt hohe Hürden für die Publikation von Forschungsergebnissen und die Weitergabe von Daten zur Validierung oder Durchführung weiterer Forschungsprojekte darstellen.

Zivilität des Diskurses sicherstellen

Nichtregierungsorganisationen (NGOs), die sich für Opfer digitaler Gewalt und gegen die Verrohung des öffentlichen Diskurses engagieren, sollten ein Verbandsklagerecht erhalten, um Rechtsverletzungen mit Bedeutung über den Einzelfall hinaus gerichtlich verfolgen zu können. Die Strafverfolgungsbehörden sollten durch Personalentwicklung, gezielte Weiterbildung und durch geeignete technische Unterstützung gestärkt werden damit strafbare Akte digitaler Gewalt wirksam geahndet werden können. Auch sollten staatliche und zivilgesellschaftliche Institutionen intensiv kooperieren, um Prävention, Opferhilfe und Rechtsdurchsetzung zu stärken.

Demokratiefreundliches Design digitaler Technologien und Infrastrukturen fördern

Erforschung und Entwicklung von Benutzungsumgebungen digitaler Dienste und plattformunabhängigen Tools sollten Transparenz und Autonomie von Nutzerinnen und Nutzern fördern, etwa durch die Bereitstellung von Zusatzinformationen über die Vertrauenswürdigkeit und die epistemische Qualität von Quellen oder die verständliche Übersicht relevanter Argumente und Positionen zu einem spezifischen Thema. Erklärbarkeit und Fairness von Algorithmen auf Basis Künstlicher Intelligenz (KI) sollten verstärkt erforscht und verwendet werden. Erklärbarkeit be-

deutet, dass wichtige Entscheidungskriterien für menschliche Nutzerinnen und Nutzer verständlich sind. Fairness heißt, dass KI-Entscheidungen im Einklang mit den grundlegenden demokratischen Werten und Grundrechten stehen.

Entwicklung der Digital- und Medienkompetenz stärken

Niedrigschwellige Maßnahmen sollten Nutzerinnen und Nutzer befähigen, Architektinnen und Architekten ihrer eigenen digitalen Informationsumgebung zu sein. Die Entwicklung von Digitalkompetenzen sollte von der Kita über die Schule, Hochschule, Weiterbildung bis zum lebensbegleitenden Lernen stattfinden. Insbesondere ist eine entsprechende Qualifikation von Erzieherinnen und Erziehern sowie Lehrerinnen und Lehrer zu gewährleisten. Querschnittsthemen der schulischen Bildung sollten der Umgang mit Daten, grundlegende Kenntnisse von Statistik und Wahrscheinlichkeitstheorie sowie Fähigkeiten zur Erfassung und Interpretation relevanten Kontextwissens sein. In den Hochschulen sollten relevante verhaltens-, sozial- und geisteswissenschaftliche Expertise in die Curricula von MINT-Disziplinen integriert sowie grundlegende technisch-mathematische und methodische Kompetenzen in allen Fächern gefördert werden. Zusätzlich sollte es verpflichtende Lehrveranstaltungen in Forschungs- und Datenethik geben.

Datenjournalismus fördern

Qualitativ hochwertiger, datenbasierter Journalismus sollte gefördert werden, der anstelle einer Fokussierung auf Einzelanekdoten und Narrative möglichst großflächige empirische Daten und langfristige Trends analysiert.

Digitale Beteiligung ausbauen

Es sollte eine staatlich geförderte Initiative etabliert werden, die neuen Formen digitaler Partizipation und darauf ausgerichtetem Journalismus gewidmet ist. Die Initiative sollte geistes- und sozialwissenschaftliche Forschung und entsprechende technische Entwicklungen fördern; Schwerpunkte sollten hierbei alternative Plattformen sowie Pionier- und Non-

Profit-Journalismus sein, mit besonderem Augenmerk für den Lokal- und Regionaljournalismus. Die Initiative sollte auch zivilgesellschaftliche Organisationen fördern, die sich dem Aufbau von Infrastrukturen für neue Partizipationsmöglichkeiten widmen, beispielsweise im Bereich von Datenspenden. Insbesondere sollten Projekte gefördert werden, die Jugendliche mit sozioökonomisch nachteiligem bzw. politikfernem Hintergrund einbinden und die Integration aller, insbesondere bisher ausgeschlossener gesellschaftlicher Gruppen im Fokus haben.

4.Referenzen

Bolin, Göran, und Julia Velkova. 2020. „Audience-Metric Continuity? Approaching the Meaning of Measurement in the Digital Everyday". *Media, Culture & Society*, März, 0163443720907017. https://doi.org/10.1177/0163443720907017.

Deutsche Akademie der Naturforscher Leopoldina, Deutsche Akademie der Technikwissenschaften, und Union der Deutschen Akademien der Wissenschaften, Hrsg. 2021. *Digitalisierung und Demokratie*. Stellungnahme / Deutsche Akademie der Naturforscher Leopoldina e. V. - Nationale Akademie der Wissenschaften. Halle (Saale): Deutsche Akademie der Naturforscher Leopoldina e. V. - Nationale Akademie der Wissenschaften.

Dolata, Ulrich. 2019. „Plattform-Regulierung. Koordination von Märkten und Kuratierung von Sozialität im Internet". *Berliner Journal für Soziologie* 29 (3–4): 179–206. https://doi.org/10.1007/s11609-020-00403-9.

EC. 2020. *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 vom 15. Dezember 2020*.

Geschke, Daniel, Anja Klaßen, Matthias Quent, und Christoph Richter. 2019. „Hass im Netz: Der schleichende Angriff auf unsere Demokratie". Jena: IDZ-Jena.

Grinberg, Nir, Kenneth Joseph, Lisa Friedland, Briony Swire-Thompson, und David Lazer. 2019. „Fake News on Twitter during the 2016 U.S. Presidential Election". *Science* 363 (6425): 374–78. https://doi.org/10.1126/science.aau2706.

Helsper, Ellen. 2021. *The Digital Disconnect: The Social Causes and Consequences of Digital Inequalities.* S.l.: SAGE PUBLICATIONS.

Karpf, David. 2019. „On Digital Disinformation and Democratic Myths". *MediaWell* (blog). 2019. https://doi.org/10.35650/MD.2012.d.2019.

Kozyreva, Anastasia, Philipp Lorenz-Spreen, Ralph Hertwig, Stephan Lewandowsky, und Stefan Herzog. o. J. „Public attitudes towards algorithmic personalization and use of personal data online: Evidence from Germany, Great Britain, and the US". Zugegriffen 23. September 2020. https://doi.org/10.31234/osf.io/3q4mg.

Kurz, Constanze, und Ingo Dachwitz. 2019. „Microtargeting und Manipulation: Von Cambridge Analytica zur Europawahl". Digitale Desinformation. Bundeszentrale für politische Bildung. https://www.bpb.de/gesellschaft/digitales/digitale-desinformation/290522/microtargeting-und-manipulation-von-cambridge-analytica-zur-europawahl.

Ladeur, Karl-Heinuz, und Tobias Gostomzyk. 2017. „Das Netzwerkdurchsetzungsgesetz und die Logik der Meinungsfreiheit". *Kommunikation und Recht*, 390–94.

Loosen, Wiebke, und Marco Dohle. 2014. *Journalismus und (sein) Publikum: Schnittstellen zwischen Journalismusforschung und Rezeptions-und Wirkungsforschung*. Springer.

Lorenz-Spreen, Philipp, Stephan Lewandowsky, Cass R. Sunstein, und Ralph Hertwig. 2020. „How Behavioural Sciences Can Promote Truth, Autonomy and Democratic Discourse Online". *Nature Human Behaviour*, Juni, 1–8. https://doi.org/10.1038/s41562-020-0889-7.

Mocanu, Delia, Luca Rossi, Qian Zhang, Marton Karsai, und Walter Quattrociocchi. 2015. „Collective Attention in the Age of (Mis)Information". *Computers in Human Behavior*, Computing for Human Learning, Behaviour and Collaboration in the Social and Mobile Networks Era, 51 (Oktober): 1198–1204. https://doi.org/10.1016/j.chb.2015.01.024.

Müller, Karsten, und Carlo Schwarz. 2020. „Fanning the Flames of Hate: Social Media and Hate Crime". SSRN Scholarly Paper ID 3082972. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3082972.

Penney, Jonathon W. 2016. „Chilling Effects: Online Surveillance and Wikipedia Use". *Berkeley Technology Law Journal* 31: 117.

Pew Research Centre. 2014. „Public Perceptions of Privacy and Security in the Post-Snowden Era".

Pfetsch, Barbara. 2020. „Democracy and Digital Dissonance: The Co-Occurrence of the Transformation of Political Culture and Communication Infrastructure". *Central European Journal of Communication*, 16.

Raue, Benjamin. 2018. „Meinungsfreiheit in sozialen Netzwerken". *Juristenzeitung*, 961–70.

Scholz, Trebor, und Nathan Schneider. 2017. *Ours to hack and to own: The rise of platform cooperativism, a new vision for the future of work and a fairer internet*. OR books.

Shmargad, Yotam, und Samara Klar. 2020. „Sorting the News: How Ranking by Popularity Polarizes Our Politics". *Political Communication* 37 (3): 423–46. https://doi.org/10.1080/10584609.2020.1713267.

Stier, Sebastian, Nora Kirkizh, Caterina Froio, und Ralph Schroeder. 2020. „Populist Attitudes and Selective Exposure to Online News: A Cross-Country Analysis Combining Web Tracking and Surveys". *The International Journal of Press/Politics* 25 (3): 426–46. https://doi.org/10.1177/1940161220907018.

Sunstein, Cass. 2018. *# Republic*. Princeton University Press.

Zuboff, Shoshana. 2018. *Das Zeitalter des Überwachungskapitalismus*. Übersetzt von Bernhard Schmid. Frankfurt New York: Campus Verlag.

Der digitale Strukturwandel von Öffentlichkeit: Demokratietheoretische Anmerkungen[1]

Thorsten Thiel

Wenn wir über digitale Öffentlichkeit nachdenken, stehen uns eine Vielzahl von Phänomenen vor Augen: die Katzenbilder und Memes des *world wide web*, die Feeds und Like-Buttons sozialer Netzwerke, global erreichbare Videostreams, die einen unmittelbar an friedlichen Demonstrationen, aber auch an terroristischen Attentaten teilhaben lassen. Hasskommentare stehen neben *Long Reads*, die Vernetzung von Familien, Freund*innen und Fremden neben anonymen Pöbeleien, die Wikipedia neben kommerzieller und politischer Manipulation. Schon diese kurze Aufzählung zeigt nicht nur die Vielgestaltigkeit digitaler Öffentlichkeit, sondern auch die Dynamik ihrer Entwicklung. Digitale Öffentlichkeit ist kein stehendes Phänomen, es kommen beständig neue Optionen hinzu, die mal aus technischen Entwicklungen, mal aus Nutzungspraktiken erwachen – man denke einfach mal an den Hashtag, dessen organisationale, aber auch popkulturelle Bedeutung.[2]

Dieser Beitrag hat das Ziel, die Konturen des digitalen Strukturwandels von Öffentlichkeit zu bestimmen, um die Frage zu beantworten, inwiefern und wie dieser für Erhalt und Entwicklung der Demokratie relevant ist. Gerade weil die Digitalisierung unserer Gesellschaft mit einer seit längerem anhaltenden Phase demokratischer Regression zusammenfällt, liegt es nahe, diese Entwicklungen unmittelbar aufeinander zu beziehen. Die Digitalisierung von Öffentlichkeit stellt in dieser Perspektive eine erodierende Kraft dar, der es zu begegnen gilt, bevor es zu spät ist.

Inwiefern dieser Diagnose zuzustimmen ist, soll im Folgenden durch eine differenzierte Betrachtung ergründet werden. Wobei im ersten Teil des Beitrags der Fokus darauf liegt, was eigentlich den digitalen Strukturwandel ausmacht und wie dieser überhaupt zu analysieren ist, bevor

1 Der vorliegende Beitrag stellt eine aktualisierte, stark überarbeitete Version eines älteren Beitrags dar: Thiel, Thorsten 2020: Öffentlichkeit, digitale. Zum neuen Strukturwandel der öffentlichen Sphäre, in: Stichworte zur Zeit: Ein Glossar, Bielefeld. S. 198–212.

2 Bernard, Andreas 2019: Theory of the Hashtag, Medford, MA.

im zweiten Teil kurz diskutiert wird, welche demokratietheoretischen Folgerungen sich aus dem Strukturwandel ziehen lassen und welche Gestaltungsmöglichkeiten sich aus demokratischer Perspektive anbieten.

Den digitalen Strukturwandel verstehen: Konzeptuelle Anmerkungen

Die Digitalisierung von Öffentlichkeit ist ein Prozess, der zu Beginn des Computerzeitalters, also ab der zweiten Hälfte des zwanzigsten Jahrhunderts einsetzt. Seit dieser Zeit nimmt die digitale Speicherung und Verarbeitung von Daten stark zu, wobei der Bereich der massenhaften öffentlichen Kommunikation hauptsächlich seit der weltweiten Adaption des (kommerziellen) Internets in der Mitte der 1990er-Jahre wahrgenommen und diskutiert wird.[3] Während zunächst die Globalität der Kommunikation und die Möglichkeit der umfassenden Verfügbarmachung von Wissensbeständen im Fokus stand, wandelt sich der Blick auf digitale Öffentlichkeit in den 2000er-Jahren entscheidend. Grund hierfür sind zwei Entwicklungen: Zum einen wird der ursprüngliche Fokus auf die Verfügbarmachung von Wissen und Information durch eine viel stärkere Betonung der individuellen Kuratierung von Kommunikation erweitert, wiesie vor allem in den sozialen Netzwerken zum Ausdruck kommt. Eine neue Form digitaler Vergesellschaftung wird so hervorgebracht.[4] Smartphones stellen ab 2008 in diesem Prozess eine weitere revolutionäre Neuerung dar: Zunächst, weil sie große Öffentlichkeit und private Interaktion so eng verbinden, dass beides oft in derselben App Platz findet. Aber auch als Sensoren vom Schrittzähler bis zum Geo-Tracking bringen die Geräte neue Möglichkeiten hervor – und dies nicht nur auf Seiten der Benutzer*innen, sondern gerade auch für die Anbieter von Technologien und Diensten, die umfassend Verhalten beobachten und auswerten können, woraus auf individueller wie gesellschaftlicher Ebene umfassende Möglichkeiten der Verhaltensinterpretation und -einwirkung resultieren.[5] Smartphones sind zudem Vorreiter in der Entwicklung, alle gesellschaftlichen Räume digital zu augmentieren. Heute werden sie weiter ergänzt durch Sensoren und Kameras, Sprachassistenten oder allgemein das Internet der Dinge. Digitale Öffentlichkeit hat insofern kein direktes Außen mehr. Sie ist kein

3 Prägend für die Frühphase der Diskussion: Rheingold, Howard 2000: Virtual Community: Homesteading on the Electronic Frontier, Cambridge, Mass.
4 Münker, Stefan 2009: Emergenz digitaler Öffentlichkeiten, Frankfurt, M.
5 Adam Greenfield, Adam (2017): Radical Technologies: The Design of Everyday Life. London/ New York: Verso.

irgendwo anders liegender *Cyberspace*, kein *Online*, in das man reingehen könnte. Vielmehr ist unsere ganze Öffentlichkeit durchwirkt von digitaler Mediation und immer wieder auf digitale Formate zurückbezogen.[6]

Digitale Öffentlichkeit meint insofern zu unterschiedlichen Zeitpunkten unterschiedliches – und die digitale Öffentlichkeit wird sich auch weiterhin durch technologische, ökonomische und soziopolitische Entwicklungen verändern. Zugleich unterscheiden sich performativ wie strukturell alle bisherigen Inkarnationen digitaler Öffentlichkeit erheblich von den ihnen vorangegangenen, nicht durch digitale Mediation geprägten Öffentlichkeitsformationen.[7]

Dies wirft die Frage auf, wie sich eine solche dynamische und komplexe Formation überhaupt analytisch beschreiben und diskutieren lässt und wie die vielgestaltigen, oft auch einander zuwiderlaufenden Entwicklungen für eine normativ-demokratietheoretische Einschätzung fassbar gemacht werden können. In der öffentlichen wie wissenschaftlichen Diskussion dominiert diesbezüglich eine Rhetorik von Chancen und Risiken, wo mal die eine, mal die andere Seite überbetont oder einfach pauschal eine Ambivalenz diagnostiziert wird. Um diese, tendenziell hilflose Betrachtungsweise zu vermeiden, soll im Folgenden ein systematisch anspruchsvolleres Untersuchungskonzept vorgeschlagen werden, welches sich auf den Begriff der digitalen Konstellation bringen lässt.[8]

Die Analyseperspektive der digitalen Konstellation nimmt nicht für sich in Anspruch, eine umfassende Theorie der digitalen Gesellschaft zu bieten, sie fungiert auch nicht als Zeitdiagnose, die das Einheitliche einer digitalen Gesellschaft bezeichnen soll. Mit dem Begriff der digitalen Konstellation soll vielmehr Digitalisierung als Prozess ernstgenommen werden, in dem Gesellschaft und Technik umfassend, dynamisch und fortlaufend in Beziehung gesetzt werden. Im Fokus steht die Ko-Evolution beider Sphären, d. h. wie digitale Technik als Teil des kollektiven Vergesellschaftungs-

6 Floridi, Luciano 2014: The Fourth Revolution: How the Infosphere is Reshaping Human Reality, Oxford, New York.

7 Baecker, Dirk 2018: 4.0 oder Die Lücke die der Rechner lässt, Leipzig.

8 Für eine ausführliche Begründung und Herleitung vgl.: Berg, Sebastian/Rakowski, Niklas/Thiel, Thorsten 2020: Die digitale Konstellation. Eine Positionsbestimmung, in: Zeitschrift für Politikwissenschaft 30: 2, 171–191 – für die exemplarische Darlegung weitere Anwendungsfelder: Thiel, Thorsten 2020: Demokratie in der digitalen Konstellation, in: Riescher, Gisela/Rosenzweig, Beate/Meine, Anna (Hrsg.): Einführung in die Politische Theorie. Grundlagen – Methoden – Debatten, Stuttgart.

prozesses Bedingungen setzt, aber auch selbst geformt wird.[9] Mit Blick auf einen konkreten Gegenstandsbereich wie digitale Öffentlichkeit werden dabei analytisch drei Ebenen des Wechselverhaltens von Technik und Gesellschaft bedeutsam: die Ebene der ‚Eigenschaften' digitaler Technik, die Ebene praktisch realisierter Affordanzen und die Ebene der gesellschaftlichen Konfiguration.

Eigenschaften digitaler Technik sind basale Mechanismen, die in der Logik des digitalen Formats selbst angelegt sind, etwa die Archivierbarkeit, Vernetzbarkeit oder Prozessierbarkeit alles Digitalen.[10] Diese abstrakten Eigenschaften bilden eine Konstante, nehmen aber in Verbindung mit Handlungspraktiken und -kontexten unterschiedliche Ausprägungen an. Welche, zeigt sich auf der zweiten Ebene, den praktisch realisierten Affordanzen. Affordanzen sind kollektiv etablierte Handlungserwartungen bzw. -formen, die sich aus dem wahrgenommenen Möglichkeitsspektrum von Gegenständen bzw. Technik ergeben. Sie verweisen auf die facettenreiche Beziehungsstruktur zwischen einem technischen Artefakt und dessen Nutzer*in, wobei die Technik nicht die Möglichkeiten der Handelnden determiniert, aber doch (vor-)strukturiert und inspiriert.[11] Auf einer gesellschaftlichen Ebene und mit Blick auf größere Komplexe wie digitale Technologie als Sammelbegriff geht es dabei nicht um einzelne Gegenstände und deren individuelle Nutzungsmöglichkeiten, sondern um die Generalisierung von Handlungsmöglichkeiten. Diese erzeugen gesamtgesellschaftliche Pfadlogiken, was weiter unten am Beispiel der *Many-to-many*-Kommunikation exemplifiziert wird. Auf der dritten Ebene, der gesellschaftlichen Konfiguration, treten schließlich allgemeine rechtliche, ökonomische und politische Einbettungen hinzu, die Form und Einsatz von Technik regulieren und strukturieren – und damit auch künftige Entwicklungsrichtungen von Technik und Technikeinsatz prägen und ausgestalten.

Eine Analyse mediatisierter Demokratie setzt voraus, dass man alle drei Ebenen in den Blick nimmt und differenziert ihre Verbindungen und

9 Ohne Verwendung des Begriffs, aber in der Methode verwandt und eine gute techniksoziologische Einbettung bietend: Katzenbach, Christian 2018: Die Regeln Digitaler Kommunikation: Governance zwischen Norm, Diskurs und Technik, Wiesbaden.

10 Vgl etwa: Lenk, Klaus 2016: Die neuen Instrumente der weltweiten digitalen Governance, in: Verwaltung & Management 22: 5, 227–240.

11 Evans, Sandra K./Pearce, Katy E./Vitak, Jessica/Treem, Jeffrey W. 2017: Explicating Affordances: A Conceptual Framework for Understanding Affordances in Communication Research, in: Journal of Computer-Mediated Communication 22: 1, 35–52.

Bedingtheiten beschreibt. Erst dadurch erhält man eine umfassende Vorstellung davon, was digitalen Strukturwandel ausmacht. Ein Verständnis für die Wucht der Entwicklung entsteht ebenso wie für die Möglichkeit des Andersseins und der bestimmenden Faktoren.[12] Für die digitale Öffentlichkeit soll dies mit Blick auf zwei zentrale Vektoren demonstriert werden: die Veränderung der gesamtgesellschaftlichen Kommunikationssituation und die Bedeutsamkeit von Daten.

a) Kommunikation in der digitalen Öffentlichkeit

Zentrales Merkmal heutiger digitaler Kommunikationsumgebungen ist die Möglichkeit direkter wechselseitiger Interaktion, die sogenannte *Many-to-many*-Kommunikation. *Many-to-many*-Kommunikation bedeutet, dass es von jedem Punkt im Netzwerk potentiell möglich ist, mit einem offenen und theoretisch das ganze Netzwerk umfassenden Adressatenkreis in Kontakt zu treten.[13] *Many-to-many*-Kommunikation ist aber mehr als nur die Erhöhung der Reichweite von Kommunikation durch das Absinken von Vermittlungskosten. Sie umfasst vielmehr ganz neue synchrone und asynchrone gruppenbezogene Interaktions- und Koordinationsformen, die ein enormes Anwachsen kommunikativer Komplexität zur Folge haben.[14] Grundlage hierfür sind algorithmische Verarbeitungsmöglichkeiten der Kommunikation (etwa Such- und andere Ordnungsfunktionen) sowie Techniken zur visuellen Orientierung des Kommunikationsverhaltens (etwa Emoticons oder die flexible Darstellung von Kommentierungen). Erhöhte kommunikative Komplexität kann insofern nur wachsen, weil sie zugleich auch wieder und wieder gebändigt wird.[15] Es gilt, Anschlussmöglichkeiten herzustellen, Zusammenhänge zu visualisieren und Optionen zu priorisieren. Pluralität wird also zugleich begünstigt und sodann im-

12 Hofmann, Jeanette 2019: Mediated democracy – Linking digital technology to political agency, in: Internet Policy Review 8: 2, in: https://policyreview.info/articles/analysis/mediated-democracy-linking-digital-technology-political-agency; 18.7.2019.

13 Klassisch hierzu: Shirky, Clay 2008: Here Comes Everybody: The Power of Organizing Without Organizations, New York.

14 Christoph Neuberger (2017): Die Rückkehr der Masse. Interaktive Massenphänomene im Internet aus Sicht der Massen- und Komplexitätstheorie, in: Medien & Kommunikationswissenschaft, 65 (3), S. 550–572.

15 Ausführlich beschrieben wird dies etwa in systemtheoretischen Ansätzen zu Digitalisierung, etwa: Nassehi, Armin 2019: Muster: Theorie der digitalen Gesellschaft, München.

mer wieder schon integriert, so wie es emblematisch die personalisierten *Feeds* aller Social-Media-Plattformen unternehmen. Wir leben insofern im Zeitalter des „communicative plenty", einer Situation, in der jeder und jedem jederzeit sehr viele Möglichkeiten der Fortführung oder Initiierung von Kommunikationen offenstehen und wir daher permanent gezwungen sind, unser Kommunikationsverhalten zu reflektieren, zu rechtfertigen oder zu modifizieren. [16]

Wie aber wird *Many-to-many*-Kommunikation politisch relevant? Hierfür müssen wir zusätzlich zu der Ebene der Eigenschaften und Affordanzen auch stärker die gesellschaftlichen Praktiken und Rahmensetzungen in den Blick nehmen. Etwa die veränderten Möglichkeiten zur kollektiven Handlungskoordination oder die Umstellungen, die sich für die etablierte massenmediale Kommunikationsinfrastruktur ergeben.

In Bezug auf die Möglichkeiten kollektiver Handlungsorganisation ist das von Alexandra Segerberg und Lance Bennett geprägte Konzept der „connective action" die eingängigste Weise, sich den veränderten Möglichkeiten zu nähern.[17] Konnektives Handeln unterscheidet sich von kollektivem Handeln, insofern es ohne die für letzteres notwendige organisationale Zentralisierung auskommt. Möglich ist dies, da der Angebotscharakter digitaler Technologie dezentral inspiriert, Handlungszusammenhänge fortführt und einzelne Handlungsakte symbolisch auflädt und/oder technologisch verbindet, wie es etwa an Formen des Hashtag-Aktivismus von #aufschrei über #blacklivesmatter bis #unteilbar deutlich wird.[18] Die für die Erzeugung kommunikativer Reichweite notwendigen Ressourcen sind in den Infrastrukturen – konkret hier: den Social-Media-Plattformen – für die Handelnden abrufbar gespeichert, was Geschwindigkeit und Skalierbarkeit ermöglicht.[19] Das ermöglichte konnektive Handeln bewirkt eine deutliche Veränderung und Ausweitung des Handlungsrepertoires, das durch soziale Bewegungen, aber eben auch einzelne Individuen kreativ

16 Selen A. Ercan/Carolyn M. Hendriks/John S. Dryzek (2019): Public Deliberation in an Era of Communicative Plenty. In: *Policy & Politics*, 47 (1), S. 19–36.

17 W. Lance Bennett/Alexandra Segerberg (2014): The Logic of Connective Action: Digital Media and The Personalization Of Contentious Politics. Cambridge: Cambridge University Press.

18 Koster, Ann-Kathrin 2020: Im Zeichen des Hashtags. Demokratische Praktiken unter algorithmisierten Bedingungen, in: Kruse, Jan-Philipp/Müller-Mall, Sabine (Hrsg.): Digitale Transformationen der Öffentlichkeit, 103–122.

19 Earl, Jennifer/Kimport, Katrina 2011: Digitally Enabled Social Change: Activism in the Internet Age, Cambridge, London.

und für die verschiedensten Zwecke genutzt werden kann.[20] Konnektives Handeln wirkt dabei nicht verdrängend, sondern zumeist komplementär zu anderen „klassischen" Formen der Ansprache, Mobilisierung oder Koordinierung. Jede dieser Handlungsweisen ist durch distinkte Vor- bzw. Nachteile charakterisiert, die Entscheidung für konnektive Handlungsformen insofern immer auch eine strategische.[21]

Die zweite Entwicklung ist die nachhaltige Veränderung der Rolle und Bedeutung von Massenmedien. In vorangegangen medialen Konstellationen war Reichweite stets direkt abhängig von finanziellen und personellen Ressourcen. Massenmedien waren damit nicht nur faktisch in der Rolle der *Gatekeeper*, sondern dadurch auch gleichsam automatisch ein Ankerpunkt für demokratische Kontrolle, wie sie etwa durch Aufsichtsinstanzen oder professionale Normen, z. B. im Journalismus, ausgeübt wird.[22] In der digitalen Konstellation werden sowohl die organisationalen wie auch die handlungspraktischen Gewissheiten erschüttert.[23] Wie schon in Bezug auf das kollektive Handeln ergibt sich eine Situation der Überlagerung. Keineswegs ist es so, dass Ressourcen und etablierte Machtpositionen nicht mehr zählen, aber die Logik digitaler Kommunikationsinfrastrukturen eröffnet neue Kanäle und Strategien, um gesellschaftsweite Diskurse anzustrengen und zu beeinflussen.[24] Die Beispiele reichen vom Twitter-Account Donald Trumps bis zu #metoo. Es ist insofern auch nicht einfach anarchische Horizontalität, die an die Stelle hierarchischer Strukturierung

---

20 Tufekci, Zeynep 2017: Twitter and Tear Gas: The Power and Fragility of Networked Protest, New Haven ; London.

21 Die Bedeutung von Organisationsformen erschließt sich erst in deren kreativer Nutzung durch Akteure an den konkreten Schnittstellen zur etablierten Politik, wobei der Rückgriff auf konnektive Handlungspraktiken vom Ausgangpunkt der Organisation politischen Protests sich zunehmend auf weitere Felder politischer Betätigung ausgeweitet hat. Vgl: Bennett, W. Lance/Segerberg, Alexandra/Knüpfer, Curd B. 2018: The Democratic Interface: Technology, Political Organization, and Diverging Patterns of Electoral Representation, in: Information, Communication & Society 21: 11, 1655–1680.

22 Habermas, Jürgen 2008: Hat die Demokratie noch eine epistemische Dimension? Empirische Forschung und normative Theorie, in: Habermas, Jürgen (Hrsg.): Ach, Europa, Frankfurt am Main, 138–191.

23 Bennett, W. Lance/Pfetsch, Barbara 2018: Rethinking Political Communication in a Time of Disrupted Public Spheres, in: Journal of Communication 68: 2, 243–253.

24 Lischka, Konrad/Stöcker, Christian 2017: Digitale Öffentlichkeit – Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen, Gütersloh; Chadwick, Andrew 2013: The Hybrid Media System: Politics and Power (Oxford Studies in Digital Politics), Oxford, New York.

tritt, wie es noch der frühe Internetdiskurs suggerierte. Vielmehr sind umkämpfte und durch sich ändernde ökonomische Imperative geprägte Bedingungen ausschlaggebend, wenn man nachvollziehen will, welche Form von Öffentlichkeit(en), sich zunehmend stabilisiert.[25] Eine ganz besondere Rolle kommt dabei einer sich neu etablierenden Klasse von *Gatekeepern* zu, den Plattformen. Diese verfügen über eine spezifische Form von Macht, die Elemente der Zugangs- und der Feinsteuerung vereint und durch Standardisierung und Algorithmisierung oftmals unbemerkt ausgeübt wird.[26]

Many-to-many-Kommunikation und der Wandel des Mediensystems resultieren somit insgesamt in einer kommunikativen Grundsituation, die dynamischer und komplexer ist als vorangegangene mediale Konstellationen. Kommunikations- und Informationsmöglichkeiten sind vielseitiger und umfassender, was ungeachtet neuer Orientierungsmöglichkeiten die individuellen Anforderungen erhöht, sich zu informieren und einzubringen. Dass zugleich öffentliche und private Kommunikation stärker in eins fallen und über dieselben Kanäle artikuliert werden, erhöht den affizierend-emotionalen Gehalt von Kommunikation und verringert das Vertrauen in Medienquellen und -formate.[27]

b) Die Datafizierung digitaler Öffentlichkeit

Während die Veränderung von Kommunikationspraktiken schon seit den frühen Tagen des Internets unmittelbar erfahren und mit großer Vehemenz diskutiert wird, wird der zweite hier anzuschneidende Aspekt, die Datafizierung, erst in jüngerer Zeit verstärkt als eigenständiger Faktor thematisiert und direkt in ihren Auswirkungen auf die Modalität politischen Handelns untersucht.

Ausgangspunkt hierfür ist die Datenform jedweder digitaler Kommunikation. Digitalisierung wird – wie oben beschrieben – zunehmend ubiquitär, was heißt, dass jedwedes gesellschaftliches Handeln erfasst, gespei-

25 Staab, Philipp/Thiel, Thorsten 2021: Privatisierung ohne Privatismus. Soziale Medien im digitalen Strukturwandel der Öffentlichkeit, in: Seeliger, Martin/Sevignani, Sebastian (Hrsg.): Ein neuer Strukturwandel der Öffentlichkeit?, Leviathan Sonderband 37, 275–297.

26 Seemann, Michael 2021: Die Macht der Plattformen: Politik in Zeiten der Internet-Giganten, Berlin.

27 Klinger, Ulrike 2018: Aufstieg der Semiöffentlichkeit: Eine relationale Perspektive, in: Publizistik 63: 2, 245–267.

chert und damit auch maschinell analysierbar gemacht wird. Hierdurch verändern sich die Möglichkeiten von Gesellschaften, etwas über sich selbst zu wissen und auf sich selbst einzuwirken.[28] Der stete Fluss von Daten über Kommunikation etwa bewirkt, dass die oben beschriebenen sozialen Netzwerke nicht nur Infrastrukturen der Kommunikation, sondern immer auch zugleich Infrastrukturen der Verhaltensbeobachtung sind. Dass dies einen politischen Effekt hat, ist durch Schlaglichter wie die Debatten um Wahlbeeinflussung durch *Cambridge Analytica* grell ins öffentliche Bewusstsein getreten. Für den weiteren Kontext des digitalen Strukturwandels sind aber nicht nur solche relativ klaren Szenarien des Missbrauchs von Datenmacht relevant, sondern es gilt gerade längerfristige Entwicklungen in ihrer Verschränkung von technischen Möglichkeiten und gesellschaftlichen Praktiken zu analysieren, wie sich etwa in Bezug auf Anonymität und Identifizierbarkeit zeigen lässt.

Anonymität und Identifizierbarkeit werden dabei in einer Weise zum Thema, die zunächst überraschen muss. Digitale Kommunikation galt – und gilt teilweise noch immer – ob ihrer technischen Vermitteltheit als besonders unpersönliche und daher zu Missbrauch einladende Form von Interaktion: „On the Internet, nobody knows you're a dog", wie es in einer berühmten, schon 1993 im New Yorker veröffentlichten Karikatur hieß. Während die Eigenschaften und auch die Affordanzen digitaler Kommunikationsmittel scheinbar eindeutig auf Anonymität und im direkten Übertrag oft auf mit dieser assoziierten Entwicklungen wie Unverbindlichkeit und Verrohung des Diskurses zu verweisen scheinen, ist die entwickelte digitale Öffentlichkeit doch weit mehr durch eine permanente und tiefe Identifizierbarkeit gekennzeichnet.[29] Eine Identifizierbarkeit, die weiter reicht, als es für vorangegangen Öffentlichkeitsformationen überhaupt in der Breite vorstellbar war. Der Grund hierfür ist (mindestens) eine doppelter: erstens die Unterschätzung des technischen Vermögens zur Identifizierung angesichts enorm großer und automatisiert auf Muster zu durchsuchender Datenmengen; zweitens der sich verändernde gesellschaftliche und ökonomische Rahmen, der Anreize setzt, Identifizierungspraktiken zu entwickeln, vor allem aber neue Akteure ermächtigt. Nicht mehr nur Staaten als herrschaftliche Akteure haben heute ein Interesse an individueller

28 Ulbricht, Lena er al 2018: Dimensionen von Big Data: Eine politikwissenschaftliche Systematisierung, in: Kolany-Raiser, Barbara/Heil, Reinhard/Orwat, Carsten/Hoeren, Thomas (Hrsg.): Big Data und Gesellschaft: Eine multidisziplinäre Annäherung, Wiesbaden, 151–231.

29 Froomkin, A. Michael 2015: From Anonymity to Identification, in: Journal of Self-Regulation and Regulation 1: 121–138.

Zuordenbarkeit und Rückverfolgung, sondern gerade private Unternehmen haben ihre Geschäftsmodelle auf Datensammlung fokussiert und damit ein Netz von Identifizierungs- und individualisierten Prognosemechanismen über die digitale Öffentlichkeit geworfen.[30] Vertikale Anonymität – also die Anonymität gegenüber ressourcenstarken Akteuren – ist im Verschwinden begriffen und horizontale Anonymität, also die Möglichkeit pseudonyme Diskurse auf der Ebene von Individuen und Gruppen zu führen, stellt hierfür keinen Ersatz dar.[31]

Den digitalen Strukturwandel durchdenken: Demokratietheoretische Folgerungen

Many-to-many-Kommunikation und Datafizierung sind Elemente des Strukturwandels digitaler Öffentlichkeit, die in ihrer konkreten Form erst erkenn- und erklärbar werden, wenn man mit der analytischen Perspektive der digitalen Konstellation die technischen und sozioökonomischen Bedingtheiten in ihrer aktuellen Verschränkung analysiert hat. Digitale Öffentlichkeit ist somit zwar nicht abschließend und umfassend beschrieben, aber es entsteht ein Bewusstsein für das sich verändernde Handlungs- und Kommunikationsumfeld, die Kräfte, die dieses justieren und die Möglichkeiten, differenziert auf die Entwicklung einzuwirken.

Auf dieser Grundlage wollen wir uns nun im Folgenden dem Verhältnis von digitaler Öffentlichkeit und Demokratie zuwenden. Was bedeuten die aufgezeigten strukturellen Veränderungen für demokratische Selbstbestimmung? Welche Möglichkeiten bieten sich in der Demokratie, den digitalen Strukturwandel von Öffentlichkeit zu begleiten und zu gestalten?

30 Zuboff, Shoshana 2019: The Age of Surveillance Capitalism, New York.

31 Ausführlicher: Thiel, Thorsten 2016: Anonymität und der digitale Strukturwandel der Öffentlichkeit, in: Zeitschrift für Menschenrechte 10: 1, 9–24; Thiel, Thorsten 2017: Anonymität und Demokratie, in: Forschungsjournal Soziale Bewegungen 30: 2, 152–161.

a) Demokratietheorie und digitale Öffentlichkeit

Die Klärung der ersten Frage setzt zunächst voraus, dass wir zum Verhältnis von Demokratie und Öffentlichkeit zurückgehen, um zu bestimmen, wie der Bezug von Demokratie auf Öffentlichkeit eigentlich aussieht. Während es nämlich ein Allgemeinplatz ist, dass demokratische Öffentlichkeit(en) ein zentrales Kennzeichen der Demokratie sind, sagt die Demokratietheorie selbst erstaunlich wenig zu Art und Form dieser Öffentlichkeit(en).[32] Grob lassen sich in der jüngeren Demokratietheorie zwei Positionen auseinanderhalten: die liberale Argumentation für eine grundrechtlich gesicherte Öffentlichkeit mit einem Fokus auf pluralistischer, individueller Interessenäußerung und die kompetitive Hervorbringung von Mehrheitsmeinungen sowie die deliberativdemokratische Perspektive, die die Inklusion und Transformation von Meinung(en) im öffentlichen Diskurs betont. Welche Impulse und Herausforderungen kreiert der digitale Strukturwandel aus diesen Perspektiven?

Aus der liberalen Perspektive sticht zunächst das Mehr an Ausdrucksmöglichkeiten hervor. Die oben mit *Many-to-Many*-Kommunikation und der Hybridisierung des Mediensystems verbundene Möglichkeit der Initiierung und Organisation gesellschaftsweiter Diskurse birgt demzufolge die Aussicht auf einen Demokratisierungsschub, da die Möglichkeiten zur Äußerung von Interessen wie zur umfassenden und kontinuierlichen Aggregation von Stimmungen zunehmen.[33] Allerdings ist auch sofort zu betonen, dass sich die Wirkmächtigkeit der Individuen weder geradlinig noch gleichmäßig erhöht. In der digitalen Öffentlichkeit werden Machtasymmetrien nicht aufgehoben, sondern zumindest teilweise gar verstärkt, da die intensiven Partizipationsformen mit hohen kognitiven und strukturellen Voraussetzungen daherkommen und Ungleichheiten teilweise auch noch invisibilisiert werden.[34]

Der Forschungsansatz der digitalen Konstellation gebietet aber, nicht einfach nur relative Gewinne und Verluste zu bestimmen, sondern ins-

---

32 Für eine gute Systematisierung vgl. aber: Renate Martinsen (2009): Öffentlichkeit in der „Mediendemokratie“ aus der Perspektive konkurrierender Demokratietheorien, in: Marcinkowski/Pfetsch (Hrsg.), Politik in der Mediendemokratie.

33 Coleman, Stephen/Blumler, Jay G. 2009: The Internet and Democratic Citizenship: Theory, Practice and Policy, Cambridge; New York.

34 Eine klassische Artikulation dieser Position bietet etwa: Hindman, Matthew 2008: The Myth of Digital Democracy, Princeton; Hindman, Matthew 2018: The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy, Princeton, New Jersey.

besondere sich verändernde Grundbedingungen zu skizzieren. Aus der liberalen Perspektive ist hier etwa auf Veränderungen im Verhältnis von Politik und Bürger*innen einzugehen: Hier wird zum Beispiel die oben herausgearbeitete Datafizierung relevant. In der heutigen digitalen Öffentlichkeit zeichnet sich nämlich ab, dass die Transmission des Bürger*innenwillens nicht länger vorrangig durch aktive Partizipation erfolgen muss, sondern die Beobachtung und Simulation des Verhaltens der Bürger*innen neben die klassischen Partizipationsformen tritt. Die permanente Datensammlung und die Kombination von Daten, die aus unterschiedlichen, häufig sehr disparaten Gründen erzeugt wurden, produziert ein allzeit abrufbares und zumindest scheinbar totales Wissen über Wünsche und Sorgen der Bürger*innen sowie Möglichkeiten, Öffentlichkeit und den öffentlichen Diskurs scheinbar gezielt zu manipulieren. Problematisch daran ist nicht nur die Frage, wie repräsentativ dieses *Demos scraping* wirklich ist, sondern vor allem, wie sehr eine ablesende Logik nicht letztlich selbst ein minimales Demokratieverständnis unterläuft, da die für liberale Modelle kennzeichnenden Kontrollpositionen aufgegeben werden.[35]

Wechselt man die Theorie und schaut aus der Perspektive von partizipatorischen oder deliberativen Demokratietheorien, so verändert sich die Einschätzung nochmals: In dieser Perspektive ist zentral, dass in einer Demokratie gruppenübergreifende Kommunikation erfolgt und eine gemeinsame Willensbildung gelingt. Der Bewertungsmaßstab ist also der Beteiligungsgrad und die Integrationsleistung von Öffentlichkeit.[36] In dieser Hinsicht ist die Ausgangsdiagnose bezüglich digitaler Öffentlichkeit oft negativ: Digitalisierung wird als ursächlich für zentrifugale Entwicklungen angesehen, da sie die Bildung von Filterblasen und Echokammern bewirke.[37] Die technisch beförderte und durch die Plattformökonomie verstärkte Entwicklung bewirke, dass es nicht mehr gelinge, den inklusi-

35 Zur jüngeren Diskussion um *demos scraping* und die Folgen der Datafizierung des Elektorats aus dem Blickwinkel unterschiedlicher Demokatietheorien vgl.: Ulbricht, Lena 2020: Scraping the Demos. Digitalization, Web Scraping and the Democratic Project, in: Democratization 27: 3, 426–442.; Bennett, Colin J./Lyon, David 2019: Data-driven elections: implications and challenges for democratic societies, in: Internet Policy Review 8: 4.; Urbinati, Nadia 2019: Judgment Alone: Cloven Citizenship in the Era of the Internet, in: Castiglione, Dario/Pollak, Johannes (Hrsg.): Creating Political Presence: The New Politics of Democratic Representation, Chicago ; London, 61–85.

36 Peters, Bernhard 2007: Der Sinn von Öffentlichkeit, in: Peters, Bernhard (Hrsg.): Der Sinn von Öffentlichkeit, Frankfurt am Main, 55–102.

37 Klassisch wird diese Diagnose aus demokratietheoretischer Perspektive durch Cass Sunstein gestellt: Sunstein, Cass R. 2001: Republic.Com, Princeton, N.J.

ven Charakter von Öffentlichkeit sowie den rational deliberativen Kern der öffentlichen Meinungs- und Willensbildung aufrecht zu erhalten.[38] Digitale Öffentlichkeit wird also als ursächlich für die Polarisierungsdynamik westlicher Demokratien angesehen, zumal neben Echokammern und Filterblasen auch *Hate Speech* und Des- bzw. Misinfomation die Grundlagen des gemeinsamen Diskurses weiter erschüttern.[39] Wobei empirisch anzumerken ist, dass in Bezug auf alle drei Phänomenbereiche die die Erosion epistemischer Voraussetzungen der Demokratie zu belegen scheinen, die Forschung sehr viel differenzierter ausfällt und oft andere Faktoren, etwa die Repräsentationsqualität des politischen Systems oder sozioökonomische Faktoren, als wichtiger für Polarisierungstendenzen erachtet werden.[40]

Auch mit Blick auf die partizipativ-deliberativdemokatische Perspektive lässt sich mit den Mitteln der analytischen Perspektive der digitalen Konstellation das Bild weiter verkomplizieren: Denkt man Integration nämlich weniger gesellschaftsübergreifend, sondern eher partiell und dynamisch, so tritt das hohe performative Moment von Öffentlichkeit(en) hervor, welches wir oben bereits als Merkmal von *many-to-many*-Kommunikation kennengelernt haben. In der digitalen Konstellation stehen Bürger*innen neue und bessere Möglichkeiten zur Verfügung, sich zusammenzuschließen, situationsbezogen zu handeln und Koalitionen zu bilden.[41] Hieraus ergeben sich Chancen für einen aktiv gestalteten Formwandel der Demokratie: Öffentlichkeit kann hier nicht nur als eine von außen auf die repräsentativen Institutionen drückende Öffentlichkeit realisiert werden, sondern durch strukturierte Beteiligungsformen direkter einbezogen wer-

---

vgl .auch die Aktualisierung: Sunstein, Cass R. 2017: #Republic: Divided Democracy in the Age of Social Media, Princeton ; Oxford.

38 Habermas, Jürgen 2021: Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit, in: Seeliger, Martin/Sevignani, Sebastian (Hrsg.): Ein neuer Strukturwandel der Öffentlichkeit?, Band Sonderband Leviathan 37, Baden-Baden, 470–500.

39 Chambers, Simone 2021: Truth, Deliberative Democracy, and the Virtues of Accuracy: Is Fake News Destroying the Public Sphere?, in: Political Studies 69: 1, 147–163.

40 Als Überblick über die Forschungsliteratur etwa: Rau, Jan Philipp/Stier, Sebastian 2019: Die Echokammer-Hypothese: Fragmentierung der Öffentlichkeit und politische Polarisierung durch digitale Medien? in: Zeitschrift für Vergleichende Politikwissenschaft 13: 3, 399–417.

41 Antić, Andreas 2018: Digitale Öffentlichkeiten und intelligente Kooperation: Zur Aktualität des demokratischen Experimentalismus von John Dewey, Potsdam.

den.[42] Die Corona-Pandemie, die ohnehin in vielerlei Hinsichten als Beschleuniger für Digitalisierungsprozesse gewirkt hat, hat beispielsweise in Deutschland *Civic Hackathons* als neues Format der direkten und kollaborativen Form der Zusammenarbeit von exekutiven Akteuren und Bürger*innen etabliert.[43]

b) Digitale Öffentlichkeit demokratisch gestalten

Unabhängig von der in Anspruch genommenen Demokratietheorie gilt, dass Demokratie auf ein stetes Werden hin ausgelegt ist. Sie ist ein Versprechen von Partizipation, von Gleichheit und Freiheit. Institutionell übersetzt sich dies in Vielgestaltigkeit und Veränderungsoffenheit. Daraus folgt, dass wir, wenn wir über Digitalisierung und Demokratie im Allgemeinen und den digitalen Strukturwandel von Öffentlichkeit im Besonderen nachdenken, nicht einfach einem Abwehrreflex nachgeben dürfen. Digitalisierung ist keine äußere Kraft, die unsere vormals wohlgeordneten Demokratien zu zersetzen droht. Und Demokratie ist nichts Statisches, für das wir die optimale Form längst gefunden hätten. Der digitale Strukturwandel von Öffentlichkeit gefährdet nicht *die* Demokratie, er kreiert vielmehr Impulse für deren Formwandel.[44] Er ist auch nicht selbst etwas Konstantes, sondern eine sozial und politisch geprägte und zu prägende Entwicklung. Die Re-Regulierung der öffentlichen Sphäre in demokratischer Absicht ist daher möglich und nötig, woran es mangelt, ist an einer aktiven Gestaltungsperspektive.[45]

---

42 Landemore, Hélène 2021: Open Democracy and Digital Technologies, in: Bernholz, Lucy/Landemore, Hélène/Reich, Rob (Hrsg.): Digital Technology and Democratic Theory, Chicago, 62-89.

43 Kirsten Rulf, Britta Kuhn, Laura Niersbach 2021: Open Social Innovation als Innovationstreiber für die Verwaltung – Von #WirVsVirus zu UpdateDeutschland, 225–234. in: Hill, Herrmann: Die Kraft zur Innovation in der Verwaltung. Baden-Baden. – Kritischer in der Gesamtschau und mit Vorschlägen für eine Weiterentwicklung des Formats: Berg, Sebastian et al. 2021: Civic Hackathons und der Formwandel der Demokratie. Politische Vierteljahresschrift. https://doi.org/10.1007/s11615-021-00341-y.

44 Hofmann, Jeanette 2019: Mediated democracy – Linking digital technology to political agency, in: Internet Policy Review 8: 2.

45 So auch: Jungherr, Andreas/Schroeder, Ralph 2021: Disinformation and the Structural Transformations of the Public Arena: Addressing the Actual Challenges to Democracy, in: Social Media + Society 7: 1.

Die aktuelle Diskussion um den digitalen Strukturwandel ist immer noch sehr stark auf tagesaktuelle Probleme fokussiert – gegenwärtig etwa auf *Fake News* oder *Hate Speech*. Erst in jüngerer Zeit hat sich ein Bewusstsein gebildet, dass es weniger um einzelne Fehlentwicklungen als um eine größere Rahmenordnung geht.[46] Politisch macht sich dies etwa in den europäischen Regulierungsinitiativen *Digital Services Act* und *Digital Markets Act* bemerkbar. Diese und weitere Regulierungspakete – etwa zu Daten oder Künstlicher Intelligenz – verdeutlichen, dass Probleme mittlerweile koordiniert und aus gesellschaftlicher wie ökonomischer Perspektive erkannt und angegangen werden. Zumindest in Europa ist daher eine Regulierungsdekade in Bezug auf digitale Öffentlichkeit zu erwarten.

Kritisch anzumerken ist hierbei aber, dass der Diskurs zum einen noch sehr einseitig in der Sprache der digitalen Souveränität geführt wird, in der es hauptsächlich um die Errichtung von Kontrollstrukturen und die Ermächtigung staatlicher Politik geht, weniger um die Demokratisierung der neu entstandenen Machtmittel.[47] Zum anderen, dass es aber zugleich noch daran mangelt, Plattformen konsequent als Infrastrukturen von Demokratie zu erkennen. Hieraus müssten Regelungsmodelle gefolgert werden, die stärker in einer Tradition öffentlich-rechtlicher Verständnisse angesiedelt sind, wo staatsferne, gesellschaftlich breit repräsentierende Aufsichtsgremien und Elemente der Dekommodifizierung ebenso bedeutsam sind wie das aktive Sicherstellen journalistisch hochwertiger Angebote.[48] Auch ein Fördern alternativer Infrastrukturen, die stärker zivilgesellschaftlich geprägt sind und die Traditionen und Positionen der netzpolitischen Zi-

46 Cohen, Joshua/Fung, Archon 2021: Democracy and the Digital Public Sphere, in: Bernholz, Lucy/Landemore, Hélène/Reich, Rob (Hrsg.): Digital Technology and Democratic Theory, 23–61.

47 Pohle, Julia/Thiel, Thorsten (2021): Digitale Souveränität. Von der Karriere eines einenden und doch problematischen Konzepts. In: Chris Piallat: Der Wert der Digitalisierung. Bielefeld: transcript Verlag. 319–340.

48 Vgl.: José van Dijck/David Nieborg/Thomas Poell (2019): Reframing platform power. In: Internet Policy Review, 8 (2); Ethan Zuckerman (2020): The Case for Digital Public Infrastructure. New York: Knight First Amendment Institute. Text abrufbar unter: https://knightcolumbia.org/content/the-case-for-digital-public-infrastructure Praktische Vorschläge unterbreiten etwa: Johannes Hillje (2019): Plattform Europa. Bonn: Dietz, J H. W.; Kagermann, Henning/Wilhelm, Ulrich 2020: European Public Sphere. Gestaltung der digitalen Souveränität Europas (acatech IMPULS), München, in: https://www.acatech.de/publikation/european-public-sphere/; 21.7.2020.

vilgesellschaft wie freie Lizenzen und Dezentralität aufgreifen, würde aus dieser Perspektive von großem Wert sein.[49]

49 Berg, Sebastian/Staemmler, Daniel 2020: Zur Konstitution der digitalen Gesellschaft. Alternative Infrastrukturen als Element demokratischer Digitalisierung, in: Oswald, Michael/Borucki, Isabelle (Hrsg.): Demokratietheorie im Zeitalter der Frühdigitalisierung, Wiesbaden, 127–147. Allgemeiner zur konstitutiven Wirkung zivilgesellschaftlicher Strategien: Berg, Sebastian/Thiel, Thorsten 2019: Widerstand und die Formierung von Ordnung in der digitalen Konstellation, in: Zeitschrift für Politische Theorie 10: 1, 67–86.

The Digital Public and its Problems: Komplexität, Verfahren und Trägerschaft als rekursive Konstitutionsprobleme einer digitalen Problemöffentlichkeit

Carsten Ochs

1. Einleitung

Als der US-amerikanische Philosoph John Dewey 1927 das Buch *The Public and its Problems* verfasste, tat er dies unter dem Eindruck sowohl neuartiger *Problemlagen*, mit denen sich die damalige US-Industriegesellschaft konfrontiert sah, als auch mit Blick auf erhöhte industriegesellschaftliche *Problemreichweiten*. Die traditionelle politische Verfasstheit der USA, so Dewey, käme mit der gewandelten soziotechnischen Situation nicht mehr zurande, denn die Komplexität und der Einflussbereich insbesondere der technisch-wissenschaftlichen Prozesse hätten ein Niveau erreicht, das weit über die lokal überschaubaren *community settings* der amerikanischen Öffentlichkeit hinausreiche: „Wir haben, kurz gesagt, die Praktiken und Ideen lokaler Stadtversammlungen geerbt. Aber wir leben, handeln und haben unser Dasein in einem kontinentalen Nationalstaat. (…) Die politischen und juristischen Formen haben sich nur stückweise und stockend, mit großer Verzögerung, der industriellen Transformation angepasst." (Dewey 1996: 102-103)

Dewey leitete hieraus die Notwendigkeit ab, die Parameter von Öffentlichkeit neu zu bestimmen, einer der neuen Situation angemessenen *Problemöffentlichkeit*. Betrachtet man den heute erreichten Stand der Digitalisierung, ihre globale Reichweite und die beständige Ausweitung der digitalen Einflusssphäre, so ergibt sich ein recht ähnliches Bild, nur eben auf nunmehr globaler „Stufenleiter." Unter den Vorzeichen datafizierter Sozialität werden Digitaltechnologien in praktisch allen gesellschaftlichen Bereichen eingesetzt, letztere dabei von vornherein so gestaltet, dass sie die Sammlung, Verarbeitung und Wiedereinspeisung digital kodierter Daten in die Vollzüge des Sozialen erlauben. Ein Großteil der sog. Innovationsaktivitäten wird von monopolartigen Digitalisierungsplayern forciert, wobei allzu oft ausgeblendet bleibt, dass hierbei immer auch neuartige soziale Praktiken entstehen, die gerade nicht im Paket mit gebrauchsfertigen zivilisatorischen Spielregeln geliefert werden. Soziodigitale Infrastrukturen

saugen soziale Praktiken gewissermaßen auf (Ochs 2021), und ist ihnen das einmal gelungen, dann sind ihre Betreiber diejenigen, die über die Regeln ihres Vollzuges bestimmen (Lamla 2019; Dolata 2020).

Spätestens seit am 6. Januar 2021 in Washington eine wütende Menge von Trump-Anhänger:innen (nicht nur, aber zumindest auch und maßgeblich) mithilfe Plattform-gesteuerter Kommunikations- und Informationsflüsse (Silverman et al. 2021) in einen rasenden Mob transformiert wurde, der zum Sturm auf das Kapitol, den Sitz der US-amerikanischen Legislative blies, und dabei auf Facebook permanent mit Werbeanzeigen für „military gear" bombardiert wurde (Mac/Silverman 2021) – spätestens seit diesem Moment ist die Plausibilität der Rede von der überwachungskapitalistischen Untergrabung der Demokratie (Zuboff 2018; Faßler 2020) nur noch schwerlich zu bestreiten.

Aber wie konnte das geschehen? Hatten sich nicht mit der durch Internet und *world wide web* ermöglichten Digitalvernetzung im Laufe der 1990er Jahre vielfach gut begründete Emanzipations- und Demokratisierungshoffnungen verbunden? Galt uns nicht die „Verbündelung" von Informationsströmen, wie sie mit den Broadcastingmedien auf den Plan trat, als tendenziell totalisierender Vergesellschaftungsmodus, Vernetzung hingegen per se als emanzipatorisches Projekt, als potentielle Alternative zu Kapitalismus und Sozialismus zumal (Flusser 1997; Benkler 2006)? Heutige Beobachter:innen digitaler Vergesellschaftung blicken demgegenüber mit einiger Ernüchterung auf digital entfachte *Hate Speech*-Diskurse, Echokammern und *Filter Bubbles*, auf *Fake News*, Propaganda und Überwachungskapitalismus, auf Verhaltensmanipulation, datenökonomische Monopole und algorithmische Diskriminierung (van Dijck 2013; Pariser 2017; Zuboff 2018; Susser et al. 2019; Mühlhoff 2021) – die seit den 2000er Jahren diskursiv als Sozialisierung des Web verkaufte Ökonomisierung des Sozialen scheint nicht aufzuhören, sozialpathologische Transformationseffekte zu zeitigen, welche den Demokratisierungspotentialen der Digitalvernetzung diametral entgegenlaufen (Ochs im Druck).

Die Problemdiagnosen sind mittlerweile ebenso zahlreich wie fundiert, und sie zeichnen, wie oben angedeutet, ein nicht eben hoffnungsfrohes Bild. Mitunter wird die Situation mit jener Phase des Industriekapitalismus verglichen, in der die negativen Konsequenzen der seinerzeit neuartigen Wirtschaftsform für eine hinreichend große Zahl von Akteuren derart massiv zu Buche schlugen, dass sich eine problem-bewusste Öffentlichkeit als betroffen erkennen konnte, woraufhin Gegenbewegungen in Gang kamen (Zuboff 2018: 598-599). Gestützt wurde die soziale Formierung von „Industrieproletariat" oder „Arbeiterklasse" (oder was da an Bezeichnungen mehr sind) nicht zuletzt durch die analytische Identifizierung der

grundlegenden Mechanismen des Industriekapitalismus, am prominentesten von Karl Marx (2003) herausgearbeitet.

Betrachtet man die Lage zeitgenössischer Digitaler Gesellschaften von dieser Warte aus, so stellt sich die Frage, ob und wo sich aktuell vergleichbare Bewegungen gegen die o.g. Verwerfungen erkennen lassen. Leider fällt die Antwort auf diese Frage bis dato eher pessimistisch aus. Die regelmäßig auftretenden Datenskandale und Anmaßungen der großen Monopolisten münden bislang nur bedingt in die Formierung einer nachhaltigen und robusten widerständigen Öffentlichkeit: Von der NSA-Affäre über den Cambridge Analytica/Facebook-Skandal bis zur öffentlich gemachten systematischen Verletzung und Abstumpfung der „Userschaft" im Rahmen von verdeckt durchgeführten Manipulationsstudien (Kramer et al. 2014) und einseitig diktierten Veränderungen der Datenschutzbestimmungen scheint es in den letzten gut zehn Jahren eigentlich eine hinreichend große Zahl öffentlich wahrnehmbarer Übergriffe gegeben zu haben, die die Formierung einer dauerhaften Problemöffentlichkeit, welche in der Ausbildung einer „digitalen Klasse für sich" resultieren könnte, nahelegen. Warum also ist von der Entstehung einer weithin vernehmbaren kollektiven Gegenbewegung – so wenig zu sehen?

Das Ziel des vorliegenden Beitrags besteht darin, einige der Hindernisse zu identifizieren, die der Formierung einer solchen Problemöffentlichkeit der digitalen Vergesellschaftung entgegenstehen. Die in diesem Zuge eingenommene pragmatistische Grundperspektive wurde bereits angedeutet: In ähnlicher Weise, in der John Dewey in den ersten Dekaden des 20. Jahrhunderts danach fragte, wie unter den geänderten Rahmenbedingungen der frühen „Organisierten Moderne" (Wagner 1998) des 20. Jahrhunderts Problemöffentlichkeiten entstehen könnten, die der Reichweite der neuartigen Problemlagen entsprächen, wird der vorliegende Beitrag die soziotechnischen Bedingungen der Formierung einer *digitalen* Problemöffentlichkeit skizzieren.

Das so orientierte Vorgehen gliedert sich in zwei Schritte: Im nächsten Kapitel (2) werden zunächst die Umrisse von Deweys öffentlichkeitstheoretischem Klassiker *The Public and its Problems* skizziert und kursorisch im Lichte zeitgenössischer digitaler Öffentlichkeit diskutiert. Dabei wird v.a. die Rekursivität[1] letzterer herausgestrichen: Digitale Problemöffentlichkei-

1 Der erste, der den Begriff der Rekursivität auf Öffentlichkeit anwendete, war m.W. Christopher Kelty (2005), der damit auf die Möglichkeit der an Internet-basierten Öffentlichkeiten Beteiligten verwies, die technologische Strukturierung dieser Öffentlichkeiten zu gestalten. Meine Verwendung des Begriffs zielt demgegenüber v.a. darauf ab, dass die Probleme digitaler Öffentlichkeit in einer von diesen

ten *problematisieren und verhandeln* Digitalität nicht nur, sondern *nutzen* diese auch zur Öffentlichkeitskonstitution. Aus diesem Grunde kommt das, was jene Öffentlichkeiten als Problem adressieren, im Rahmen ihrer Formierung immer schon rekursiv zum Tragen. Ob dies *unweigerlich* zu einer Lähmung der fraglichen Öffentlichkeiten führt, wäre empirisch zu ermitteln und kann hier nicht abschließend geklärt werden. Die an Dewey anschließende und an die Betrachtung digitaler Öffentlichkeit angeschlossene Erörterung soll aber Rekursivität als solche im Sinne eines analytisch in Rechnung zu stellenden Charakteristikums herausarbeiten, gegen das die Formierung digitaler Öffentlichkeit anzuarbeiten gezwungen ist.

Das darauffolgende Kapitel (3) wird drei konkrete Problemfelder umreißen, in denen die zeitgenössische Formatierung von Digitalität auf eine Weise zum Tragen kommt, die der Ausbildung von Problemöffentlichkeiten entgegensteht. Als erstes kommt dabei die Komplexität und Opazität der plattform-artigen und algorithmischen Strukturierung digitaler Öffentlichkeit in den Blick. An diesem Punkt stellt sich die Frage, ob und wie unbeobachtbare Komplexität überhaupt zum *Gegenstand* von Demokratisierung gemacht werden könnte. Sofern auf diese Frage positive Antworten gefunden werden können, stellt sich als zweite Problematik die Frage nach den *Verfahren* der Demokratisierung digitaler Öffentlichkeiten, und dabei insbesondere nach institutioneller Innovation, d.h. nach zu erfindenden Institutionen, die den neuartigen Problemlagen gerecht zu werden vermögen. Hergebrachte Institutionen müssen in diesem Kontext, trotz ihrer teilweise beobachtbaren Überforderung, keineswegs als technikgeschichtliche Ladenhüter abgeschrieben, sondern können vielmehr in konstruktiver Weise als Nährboden institutioneller Neuerfindung vorgestellt werden. Neben den Fragen nach dem Gegenstand und den Verfahren der Demokratisierung des Digitalen kommen schließlich drittens, und direkt an die Frage der Institutionenbildung anschließend, die *Trägergruppen* der Demokratisierung zur Sprache. Während die zivilisatorischen Mechanismen, die den Verwerfungen des Industriekapitalismus entgegengesetzt wurden, den Profiteur:innen des Frühkapitalismus von ganz bestimmten Gruppen in intensiv geführten und weithin sichtbaren Konflikten abgetrotzt worden sind, stellt sich heute in ähnlicher Weise die Frage nach den Träger:innen

---

Problemen geplagten Öffentlichkeit verhandelt werden (müssen). Der Bedeutungswandel zwischen den beiden Verwendungsweisen von „Rekursivität" geht wohl zumindest z.T. auf den geänderten politisch-ontologischen Status des Digitalen zurück.

der Demokratisierung der überwachungskapitalistischen Wertschöpfungslogik.

Die im Laufe des umrissenen Argumentationsganges gewonnenen Einsichten werden schließlich (4) in die Forderung nach politisch-regulatorischer Innovation überführt.

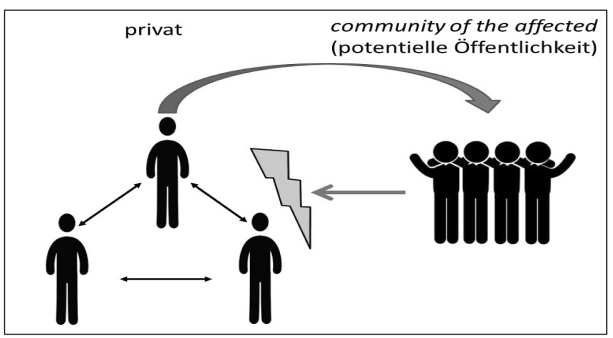
2. *Deweys Problemöffentlichkeiten*

Die Ausarbeitung vieler der mittlerweile als klassisch geltenden Öffentlichkeitstheorien der Soziologie des 20. Jahrhunderts wurde durch konkrete gesellschaftliche Problemlagen motiviert. Während etwa Jürgen Habermas (1990) die instrumentelle Verödung massenmedialer Öffentlichkeit zum Anlass nahm, die Entstehung und die Grundstrukturen einer idealtypischen (und vermutlich auch allzu idealisierend gedachten) Form bürgerlicher Öffentlichkeit sozialhistorisch zu rekonstruieren, suchte Hannah Arendt (2002) im Ideal der antiken Polis des griechischen Stadtstaates einen normativen Gegenhalt zur zeitgenössischen Öffentlichkeit der „Massengesellschaft." Ebenso unzufrieden mit dem Zustand der Öffentlichkeit des 20. Jahrhunderts zeigte sich Richard Sennett (2008), der „Verfall und Ende des öffentlichen Lebens" v.a. auf eine sozialpsychologisch analysierbare Personalisierung des öffentlichen Handelns zurückführte: seitdem jede öffentliche Handlung als persönlicher Ausdruck des individuellen Selbst gelte, habe sich Öffentlichkeit immer weiter zu einer angstbesetzten Sphäre entwickelt, in der die Furcht vor Entbergung des eigenen Wesenskerns das Handeln lähme. Wie der kurze Durchgang durch die drei Klassiker der Öffentlichkeitsforschung verdeutlicht, tendierten Soziologie und Sozialphilosophie des 20. Jahrhunderts v.a. dahin, Öffentlichkeit als Verfallsform zu beschreiben, deren Abstiegsgeschichten gegen die Hintergrundannahme idealisierter historischer Vor-Formen erzählt wurden (bürgerliche, antike, spätabsolutistische Öffentlichkeit).

Bereits vor den genannten, aber zunächst noch von der Erfahrung totalitärer Gewaltöffentlichkeit verschont, hatte John Dewey schon 1927 darüber nachgedacht, welche gesellschaftliche Rolle Öffentlichkeit wohl spielen könnte. Wie die drei o.g. Theorien war auch Deweys Auseinandersetzung mit Öffentlichkeit von einer deutlich vernehmbaren Unzufriedenheit mit deren Rolle in der Gesellschaft seiner Zeit motiviert. Anders als Arendt, Habermas und Sennett verzichtete Dewey aber auf die voraussetzungsvolle normative Idealisierung historisch rekonstruierbarer Öffentlichkeitstypen und versuchte stattdessen, den handlungspraktischen Kern des Öffentlichen analytisch freizulegen: „Wir müssen auf jeden Fall mit

vollzogenen Handlungen beginnen, nicht mit hypothetischen Gründen für diese Handlungen, und ihre Folgen betrachten. (…) Wir nehmen dann als unseren Ausgangspunkt die objektive Tatsache, daß menschliche Handlungen Folgen für andere haben, daß einige dieser Folgen wahrgenommen werden und daß ihre Wahrnehmung zu dem anschließenden Bestreben führt, die Handlung zu kontrollieren, um einige der Folgen zu sichern und andere zu vermeiden." (Dewey 1996: 26, 27) Nach pragmatistischer Denkart setzt Dewey sodann an den Folgen an und differenziert diese in „jene, welche die direkt mit einer Transaktion befassten Personen beeinflussen und diejenigen, welche andere außer den unmittelbar Betroffenen beeinflussen. In dieser Unterscheidung finden wir den Keim der Unterscheidung zwischen dem Privaten und dem Öffentlichen. Wenn die indirekten Folgen anerkannt werden und versucht wird, sie zu regulieren, entsteht etwas, das die Merkmale eines Staates besitzt. Wenn die Folgen einer Handlung hauptsächlich auf die direkt in sie verwickelten Personen beschränkt sind oder auf sie beschränkt gehalten werden, ist die Transaktion eine private." (ebd.: 27) In der auf Dewey gefolgten und an diesen anschließenden Öffentlichkeitstheorie wird diese Denkfigur als „community of the affected" bezeichnet (Marres 2012: 31 ff.). Visualisieren lässt sich das skizzierte Verständnis von öffentlich/privat zunächst so:

Abb. 1: Deweys Problem-generierte Öffentlichkeiten



Die Entstehung von Öffentlichkeiten ergibt sich Dewey zufolge also daraus, dass sich die Aktivitäten „privater" Handlungszusammenhänge auf Akteure auswirken (für diese also Folgen hervorrufen), welche außerhalb des eigentlichen Handlungszusammenhangs stehen, und welche daher zunächst auch keinen Einfluss auf die fraglichen Aktivitäten haben. Man kann sich dies Konstellation beispielhaft an den Grillaktivitäten in einem Mietshaus vergegenwärtigen. Wenn ich im Sommer mit meinen

Nachbar:innen auf dem Balkon meiner Wohnung grille, ohne die vielen anderen Mietparteien dazu zu laden, die im Haus wohnen, und wenn der durch das Grillen hervorgerufene Rauch in alle anderen Wohnung zieht, ohne dass die Bewohner:innen dieser Wohnungen an den gegrillten Würstchen teilhätten, dann läge hier ein privater Handlungszusammenhang vor (ich und die Nachbar:innen), der Folgen für Dritte zeitigen würde (Rauchbelästigung anderer Mietparteien). Letztere bildeten dann eine „community of the affected", und das Demokratie-Problem von Sozialformationen besteht darin, dass diese quasi-*community* zum einen indirekt in die Handlungsketten der „privaten Akteure" involviert, sofern sie von deren Handlungsfolgen betroffen ist, zum anderen aber über keinerlei Möglichkeiten der Einflussnahme auf das Geschehen in den „privaten Handlungszusammenhängen" verfügt.

In diesem Sinne geht die Öffentlichkeitskonzeption Deweys von der Frage aus, was passiert, wenn zunächst als privat verstandene Handlungen gewissermaßen „nach außen" dringen, um so (potentiell) Öffentlichkeiten hervorzurufen, die dann in der Lage sind, auf die externe Folgen hervorrufenden Handlungen einzuwirken. Auf eben diese Konstellation spielt der Begriff der Problemöffentlichkeiten an (ebd.: 56). Das Dewey'sche Konzept der Problemöffentlichkeiten lehnt somit die Identifizierung des Privaten mit dem Individuellen bzw. des Öffentlichen mit dem Gesellschaftlichen ausdrücklich ab (ebd.: 27 ff.). Öffentlichkeit wird dementsprechend auch nicht als einmal installierte und daraufhin fortbestehende gesellschaftliche Sphäre gedacht, sondern als eine Form, in der Gesellschaften praktisch mit ihren Problemen umgehen. Denkt man über Öffentlichkeit auf diese Weise als *The Public and its Problems* nach, dann kann diese schlechterdings nicht unter Absehung von ihren (Streit-)*Gegenständen*, den *Issues*, nachgedacht werden (Marres 2007), noch kann Problemöffentlichkeit bestimmt werden, ohne Bezug auf die spezifischen *Verfahren* ihrer Konstitution und *Trägergruppen* (Latour 2001; 2005; Lamla 2013).

Den Kern öffentlicher Auseinandersetzung in demokratischen Gesellschaften bestimmt Dewey damit dann eher analytisch, als normativ, über spezifische „Bedingungen (…), welche erfüllt sein müssen, wenn die *Große Gesellschaft* eine *Große Gemeinschaft* werden soll; eine Gesellschaft, in der die sich immer weiter ausdehnenden und kompliziert verzweigenden Folgen assoziierter Tätigkeiten im vollen Sinne dieses Wortes bekannt sein sollen, so daß eine organisierte *Öffentlichkeit* entsteht. Die höchste und allerschwierigste Form der Untersuchung und eine subtile, empfindsame, lebendige und empfängliche Kunst der Kommunikation müssen von der physischen Apparatur der Übertragung und Verbreitung Besitz ergreifen und ihr Leben einhauchen. Wenn das Maschinenzeitalter seine Maschine-

rie auf diese Weise vervollkommnet, wird sie ein Mittel des Lebens und nicht sein despotischer Gebieter sein. Die Demokratie wird dann zeigen, was in ihr steckt, denn Demokratie ist ein Name für ein Leben in freier und bereichernder Kommunion." (Dewey 1996: 155) Es sind die Kommunikationskanäle, -möglichkeiten und -formen, auf die Dewey hier anspielt, das Postwesen, die telegraphische und telefonische Nachrichtenkommunikation, die Reichweite der Presse usw., allesamt Formen von Medientechnologie, die „schnelle und leichte Zirkulation von Ansichten und Informationen fördert, und fortwährende und verzweigte Interaktionen erzeugt, die weit über die Grenzen der von Angesicht zu Angesicht bestehenden Gemeinschaften [face-to-face-communities] hinausreichen. Die politischen und juristischen Formen haben sich nur stückweise und stockend, mit großer Verzögerung, der industriellen Transformation angepaßt. Die Aufhebung der Entfernung, der physischen Triebkräfte zugrunde liegen, hat die neue Form politischer Assoziation ins Leben gerufen." (ebd.: 103)

Dewey lässt sich an dieser Stelle so interpretieren, dass die Industrialisierung der Kommunikation dazu beitragen können soll, dass die Probleme der Industrialisierung öffentlichen Lösungen zugeführt werden. Legt man diesen Gedanken der aktuellen Situation zugrunde, dann suggeriert dies eine digital-kommunikative Lösung der digitalen Gesellschaftsprobleme. Jedoch stellt sich an diesem Punkt die Frage, inwieweit die aktuelle Situation tatsächlich in Analogie zu der von Dewey analysierten gesehen werden kann. Denn während die Industrialisierung *der Kommunikation* der US-amerikanischen Industriemoderne des frühen 20. Jahrhunderts lediglich eine, und kaum zentrale Facette des Industrialisierungsprozesses darstellte, gilt für Digitalisierung das Gegenteil. Die Industrialisierung der Kommunikation ergab sich im Sog der Industrialisierung materieller Produktionsformen (Beniger 1986), wobei die Fabrikation von Öffentlichkeit und von industrietypischen Produkten nicht annähernd so stark konvergierte, wie dies mit Blick auf die Digitalisierung der Fall ist. Denn wenn etwa die gesellschaftlichen Digitalisierungsprobleme angesprochen sind, die digitale Dienste hervorrufen – *Fake News*, suchterzeugende App-Mechanismen, Polarisierung gesellschaftlicher Kommunikation, Manipulation, Monopolbildung – dann treten die Organisationen, die die Probleme erzeugen, und die, die die Öffentlichkeit zur Verhandlung ihrer Lösung bereitstellen immer schon „in Personalunion" auf. Zwar mögen *US Steel* und die *Washington Post* beides Produkte der US-amerikanischen Industrialisierung sein, jedoch war es geradezu *business model* der letzteren Organisation (der Zeitung), Öffentlichkeit für Probleme herzustellen, die von Organisationen des ersteren Typs hervorgerufen worden waren (z.B. Arbeitsbedingungen, Entlohnung, Umweltprobleme usw.). wir haben es

hier strukturell also mit einem anderen Verhältnis zu tun: digitale Problemöffentlichkeiten stellen sich insofern als rekursive Öffentlichkeiten dar, als die Probleme, die sie adressieren, gleichzeitig die Rahmenbedingungen bilden, unter denen sie agieren können.[2] Die öffentliche Diskussion der Folgen von Algorithmisierung vollzieht sich in den Infrastrukturen derer, die die Algorithmisierung kontrollieren; die Diskussion über *Filter Bubbles* in *Filter Bubble*-Öffentlichkeiten; *Fake News*-Debatten werden von *Fake News* durchzogen usw.

Eben diese strukturelle Eigentümlichkeit gilt es zu berücksichtigen, wenn wir die Gegenstände, Verfahren und Trägergruppen digitaler Öffentlichkeit danach durchleuchten, wie sie die Emergenz digitaler Problemöffentlichkeiten befördern oder behindern: digitale Öffentlichkeiten tendieren dazu, von den Problemen geplagt zu werden, die sie doch adressieren möchten.

3. Widerstände digitaler Problemöffentlichkeiten

Wird Öffentlichkeit als kollektiver Behandlungsmodus gefasst, der durch Aufkommen konkreter gesellschaftlicher Problemlagen ins Leben gerufen wird, dann lassen sich, wie oben angemerkt, analytisch drei Komponenten unterscheiden, zwischen denen sich dieser Modus aufspannt: Problemöffentlichkeiten versammeln sich um spezifische Streit-Gegenstände herum, sie tun dies auf je spezifische, mehr oder weniger stark institutionalisierte Verfahrensweise, und sie rufen jeweils bestimmte Betroffenengruppen zusammen (Dewey 1996; Habermas 1998; Latour 2005; Marres 2007; Lamla 2013). Die folgende Problemanalyse wird nun nacheinander diese drei Dimensionen kursorisch behandeln. Dabei geht es nicht um eine erschöpfende Analyse der jeweiligen Problemdimension, sondern vielmehr um Problemaufrisse, die sich zu einer tentativen Gesamtskizze zusammenfügen.

3.1 Gegenstand der Demokratisierung: Soziotechnische Opazität

Als „Gegenstand" der Demokratisierung können Konstellationen gelten, die nicht nur ökonomische, organisationale sowie technische Charakteristika aufweisen, sondern letztere auch zu spezifischen soziotechnischen

2 Vgl. dazu noch einmal Kelty (2005: 202) sowie FN 1.

Formen zusammenschmieden, namentlich zu *Plattformen* (Lovink 2017). „Plattform" meint in dem Zusammenhang „a programmable digital architecture designed to organize interactions between users – not just end users but also corporate entities and public bodies." (van Dijck et al. 2018: 4) In diesem Sinne sind Plattformen Intermediäre, die verschiedene Nutzerinnengruppen in Beziehung setzen: „customers, advertisers, service providers, producers, suppliers, and even physical objects." (Srnicek 2017: 439) Es lassen sich sektorale und infrastrukturelle Plattformtypen unterscheiden: Erstere besetzen tendenziell spezielle Geschäftsfelder, so wie *Uber* das datafizierte Transportwesen; letztere „form the heart of the ecosystem upon which many other platforms and apps can be built. They also serve as online gatekeepers through which data flows are managed, processed, stored, and channeled. (ebd.: 13) Damit sind die Basis-Komponenten von Plattformen schon angedeutet: Daten, Algorithmen, Interfaces, spezifische Eigentumsordnungen, Geschäftsmodelle und Nutzungsvereinbarungen (van Dijck et al. 2018: 9). Indem Plattformen diese zum Einsatz bringen, strukturieren beziehungsweise „kuratieren" sie Sozialität (Dolata 2020).

In *ökonomischer* Hinsicht sind Plattformen „geared toward the systematic collection, algorithmic processing, circulation, and monetization of user data." (van Dijck et al. 2018: 4) Sie folgen dabei der Logik des Überwachungskapitalismus, d.h. sie richten menschliche Erfahrungen auf eine Art und Weise zu, dass diese sich in digital kodierte (Verhaltens-)Daten übersetzt, welche sich dann sammeln und auswerten lassen, um weiteres Verhalten vorherzusagen und nach Maßgabe der Interessen zahlungswilliger Kunden (Produktverkäufer; Parteien; Interessenlobbies aller Art) zu beeinflussen (Zuboff 2018). Sozialität, d.h. die Praktiken und Beziehungen, die im Zuge der Nutzung von Plattform-Infrastrukturen entstehen, werden dabei auf eine Weise vorgeformt, die sich am Interesse der Plattformbetreibenden orientiert, Verhaltensbeeinflussungspotentiale zu produzieren und zu verkaufen (Ochs 2021).

Die unternehmensmäßige *Organisationsform* der Plattformen läuft darauf hinaus, Soziales und Ökonomie eng miteinander zu verzahnen, dabei jedoch die betriebswirtschaftliche Hoheit über die mögliche Gestaltung der entstehenden Sozialformen zu behalten (Ochs et al. 2021). Plattformerfolg basiert auf Netzwerkeffekten: „the more numerous the users who use a platform, the more valuable that platform becomes" (Srnicek 2017: 45). Aus Sicht der Einzelperson ist es etwa wenig sinnvoll, sich in einem Sozialen Netzwerk anzumelden, dem wenige „User:innen" angehören, denn das Geselligkeits- und Vernetzungsversprechen dieser Netzwerke ist ja umso größer, je größer die Gesamtzahl der Nutzenden. Wenn Netzwerke eine

gewisse Mitgliedschaftsschwelle überschritten haben, erlangen sie daher praktisch gesehen Monopolstatus, denn es wird dann immer unattraktiver für Neulinge, sich bei einem konkurrierenden Netzwerk anzumelden. Der Netzwerkeffekt besteht also darin, dass jede:r neue „User:in" das Netzwerk nicht nur vergrößert, sondern damit auch gleichzeitig die Wahrscheinlichkeit erhöht, dass Neulinge sich ebenfalls für dieses Netzwerk entscheiden.

In *technischer* Hinsicht können Plattformen in zweierlei Hinsicht als opake Gebilde gelten. Zum einen haben Akteure außerhalb der der Plattform-betreibenden Unternehmen immer nur (in mühsamem *reverse engineering* erworbene) Teil-Expertise bzgl. der genauen Funktionsweise der eingesetzten Technologien (z.B. bzgl. des Datenflusses der Apps, der Auswert- und Targetingverfahren, der Strukturierung der Kommunikationsflüsse usw.). NGOs wie *Algorithm Watch* versuchen an dieser Stelle mehr Transparenz zu schaffen, was aber mitunter durch die extremen Machtasymmetrien verunmöglicht wird (Kayser-Bril 2021), die sich ihrerseits u.a. den bestehenden Eigentumsverhältnissen verdanken (Algorithmen gelten als Geschäftsgeheimnisse, als Privateigentum – hier wird also paradoxerweise durchaus Privatheit eingefordert). Die dadurch hervorgerufene Opazität der technischen Strukturierung sozialer Kommunikations- und Interaktionsformen wird weiter verschärft durch den ausgeweiteten Einsatz von rekursiv „lernenden", d.h. mithilfe von statistischer Prognostik auf sich selbst einwirkenden Algorithmen der sog. „Künstlichen Intelligenz." Indem diese die „Blackbox-Haftigkeit" der algorithmischen Systeme erhöhen und so praktisch unbeobachtbare Komplexität erzeugen, fördern sie die Intransparenz soziodigitaler Plattformen (Sudmann 2018).

Die resultierende Opazität charakterisiert den hier interessierenden Gegenstand der Demokratisierung, die soziodigitalen Plattform-Konstellationen, in maßgeblicher Weise. Durch diese wird die öffentliche Problematisierung und Verhandlung von „Digitalisierung" erheblich erschwert (z.B. wird etwaiger diskriminierender Bias durch KI-Systeme von den davon Betroffenen im Zweifelsfall gar nicht erst wahrgenommen, was die Wahrscheinlichkeit von Protest herabsetzt).

3.2 Verfahren der Demokratisierung: Formierung von Problemöffentlichkeiten der technoscience im Jenseits etablierter Institutionen

Trotz der Opazität der technoökonomischen Plattform-Strukturierung des Digitalen muss festgestellt werden, dass die praktische technowissenschaftliche Undurchschaubarkeit, mit der sich menschliche Sozialakteure gegenwärtig konfrontiert sehen, erstmal kein neues, genuin digitales Phänomen

darstellt. Wie oben ausgeführt, wurde schon Deweys 1927 vorgenommene Reformulierung der Öffentlichkeitstheorie durch die stetige Steigerung der Reichweite und Komplexität technowissenschaftlich gestützter Handlungsketten motiviert, und noch allgemeiner ließen sich die benannten Steigerungsprozesse als soziologischen Charakteristikum der Moderne schlechthin perspektivieren (Elias 1997).

Demgegenüber durchaus als Neuerung galten Ulrich Beck (1986) gegen Mitte der 1980er Jahre die hausgemachten gesellschaftlichen Gefahren, die die Technowissenschaften zu erzeugen begonnen hatten. Während Technik und ihre epistemische Grundlage noch bei Marx als Mittel der Gesellschaft zur Beherrschung der Natur gegolten hatte, drehte sich der analytische Wind spätestens mit der radioaktiven Wolke, die nach dem Super-GAU von Tschernobyl gen Westen zog: Die Technowissenschaften galten nunmehr als soziales Instrumentarium, das sich im Zweifelsfall gegen Gesellschaft selbst richtet, mithin als gesellschaftlich erzeugte Gefährdung der Gesellschaft. Für Beck führte diese Verlagerung in eine „Zweite Moderne", und der dystopische Diskurs um die demokratiegefährenden Effekte soziodigitaler Infrastrukturen kann in eine gewisse Kontinuität zu solcherlei Selbstgefährdungsdiagnosen gestellt werden.

Jenseits der Gefährdungsfrage stellt sich indes die Problematik der demokratischen Governance der technowissenschafttlichen Erzeugnisse, und auch hierbei handelt es sich um eine bereits seit langem diskutierte Thematik. Insbesondere die soziologische und interdisziplinäre Wissenschafts- und Technikforschung der *science and technology studies* (STS) hat auf die immer stärkere technowissenschaftliche Fundierung moderner Gesellschaften hingewiesen (Haraway 1988) und in dem Kontext die Frage nach den Möglichkeiten einer demokratischen Governance eben dieser Fundierung aufgeworfen (Irwin 2001; Jasanoff 2003): „Concerns about public participation and democratic engagement with science have animated the field of science and technology studies (STS) since its inception (…) and have remained central in its efforts to attend to the social dimensions of science and innovation" (Kearnes/Chilvers 2020: 348). Die Plausibilität der Beschäftigung mit der hier angesprochenen Frage leuchtet unmittelbar ein, wenn man sich vergegenwärtigt, dass Vergesellschaftung in immer stärkerem Maße mithilfe jener Produkte erfolgt, die aus den Laboren und Designwerkstätten der Technowissenschaften stammen. In der Folge wird die Frage danach, wem ein Mitspracherecht bei der Fabrikation der fraglichen Dinge einzuräumen, und auf welche Weise dieses Recht auszuüben wäre, immer dringlicher (Latour 2001; Voß/Amelung 2016).

Einschlägige Forschungen haben vor diesem Hintergrund die Notwendigkeit des Einbezugs von Lai:innen-Perspektiven betont (Callon et al.

2001), etwa im Rahmen von sog. „citizen panels", und die Notwendigkeit einer Neuerfindung von Aushandlungsverfahren jenseits etablierter Institutionen herausgekehrt (Marres 2007). Aufgrund der weiter oben konstatierten Rekursivität der digitalen Öffentlichkeit ist der skizzierten Problematik jedoch nicht eben leicht beizukommen. Denn während im Falle der Bildung einer Problemöffentlichkeit, die sich bspw. mit dem Problem des Klimawandels beschäftigt die „Produktionsmittel" der Problemerzeugung und der Öffentlichkeitsbildung in verschiedenen Händen liegen, gilt dies im Falle der rekursiven digitalen Öffentlichkeit gerade nicht. Das Medium, in dem die Neuerfindung von Institutionen und Verfahren verhandelt werden soll, die mit den Problemen umgehen, die das Medium selbst erzeugt hat, wird durch das Medium selbst gebildet. Schon die reichlich verschachtelte Problembeschreibung weist auf die Selbstreferenzialität der Problemlage hin. Sie wirkt wie Sand im Getriebe der sich ausbildenden Problemöffentlichkeit.

3.3 Trägergruppe der Demokratisierung: (Wie) Können aus Betroffenen Öffentlichkeiten werden?

Dabei fordert die Ökonomin Shoshana Zuboff in ihrer Abhandlung zur Entstehung des Überwachungskapitalismus genau umgekehrt „Seid Sand im Getriebe" von den „User:innen" der Datenökonomie. Sie spricht damit zumindest implizit die Frage an, wie sich jene Akteursgruppen, die von den weitreichenden Folgen der umfassenden Digitalisierungs- und Datafizierungsprozesse betroffen sind, als solche kollektiv wahrnehmen und organisieren können. Die Problematik besteht in dieser Hinsicht v.a. darin, dass Akteure in zeitgenössischen soziodigitalen Gefügen als atomisierte „User" adressiert werden (Faßler 2012), die auf die Generierung idiosynkratischer Schwarm-Sozialität (Zuboff 2018) und Sichtbarkeit hin orientiert sind (Lamla/Ochs 2019; Stalder 2019). Wie kann sich vor Hintergrund des Versprechens der Datenökonomie, Nutzerinnen-Wünsche zu erfüllen, von denen diese selbst noch nichts wussten, ein hinreichendes Maß an „Reibung" einstellen, so dass sich Nutzungspopulationen als Betroffene öffentlich wahrnehmen und organisieren?

Betrachtet man das Problem historisch, dann wird die gewandelte Konstellation schnell ersichtlich: Mit der Formierung der Industriegesellschaft geht die Erfindung sozialpartnerschaftlicher Kompromissagenturen einher, die es überhaupt erst ermöglichen, dass diese Gesellschaft ihre eigenen Innovationen überlebt. Gewerkschaften, Betriebsräte und Aufsichtsräte ermöglichten zumindest bis zu einem bestimmten Grad eine gewisse

Zähmung jener Verwerfungen, deren ungehinderte Entfaltung die unmittelbare Selbstzerstörung der Industriegesellschaft nach sich gezogen hätte (ob diese Zähmung langfristig erfolgreich war, darf heute angesichts der industriekapitalistischen Zerstörung planetarer Lebensgrundlagen durchaus bezweifelt werden, womit John Maynard Keynes' süffisante Replik an die neoliberale Ökonomik noch einmal um eine ganz neue Bedeutungsschicht erweitert wird: „in the long run, we're all dead!"). Die Formierung dieser Kompromissagenturen verdankt sich vermutlich zu nicht geringem Teil der Ausbildung einer widerständigen Trägergruppe, zuweilen als „Arbeiterklasse" bezeichnet.

Mir geht es hier gewiss nicht um eine quasi-mythische Überhöhung der Dynamik, die mithilfe dieses Begriffes gerne beschrieben wird, sondern bloß um die nüchterne Feststellung, dass dem, was als „Arbeiterklasse" beschrieben wird, die Formierung einer Gegenmacht zugrunde lag, die sich herausbilden konnte, weil sie – bspw. in der Fabrik – direkt und spürbar mit den Effekten und Zumutungen der Herrschaftsapparate konfrontiert war (Giddens 1981: 176).

Wie sich eine auf die Machteffekte und Zumutungen der Digitalisierung antwortende Gegenmacht formieren soll, bleibt indessen fraglich, sofern „User:innen" sich mit Herrschaftsapparaten konfrontiert sehen, deren Machtausübung in erster Linie als Manipulation, und insofern unmerklich erfolgt (Susser et al. 2019).

Auch an dieser Stelle lähmen Charakteristika der Digitalisierung somit die Formierung einer effektiven Problemöffentlichkeit.

4. Schluss

Damit sind nun einige maßgebliche Faktoren, die sich einer Demokratisierung der Digitalisierung entgegenstellen, identifiziert. Dass hierauf letztlich nur politisch-regulatorische Antworten gegeben werden können, wird in dem Maße einsichtig, in dem die allerorten anzutreffende Rede vom epochalen Wandel von der industriellen zur digitalen Moderne tatsächlich ernst genommen wird. Die Industriemoderne konnte mit zahlreichen sozialpolitischen Innovationen aufwarten, und obwohl in keiner Weise einzusehen ist, warum die digitale Transformation nicht gesellschaftliche Selbsterneuerungsprozesse ähnlichen Ausmaßes nötig haben sollte, wird im Zusammenhang mit dieser gerne so getan, als könne man sie irgendeinem behaupteten „freien Spiel der Kräfte" überlassen.

Der vorliegende Beitrag hat einige der Faktoren benannt, die die Freiheit der Aushandlungen der Gestalt des Soziodigitalen deutlich einschrän-

ken. Die Rekursivität digitaler Öffentlichkeit kommt zum Tragen, wenn in den Foren der Plattformen opake technoökonomische und organisationale Plattform-Macht verhandelt werden soll; die Etablierung angemessener Verfahren und Institutionen sozialer Modellierung digitaler Infrastrukturen wird schwergängig, wenn der Streit darüber von vornherein interessengeleitet im Sinne der Betreiber soziodigitaler Infrastrukturen technisch strukturiert wird; und wie die an der Entwicklung soziodigitaler Infrastrukturen nicht direkt Beteiligten, wohl aber davon Betroffenen in eine sich selbst so wahrnehmenden Trägergruppe gesellschaftlicher Innovation transformiert werden könnten, scheint derzeit durchaus fraglich.

Dem Geiste Deweys gerecht werdend, gibt es dennoch keinen Grund für Defätismus. Angelehnt an dessen oben zitierte Worte und in leichter Abwandlung können wir feststellen: „Wir haben, kurz gesagt, die Praktiken und Ideen nationaler Staatsversammlungen geerbt. Aber wir leben, handeln und haben unser Dasein in einem globalen Vergesellschaftungsgefüge." Unsere Aufgabe wird folglich darin bestehen, Problemöffentlichkeiten und Praxisformen der Demokratie zu erfinden, die der Reichweite der hierbei entstehenden Problemlagen angemessen sind.

Literatur

Arendt, H. (2002): Vita activa oder Vom tätigen Leben. München.

Beck, U. (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt/M.

Beniger, J. (1986): The Control Revolution. Technological and Economic Origins of the Information Society. Cambridge, MA, London.

Benkler, Y. (2006): The Wealth of Networks. How Social Production Transforms Markets and Freedom. New Haven, London.

Callon, M./Lascoumes, P./Barthe, Y. (2001): Acting in an Uncertain World: An Essay on Technical Democracy. Cambridge/London.

Chilvers, J./Kearnes, M. (2020): Remaking Participation in Science and Democracy. In: Science, Technology & Human Values 45(3), S. 347-380.

Dewey, J. (1996): Die Öffentlichkeit und ihre Probleme. Bodenheim.

Dolata, U. (2020): Plattform-Regulierung. Organisierung von Märkten und Kuratierung von Sozialität im Internet. In: Berliner Journal für Soziologie 29(3), S. 179–206.

Elias, N. (1997): Über den Prozeß der Zivilisation. Soziogenetische und psychogenetische Untersuchungen, Bd. 1. Frankfurt/M.

Faßler, M. (2020): Partizipation ohne Demokratie. Über die Folgen der Netz- und Geopolitik von Facebook, Google, Amazon & Co. Paderborn.

Faßler, M. (2012): Kampf der Habitate. Neuerfindungen des Lebens im 21. Jahrhundert. Wien.

Flusser, V. (1997): Medienkultur. Frankfurt/M.

Giddens, A. (1981): A Contemporary Critique of Historical Materialism. Stanford, CA.

Habermas, J. (1990): Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft. Frankfurt/M.

Habermas, J. (1998): Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Frankfurt/M.

Haraway, D. (1988): Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. In: Feminist Studies 14(3), S. 575-599.

Irwin, A. (2001): Constructing the Scientific Citizen: Science and Democracy in the Biosciences. In: Public Understanding of Science 10(1), S. 1-18.

Jasanoff, S. (2003): Technologies of Humilty: Citizen Participation in Governing Science. In: Minerva 41(3), S. 223-244.

Kayser-Bril, N. (2021): Nach Drohungen von Facebook: AlgorithmWatch sieht sich gezwungen, Instagram-Forschungsprojekt einzustellen. In: Algorithm Watch, abrufbar unter: https://algorithmwatch.org/de/instagram-forschung-von-facebook-gestoppt/ (2.12.21).

Kelty, C. (2005): Geeks, social Imagineries, and Recursive Publics. In: Cultural Anthropology (20(2), S. 185-214.

Kramer, A./Guillory, J./Hancock, J. (2014): Emotional Contagion Through Social Networks. In: Proceedings of the National Academy of Sciences 111(24), S. 8788-8790, abrufbar unter: doi: 10.1073/pnas.1320040111 (2.12.21).

Lamla, J. (2019): Selbstbestimmung und Verbraucherschutz in der Datenökonomie. In: Aus Politik und Zeitgeschichte (APuZ) 69 (24-26/2019), S. 49-54.

Lamla, J. (2013): Verbraucherdemokratie. Politische Soziologie der Konsumgesellschaft. Berlin.

Lamla, J./Ochs, C. (2019): Selbstbestimmungspraktiken in der Datenökonomie: Gesellschaftlicher Widerspruch oder ‚privates' Paradox? In: Blättel-Mink, B./Kenning, P. (Hg.): Paradoxien des Verbraucherverhaltens. Wiesbaden, S. 25-39

Latour, B. (2005): Von der Realpolitik zur Dingpolitik. oder Wie man Dinge öffentlich macht. Berlin.

Latour, B. (2001): Das Parlament der Dinge. Für eine politische Ökologie. Frankfurt/M.

Lovink, G. (2017): Im Bann der Plattformen. Die nächste Runde der Netzkritik. Bielefeld.

Mac, R./Silverman, C. (2021): Facebook Has Been Showing Military Gear Ads Next To Insurrection Posts. In: BuzzFeed.News, January 13, 2021, abrufbar unter: https://www.buzzfeednews.com/article/ryanmac/facebook-profits-military-gear-ads-capitol-riot (2.12.21).

Marres, N. (2012): Material Participation. Technology, the Environment and Everyday Publics. Basingstoke.

Marres, N. (2007): The Issue Deserves More Credit: Pragmatist Contributions to the Study of Involvement in Controversy. In: Social Studies of Science 37(5), S. 759-780.

Marx, K. (2003): Das Kapital. Kritik der politischen Ökonomie. Köln.

Mühlhoff, R. (2021): Predictive Privacy: Towards an Applied Ethics of Data Analytics. In: Ethics and Information Technology, abrufbar unter: doi:10.1007/s10676-021-09606-x

Ochs, C. (2021): Digital Infrastructures Suck: Zur digitalen Absorption des Sozialen. In: Hamburger Journal für Kulturanthropologie, Nr. 13 (2021), S. 127-138.

Ochs, C. (im Druck): Datenbasierte Sichtbarkeit: Gesellschaftsstrukturelle Bedingungen zeitgenössischer Technikgestaltung. In: Friedewald, Michael/Hansen, Marit/Kreutzer Michael (Hg.): Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg. Wiesbaden.

Ochs, C./Büttner, B./Lamla, J. (2021): Trading Social Visibility for Economic Amenability: Data-Based Value Translation on a 'Health- and Fitness-Platform'. In: Science, Technology & Human Values 46(3), S. 480-506. https://journals.sagepub.com/eprint/WINPWI8VSE4QYKQRIGCF/full

Pariser, E. (2017): Filter Bubble. Wie wir im Internet entmündigt werden. München.

Sennett, R. (2008): Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität. Berlin.

Silverman, R./Mac, R./Lytvynenko, J. (2021): Facebook Knows It Was Used To Help Incite The Capitol Insurrection. BuzzFeed.News, April 22, 2021, abrufbar unter: https://www.buzzfeednews.com/article/craigsilverman/facebook-failed-stop-the-steal-insurrection (2.12.21).

Srnicek, N. (2017): Platform Capitalism. Cambridge, UK/Oxford, UK.

Stalder, F. (2019): Autonomie und Kontrolle nach dem Ende der Privatsphäre. In: Stempfhuber, M./Wagner, E. (Hg.): Praktiken der Überwachten. Öffentlichkeit und Privatheit im Web 2.0. Wiesbaden, S. 97–110.

Sudmann, A. (2018): Einleitung. In: Engemann, C./Sudmann, A. (Hg.): Machine Learning. Medien, Infrastrukturen und Technologien der Künstlichen Intelligenz. Bielefeld, S. 9-23.

Susser, D./Roessler, B./Nissenbaum, H. (2019): Online Manipulation: Hidden Influences in a Digital World. In: Georgetown Law Technology Review 1 (2019), abrufbar unter: https://ssrn.com/abstract=3306006 (2.12.21).

van Dijck, J. (2013): The Culture of Connectivity. A Critical History of Social Media. Oxford, New York.

van Dijck, J./Poell, T./de Waal, M. (2018): The Platform Sciety. Public Values in a Connective World. New York.

Voß, G./Amelung, N. (2016): Innovating Public Participation Methods: Technoscientization and Reflexive Engagement. In: Social Studies of Science 46(5), S. 749-772.

Wagner, P. (1998): A Sociology of Modernity. Liberty and Discipline. London.

Zuboff, S. (2018): Das Zeitalter des Überwachungskapitalismus. Frankfurt, New York: Campus Verlag.

„Funktion und Verantwortung von Plattformen als Informations-Intermediäre“

Gerald Spindler

I. Einleitung

Plattformen als Informations-Intermediäre sind nicht mehr wegzudenken aus dem öffentlichen Leben. Sie fungieren als Vermittler von Meinungen, Inhalten, stellen Kontakte zwischen Individuen her, dienen aber auch gleichzeitig der Massenkommunikation. Ohne Intermediäre wären zahlreiche Inhalte im Netz nicht auffindbar, Verknüpfungen ließen sich nicht herstellen. Gleichzeitig arbeiten Intermediäre automatisiert und agieren im Prinzip „neutral“ im Sinne rein technisch arbeitender Vermittler – was sich allerdings durch den Einsatz von Künstlicher Intelligenz verändert hat.

Umgekehrt stellt sich die Frage, welche Verantwortung solche Intermediäre mit einer enormen Reichweite und Gewichtigkeit für die öffentliche Meinungsbildung besitzen – quasi im Spannungsverhältnis zwischen automatisierten Technologien einerseits und der gesteigerten Kommunikation bzw. Gatekeeper-Funktion der Plattform andererseits. Anders als tradierte Massenkommunikationsmedien leiten – im Grundsatz jedenfalls – Plattformen „ungefiltert“ alle Inhalte und Meinungen weiter, wobei sie (im begrenzten Maße) durchaus die Möglichkeit haben (könnten), Inhalte zu strukturieren und zu filtern.

Vor diesem Hintergrund wird zunächst die Rolle der Plattformen näher beleuchtet (II.), anschließend die Frage der Verantwortlichkeit im Spannungsverhältnis zwischen Individual- und Massenkommunikation (III.). Maßgeblich werden dann kurz die bestehenden Regelungen zur Regulierung der Plattformen und die anstehenden europäischen Regulierungsvorschläge erörtert (IV.). Schließlich werden kurz die Vor- und Nachteile der jeweiligen Regulierungsansätze diskutiert (V.)

II. Rolle der Plattformen als Informations-Intermediäre

A. Funktionsweise und Arten von Plattformen

Betrachtet man die Plattformen im Netz genauer, wird man sich schnell bewusst, dass es „die" Plattform als Oberbegriff schlechthin kaum gibt. Vielmehr existiert eine ganze Bandbreite von Intermediären, die sich als Plattform im Sinne der Vermittlung von Nachrichten und Kommunikationskontakten einordnen lassen können. Angefangen bei „klassischen" sozialen Netzwerken wie Facebook, Instagram oder Twitter über solche, die berufsspezifischer Natur sind, wie XING oder LinkedIn, Blogportalen oder Wissensvermittlungsplattformen mit Mitwirkungsmöglichkeiten wie Wikipedia oder Videosharingplattformen für user generated content wie YouTube oder Bewertungsplattformen, etwa für Ärzte (Jameda), bis hin zu Suchmaschinen, die über das Ranking von Suchergebnissen und autocomplete-Funktionen von eingegebenen Suchbegriffen ebenfalls geeignet sind, bestimmte Inhalte zu priorisieren, reicht die Palette – ohne dass diese Aufzählung für sich in Anspruch nehmen könnte, erschöpfend zu sein.

Allen „Plattformen" ist ihre Eigenart gemein, dass sie einerseits die Möglichkeit der Individualkommunikation ermöglichen, gleichzeitig aber auch größere Personenkreise bis hin zur vollständigen Öffentlichkeit adressiert werden können. So können auf sozialen Netzwerken wie Facebook einerseits individuelle Nachrichten an einen Adressaten gerichtet werden, andererseits aber auch Nachrichten „gepostet" werden, die dann von jedermann auf dem Netzwerk eingesehen werden können. Zwischenabstufungen existieren indes ebenso, indem der zur Einsichtnahme zugelassene Personenkreis näher definiert bzw. auf „Freunde" oder andere Adressatengruppen eingegrenzt werden kann.[1] Aber auch die klassischen Messenger-Dienste wie WhatsApp oder Telegram oszillieren zwischen reiner Individualkommunikation im Sinne von Punkt-zu-Punkt-Nachrichtenaustausch und Massenkommunikation durch entsprechend große WhatsApp-Gruppen oder Telegram-Kanäle. Andere Plattformen wie Twitter zielen zumindest primär auf die vornherein unbegrenzte Massenkommunikation, die nur davon abhängt, ob man einem bestimmten „Sender" von Nachrichten „folgt". Ergänzend sind aber auch auf Twitter Direktnachrichten im Sinne der Individualkommunikation möglich.

1 Vgl. den Hilfebereich von Facebook, abrufbar unter https://www.facebook.com/help/211513702214269 (zuletzt abgerufen am 13. Dezember 2021).

Schließlich entsprechen Videosharing-Plattformen wie YouTube oder Bewertungsplattformen wie Jameda, die grundsätzlich keine Eingrenzungsmöglichkeiten des zu adressierenden Personenkreises kennen, eher einer One-to-Many Kommunikation. Insoweit hat zwischenzeitlich insbesondere YouTube mit der Einführung der Nicht-gelistet sowie mit der Privat-Funktion die Möglichkeit geschaffen, Inhalte auch einem begrenzten Publikum zugänglich zu machen.[2]

Gerade dieses „Umschlagsmoment“ macht aber auch ihre rechtliche Behandlung und Einordnung schwierig, da das Recht bislang traditionell zwischen Individual- und Massenkommunikation unterschied, zusammen mit Kompetenzabgrenzungen zwischen Bund (als zuständig primär für die Individualkommunikation) und Ländern (als zuständig für die Massenkommunikation).[3] Auch auf europäischer Ebene setzt sich diese Dichotomie im Prinzip fort, in Gestalt der Unterscheidungen zwischen Telekommunikation oder „electronic communication“ einerseits und audio-visuellen Medien (AVM-Richtlinie) andererseits.

B. Einfluss auf Meinungsbildung und demokratische Prozesse

Der Einfluss von Internet-Intermediären auf die Meinungsbildung und demokratische Prozesse ist nicht erst seit den Vorkommnissen rund um die US-Präsidentschaftswahlen im Jahr 2016[4] und den Einfluss von „fake

2 S. dazu https://support.google.com/youtube/answer/157177 (zuletzt abgerufen am 22. Dezember 2021).

3 Zur ursprünglichen Abgrenzung zwischen Tele- und Mediendiensten: *Spindler*, Gutachten F zum 69. Deutschen Juristentag, „Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung“, 2012, S. 39; *Ladeur/Gostomzyk*, NJW 2012, 710, 712 ff.; Spindler/Schuster/*Mann/Smid*, Recht der elektronischen Medien, 4. Aufl. 2019, Siebter Teil, Rn. 9; a.A. *Bruns*, AfP 2011, 421, 424 ff.; *Gounalakis*, NJW 1997, 2993, 2995 f.

4 Zum Einsatz von Social Media im Wahlkampf 2016 s. *von Blumencron*, „Das Ende des Wahlkampfs, wie wir ihn kennen“, abrufbar unter https://www.faz.net/aktuell/politik/von-trump-zu-biden/donald-trump-siegt-bei-us-wahl-2016-durch-social-media-14559570.html (zuletzt abgerufen am 09. Dezember 2021); zu Desinformationskampagnen im US-Wahlkampf 2020 s. *Stadtlich*, „Falschinformationen zur US-Wahl“, abrufbar unter https://www.deutschlandfunk.de/falschinformationen-zur-us-wahl-stresstest-fuer-soziale-100.html (zuletzt abgerufen am 09. Dezember 2021); zur Rolle der Medien bei der Erstürmung des Capitols s. *Klein*, „Nach Sturm auf US-Kapitol, Die Rolle der Medien bei den Ausschreitungen“, abrufbar unter https://www.deutschlandfunk.de/nach-sturm-auf-us-kapitol-die-rolle-der-medien-bei-den-100.html#a3 (zuletzt abgerufen am 09. Dezember 2021); Überblicksartig zu Desin-

news“[5] bekannt.[6] Schon früher wurden die Gefahren, aber auch Chancen für die Meinungsbildung über Internet-Intermediäre eingehend diskutiert.[7] Schwerpunkte in der rechtswissenschaftlichen Diskussion liegen So können neben der Behandlung von „fake news“ auch im Umgang mit Filterblasen[8] bzw. Echo-Kammern („echo chambers“)[9]. Dabei wird der einzelne Nutzer nur noch mit solchen Inhalten konfrontiert, die zuvor (algorithmenbasiert) auf Grundlage von Daten über das bisherige Nutzungsverhalten selektiert wurden, um den individuellen Präferenzen des Einzelnen zu entsprechen. Die Gefahr für einen offenen und ungehinderten Meinungsaustausch wird insoweit vor allem in Zusammenhang mit der enormen Relevanz von sozialen Plattformen als Informationsquelle in der Informationsgesellschaft deutlich. Gegenwärtig stehen insbesondere Proteste gegen Corona-Maßnahmen, die sich etwa über Telegramkanäle organisieren, in der deutschen medialen Öffentlichkeit.[10] Aus grenzüberschreitender Perspektive ist außerdem ein Verfahren in den USA von Interesse, das eine Schadensersatzforderung der muslimischen Minderheit der Rohingya in Myanmar gegen Facebook sowie dessen Mutterkonzern Meta zum Gegenstand hat. Dabei wird die Rolle des sozialen Netzwerks bei der Verfolgung der Minderheit durch das staatliche Militärregime ab

---

formationskampagnen auf Social Media im Bundestagswahlkampf 2021 s. den Überblick bei Bundeszentrale für politische Bildung, „Desinformation und Bundestagswahl 2021“, abrufbar unter https://www.bpb.de/gesellschaft/digitales/digitale-desinformation/338916/desinformation-und-bundestagswahl-2021 (zuletzt abgerufen am 09. Dezember 2021).

5 Zum Begriff s. Wissenschaftlicher Dienst des Deutschen Bundestages, „Fake News Definition und Rechtslage“, Az. WD 10 – 3000 – 003/17; *Holznagel*, MMR 2018, 18; Zu historischen Beispielen der Verwendung von „fake news“ s. *Pfeifer*, CR 2017, 809, 809.

6 S. dazu die Angaben zu fake news bei https://euvsdisinfo.eu/.

7 S. dazu *Spindler*, Gutachten F zum 69. Deutschen Juristentag, „Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung“, 2012, S. 10 ff.

8 *Pariser*, „The Filter Bubble“, 2011; ausf. zu Implikationen für die Meinungsvielfalt s. *Schillmöller*, Inter 2020, 150.

9 *Stegmann/Stark/Magin*, „Echo Chambers“, 2021, S. 1 ff.; *Stark/Stegmann*, „Are Algorithms a Threat to Democracy?“, 2020, S. 14, die derzeit allerdings von einem überschätzten Phänomen ausgehen (vgl. S. 25 f.); *Magin/Geiß/Jürgens/Stark*, „Schweigespirale oder Echokammer?“, in: Weber/Mangold/Hofer/Koch, Meinungsbildung in der Netzöffentlichkeit, 2019, S. 93 ff.

10 *MDR Aktuell*, „Wie Michael Kretschmer bei Telegram beleidigt und bedroht wird“, abrufbar unter https://www.mdr.de/nachrichten/deutschland/politik/angriffe-sachsen-ministerpraesident-kretschmer-telegram-100.html (zuletzt abgerufen am 09. Dezember 2021).

dem Jahr 2017 zu beurteilen sein.[11] Die Mittel der Desinformation reichen dabei von Verzerrungen und dem lediglich ausschnittsweisen Zeigen von Bildern, Videos oder anderen Nachrichten, was schließlich zu Mobbing in Form von „hate speech“[12] oder gar Mord-Aufrufen[13] führen kann.
Ein besonders großes Ausmaß nehmen derzeit Desinformationen ein, die in Zusammenhang mit der Corona-Pandemie stehen. In Reaktion hierauf haben sowohl die Europäische Kommission[14] als auch die Bundesregierung[15] umfangreiche Informations- und Factchecking-Portale eingerichtet.

C. Verstärkung durch den Einsatz von Künstlicher Intelligenz

Zum Zwecke einer personalisierten Nutzung der Plattformen sowie vor dem Hintergrund der enormen Datenmengen müssen die vorhandenen Inhalte gefiltert, sortiert und schließlich personalisiert zur Verfügung gestellt werden.[16] Damit wird auch der Wandel von dem „Medienfilter“ der klassischen Massenmedien hin zum „Filtermedium“ in Form der neuen Medien weiter zementiert.[17] Diese Prozesse laufen bereits seit Längerem weitestgehend Algorithmen basiert ab, um ein ansonsten personal- und

---

11 *Kreye*, „Warum die Rohingya Facebook verklagen“, abrufbar unter https://www.sueddeutsche.de/politik/rohingya-facebook-meta-klage-1.5482494 (zuletzt abgerufen am 10. Dezember 2021).

12 So etwa im Fall Renate Künast, vgl. MMR-Aktuell 2019, 421364; *Löber/Roßnagel*, MMR 2019, 71.

13 *MDR Aktuell*, „Wie Michael Kretschmer bei Telegram beleidigt und bedroht wird“, abrufbar unter https://www.mdr.de/nachrichten/deutschland/politik/angriffe-sachsen-ministerpraesident-kretschmer-telegram-100.html (zuletzt abgerufen am 09. Dezember 2021); *Locke*, „Ermittlungen nach Mordplänen gegen Kretschmer, abrufbar unter https://www.faz.net/aktuell/politik/inland/ermittlungen-nach-mordplaenen-gegen-michael-kretschmer-17673774.html (zuletzt abgerufen am 09. Dezember 2021).

14 Abrufbar unter https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation_de (zuletzt abgerufen am 09. Dezember 2021).

15 Abrufbar unter https://www.bundesregierung.de/breg-de/themen/corona-informationen-impfung/mythen-impfstoff-1831898 (zuletzt abgerufen am 09. Dezember 2021).

16 *BBC News*, „Rohingya sue Facebook for $150bn over Myanmar hate speech”, abrufbar unter https://www.bbc.com/news/world-asia-59558090 (zuletzt abgerufen am 10. Dezember 2021).

17 *Kersten*, „Schwarmdemokratie“, 2017, S. 127 ff.; *Ingold*, „Governance of Algorithms, Kommunikationskontrolle durch “Content Curation” in sozialen Netzwerken“, in: Unger/von Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, S. 183, 189.

kostenintensives redaktionelles Kuratieren[18] zu vermeiden. Mit dem Einsatz künstlicher Intelligenz etwa in Form von Deep Learning wurden die dabei entstehenden Effekte der Content-Selektierung und -Priorisierung noch weiter intensiviert: So ist etwa die Anzahl der variablen Kriterien, die der Facebook Algorithmus für die persönliche Relevanzentscheidungen eines Inhalts auf der Plattform heranzieht, von ursprünglich 3 Kriterien auf ca. 100.000 im Jahr 2013 angestiegen.[19] Durch künstliche Intelligenz lassen sich somit noch präzisere Nutzerprofile herstellen, die die Anpassung der angebotenen (meinungsbildenden) Inhalte an die (vermeintlichen) persönlichen Präferenzen der Nutzer erlauben.[20] Der Intermediär nimmt dabei bewusst Einfluss auf die Nutzer, indem deren Verhalten ausgewertet wird und die gewonnenen Erkenntnisse sowohl im Rahmen der Anzeige von Werbung als auch der empfohlenen Inhalte Berücksichtigung finden („Recommender Systeme").[21] Aufgrund der Fähigkeit von künstlicher Intelligenz, auch sich veränderndes Verhalten von Nutzern zu „lernen" und dann Inhalte entsprechend anzupassen, hat gerade der Einsatz von künstlicher Intelligenz ein hohes Manipulationspotential[22] - was nicht zuletzt auch in Zusammenhang mit der monopolartigen Stellung der geringen Anzahl an wirkmächtigen Intermediären in der Welt der neuen Medien und der mangelnden Transparenz hinsichtlich der verwendeten Algorithmen steht.[23]

---

18 Ausführlich dazu *Ingold*, „Governance of Algorithms, Kommunikationskontrolle durch "Content Curation" in sozialen Netzwerken", in: Unger/von Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, S. 183 ff.

19 *McGee*, "EdgeRank is Dead: Facebook's News Feed Algorithm Now Has Close To 100K Weight Factors", 2013, abrufbar unter http://marketingland.com/edgerank-is-dead-facebooks-news-feed-algorithm-now-has-close-to-100k-weight-factors-55908 (zuletzt abgerufen am 10. Dezember 2021); die genaue Gewichtung der einzelnen Kriterien ist indessen unbekannt.

20 Ausführlich dazu *Hoffmann-Riem*, AöR 142 (2017), 1, 10 ff.

21 *Hoffmann-Riem*, AöR 142 (2017), 1, 10 ff.; *Ingold*, „Governance of Algorithms, Kommunikationskontrolle durch "Content Curation" in sozialen Netzwerken", in: Unger/von Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, S. 183, 188 ff.; *Kaiser/Reiling*, „Meinungsfilter durch soziale Medien – und das demokratische Ideal der Meinungsvielfalt?", in: Unger/von Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, S. 85 ff.; *Drexl*, ZUM 2017, 529, 533; *Eifert*, NJW 2017, 1450, 1451; *Gillespie*, „Custodians of the Internet", 2018, S. 24 ff.

22 *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498, 499; *Drexel*, ZUM 2017, 529, 536; zu vergleichbaren Gefahren bei Suchmaschinenanbietern s. *Kreile*, ZUM 2017, 268, 274; *Dörr/Natt*, ZUM 2014, 829, 835 f.

23 *Schillmöller*, Inter 2020, 150, 151; *Schwartmann/Hermann/Mühlenbeck*, MMR 2019, 498, 499 ff.

III. Verantwortung der Informations-Intermediäre

A. Unterschiede gegenüber herkömmlichen Informations-Intermediären und Konvergenztendenzen

Die Unterschiede zu den herkömmlichen Informationsintermediären, insbesondere TV und Rundfunk einerseits und der Presse andererseits sind ebenfalls seit zwei Jahrzehnten bekannt. So gilt nach wie vor als Rundfunk nach § 2 Abs. 1 S. 1 MStV nur das sequentiell wahrnehmbare Programm one-to-many, nicht aber der individuell „on demand“ verfügbare Inhalt,[24] wie er prägend für fast alle Internet-Inhalteanbieter ist. Demgegenüber wird die Presse traditionell durch ihren Informationsträger – das gedruckte Papier – unterschieden, selbst die elektronische Presse unterfällt nicht den Länder-Pressegesetzen.[25] Diese Unterscheidung gegenüber Informations-Intermediären, die sich durch on-demand-Abrufe und nicht-sequentielle Programmdarbietungen unterscheiden, hat mannigfaltige Konsequenzen in rechtlicher Hinsicht, da die Länder aufgrund von Art. 30, 70 GG die Kompetenzen im Bereich der Medienregulierung haben. So bestimmt auch § 1 Abs. 3, 4 TMG, dass der Bereich der Presse wie des Rundfunks von der Anwendbarkeit des TMG zugunsten des (Länder-) MStV oder der Pressegesetze ausgenommen ist.[26]

Gleichzeitig kommt es aber auch zu immer größeren Konvergenzen[27] zwischen den verschiedenen Medien: So lässt sich die elektronische Presse häufig nicht mehr von der gedruckten Presse unterscheiden, sondern weist zusätzliche Informationsmöglichkeiten auf. Ebenso werden durchgängig

---

24 So werden etwa Mediatheken als „rundfunkähnliche Telemedien“ iSd § 2 Abs. 2 Nr. 13 MStV behandelt, womit die Regelungen der §§ 17-25, 74-77 MStV Anwendung finden, s. BeckOK InfoMedienR/*Martini*, 34. Ed. 1.2.2021, MStV § 2 Rn. 100.

25 Spindler/Schmitz/*Spindler*, 2. Aufl. 2018, TMG § 1 Rn. 65 ff.; zur Unterscheidung von hybriden Diensten auf europäischer Ebene s. EuGH Urt. v. 21.10.2015 – C-347/14 Rn. 25 ff. = GRUR 2016, 101, 103 – *New Media Online* m. Anm. v. *Spindler*, JZ 2016, 147; Hoeren/Sieber/Holznagel/*Holznagel/Hartmann*, Handbuch Multimedia-Recht, 56. EL Mai 2021, Teil 3 Rn. 38; *Jäger*, ZUM 2019, 477, 478.

26 BeckOK InfoMedienR/*Martini*, 34. Ed. 1.2.2021, TMG § 1 Rn. 13 ff.; Spindler/Schmitz/*Spindler*, 2. Aufl. 2018, TMG § 1 Rn. 65 ff. mwN.

27 S. dazu bereits *Kluth/Schulz*, „Konvergenz und regulatorische Folgen, Gutachten im Auftrag der Rundfunkkommission der Länder“, 2014, Arbeitspapiere des Hans-Bredow-Instituts Nr. 30, abrufbar unter https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/d74b139d80000c12483526a23a55bf89f9d971c6.pdf (zuletzt abgerufen am 13. Dezember 2021).

TV-Sendungen inzwischen über das Internet per Live-Streaming oder auch zeitversetzt als Near-Video-on-Demand angeboten; auch über längere Zeiträume hinweg lassen sich Sendungen über Mediatheken nachverfolgen. Damit verliert die frühere scheinbar trennscharfe Unterscheidung viel an ihrem Gewicht[28] und führt zu Verwerfungen zwischen den einzelnen Regelungsmaterien, die nur bedingt durch den neuen MStV aufgefangen werden können. Der Anwendungsbereich des MStV erstreckt sich gem. § 1 Abs. 1 MStV neben dem Rundfunk nunmehr auch auf Telemedien, sodass zumindest im Ausgangspunkt versucht wird, der sich wandelnden Medienlandschaft Rechnung zu tragen.[29] Unter dem Begriff des Telemediums wird schließlich in § 1 Abs. 8, § 2 Abs. 2 Nr. 14-16 MStV weiterführend zwischen Medienplattformen, Benutzeroberflächen und Medienintermediären differenziert, um auch insoweit den bestehenden Facettenreichtum rechtlich abzubilden. Gleichwohl werden insbesondere die damit einhergehenden zusätzlichen Anforderungen – etwa an die Transparenz und Diskriminierungsfreiheit – an die einzelnen Telemedien als nicht ausreichend oder zu unpräzise kritisiert.[30]

B. Verantwortlichkeit der Informations-Intermediäre: Die (bisherige) Rolle der Haftungsfreistellungen nach Art. 12 ff. E-Commerce-RL

Der geschilderten herausragenden Rolle der Informations-Intermediäre im Rahmen der Meinungsbildung und der demokratischen Prozesse entspricht bislang aber nicht eine gesteigerte Verantwortlichkeit der Intermediäre.[31] Vielmehr profitieren sie generell von den in Art. 12 ff. E-Commerce-RL bzw. §§ 7 ff. TMG festgeschriebenen Verantwortlichkeitsprivilegierungen, insbesondere beim für Plattformen anwendbaren Host-Providing nach § 10 TMG bzw. Art. 14 E-Commerce-RL, wonach der Betreiber eines Hosting-Dienstes nur dann für rechtswidrige Aktivitäten und Inhalte ver-

28 *Wagner*, GRUR 2020, 329, 331 ff., der die Rollen der „neuen Intermediäre" am Beispiel von Suchmaschinen, sozialen Netzwerken und YouTube herausarbeitet.

29 *Flamme*, MMR 2021, 770, 771.

30 So etwa in Bezug auf Medienintermediäre: BeckOK InfoMedienR/*Zimmer/Liebermann,* 34. Ed. 1.2.2021, TMG § 94 Rn 42 ff., 67 ff.; *Schwartmann/Hermann/Mühlenbeck*, „Tranzparenz bei Medienintermediären", 2020, S. 155 f., abrufbar unter https://www.ma-hsh.de/infothek/publikationen/ma-hsh-gutachten-transparenz-bei-medienintermediaren.html (zuletzt abgerufen am 13. Dezember 2021); *Kühling*, ZUM 2021, 461, 470; *Siara*, MMR 2020, 523, 526.

31 *Wagner*, GRUR 2020, 329, 333.

antwortlich ist, wenn er von diesen bzw. bei zivilrechtlichen Schadensersatzansprüchen von offensichtlichen Umständen, die darauf hinweisen, Kenntnisse hatte, Art. 14 S. 1 Nr. 1, 2 E-Commerce-RL. Nach der Rechtsprechung des EuGH kommen zwar aktive Host-Provider, also solche, die denjenigen, der Nachrichten sowie Inhalte speichert, in seinen Aktivitäten unterstützen, nicht in den Genuss der Haftungsprivilegierungen.[32] Jedoch hat der EuGH jüngst für die Plattform YouTube entschieden, dass selbst das Einblenden von personalisierter Werbung sowie die Aufbereitung von Suchergebnissen anhand der persönlichen Präferenzen des Nutzers nicht zur Annahme einer aktiven Rolle des Plattformbetreibers führen.[33] Insoweit stellte das Gericht auch auf das Vorhandensein technischer Vorkehrungen zur Verhinderung von Urheberrechtsverletzungen (Benachrichtigungsverfahren, Meldebutton und Content ID-Verfahren) und auf entsprechende Verbote in den allgemeinen Nutzungsbedingungen bzw. den Community-Richtlinien ab.[34] Damit bleibt es in aller Regel bei der Anwendung der Haftungsprivilegierungen - gerade für Informations-Intermediäre wie YouTube, auch wenn die Entscheidung des EuGH in einem urheberrechtlichen Kontext erging.

Relativiert wird die Haftungsprivilegierung aber durch die Haftung der Informations-Intermediäre auf Unterlassung und Sperrung von rechtswidrigen Inhalten.[35] Denn Art. 14 Abs. 3 E-Commerce-RL sieht vor, dass die Möglichkeit von „injunctions“ gegenüber Host-Providern aufgrund mitgliedstaatlicher Normen unberührt bleibt, womit die gesamte Störerhaftung nach deutschem Recht weiterhin auf Informations-Intermediäre Anwendung findet. Auch der EuGH hat dies unlängst in der Glawischnig-Piesczek-Entscheidung bekräftigt, in der es das Gericht (allerdings nach österreichischem Recht) als mit Art. 14 E-Commerce-RL vereinbar ansah, dass eine verleumdete Politikerin weltweite Unterlassung und Sperrung solcher Posts gegenüber Facebook verlangte.[36] Ausschlaggebend sind daher nach wie vor das Ausmaß an zumutbaren Kontroll- und Prüfpflichten der Host-

32 Grundlegend EuGH Urt. v. 12.7.2011 – C-324/09 = GRUR 2011, 1025 – *L`Oreal SA ua*; Spindler/Schmitz/*Spindler*, 2. Aufl. 2018, TMG § 1 Rn. 8 ff., 18 ff.; BeckOK InfoMedienR/*Paal/Hennemann*, 34. Ed. 1.2.2021, TMG § 10 Rn. 3, 22 ff.; *Wimmers/Barudi*, GRUR 2017, 327, 332.

33 EuGH Urt. v. 22.6.2021 – C-682/18, C-683/18 Rn. 84 f., 95 f. = NJW 2021, 2571, 2575, 2576 – *YouTube und Cyando*; dazu *Spindler*, NJW 2021, 2554.

34 EuGH Urt. v. 22.6.2021 – C-682/18, C-683/18 Rn. 93 f. = NJW 2021, 2571, 2576 – *YouTube und Cyando.*

35 *Wagner,* GRUR 2020, 329, 333.

36 EuGH Urt. v. 3.10.2019 – C-18/18, MMR 2019, 798 – *Glawischnig-Piesczek*; dazu *Spindler*, NJW 2019, 3274.

Provider, wobei die (deutsche) Rechtsprechung hier weitere Details entwickelt hat, auf die noch zurückzukommen sein wird.[37]

IV. Möglichkeiten und bestehende Ansätze der Regulierung

Wie bereits skizziert, zeichnen sich die rechtlichen Regulierungsansätze durch eine „Dichotomie" von zivil- und öffentlichen Regulierungsansätzen aus, die einerseits den Ansatz aus einer Mikroperspektive (zivilrechtliche Ansprüche), andererseits aus einer Makroperspektive (öffentlich-rechtliche Regulierung) verfolgen. In diesem Gefüge sind zudem die europäischen Ansätze bzw. Vorschläge zu verorten, allen voran der Vorschlag eines „Digital Services Acts".

A. Zivil- und öffentlich-rechtliche Regulierungsansätze

1. Zivilrechtliche Ansatzpunkte

Aus zivilrechtlicher Perspektive kommen im Hinblick auf die Verantwortlichkeit der Informations-Intermediäre vor allem die vertragsrechtlichen Ansprüche auf Zulassung von Inhalten sowie die kommunikations(delikts)rechtlichen Ansprüche der §§ 823, 824 BGB in Betracht,[38] daneben die Ansprüche aus den landespresserechtlichen Regelungen. Der MStV enthält dagegen nur öffentlich-rechtliche Normen und Regulierungen mit Sanktionsmöglichkeiten in § 109 MStV bzw. Bußgeldern nach § 115 MStV.[39]

a) Vertragsrecht und Grundrechtsbindung

Gerade im Hinblick auf die Bekämpfung von „hate speech" und „fake news" stehen zunehmend die Auseinandersetzungen von Nutzern sozialer Netzwerke gegenüber den Informations-Intermediären im Fokus gerichtlicher Entscheidungen, da die Intermediäre sich auf ihre „community stan-

37 IV.A.1.a).
38 Hierzu eingehend *Oster*, „Kommunikationsdeliktsrecht: Eine transnationale Untersuchung am Beispiel des Ehrschutzes", 2016.
39 *Ory*, ZUM 2021, 472, 475.

dards“ berufen, die ihnen einen über das gesetzliche Maß hinausgehenden Spielraum einräumen, Inhalte, die gegen die Standards verstoßen, zu sperren oder zu löschen.[40] Der III. Zivilsenat hielt auch für marktbeherrschende soziale Netzwerke wie Facebook die Vereinbarung solcher Standards im Rahmen der AGB für zulässig, knüpft dies allerdings an prozedurale Absicherungen für die Rechte der Nutzer. Derartige community standards sind demnach nur zulässig, wenn sie eine Art Rechtsbehelfsverfahren für die Nutzer im Sinne des rechtlichen Gehörs vor einer Sperrung oder Löschung vorsehen, indem dem Nutzer Gelegenheit gegeben werden muss, Stellung zu den Vorwürfen gegen ihn zu nehmen.[41] Zwar hält der BGH Facebook als marktmächtiges Unternehmen nicht für unmittelbar an die Grundrechte gebunden, da „(d)ie Marktmacht der Beklagten […] nicht gleichzusetzen (sei) mit der Monopolstellung staatlicher Unternehmen auf dem Gebiet der öffentlichen Daseinsvorsorge wie etwa früher der Post (...)“. Insbesondere übernehme Facebook „...nicht die - vom Bundesverfassungsgericht […] als Voraussetzung für eine staatsgleiche Grundrechtsbindung genannte - Bereitstellung der Rahmenbedingungen öffentlicher Kommunikation wie etwa die Sicherstellung der Telekommunikationsdienstleistungen“.[42] Dennoch verlangt das Gericht aufgrund der Eröffnung

---

40 Näher dazu *Spindler*, CR 2019, 238; *Holznagel*, CRi 2020, 103; *ders.*, CR 2019, 518; *Lüdemann*, MMR 2019, 279; *McColgan*, RDi 2021, 605; *Friehe*, NJW 2020, 1697, 1699; *König*, AcP 219 (2019), 611; *Beurskens*, NJW 2018, 3418; *Ring*, MDR 2018, 1469; *Löber/Roßnagel*, MMR 2019, 71, 75; *Hennemann/Heldt*, ZUM 2021, 981; Hoeren/Sieber/Holznagel/*Redeker*, Handbuch Multimedia-Recht, 56. EL. Mai 2021, Teil 12 Rn. 76 ff.; BeckOK IT-Recht/*Munz*, 4. Ed. 1.10.2021, BGB § 307 Rn. 211 ff.; abl. ggü. eigener Grenzen der Plattformbetreiber *Labusga/Elsaß/Tichy*, CR 2017, 234; *Müller-Riemenschneider/Specht*, MMR 2018, 545, 547.

41 BGH Urt. v. 29.07.2021 – III ZR 179/20 Rn. 84 = ZUM 2021, 953, 964; in Bezug auf Suchmaschinenanbieter s. BGH Urt. v. 27.02.2018 – VI ZR 489/16 Rn. 32 = NJW 2018, 2324, 2327; BGH Urt. v. 01.03.2016 – VI ZR 34/15 Rn. 24 = GRUR 2016, 855, 857 unter Verweis auf BGH Urt. v. 25.10.2011 – VI ZR 93/10 Rn. 25 ff. = GRUR 2012, 311, 313 – *Blog-Eintrag*; *Hennemann/Heldt*, ZUM 2021, 981, 991 sehen die Relevanz entsprechender Klauseln auch vor dem Hintergrund des in § 3b NetzDG vorgesehenen weitreichenden Gegendarstellungsverfahrens weiterhin als gegeben.

42 BGH Urt. v. 29.7.2021 – III ZR 179/20 Rn. 59 = ZUM 2021, 953, 961; s. dazu auch BVerfG Beschl. v. 6.11.2019 – 1 BvR 16/13, NJW 2020, 300 – *Recht auf Vergessen I*; BVerfG Urt. v. 22.2.2011 – 1 BvR 699/06 Rn. 59 = NJW 2011, 1201, 1203 f.– *Versammlungsfreiheit im Flughafen*; BVerfG Beschl. v. 18.7.2015 – 1 BvQ 25/15 = NJW 2015, 2485 – *Bierdosen-Flashmob;* OLG Braunschweig, Urt. v. 5.2.2021 – 1 U 9/20, Rn. 143 ff. = ZUM-RD 2021, 398, 411; OLG Düsseldorf, Urt. v. 4.12.2020 – 7 U 131/19, Rn. 28 ff. = GRUR-RS 2020, 41440; OLG Brandenburg, Urt. v. 30.11.2020 – 1 U 37/19, Rn. 12 f. = GRUR-RS 2020, 35273; OLG Hamm, Beschl. v. 15.9.2020

öffentlicher Kommunikationsräume im Rahmen einer Abwägung der sich gegenüberstehenden Grundrechte der Betreiber des Netzwerkes einerseits und der Nutzer andererseits,[43] dass dem Nutzer, dessen Inhalt geblockt oder gelöscht werden sollen, Gelegenheit zur Stellungnahme gegeben wird, und dass der Netzwerkbetreiber verpflichtet ist, die zugrundeliegenden Tatsachen zu überprüfen und den Sachverhalt aufzuklären.[44]

Damit adressiert die zivilrechtliche Rechtsprechung bereits auf der vertragsrechtlichen Ebene das grundlegende Trilemma, in dem sich Informations-Intermediäre befinden, indem sie sich im Dreieck zwischen gegenläufigen Interessen und Grundrechten von Inhalteanbietern und betroffenen Nutzern und ihrer eigenen Stellung befinden.[45] Mit der Einbindung von community standards und der entsprechenden Entscheidungsbefugnis sehen sich die Informations-intermediäre unversehens in der Rolle eines „privaten" Richters – ohne selbst über entsprechende verfahrensrechtliche Absicherungen per se zur verfügen.

Umgekehrt werden offenbar von den größeren Informations-Intermediären inzwischen automatisierte Verfahren eingesetzt, um unerwünschte Inhalte herauszufiltern[46] – ähnlich den aus der urheberrechtlichen Diskus-

– 29 U 6/20, GRUR-RS 2020, 25382; OLG Schleswig, Urt. v. 26.2.2020 – 9 U 125/19, Rn. 56 ff. = GRUR-RS 2020, 8539; OLG Karlsruhe, Beschl. v. 28.2.2019 – 6 W 81/18, Rn. 24 ff. = MMR 2020, 52, 53; OLG Stuttgart, Beschl. v. 6.9.2018 – 4 W 63/18, Rn. 29 f. = MMR 2019, 110, 111 f.; OLG Dresden, Beschl. v. 8.8.2018 – 4 W 577/18, Rn. 17 ff. = NJW 2018, 3111, 3113 f.; Hoeren/Sieber/Holznagel/*Redeker*, Handbuch Multimedia-Recht, 56. EL. Mai 2021, Teil 12 Rn. 76 ff.; BeckOK InfoMedienR/*Knoke/Krüger*, 34. Edn. 1.2.2021, NetzDG § 3 Rn. 25, 30, 32; *König*, AcP 2019, 611, 635 ff.; *Löber/Roßnagel*, MMR 2019, 71, 75; *Lüdemann*, MMR 2019, 279, 280 ff.; *Ring*, MDR 2018, 1469, 1474; *Spiegel/Heymann*, K&R 2020, 344, 348 f.; *Spindler*, CR 2019, 238, 242 ff.

43 BGH Urt. v. 29.7.2021 – III ZR 179/20 Rn. 60 ff. = ZUM 2021, 953, 961.

44 BGH Urt. v. 29.7.2021 – III ZR 179/20 Rn. 83 ff. = ZUM 2021, 953, 964; s. auch *Raue*, JZ 2018, 969.

45 In diese Richtung auch *Holznagel*, CR 2021, 733, 736, der insbesondere mit Blick auf Art. 18 DSA-E vor einer Fehlentwicklung durch zu weitreichende Nutzerrechte warnt; *ders.*, „The Digital Services Act wants you to ´sue´ Facebook over content descisions in private de facto courts", 2021, abrufbar unter https://verfassungsblog.de/dsa-art-18/ (zuletzt abgerufen am 16. Dezember 2021); *Wimmers*, „The Out-of-court dispute settlement mechanism in the Digital Services Act - A disservice to its own goals", abrufbar unter https://www.jipitec.eu/online-first-articles-1/5357 (zuletzt abgerufen am 16. Dezember 2021).

46 Dazu *Cornils*, NJW 2021, 2465, 2467.

sion bekannten „Upload“-Filtern, wie sie zumindest implizit in Art. 17 Abs 4 b) DSM-RL vorgesehen sind.[47]

b) Persönlichkeitsrechtliche Ansprüche

Quasi die andere Seite der Medaille der vertragsrechtlichen Ansprüche von Nutzern, die die Wiedergabe ihrer Inhalte vertragsrechtlich erzwingen wollen, sind die persönlichkeitsrechtlichen Ansprüche von Betroffenen – einschließlich der Rechtsstreitigkeiten um Bewertungsportale:

Ähnlich der hinsichtlich vertragsrechtlicher Ansprüche vorgestellten Entscheidung des III. Zivilsenats des BGH hat dessen VI. Zivilsenat[48] bereits einige Zeit früher in einem die Persönlichkeitsrechte betreffendem Urteil ein ähnliches Verfahren eingefordert: Im entschiedenen Fall ging es um falsche bzw. ehrverletzende Äußerungen im Rahmen eines Blogs, der bei einem Informations-Intermediär gehostet wurde. Der Betroffene begehrte von dem Intermediär die Unterlassung bzw. die Sperrung der ehrverletzenden Inhalte. Der VI. Zivilsenat hielt den Intermediär für verpflichtet, im Rahmen der Störerhaftung demjenigen, der den inkriminierten Inhalt hochgeladen hatte, zur Stellungnahme aufzufordern; käme er dieser Aufforderung nicht nach, müsse der Inhalt geblockt werden, andernfalls würde seine Stellungnahme dem Beschwerdeführer wiederum zur Äußerung übermittelt werden. Sollte dieser sich seinerseits nicht dazu äußern, müsse der Intermediär die Inhalte weiterhin speichern bzw. bereithalten.[49]

Diese Rechtsprechung wird flankiert durch Entscheidungen zu Bewertungsportalen, in denen der BGH deren Betreiber grundsätzlich ebenfalls dazu verpflichtete, die einer Bewertung zugrundeliegenden Tatsachen

47 Eingehend zur Diskussion um die Upload-Filter *Jäger*, ZUM 2021, 903; *Klaas*, ZRP 2021, 74; *Geiger/Jütte*, GRUR Int. 2021, 517, 534 ff.; *Barudi*, „Das neue Urheberrecht“, 1. Aufl. 2021, § 1 Rn. 90 ff.; *Müller-Terpitz*, ZUM 2020, 365; s. auch *Spindler*, WRP 2021, 1111; *ders.* GRUR 2020, 253; *Frey/Rudolph*, MMR 2021, 671, 673.

48 BGH Urt. v. 25.10.2011 – VI ZR 93/10 = GRUR 2012, 311 – *Blog-Eintrag*; s. zum grundrechtlichen Hintergrund ausf. Hornung/Müller-Terpitz/*Müller-Terpitz*, Rechtshandbuch Social Media, 2. Aufl. 2021, S. 255 ff.

49 BGH Urt. v. 25.10.2011 – VI ZR 93/10 = GRUR 2012, 311 – *Blog-Eintrag*; *Rühl*, LMK 2012, 338417; *Gaugenrieder*, EWiR 2012, 241.

nach Beschwerdeeingang zu eruieren und zu überprüfen.[50] Demnach setzt die Abwägung der widerstreitenden (grundrechtlichen) Interessen die aktive Sachverhaltserforschung durch den Provider voraus. Nach der Beschwerde durch den Betroffenen hat der Intermediär zu diesem Zweck dem für den Inhalt verantwortlichen Nutzer Gelegenheit zur Stellungnahme zu geben. Im Anschluss soll dem Betroffenen die Möglichkeit einer Erwiderung auf die Stellungnahme gegeben werden. Schließlich hat der Intermediär über unklare Sachverhalte quasi „Beweis" zu erheben. Die in diesem Verfahren gewonnenen Erkenntnisse dienen als Grundlage für die Entscheidung über die Löschung oder den Verbleib des Inhalts auf der Plattform.[51] Wie bereits aus den zuvor genannten zivilrechtlichen Ansatzpunkten bzw. Entscheidungen bekannt, trifft auch hier wieder maßgeblich den Intermediär ein Pflichtenkanon, der ihn die Rolle des Vermittlers zwischen dem (potentiell) Geschädigten und dem (potentiellen) Schädiger zuteilt.

2. *Öffentlich-rechtliche Ansätze*

Eher aus der Makroperspektive greifen dagegen die öffentlich-rechtlichen Ansätze zur Erfassung und Regulierung der Verantwortlichkeit der Informations-Intermediäre ein, die Überwachungs- und Risikomanagementpflichten der Betreiber solcher Plattformen festlegen:

a) Nationale Ansätze

Aus nationaler Sicht sind hier vor allem das Netzwerkdurchsetzungsgesetz (NetzDG) als auch die Regelungen im neuen Medienstaatsvertrag (MStV) von Interesse:

50 BGH Urt. v. 01.03.2016 – VI ZR 34/15 Rn. 23 f. = GRUR 2016, 855, 857 unter Verweis auf BGH Urt. v. 25.10.2011 – VI ZR 93/10 Rn. 25 ff. = GRUR 2012, 311, 313 – *Blog-Eintrag.*

51 Ausf. zu den Prüfpflichten des Intermediärs s. *Schuster,* GRUR 2013, 1201; *Schilling*, GRUR-Prax 2015, 313.

(1) Das Netzwerkdurchsetzungsgesetz (NetzDG)

Der grundsätzliche Ansatz des NetzDG besteht darin, die Plattformbetreiber zur effizienten Behandlung von Beschwerden zu verpflichten, zum einen zur Einrichtung eines Beschwerdemanagementsystems, zum anderen zur Löschung und Sperrung von rechtswidrigen Inhalten innerhalb einer Woche, bei evident rechtswidrigen Inhalten sogar binnen 24 Stunden. Durchgesetzt werden diese Pflichten durch Bußgelder sowie Transparenz- und Publizitätspflichten. Demgegenüber hat bisher ein Anspruch des Betroffenen auf Wiederherstellung seiner Inhalte keine Berücksichtigung gefunden.

(a) Der Anwendungsbereich: Soziale Netzwerke - von der individuellen Kommunikation zur Massenkommunikation

Der Gesetzgeber versucht das Phänomen dadurch in den Griff zu bekommen, dass in § 1 Abs. 1 NetzDG als soziales Netzwerk ein Telemediendienst definiert wird, der dazu bestimmt ist, dass „beliebige Inhalte mit anderen Nutzern“ geteilt oder „der Öffentlichkeit zugänglich“ gemacht werden.[52] Mit § 1 Abs. 1 S. 3 NetzDG sollen Plattformen ausgenommen werden, „die zur Individualkommunikation oder zur Verbreitung spezifischer Inhalte bestimmt sind“. Damit versucht der Gesetzgeber der Kritik am RegE[53] Rechnung zu tragen, dass der Anwendungsbereich viel zu breit geraten war und selbst Messaging- und Maildienste unter die Definition der Netzwerke fielen.[54] Selbst für Messengerdienste, die der Gesetzgeber ausdrücklich ausnehmen will, ergeben sich allerdings nach wie vor Zweifel:

52 Begr. RegE BT-Drs. 18/12356, S. 19 unter Verweis auf BGH, 8.7.1993 – I ZR 124/91 = GRUR 1994, 45, 46 – *Verteileranlagen*; BGH, 11.7.1996 – I ZR 22/94 = GRUR 1996, 875, 876 – *Zweibettzimmer im Krankenhaus* und BGH, 22. 4. 2009 – I ZR 216/06 = GRUR 2009, 845, 848 – *Internet-Videorecorder*; vgl. Begr. Rechtsausschuss BT-Drs. 18/13030, S. 19, Begr. RegE BT-Drs. 18/12727, S. 28.

53 Stellungnahme Bitkom vom 30. 3. 2017, S. 5, abrufbar unter https://www.bitkom.org/sites/main/files/file/import/FirstSpirit-1492755732142201704 20-Bitkom-Stellungnahme-zum-Regierungsentwurf-NetzwerkDG.pdf (zuletzt abgerufen am 4. Mai 2022); ähnlich Stellungnahme eco Verband der Internetwirtschaft e. V., 30. 3. 2017, S. 4 abrufbar unter https://www.eco.de/wp-content/uploads/dlm_uploads/2020/05/20200505_eco-stn-zur-anhoerung-im-rechtsausschuss-eines-gesetzes-zur-bekaempfung-des-rechtsextremismus-und-der-hasskriminalitaet.pdf (zuletzt abgerufen am 4. Mai 2022).

54 Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

Warum sollten etwa große WhatsApp-Gruppen nicht dem Begriff der sozialen Netzwerke unterfallen (da Messengerdienst), kleine Twittergruppen bzw. Follower dagegen schon? Die Unterscheidung zwischen Individual- und Massenkommunikation ist gerade im Zeitalter des Internet schon immer fragwürdig gewesen.[55] Dies wird derzeit auch am Verfahren des Bundesamtes für Justiz gegen den Messengerdienst „Telegram" deutlich, auf dem sich zahlreiche Kanäle von zigtausenden „Followern" finden.[56]

Nach Auffassung des Gesetzgebers sollen in diesem Rahmen ferner berufliche Netzwerke wie XING oder LinkedIn nicht unter den Begriff des sozialen Netzwerks fallen, da sie nur darauf angelegt seien, spezifische Inhalte zu verbreiten.[57] Auch Online-Spiele, Fachportale oder Verkaufsplattformen sollen unter diese Ausnahme fallen.[58] Offen bleibt, was „spezifische" Inhalte sind.

Das Gesetz lässt sich nur durch eine restriktive Interpretation dergestalt retten, dass ausschließlich Plattformen mit überwiegend meinungsbildenden Inhalten gemeint sind, worauf auch die Mehrzahl der genannten Delikte hinweist – was seinerseits allerdings immer noch breit gefasst ist. Welche Form der Inhalt hat, spielt dabei keine Rolle, ob Video, Musik oder Text.[59]

Ferner beschränkt das Gesetz den Begriff auf Betreiber von Plattformen mit Gewinnerzielungsabsicht; rein private Kommunikationsplattformen oder non-profit Plattformen sind damit ausgeschlossen. Versteht man in den einschlägigen Lizenzen wie creative commons den Begriff „non-commercial" in der gleichen Weise, sind Plattformen wie Wikipedia vom NetzDG ausgenommen.[60] Allerdings herrscht hier nach wie vor große

55 Näher dazu Spindler/Schmitz/*Spindler*, 2. Aufl. 2018, TMG § 1 Rn. 44 f.; ebenfalls krit. etwa: *Roßnagel*, NVwZ 2007, 743, 745; *Bizer*, DuD 2007, 40.

56 FAZ, „Bundesamt für Justiz geht gegen Telegram vor", 14.6.2021, abrufbar unter: https://www.faz.net/aktuell/wirtschaft/digitec/telegram-bundesamt-fuer-justiz-geht-gegen-messengerdienst-vor-17388586.html (zuletzt abgerufen am 22. Dezember 2021).

57 Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

58 Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

59 Begr. RegE BT-Drs. 18/12356, S. 19.

60 Für eine restriktive Auslegung bei Nutzungsrechteeinräumung: LG Köln Urt. v. 5. 3. 2014 – 28 O 232/13 = MMR 2014, 478, 480 f. m. krit. Anm. *Jaeger/Mantz*: „rein private Nutzung"; unter Anwendung des § 305c Abs. 2 BGB weitergehend: OLG Köln Urt. v. 31. 10. 2014 – 6 U 60/14, K&R 2015, 57 ff. = MMR 2015, 331 Rn. 87: „keinen direkten finanziellen Vorteil"; zu den Grenzfällen und für Einzelfallauslegung plädierend: *Kreutzer*, „Open Content Lizenzen", 2011, S. 44 ff.

Unsicherheit, ob der Begriff in gleicher Weise wie im deutschen Recht zu verstehen ist.[61]

§ 1 Abs. 2 NetzDG schränkt den Anwendungsbereich auf große soziale Netzwerke mit mehr als 2 Mio. im Inland registrierte Nutzer ein. Dabei spielt es nach Auffassung des Gesetzgebers keine Rolle, „in welchem Land der jeweilige Nutzer hauptsächlich aktiv ist“.[62]

Das NetzDG soll nicht für „Plattformen mit journalistisch-redaktionell gestalteten Angeboten (gelten), die vom Diensteanbieter selbst verantwortet werden“, § 1 Abs. 1 S. 2 NetzDG. Für diese sollten die Vorschriften der §§ 74 ff. MStV eingreifen.[63] Damit ist wieder die Frage aufgeworfen, was man unter „journalistisch-redaktionell gestaltet“ verstehen kann. Hier wird es auf eine aktive Gestaltung und Einzelauswahl bzw. Zusammenstellung von Beiträgen ankommen; allein die Einrichtung von bestimmten Inhaltskategorien, unter denen dann Blogs oder Beiträge abgelegt werden können, reicht hierfür nicht.[64] Zudem müssen diese Angebote vom Anbieter „selbst verantwortet“ werden – dieser sonst im NetzDG nicht verwandte Begriff ist in derselben Weise wie § 10 S. 2 TMG zu verstehen, der auf die Aufsicht des Telemedienanbieters gegenüber denjenigen, die Inhalte einstellen, abstellt. Eine reine Moderation z. B. genügt hierfür nicht, da Inhalte nicht für den Anbieter bzw. in dessen Auftrag angefertigt werden.

Unklar und wichtig für die Verbreitung von hate speech und fake news ist, ob auch Gästeforen von (online) Zeitungen unter die Ausnahme des § 1 Abs. 3 NetzDG fallen: Dagegen spricht auf den ersten Blick, dass es sich hier nicht um journalistisch-redaktionelle Angebote des Diensteanbieters handelt, sondern eindeutig um fremde, nicht verantwortete Beiträge. Doch sind diese Gästeforen Teil des gesamten Angebots solcher Plattformen – und die Ausnahme bezieht sich auf die Plattform als solche und nicht auf einzelne Bestandteile der Plattform.

Das NetzDG enthält keinerlei Norm, die die internationale Anwendbarkeit, etwa in Gestalt auf nur im Inland ansässige soziale Netzwerkanbieter,

---

61 Zu den Schwierigkeiten der Auslegung generischer Lizenzversionen etwa: OLG Köln Urt. v. 31. 10. 2014 – 6 U 60/14 = K&R 2015, 57 ff. = MMR 2015, 331 Rn. 74 ff., insbes. 79, 86; *Kreutzer*, „Open Content Lizenzen“, 2011, S. 42 f.; *Jaeger/Mantz*, MMR 2014, 480 f.

62 Begr. RegE BT-Drs. 18/12356, S. 20.

63 Begr. RegE BT-Drs. 18/12356, S. 19.

64 Näher dazu Spindler/Schmitz/*Spindler*, 2. Aufl. 2018, TMG § 1 Rn. 66 ff.; ferner Binder/Vesting/*Held*, Rundfunkrecht, 4. Aufl. 2018, RStV § 54 Rn. 38 ff.; Spindler/Schuster/*Fricke*, Recht der elektronischen Medien, 4. Aufl. 2019, UrhG § 87f Rn. 6; BeckOK InfoMedienR/*Martini*, 34. Ed. 1.2.2021, MStV § 2 Rn. 19; *Leitgeb*, ZUM 2009, 39, 42; *Weiner/Schmelz*, K&R 2006, 453, 456 f.

beschränkt. Da das NetzDG nur bei der Mindestzahl von 2 Mio. registrierten Nutzern im Inland anwendbar ist, stellte es offenbar allein auf die Abrufbarkeit oder das Einstellen solcher Inhalte durch Nutzer im Inland ab – vorbehaltlich der internationalen Anwendbarkeit der in § 1 Abs. 3 NetzDG aufgeführten Inhalte. Darüber hinaus stellt § 4 Abs. 3 NetzDG zudem klar, dass eine Bebußung auch dann stattfindet, wenn die Handlung (bzw. Unterlassung) des Betreibers des Netzwerkes nicht im Inland vorgenommen wurde, worunter der Gesetzgeber offenbar den Handlungsort versteht.[65] Das NetzDG findet mithin auf alle Anbieter Anwendung, unabhängig davon ob sie im Inland, in EU-Mitgliedstaaten oder in Drittstaaten niedergelassen sind.

Sofern das NetzDG nunmehr jedoch engere Regelungen vorsieht als das Herkunftsland des Netzwerkanbieters, kollidiert es mit dem in Art. 3 Abs. 1 ECRL normierten Herkunftslandprinzip.[66] Demnach obliegt es zum Zwecke des reibungslosen, elektronischen Dienstleistungsverkehrs im Binnenmarkt allein dem Herkunftsland des Netzwerks sicherzustellen, dass dieses den in diesem Mitgliedsstaat geltenden innerstaatlichen Vorschriften entspricht.[67]

(b) Rechtswidrige Inhalte

Die Pflichten, die das NetzDG den Betreibern sozialer Netzwerke auferlegt, greifen aber nur bezüglich bestimmter strafrechtlicher Delikte ein, die § 1 Abs. 3 NetzDG abschließend aufzählt. Der Katalog des § 1 Abs. 3 NetzDG bezieht sich im Wesentlichen auf Kommunikationsdelikte, aber auch auf Delikte gegen die öffentliche Ordnung, etwa § 130 StGB,[68] und nunmehr auch auf § 201 a StGB und damit der Verletzung des höchstper-

65 Begr. RegE BT-Drs. 18/12356, S. 28.

66 Ausführlich dazu *Spindler*, ZUM 2017, 473, 474; deutliche Zweifel auch bei Wissenschaftlicher Dienst des Deutschen Bundestages, Entwurf eines Netzwerkdurchsetzungsgesetzes – Vereinbarkeit mit dem Herkunftslandprinzip, 29. 5. 2017, PE 6 – 3000 – 32/17; wie hier jetzt auch *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433, 434.

67 Zum Zweck des Herkunftslandprinzips vgl. EuGH Urt. v. 25.10.2011 – C-509/09 Rn. 66 = NJW 2012, 137, 141 – *eDate Advertising*.

68 Zum Eintritt eines Erfolgs im Inland (§ 9 Abs. 1 3.Var. StGB) bei Volksverhetzung auf ausländischem Server: BGH Urt. v. 12.12.2000 – 1 StR 184/00 = ZUM-RD 2001, 103, 107 – *Toeben*; nunmehr durch BGH Urt. v. 3.5.2016 – 3 StR 449/15 = NStZ 2017, 146 aufgegeben; ausführlich zur Diskussion *Schwiddessen*, CR 2017, 443, 447 f.; *Handel*, MMR 2017, 227, 228 f.

sönlichen Lebensbereichs durch Bildaufnahmen. Dadurch, dass der Gesetzgeber explizit nur auf rechtswidrige Inhalte (einschließlich der besonderen Rechtfertigung nach § 193 StGB) abstellt, kommt es nicht darauf an, ob die Delikte auch schuldhaft begangen worden sind.[69]

Inzwischen sieht § 3a NetzDG auch eine verstärkte Zusammenarbeit zwischen den sozialen Netzwerkbetreibern und den Strafverfolgungsbehörden in Gestalt einer Meldepflicht über bestimmte schwerwiegende Delikte vor, die eine gefährliche Wirkung auf das demokratische System und die öffentliche Ordnung haben können, nicht aber etwa die Antragsdelikte; denn bislang erlangten Strafverfolgungsbehörden von den wenigsten Taten auf sozialen Netzwerken Kenntnis.[70] Kritisch wird dazu angemerkt, dass die sozialen Netzwerkbetreiber immer mehr sich in der Rolle von Gehilfen der Strafverfolgungsbehörden befinden.[71]

(c) Berichts- und Organisationspflichten, insbesondere Einrichtung eines Beschwerdemanagementsystems

Einer der Kernpunkte des NetzDG besteht in der Pflicht zur Einrichtung eines wirksamen und transparenten Beschwerdemanagementsystems nach § 3 Abs. 1 S. 1 NetzDG und der Veröffentlichung von diesbezüglichen Berichten gem. § 2 NetzDG.

§ 3 Abs. 4 NetzDG erlegt der „Leitung“ des sozialen Netzwerks eine Pflicht zur ordnungsgemäßen Organisation auf, indem monatliche Kontrollen des Beschwerdemanagements durchgeführt und „organisatorische Unzulänglichkeiten“ im Umgang mit Beschwerden sofort beseitigt werden müssen. Zudem muss wiederum die Leitung des sozialen Netzwerks für die mit dem Beschwerdemanagement betrauten Personen mindestens

69 Begr. RegE BT-Drs. 18/12356, S. 20.

70 Begr. RegE BR-Drs. 87/20, S. 1 f.

71 *Höferlein/Widlok*, MMR 2021, 277, 277 f.; Stellungnahme Direktorenkonferenz der Landesmedienanstalten v. 17.1.2020, S. 4, abrufbar unter https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/011720_Stellungnahme_SchrVors_RefE__Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf; jsessionid=00D54FBFD972118F2BBBFA4664A8D568.2_cid297?__blob=publicationFile&v=2 (zuletzt abgerufen am 4. Mai 2022); Stellungnahme Bitkom v. 17.1.2020, S. 7 f., abrufbar unter https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2020/Downloads/011720_Stellungnahme_Bitkom_RefE__Belaempfung-Rechtsextremismus-Hasskriminalitaet.pdf; jsessionid=00D54FBFD972118F2BBBFA4664A8D568.2_cid297?__blob=publicationFile&v=3 (zuletzt abgerufen am 4. Mai 2022).

halbjährlich deutschsprachige Schulungs- und Betreuungsangebote machen.

Schließlich sollten nach Auffassung des nationalen Gesetzgebers die Berichts- und Organisationspflichten durch Audits und Zertifizierungen flankiert werden, deren Voraussetzungen vom BMJV mit den Beteiligten bis 2018 erarbeitet werden sollten – soweit ersichtlich, sind hier noch keine Ergebnisse vorgetragen worden. Demnach sollen entsprechende Zertifizierungen eine positive Vermutungswirkung für die Bewertung des Beschwerdemanagementsystems entfalten.[72]

Nach § 2 Abs. 1 NetzDG muss halbjährlich in deutscher Sprache über den Umgang mit Beschwerden im Bundesanzeiger sowie (kumulativ) auf der eigenen Homepage berichtet werden. Die im Bericht anzusprechenden Aspekte sind in § 2 Abs. 2 NetzDG näher aufgeschlüsselt und entsprechen quasi spiegelbildlich den materiellen Organisationspflichten, enthalten aber auch die Pflicht zur Angabe, wie viele und welche Beschwerden anhängig waren (§ 2 Abs. 2 Nr. 3 NetzDG). Auch muss der Bericht Angaben über die Löschung oder Sperrung von rechtswidrigen Inhalten innerhalb der jeweiligen Fristen (§ 2 Abs. 2 Nr. 8) sowie einer eventuellen Abgabe an die unabhängige Stelle nach § 3 Abs. 2 Nr. 3 b NetzDG enthalten, § 2 Abs. 2 Nr. 7 NetzDG. Auch müssen nunmehr nach § 1 Abs. 4 NetzDG Berichte über jede (!) Beanstandung eines Inhalts erstattet werden, um zu verhindern, dass die Plattformbetreiber, Beschwerden gegen Gemeinschaftsrichtlinien nicht mit in den anzufertigenden Bericht aufnehmen.[73]

(d) Pflichten zur Löschung und Sperrungen

Teil des Beschwerdemanagementsystems, aber nicht nur rein organisatorischer Natur sind die von § 3 Abs. 2 Nr. 2, 3 NetzDG vorgesehenen Pflichten zur Löschung und Sperrung der von § 1 Abs. 3 NetzDG in Bezug genommenen Inhalte. Diese Pflichten trennen sich auf in die Pflicht zur Löschung offensichtlich rechtswidriger Inhalte innerhalb von 24 Stunden nach Eingang der Beschwerde gem. § 3 Abs. 2 Nr. 2 NetzDG, und anderen rechtswidrigen Inhalten, für die eine Frist von 7 Tagen oder unter bestimmten Bedingungen auch ein längerer, nicht spezifizierter Zeitraum

72 Begr. Rechtsausschuss BT-Drs. 18/13013, S. 18.

73 Begr. FragE BT-Drs. 19/17741, S. 42; *Kalbhenn/Hemmert-Halswick*, MMR 2021, 518, 521; BeckOK InfoMedienR/*Hoven/Gersdorf*, 34. Ed. 1.5.2021, NetzDG § 1 Rn. 48.

gilt. Für die Auslösung der Pflichten ist nach § 3 Abs. 2 Nr. 2, 3 NetzDG nur eine Beschwerde mit konkretem Inhalt geeignet; damit sollen allgemein gehaltene Beschwerden, die den Netzwerkbetreiber nicht in die Lage versetzen, einen konkreten Inhalt zu löschen bzw. zu sperren, aus dem NetzDG ausgenommen werden.[74] Damit erreicht der Gesetzgeber nunmehr einen Gleichklang mit Art. 14 E-Commerce-RL, der ebenfalls nur auf einen konkreten Inhalt bezogen ist;[75] allgemeine Benachrichtigungen eines Providers lösen auch in Art. 14 E-Commerce-RL (bzw. § 10 TMG) keine Pflichten zur Löschung aus.[76]

Die Pflicht zur Löschung offensichtlich rechtswidriger Inhalte ist in mehrfacher Hinsicht problematisch: Denn ist nach wie vor schwer zu beantworten, wann es sich um offensichtlich rechtswidrige Inhalte handelt; wie bekannt, sind gerade Kommunikationsdelikte immer unter Berücksichtigung der Meinungsfreiheit auszulegen und eine praktische Konkordanz der betroffenen Grundrechte herbeizuführen, was nicht selten zu langwierigen Verfahren und völlig unterschiedlichen Entscheidungen der jeweiligen Gerichte führt.[77] Das Gesetz legt letztlich nach wie vor – trotz Nachbesserungen im parlamentarischen Verfahren – das Risiko einer richtigen rechtlichen Beurteilung dem Betreiber des Netzwerkes auf; die Erleichterungen des § 3 Abs. 1 Nr. 3 NetzDG beziehen sich nur auf die nicht-offensichtlich rechtswidrigen Inhalte.

Um Bedenken gegen eine unverhältnismäßige Beeinträchtigung der Meinungsfreiheit, insbesondere des „Overblocking“, Rechnung zu tragen, hat der Gesetzgeber im Rahmen der Novellierung des NetzDG 2021 ein Gegenvorstellungsverfahren eingeführt.[78] Dies folgt grosso modo dem be-

---

74 Begr. Rechtsausschuss BT-Drs. 18/13013, S. 20.

75 S. zur noch im RegE vorhandenen Diskrepanz zu Art. 14 E-Commerce-RL *Spindler*, ZUM 2017, 473, 481.

76 Wohl allg. M., s. dazu etwa BGH Urt. v. 17.8.2011 – I ZR 57/09, K&R 2011, 727 ff. = BGHZ 191, 19, Rn. 28 = GRUR 2011, 1038 – *Stiftparfüm*; Spindler/Schmitz/*Spindler*, 2. Aufl. 2018, TMG § 10 Rn. 24; BeckOK InfoMedienR/*Paal*, 34. Ed. 1.11.2021, TMG § 10 Rn. 40.

77 S. etwa die verschiedenen Caroline -Entscheidungen: BGH Urt. v. 6.3.2007 – VI ZR 51/06, BGHZ 171, 275 = ZUM 2007, 651; BVerfG Beschl. v. 26.2.2008 – 1 BvR 1602/07, BVerfGE 120, 180 = ZUM 2008, 420 – *Caroline von Monaco III*; hingegen EGMR Urt. v. 7.2.2012 – 40660/08, 60641/08, K&R 2012, 179 = ZUM 2012, 551 – *Caroline von Hannover II*.

78 Zu kritischen Anmerkungen in der Literatur vgl. etwa *Peukert*, MMR 2018, 572; *Kettmann*, Stellungnahme zum NetzDG, Ausschuss für Recht und Verbraucherschutz, 15. Mai 2019, abrufbar unter https://www.hans-bredow-institut.de/uploads/media/default/cms/media/up8o1iq_NetzDG-Stellungnahme-Kettemann190515.pdf (zuletzt abgerufen am 11. Oktober 2021).

reits im Bereich der Störerhaftung vom BGH eingeschlagenem Weg bei Blogs, indem der Provider den Blogger nach Eingang einer Beschwerde zur Stellungnahme auffordern muss, umgekehrt der Blogger nach der Stellungnahme seinerseits den Beschwerdeführer zu einer Replik.[79] Allerdings greift dieses Verfahren erst nach der Löschung ein, mithin wird der Inhalt zunächst gelöscht, was den verfassungsrechtlichen Vorgaben des BVerfG[80] kaum entsprechend dürfte, da zum Schutz der Meinungsfreiheit eine vorherige Gelegenheit zur Stellungnahme für erforderlich gehalten wird.[81] Das Gegenvorstellungsverfahren ist nach § 3b Abs. 3 NetzDG nicht auf die Überprüfung von Beschwerden beschränkt, die sich gegen rechtswidrige Inhalte i.S.d. § 1 Abs. 3 NetzDG wenden, sondern soll auch zur Anwendung kommen, wenn mit der Beschwerde die Verletzung von Gemeinschaftsstandards gerügt wird oder im Rahmen einer Content-Moderation eingelegt wurde.[82] Nach der Antragstellung muss der Netzwerkbetreiber der Gegenseite die Möglichkeit zur Stellungnahme binnen einer angemessenen Frist gem. § 3b Abs. 2 Nr. 1 NetzDG geben und den Inhalt dieser Stellungnahme dem Antragsteller übermitteln (§ 3b Abs. 2 Nr. 2 NetzDG). Die daraufhin zu erfolgende Überprüfungsentscheidung durch den Netzwerkanbieter ist schließlich beiden Verfahrensbeteiligten zu übermitteln und bedarf gem. § 3b Abs. 2 Nr. 4 NetzDG einer einzelfallbezogenen Begründung. Die Möglichkeit, den Rechtsweg zu beschreiten, bleibt von diesem plattforminternen Gegenvorstellungsverfahren gem. § 3b Abs. 4 NetzDG unberührt. Dennoch wird der Plattformbetreiber noch stärker in die Rolle eines privaten Richters gedrängt.[83]

Bei Inhalten, die nicht offensichtlich rechtswidrig sind, sieht § 3 Abs. 2 Nr. 3 NetzDG grundsätzlich eine unverzügliche Löschung bzw. Sperrung

79 BGH Urt. v. 25.10.2011 – VI ZR 93/10, K&R 2012, 110 ff. = BGHZ 191, 219 = ZUM-RD 2012, 82 Rn. 27 ff. – *Blog-Eintrag*; zu dem Procedere bei Bewertungsportalen s. BGH Urt. v. 23.9.2014 – VI ZR 358/13, K&R 2014, 802 ff. = BGHZ 202, 242 Rn. 36 = ZUM-RD 2015, 154 – *Ärztebewertung II*; darüber hinaus hat der BGH im Hinblick auf rechtswidrige Inhalte auf Online-Bewertungsportalen einen Auskunftsanspruch des Betroffenen gegen den Portalbetreiber diskutiert, diesen jedoch aufgrund von § 12 Abs. 2 TMG verneint, BGH Urt. v. 1.7.2014 – VI ZR 354/13, BGHZ 201, 380 Rn. 9 ff. = ZUM 2014, 793 – *Ärztebewertung I*; hierzu *Spindler*, in: FS Bamberger 2017, S. 313, 316 ff., 318.

80 BVerfG Beschl. v. 11.4.2018 – 1 BvR 3080/09 = BVerfGE 148, 267, 285 f. – *Stadionverbot*.

81 *Ladeur/Gostomzyk*, K&R 2017, 390, 393; *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433, 435.

82 Vgl. auch *Cornils*, NJW 2021, 2465, 2468.

83 aA: *Kalbhenn/Hemmert-Halswick*, MMR 2020, 518, 520 f.

vor, die aber „in der Regel“ innerhalb von 7 Tagen bewerkstelligt werden soll. Das Gesetz sieht aber auch eine Überschreitung der „Regelfrist“ von 7 Tagen in zwei Fällen vor, einmal nach § 3 Abs. 2 Nr. 3 a) NetzDG wenn die Rechtswidrigkeit von unwahren Tatsachenbehauptungen oder „anderen tatsächlichen Umständen“ abhängt, zum anderen wenn die Beschwerde zur Entscheidung an eine anerkannte Einrichtung der regulierten Selbstregulierung abgegeben wird – was aber nicht für offensichtlich rechtswidrige Inhalte eingreift. Die Notwendigkeit einer komplexen rechtlichen Würdigung vermag daher den Betreiber sozialer Netzwerke nach § 3 Abs. 2 Nr. 3 a) NetzDG nicht zu entlasten – lediglich tatsächliche Umstände bzw. Zweifel sowie die Stellungnahme des Äußernden sind hier fristverlängernd. Der Gesetzgeber will in diesen Fällen aber kein Bußgeld gegen den Netzwerkbetreiber verhängen, wenn sich dessen Einschätzung ex post als falsch herausstellt.[84]

Der Betreiber des Netzwerkes ist an die Entscheidung der Einrichtung, ob zu löschen ist oder nicht, gebunden. Interessanterweise – und in Parallele zum JMStV und der die KJM bindenden Einschätzungsprärogative der Einrichtungen der freiwilligen Selbstkontrolle (der FSM)[85] – gilt die Bindung aber auch gegenüber der Bußgeldbehörde, der es verwehrt ist, zu einer anderen Einschätzung als die Einrichtung zu kommen.[86] Umgekehrt sieht das NetzDG nicht vor, dass die Einrichtung die Annahme der Beschwerde verweigern kann, z. B. bei evident rechtswidrigen Fällen; in Betracht kommt hier aber auch, dass ein Anbieter eines sozialen Netzwerks nicht seinen finanziellen Pflichten aus der Unterhaltung der Einrichtung nachgekommen ist. Da das NetzDG die Ausgestaltung der Rechtsverhältnisse der Einrichtung den Beteiligten überlässt, muss es auch die Möglichkeit der Einrichtung geben, die Überweisung einer Beschwerde zurückzuweisen.

---

84 Begr. Rechtsausschuss BT-Drs. 18/13013, S. 21.

85 Spindler/Schuster/*Erdemir*, Recht der elektronischen Medien, 4. Aufl. 2019, JMStV § 20 Rn. 26 ff.; ferner *Nell*, „Beurteilungsspielraum zugunsten Privater“, 2010, S. 95, 309 ff.; Bornemann/Erdemir/*Bornemann*, 2. Aufl. 2021, JMStV § 20 Rn. 44; *Hopf/Braml*, MMR 2009, 153, 156 f.; zur Parallelvorschrift im Rundfunk (§ 20 Abs. 3): Ausführlich *Prütting*, K&R 2013, 775, 778; *Cole*, ZUM 2005, 462, 469.

86 Begr. Rechtsausschuss BT-Drs. 18/13013, S. 23 spricht hier ausdrücklich von einer Begrenzung des „Einschätzungsspielraums“ der Bußgeldbehörde. Allerdings bleibt unklar, warum die Bußgeldbehörde einen solchen Spielraum genießen sollte, ist doch ihre Entscheidung gerichtlich in Gänze nachprüfbar.

(e) Verfassungsrechtliche Probleme

Sowohl vor als auch mit der Einführung des NetzDG im Jahr 2017 wurden in der Literatur verbreitet verfassungsrechtliche Bedenken gegen das Gesetz geäußert.[87] Dabei standen sowohl Fragen der formellen als auch der materiellen Verfassungsmäßigkeit zur Debatte:

Im Mittelpunkt der Diskussion um die formelle Verfassungsmäßigkeit steht die fehlende Gesetzgebungskompetenz des Bundes, die nach Art. 70 Abs. 1 GG grundsätzlich bei den Ländern liegt. Der Bund darf hingegen nur tätig werden, soweit ihm nach Art. 73, 71 GG die ausschließliche, bzw. nach Art. 74, 72 GG die konkurrierende Gesetzgebungskompetenz zugeschrieben ist. Diese ist allerdings aufgrund der auf Inhalte bezogenen Regulierung zweifelhaft. Die Einordnung des Gesetzgebers im Rahmen des Rechts der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG)[88] kann schon aufgrund der außerordentlichen Bedeutung der Grundrechte des Art. 5 Abs. 1 GG nicht durchgehalten werden.[89] Die Gesetzgebungskompetenz für Regelungen betreffend die Gewährleistung der verfassungsmäßigen Ordnung im Bereich der Telemedien – inklusive der allgemeinen Gesetze – verbleibt damit nach Art. 70 Abs. 1 GG bei den Ländern.[90] Auch der angeführte Jugendschutz aus Art. 74 Abs. 1 Nr. 7 GG vermag nicht zu überzeugen, da die Regelungen des NetzDG weit über den originären Bereich des Jugendschutzes hinausgehen.[91]

Neben den Bedenken bezüglich der Gesetzgebungskompetenz ist weitergehend auch ein Verstoß gegen den Bestimmtheitsgrundsatz in Betracht zu ziehen. Als spezielle Ausformung des Rechtsstaatsprinzips folgt aus Art. 20 Abs. 3 GG, dass gesetzliche Tatbestände derart präzise formuliert sein müssen, dass der jeweilige Normadressat sein Handeln kalkulieren kann, weil

87 *Papier*, NJW 2017, 3025; *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433; *Gersdorf*, MMR 2017, 439; *Liesching*, MMR 2018, 26; *Ladeur/Gostomzyk*, K&R 2017, 390; *Wimmers/Heymann*, AfP 2017, 93; *Spindler*, K&R 2017, 533; *Kalbhenn/Hemmert-Halswick*, MMR 2020, 518; *Nolte*, ZUM 2017, 552; *Heckmann/Wimmers*, CR 2017, 310; *Müller-Franken,* AfP 2018, 1; *Koreng*, GRUR-Prax 2017, 203.

88 Begr. RegE BT-Drs. 18/12356, S. 13.

89 *Liesching*, MMR 2018, 26; *Gersdorf*, MMR 2017, 439, 441; *Hain/Ferreau/Brings-Wiesen*, K&R 2017, 433, 434 f.; *Ladeur/Gostomzyk*, K&R 2017, 390; *Wimmers/Heymann*, AfP 2017, 93, 97; Spindler/Schuster/*Hain*, Recht der elektronischen Medien, 4. Aufl. 2019, Erster Teil, C. Verfassungsrecht, Rn. 164.

90 Ebd.

91 Liesching/*Liesching*, 1. Aufl. 2018, NetzDG Einleitung, Rn. 5; Spindler/Schuster/*Hain*, Recht der elektronischen Medien, 4. Aufl. 2019, Erster Teil, C. Verfassungsrecht, Rn. 164; *Gersdorf*, MMR 2017, 439, 441.

die Folgen der Regelung für ihn voraussehbar und berechenbar sind.[92] Der Bestimmtheitsgrundsatz wird für den Bereich des Strafrechts, der hier aufgrund der Bußgeldvorschriften in § 4 NetzDG eröffnet ist,[93] schließlich in Art. 103 Abs. 2 GG nochmal explizit aufgenommen und verschärft.[94]
In diesem Zusammenhang begegnen verschiedene Begriffe des NetzG Bedenken hinsichtlich der verfassungsrechtlich erforderlichen Bestimmtheit, etwa der „offensichtlich rechtswidrigen Inhalte“ in § 3 Abs. 2 Nr. 2 NetzDG Bedenken. Einerseits die Kenntnis der Dogmatik der Kommunikationsdelikte sowie andererseits deren korrekte Anwendung im Einzelfall kann von den Netzwerkanbietern jedoch kaum erwartet werden.[95] Für den Normadressaten ist folglich nicht kalkulierbar, welche konkreten Pflichten zu erfüllen sind.[96] Gleichermaßen vage und unbestimmt sind auch die Begriffe der „organisatorischen Unzulänglichkeit“ in § 3 Abs. 4 S. 2 NetzDG sowie der „Schulungs- und Betreuungsangebote“ in § 3 Abs. 4 S. 4 NetzDG.

Im Rahmen der materiellen Verfassungsmäßigkeit des NetzDG wird außerdem die Verletzung verschiedener Grundrechte kritisiert, sowohl hinsichtlich der betroffenen Nutzer als auch der Netzwerkbetreiber. Hinsichtlich der Meinungs- und Informationsfreiheit der Nutzer aus Art. 5 Abs. 1 GG greift die Pflicht zur Löschung rechtswidriger Inhalte nach § 3 Abs. 2 NetzDG in die Kommunikationsgrundrechte der Nutzer ein.[97] In diesem Rahmen liegt der Fokus der Kritik darauf, dass die Beurteilung der Rechtswidrigkeit des Inhalts den Netzwerkanbietern und nicht etwa den Gerichten obliegt. Stattdessen liegen „Zweifels-Löschungen“ und sogenannte „Chilling“-Effekte im Sinne einer systematischen Tendenz zur Löschung von Inhalten um Bußgelder zu vermeiden, näher.[98]

Aufseiten der Netzwerkanbieter kommen insbesondere die Verletzung der Berufsfreiheit aus Art. 12 Abs. 1 GG sowie der Eigentumsfreiheit aus Art. 14 Abs. 1 GG in Betracht.[99] Die Einführung der weitreichenden Sperr-

92 BVerfG Beschl. v. 03.03.2004 - 1 BvF 3/92 = BVerfGE 110, 33, 53 f.; Sachs/*Sachs*, 9. Aufl. 2021, GG Art. 20 Rn. 129; BeckOK GG/*Huster/Rux*, 48. Ed. 15.8.2021, GG Art. 20 Rn. 182.
93 *Liesching*, MMR 2018, 26, 27.
94 Sachs/*Degenhart*, 9. Aufl. 2021, GG Art. 103 Rn. 63.
95 *Lüdemann*, MMR 2019, 279, 282; *Ladeur*, in: Eifert/Gostomzyk (Hrsg.), Netzwerkrecht, S. 160, 184.
96 *Liesching*, MMR 2018, 26, 27.
97 *Liesching*, MMR 2018, 26, 27; *Gersdorf*, MMR 2017, 439, 442.
98 *Papier*, NJW 2017, 3025, 3030; *Feldmann*, K&R 2017, 292, 295; *Guggenberger*, ZRP 2017, 98, 100.
99 So auch Begr. RegE BT-Drs. 18/12356, S. 20.

und Löschpflichten sowie die damit erforderliche Beurteilung im rechtlich komplexen Sachgebiet der Meinungsfreiheit unterliegen dem NetzDG nach jedoch keinerlei einschränkenden Maßgaben im Sinne eines Zumutbarkeitskriteriums. Stattdessen obliegt es hier den Anbietern eigenverantwortlich und für den Fall einer „falschen" Beurteilung auch bußgeldbewährt gegen Fakenews und Hassrede im Netz vorzugehen.[100]

(2) Medienstaatsvertrag (MStV)

Verantwortlichkeiten der Intermediäre werden auch durch den neuen MStV geregelt, der seit November 2020 den bis dahin geltenden Rundfunkstaatsvertrag (RStV) ersetzt. Vom Anwendungsbereich werden Rundfunk und Telemedien nun gleichermaßen erfasst, wobei für die verschiedenen Medienakteure jeweils individuelle Pflichtenkataloge vorgesehen sind.

(a) Rundfunk

Für den Rundfunkbereich sieht § 2 Abs. 1 MStV lediglich geringfügige redaktionelle Änderungen am Rundfunkbergriff vor. Damit gilt auch weiterhin jeder lineare Informations- und Kommunikationsdienst als Rundfunk, der an die Allgemeinheit gerichtet und zum zeitgleichen Empfang bestimmter Veranstaltungen und Verbreitung von journalistisch-redaktionell gestalteten Angeboten in Bewegtbild oder Ton entlang eines Sendeplans mittels Telekommunikation bestimmt ist. Mit Blick auf die Einordnung von Live-Streaming Angeboten im Internet, wie etwa dem „BILD Live"-Format[101] oder dem kommentierten Livestream von Online-Games, versucht der MStV mit der Legaldefinition in § 2 Abs. 2 Nr. 2 MStV für Klarheit zu sorgen. Demnach handelt es sich bei einer auf Dauer angelegten, vom Veranstalter bestimmten und vom Nutzer nicht veränderbaren Festle-

100 Vgl. etwa zum einschränkenden Kriterium bei der Störerhaftung BGH Urt. v. 1.3.2016 – VI ZR 34/15, BGHZ 209, 139 = MMR 2016, 418 Rn. 22; BGH Urt. v. 25.10.2011 – VI ZR 93/10, BGHZ 191, 219 = MMR 2012, 124 Rn. 22 mwN; s. auch *Gersdorf*, MMR 2017, 439, 446.

101 S. dazu VG Berlin Urt. v. 26.9.2019 – VG 27 K 365.18 = MMR 2020, 267; zurückhaltender indessen OVG Berlin-Brandenburg Beschl. v. 2.4.2019 – OVG 11 S 72.18 = ZUM-RD 2020, 412.

gung der inhaltlichen und zeitlichen Abfolge von Sendungen um einen Sendeplan.[102]
Doch selbst wenn ein Angebot nach diesen Vorschriften als Rundfunk einzuordnen ist, sieht § 54 Abs. 1 MStV eine Ausnahme von der ansonsten für den privaten Rundfunk bestehenden Zulassungspflicht nach § 52 Abs. 1 S. 1 MStV vor. Private Rundfunkprogramme, die entweder nur eine geringe Bedeutung für die individuelle oder öffentliche Meinungsbildung entfalten (§ 54 Abs. 1 S. 1 Nr. 1 MStV)[103] oder die im Durchschnitt von sechs Monaten weniger als 20.000 gleichzeitige Nutzer erreichen bzw. in ihrer prognostizierten Entwicklung erreichen werden (§ 54 Abs. 1 S. 1 Nr. 2 MStV)[104], sind demnach zulassungsfrei.

(b) Telemedien

Mit den Regulierungen von Medienplattformen, Benutzeroberflächen sowie Medienintermediären betritt der MStV weitgehend Neuland. Im Vergleich zum bisherigen RStV, der lediglich die Begriffe Telemedium und Plattform kannte, wird nun ein erheblich differenzierendes System etabliert:

Gemeinsamer Ausgangspunkt der Definitionen der Medienakteure ist der Begriff des Telemediums, der nach § 1 Abs. 1 S. 3 MStV negativ zu bestimmen ist und alle elektronischen Informations- und Kommunikationsdienste erfasst, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG sind, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, oder telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 1 Abs. 1 S. 1 und 2 MStV sind. In Abgrenzung zum technikbezogenen Telekommunikationsbegriff bildet bei Telemedien somit der Inhalt den Begriffskern.[105] Vom Rundfunk unterscheidet sich das Telemedium außerdem dadurch, dass es sich um einen nicht linearen Dienst handelt, der der Allgemeinheit von Orten und Zeiten ihrer Wahl zugänglich ist.[106]

---

102 BeckOK InfoMedienR/*Martini*, 34. Ed. 1.2.2021, MStV § 2 Rn. 33; *Siara*, MMR 2020, 370, 371.
103 BeckOK InfoMedienR/*Martini*, 34. Ed. 1.2.2021, MStV § 54 Rn. 6 ff.; *Schechinger*, ZUM 2021, 494, 498.
104 BeckOK InfoMedienR/*Martini*, 34. Ed. 1.2.2021, MStV § 54 Rn. 14 ff.; *Schechinger*, ZUM 2021, 494, 498 ff.
105 Vgl. auch *Gerecke/Stark*, GRUR 2021, 816, 816.
106 *Ory*, ZUM 2021, 472, 473 f.

Zentraler Gedanke hinter der Regulierungsbemühungen ist neben der Pluralismus- und Meinungsvielfaltssicherung auch die Sicherung journalistischer Standards bei allen verfügbaren Medienangeboten. Daher müssen Telemedien, die journalistisch-redaktionelle Angebote enthalten und in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden, nach § 19 Abs. 1 MStV den „anerkannten journalistischen Grundsätzen" entsprechen. In Bezug auf politische Werbung trifft die Telemedienanbieter zusätzlich eine Kennzeichnungspflicht der entsprechenden Inhalte, die auch die Benennung des Werbetreibenden oder Auftraggebers erfasst (§ 22 Abs. 1 S. 3 MStV).[107]

Daran anknüpfend ist eine Medienplattform nach § 2 Abs. 2 Nr. 14 MStV jedes Telemedium, soweit es Rundfunk, rundfunkähnliche Telemedien oder Telemedien nach § 19 Abs. 1 MStV zu einem vom Anbieter bestimmten Gesamtangebot (auch mittels einer softwarebasierten Anwendung) zusammenfasst.[108] Dabei kommen sowohl eigene als auch Angebote Dritter in Betracht.[109] Beispielhaft seien hier Dienste wie Apple TV, Netflix und Amazon Prime Video genannt, die ein vom Anbieter zusammengefasstes Gesamtangebot enthalten.[110] Entsprechende Medienakteure unterliegen insbesondere dem in § 82 Abs. 2 MStV statuierten Diskriminierungsverbot bei der Entscheidung über den Zugang zur Medienplattform. Zudem muss die Medienplattform nach § 85 MStV auch die der Sortierung, Anordnung und Präsentation der angebotenen Inhalte zugrunde liegenden Grundsätze gegenüber den Nutzern transparent machen.[111] Gegenüber den Landesmedienanstalten müssen die Medienplattformen schließlich nicht nur die Zugangsbedingungen wie Entgelte und Tarife offenlegen (§ 83 Abs. 1 MStV), sondern nach § 79 Abs. 2 MStV auch den Betrieb der Plattform selber einen Monat vor Inbetriebnahme anzeigen.[112]

Mit dem Medienplattformbegriff eng verbunden sind Benutzeroberflächen, die nach § 2 Abs. 2 Nr. 15 MStV zu Orientierungszwecken textliche,

107 S. dazu auch MStV-Begründung, S. 23.

108 Zur Abgrenzung und zum Begriff des „Gesamtangebots" *Ory*, ZUM 2021, 472, 479; *Siara*, 2020, 523, 523 f.

109 Eine Ausnahme gilt jedoch für ausschließlich eigene Angebote, vgl. § 2 Abs. 2 Nr. 14 S. 3 2. Alt MStV; zu der weiteren Ausnahme s. *Siara*, MMR 2020, 523, 524.

110 Ein anderes Beispiel ist der Dienst Sky Q.

111 Hierzu *Ory*, ZUM 2021, 472, 477 f.

112 Die Anzeigepflicht gilt jedoch nur für die von § 78 S. 1, 2 MStV erfassten Medienplattformen.

bildliche oder akustische vermittelte Übersichten über Angebote oder Inhalte einzelner oder mehrerer Medienplattformen geben und die unmittelbare Ansteuerung von Rundfunk, rundfunkähnlichen Telemedien oder Telemedien nach § 19 Abs. 1 MStV ermöglichen.[113] So ist etwa die Programmübersicht sowie eine Übersicht der zur Verfügung stehenden Diensteanbieter auf dem Bildschirm eines (Smart)-TV als Benutzeroberfläche einzuordnen.[114] Auch die Überblicks- und Auswahlebenen in Mediatheken sind entsprechend einzuordnen. Darüber hinaus sind auch akustische Benutzeroberflächen wie Sprachsteuerungsassistenten (bspw. Apples Siri oder Amazons Alexa) erfasst.
Für Benutzeroberflächen gelten zunächst die zuvor beschrieben Transparenz- und Anzeigepflichten. Weitergehend enthält § 84 MStV gesteigerte Anforderungen an die Auffindbarkeit von Rundfunk, rundfunkähnlichen Telemedien sowie Telemedien nach § 19 Abs. 1 MStV. So dürfen nach § 84 Abs. 2 S. 1 MStV etwa gleichartige Angebote oder Inhalte bei der Auffindbarkeit (insb. Sortierung, Anordnung und Präsentation) nicht ohne sachlichen Grund unterschiedlich behandelt und nicht unbillig behindert werden.[115] Zugunsten des gesamten Rundfunks bestimmt § 84 Abs. 3 S. 1 MStV außerdem, dass dieser auf der ersten Auswahlebene unmittelbar erreichbar und leicht auffindbar sein muss. Vor dem Hintergrund der Vielfalts- bzw. Pluralitätssicherung werden außerdem solche Telemedienangebote des öffentlich-rechtlichen Rundfunks, der Fernsehprogramme i.S.d. § 59 Abs. 4 MStV sowie private Angebote privilegiert, die in einem besonderen Maße einen Beitrag zur Meinungs- und Angebotsvielfalt im Bundesgebiet leisten (§ 84 Abs. 3, 4 MStV). Sie müssen ebenfalls leicht auffindbar sein.

Zuletzt wird in § 2 Abs. 2 Nr. 16 MStV der Begriff des Medienintermediärs eingeführt, der jedes Telemedium erfasst, das auch journalistisch-redaktionelle Angebote Dritter aggregiert, selektiert und allgemein zugänglich präsentiert.[116] Von den Medienplattformen unterscheiden sie sich gerade dadurch, dass sie die verfügbaren Inhalte zu keinem Gesamtangebot zusammenfassen, wobei als Unterscheidungskriterien einzelfallabhängig etwa die Gestaltung, der Inhalt, der Empfängerkreis oder die technische

113 Näher zum Begriff *Ory*, ZUM 2021, 472, 480; *Siara*, 2020, 523, 524.
114 *Siara*, MMR 2020, 523, 524; *Ory*, ZUM 2019, 139, 144.
115 Zu diesen Pflichten näher *Ory*, ZUM 2021, 472, 476.
116 Näher zum Begriff *Siara*, MMR 2020, 523, 525; *Gerecke/Stark*, GRUR 2021, 816, 818.

Struktur herangezogen werden können.[117] Damit unterfallen dieser Definition etwa Dienste wie Facebook, Instagram oder Telegram, soweit die Accounts der Nutzer öffentlich zugänglich sind.[118] Auch YouTube ist dieser Dienstekategorie zuzuordnen, da die Plattform insbesondere kein Gesamtangebot generiert, sondern der Allgemeinheit grundsätzlich jeden Upload ermöglicht.[119]

Als Telemedien müssen auch die Medienintermediäre zunächst den allgemeinen Grundsätzen der §§ 17 ff. MStV entsprechen. Der besondere Pflichtenkatalog ergibt sich sodann aus den §§ 91 ff. MStV. Hiervon werden nach § 91 Abs. 2 MStV zunächst nur solche Medienintermediäre adressiert, die monatlich mehr als eine Millionen Nutzer erreichen oder i.R.e. Prognose erreichen werden, keine Online-Marktplätze sind und nicht ausschließlich privaten oder familiären Zwecken dienen. Zugunsten der effektiven Durchführung eines Ordnungswidrigkeitsverfahrens i.S.v. § 115 MStV müssen diese Medienintermediäre im Inland einen Zustellungsbevollmächtigten benennen, der jedoch auch unternehmensextern bestellt werden kann.[120]

Die für die Medienintermediäre relevanten Transparenzpflichten ergeben sich aus § 93 MStV. Wie bereits von den zuvor beschriebenen Medienakteuren bekannt, sind die Kriterien, die für die Entscheidung über den Zugang eines Inhalts zu und Verbleib dieses Inhalts bei einem Gatekeeper auf der Plattform herangezogen werden, von dem Intermediär leicht wahrnehmbar, unmittelbar erreichbar und ständig verfügbar zu halten. Dieselbe Pflicht besteht außerdem in Bezug auf die Kriterien einer Aggregation, Selektion und Präsentation von Inhalten und deren Gewichtung, wovon auch die grundsätzliche Funktionsweise der verwendeten Algorithmen gehört. Insoweit ist ein Ausgleich zwischen dem Informationsinteresse der Allgemeinheit und dem Geschäftsgeheimnisinteresse der Medienintermediäre zu suchen. Der Umfang der Transparenzpflicht ist somit auf eine grundsätzliche bzw. vereinfachte Darstellung der Funktionsweise der Algorithmen sowie der herangezogenen Kriterien beschränkt. Eine detaillierte Beschreibung des Algorithmus oder die Benennung der Entwickler ist hingegen nicht erforderlich.[121]

---

117 MStV-Begründung, S. 11; ausf. zur Abgrenzung s. *Ory*, ZUM 2021, 472, 478; *Siara*, MMR 2020, 523, 523 f.

118 *Ory*, ZUM 2019, 139, 145.

119 *Ory*, ZUM 2021, 472, 479; *Siara*, MMR 2020, 523, 525.

120 MStV-Begründung, S. 49.

121 MStV-Begründung, S. 50; *Gerecke/Starck*, GRUR 2021, 816, 819.

Darüber hinaus besteht bereits nach § 18 Abs. 3 MStV eine Kennzeichnungspflicht von automatisiert erstellten Inhalten. Diese Verpflichtung wird in § 93 Abs. 4 MStV nochmals aufgegriffen und für Medienintermediäre, die soziale Netzwerke anbieten, explizit für anwendbar erklärt. Die Landesgesetzgeber versuchen damit insbesondere die Problematik um Social Bots zu adressieren, die vor allem bei Diskussionen von politischer sowie gesellschaftlicher Relevanz durch das automatisierte Liken, Teilen und Kommentieren von Inhalten versuchen, den öffentlichen Diskurs zu verzerren.[122]
Abschließend verfolgen auch die Diskriminierungsverbote des § 94 MStV die Leitidee der Meinungsvielfaltssicherung.[123] Dementsprechend dürfen journalistisch-redaktionell gestaltete Angebote, auf deren Wahrnehmbarkeit die Medienintermediäre besonders hohen Einfluss haben, von diesen nicht diskriminiert werden. Eine Diskriminierung liegt bei der systematischen Abweichung von den nach § 93 Abs. 1-3 MStV zu veröffentlichenden Kriterien vor, wenn hierfür kein sachlicher Grund vorliegt. Damit schadet eine auf einen Einzelfall beschränkte Diskriminierung nicht.[124]

Zuletzt führt der MStV den Begriff des Video-Sharing-Dienstes im Umsetzung des Art. 28b AVM-RL ein, bei dem es sich nach § 2 Abs. 2 Nr. 22 MStV um ein Telemedium handelt, das dazu dient, Sendungen mit bewegten Bildern oder nutzergenerierte Videos, für die der Anbieter keine redaktionelle Verantwortung trägt, bereitzustellen. Für entsprechende Dienste gilt ein Dreiklang an Regulierung: Zunächst müssen die allgemeinen Grundsätze der §§ 17 ff. MStV beachtet werden. Daran schließen sich die zuvor skizzierten Regelungen für die einzelnen Medienakteure an, die schließlich in den §§ 97 MStV nochmals verschärft werden.[125] Anbieter von Video-Sharing-Diensten müssen gem. § 98 Abs. 2 MStV sicherstellen, dass die in ihren Diensten vermarktete, verkaufte oder zusammengestellte Werbung den Vorgaben des § 8 Abs. 1, Abs. 3 Satz 1 und 2, Abs. 7 und 10 MStV sowie § 6 Abs. 2, 7 des Jugendmedienschutz-Staatsvertrages entspricht. Die Werbung in den Diensten muss damit etwa als solche leicht erkennbar sowie vom redaktionellen Inhalt unterscheidbar sein und darf keine die Menschenwürde verletzende, diskriminierende oder irreführende Inhalte enthalten.

122 MStV-Begründung, S. 20, 50; *Paal/Heidtke*, ZUM 2020, 230, 231; *Gerecke/Starck*, GRUR 2021, 816, 819.
123 *Ory*, ZUM 2021, 472, 477.
124 *Gerecke/Starck*, GRUR 2021, 816, 820.
125 *Siara*, MMR 2020, 523, 526.

b) Europäische Ansätze und rechtspolitische Vorschläge

(1) AVMD-Richtlinie

Die AVMD-Richtlinie[126] erstreckt ihren Anwendungsbereich auf lineare und nicht-lineare audiovisuelle Mediendienste. Seit der letzten Reform im November 2018 enthält sie außerdem Regelungen für Video-Sharing Dienste, die auf nationaler Ebene überwiegend im MStV sowie teilweise auch im TMG umgesetzt wurden.[127] Die Reform der Richtlinie ist vor dem Hintergrund der zunehmenden Konvergenz der Medien sowie der zwischenzeitlichen Etablierung neuer Medienakteure notwendig geworden.[128] Der Europäische Gesetzgeber verfolgt dabei das Ziel, die Regelungsdichte und -intensität linearer und nicht-linearer Angebote (weiter) anzugleichen.[129] Lineare und nicht-lineare Angebote unterscheiden sich gem. Art. 1 Abs. 1 lit. f, g AVMD-RL durch die Abruf- und Zugriffsmöglichkeiten von Nutzern auf Sendungen bzw. Diensten, die entweder zum zeitgleichen Empfang (lineare audiovisuelle Mediendienste) oder zu einem nutzerseitig frei gewählten Zeitpunkt (nicht-lineare audiovisuelle Mediendienste) bereitgestellt werden. Im Zuge der letzten Reform wurde schließlich mit den Video-Sharing-Diensten in Art. 1 Abs. 1 lit. aa AVMD-RL eine dritte Dienstekategorie eingeführt. Dabei handelt es sich um Dienstleistungen im Sinne der Art. 56 und 57 AEUV, bei der der Hauptzweck der Dienstleistung oder eines trennbaren Teils der Dienstleistung oder eine wesentliche Funktion der Dienstleistung darin besteht, Sendungen oder nutzergenerierte Videos, für die der Video-Sharing-Plattform-Anbieter keine redaktionelle Verantwortung trägt, der Allgemeinheit über elektronische Kommunikationsnetze im Sinne des Art. 2 lit. a der RL/2002/21/EG zur Information, Unterhaltung oder Bildung bereitzustellen, und deren Organisation vom Video-Sharing-Plattform-Anbieter bestimmt wird, auch mit automatischen Mitteln oder Algorithmen. Die fehlende redaktionelle Verantwortung des Vi-

126 Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 14. November 2018 zur Änderung der Richtlinie 2010/13/EU zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) im Hinblick auf sich verändernde Marktgegebenheiten, ABl. 2018, L 303/69.

127 BT-Drs. 17/718, S. 7; *Zurth/Pless*, ZUM 2019, 414, 418.

128 ErwGr 1 AVMD-RL.

129 Hoeren/Sieber/Holznagel/*Holznagel/Hartmann*, Handbuch Multimedia-Recht, 57. EL September 2021, Teil 3, Rn. 30; *Jäger*, ZUM 2019, 477.

deo-Sharing-Anbieters dient damit als zentrales Unterscheidungskriterium zu den zuvor genannten Mediendiensten.

Gegenüber der bis 2018 geltenden Rechtslage ist in Bezug auf die Regulierung audiovisueller Mediendienste insbesondere die in Art. 30 AVMD-RL neu aufgenommene Vorgabe hervorzuheben, dass die Mitgliedsstaaten unabhängige nationale Medienregulierungsanstalten benennen müssen, die rechtlich von Regierungsstellen getrennt sowie funktionell unabhängig von ihren jeweiligen Regulierungen und anderen öffentlichen oder privaten Einrichtungen sein müssen (Art. 30 Abs. 1 AVMD-RL).[130]

Für Video-Sharing-Anbieter ist in Art. 28b AVMD-RL eine Dichotomie an Regelungssträngen vorgesehen: Einerseits sind Minderjährige vor entwicklungsgefährdenden Inhalten (Art. 28b Abs. 1 lit. a AVMD-RL) sowie die Allgemeinheit vor Hass- und Gewaltaufrufen zu schützen (Art. 28b Abs. 1 lit. b AVMD-RL).[131] Andererseits trifft die Dienste auch eine Kennzeichnungspflicht und eine inhaltliche Regulierung von Werbung, Sponsoring und Produktplatzierung (Art. 28 Abs. 2 AVMD-RL).[132] In der praktischen Umsetzung kommen für Inhalte, die der Anbieter nicht selbst vermarktet, verkauft oder zusammengestellt hat, insoweit die Aufnahme entsprechender Klauseln in die Dienste-AGB in Betracht. Ergänzend sollen organisatorische Vorkehrungen wie transparente und nutzerfreundliche Melde- (Art. 28 Abs. 3 lit. b AVMD-RL) und Beschwerdesysteme (Art. 28 Abs. 3 lit. i AVMD-RL) diensteseitig vorgehalten werden. In Bezug auf die Meldesysteme ist die AVMD-RL auch im Kontext der ECRL zu sehen, sodass die an die VSD zu richtenden Pflichten nach einer Meldung eines rechtswidrigen Inhalts nicht über ein notice-and-take-down Verfahren hinaus gehen können.[133]

Die Umsetzung der zuvor genannten Maßnahmen soll nach Art. 28b Abs. 4 AVMD-RL i.V.m. Art. 4a Abs. 1 AVMD-RL mit den Mitteln der Ko- und Selbstregulierung erfolgen, wobei hier die Verhaltenskodizes der Dienste maßgeblich sein werden. Einschränkend sieht jedoch Art. 28b Abs. 6, Art. 4a Abs. 3 AVMD-RL die Möglichkeit vor, dass die Mitgliedsstaaten den VSD-Anbietern schärferer Maßnahmen auferlegen können,

130 Ausf. dazu *Gundel*, ZUM 2019, 131, 136 f.

131 Kritisch mit Blick auf den Umfang der die Diensteanbieter treffenden Pflichten Hoeren/Sieber/Holznagel/*Holznagel/Hartmann*, Handbuch Multimedia-Recht, 57. EL September 2021, Teil 3 Rn. 66.

132 *Jäger*, ZUM 2019, 477; zur Kennzeichnung nutzergenerierter Werbung in sozialen Netzwerken im RStV s. *Zurth/Pless*, ZUM 2019, 414; *dies.* ZUM 2019, 457.

133 ErwGr 48 AVMD-RL; Hoeren/Sieber/Holznagel/*Holznagel/Hartmann*, Handbuch Multimedia-Recht, 57. EL September 2021, Teil 3Rn. 65.

wenn sich insbesondere die Verhaltenskodizes als ungenügend herausgestellt haben.[134]

(2) Der Vorschlag eines EU Digital Services Acts

Vor dem Hintergrund des deutschen NetzDG und vergleichbaren Vorschlägen bzw. Gesetzen in anderen EU-Mitgliedstaaten sowie dem Reformbedarf für die nunmehr fast 20 Jahre alte E-Commerce-RL erklärt sich auch der groß angelegte Vorschlag der EU-Kommission für einen neuen Digital Services Act – der bewusst gerade Risiken durch fake news und Hass-Botschaften und die Rolle der Plattformbetreiber adressiert:

(a) Pflichten und Haftungsprivilegierungen für Host-Provider

Löscht oder blockiert ein Provider einen Inhalt, muss er den betroffenen Nutzer spätestens in diesem Zeitpunkt über die Gründe unterrichten, die den Provider zu dieser Entscheidung bewogen haben, Art. 15 Abs. 1 DSA. Wiederum konkretisiert Art. 15 Abs. 2 DSA die Anforderungen an diese Benachrichtigung des Nutzers, indem u.a. die territoriale Reichweite der Maßnahme anzugeben ist, zudem die Angabe der Tatsachen und Umstände, die der Entscheidung zugrunde liegen, einschließlich der Information darüber, ob die Entscheidung aufgrund einer Beschwerde getroffen wurdes sowie die Unterrichtung darüber, ob automatisierte Verfahren zur Entscheidung und zur Identifizierung der Inhalte verwandt wurden. Im Fall rechtswidriger Inhalte ist zudem die Rechtsgrundlage anzugeben und einer Erklärung, warum der konkrete Inhalt darunterfallen soll, ebenso im Falle des Verstoßes gegen die vertraglichen Nutzungsbedingungen. Schließlich ist über Abhilfemöglichkeiten für den betroffenen Nutzer aufzuklären, sei es durch interne Beschwerdemanagementsysteme, außergerichtliche Streitbeilegungsmöglichkeiten oder gerichtliche Rechtsbehelfe. Gerade in Bezug auf die Möglichkeit, Rechtsschutz nachzusuchen, verlangt Art. 15 Abs. 3, ErwGr 42 DSA, dass die dem Nutzer erteilte Information ihn in die Lage versetzen muss, die in der Information genannten Rechtsbehelfe zu ergreifen.

Gerade diese Pflichten können aber die vertragsrechtlichen Pflichten aus dem Teilnahmevertrag mit den Nutzern konkretisieren und stellen

134 *Gundel*, ZUM 2019, 131, 133.

mindestens gesetzliche Leitbilder, eher sogar zwingende öffentlich-rechtliche Normen dar, die nicht abbedungen werden können.

Dagegen sieht Art. 15 DSA kein rechtliches Gehör für den betroffenen Nutzer vor einer Entscheidung des Providers über die Löschung oder Sperrung des Inhalts vor – was sich indirekt auch aus dem explizit geregelten Verfahren für Online-Plattformen nach Art. 17 DSA ergibt.[135] Ebenso wenig enthält Art. 15 DSA einen unmittelbaren Anspruch des Nutzers auf Wiederherstellung seines Inhalts; insoweit bleibt es beim nationalen Recht, hier vor allem des Vertragsrechts, dass Nutzer ihre Ansprüche auf Wiederherstellung der Inhalte geltend machen können.[136] Allenfalls kann aus Art. 15 Abs. 3 DSA implizit ein solcher Anspruch abgeleitet werden. Ob dies verfassungsrechtlichen Anforderungen standhält, kann hier nicht vertieft werden, kann aber mit Fug und Recht sehr bezweifelt werden.

(b) Erhöhte Pflichten für Online-Plattformen

Eine der zentralen Neuerungen des DSA betrifft erhöhte Pflichten von online-Plattformen gegenüber den „normalen“ Host-Providern; diese richten sich zum einen auf Verschärfungen des Beschwerdemanagements und Berichtspflichten gegenüber Aufsichtsbehörden, ebenso auf die Einrichtung außergerichtlicher Streitschlichtungsmechanismen bis hin zur Einführung von trusted flaggers und Vorkehrungen gegen den Missbrauch von Beschwerden. Online-Plattformen sind nach Art. 2 h) und i) DSA eine Unterkategorie der Host-Provider, die Informationen auf Anforderung durch einen Nutzer an die Öffentlichkeit verbreiten und zugänglich machen, ganz im Sinne der Definition des öffentlichen Zugänglichmachens in Art. 3 Abs. 1 InfoSoc-RL. ErwGr 14 DSA stellt hierzu klar, dass geschlossene Gruppen von Nutzern nicht unter den Begriff der Öffentlichkeit fallen, ebenso wenig die individuelle Kommunikation etwa durch Emails oder

135 S. auch *Rössel*, ITRB 2021, 35, 40.

136 Für Anspruch aus Vertrag sui generis OLG München Urt. v. 7.1.2020 – 18 U 1491/19 Pre = GRUR-RS 2020, 2103 Rn. 61, 117; ähnlich OLG München Beschl. v. 24.8.2018 – 18 W 1294/18 = NJW 2018, 3115, 3116 Rn. 12, 18; OLG Oldenburg Urt. v. 1.7.2019 – 13 W 16/19 = GRUR-RS 2019, 16526 Rn. 7; für Qualifizierung des Anspruchs als Erfüllungsanspruch OLG Düsseldorf Urt. v. 4.12.2020 – 7 U 131/19 = GRUR-RS 2020, 41440 Rn. 23; ähnlich *Beurskens*, NJW 2018, 3418, 3419 f.; zur ähnlichen Diskussion zum NetzDG *Spindler*, CR 2018, 238, 239; *Peukert*, MMR 2018, 572; *Friehe*, NJW 2020, 1697, 1698 f.; *Niggemann*, CR 2020, 326, 329.

Messenger-Dienste, wie sie durch Art. 2 Nr. 4, 5 Elektronische Kommunikationskodex-RL[137] definiert werden. Wie schon zum NetzDG erscheint gerade im Fall von Messenger-Diensten diese Abgrenzung aber mehr als zweifelhaft, etwa bei offenen Telegramm- oder Whatsapp-Gruppen. Zweifelhaft ist auch die in Art. 2 h) DSA vorgesehen Ausnahme, dass untergeordnete Dienste nicht unter die Definition fallen, solange diese nicht der Umgehung des DSA dienen, etwa nach ErwGr 13 DSA die Kommentarfunktion einer elektronischen Presse. Damit könnte aber eine empfindliche Anwendungslücke in der Bekämpfung von hate speech entstehen, da gerade derartige Kommentarfunktionen genutzt werden, um fake news etc. zu verbreiten, zumal die elektronische Presse nicht unter die AVM-RL fällt, ErwGr 28 AVM-RL.

Inwiefern diese Pflichten alle nur öffentlich-rechtlicher Natur sind und keine Auswirkungen auf zivilrechtliche und ggf. auch strafrechtliche Pflichten haben, erscheint offen und kann nur im Hinblick auf die jeweilige Norm beantwortet werden, insbesondere ob sie auch vertragsrechtliche Pflichten konkretisieren oder als Schutzgesetze im Hinblick auf § 823 Abs. 2 BGB qualifiziert werden können, vergleichbar der Diskussion um die finanzmarktrechtlichen Pflichten nach der MiFiD II.[138] Jedenfalls sieht der DSA keine auf die in Kapitel III und IV genannten Pflichten bezogenen Schadensersatzansprüche vor, sondern belässt es vielmehr bei Bußgeldern in Art. 42 DSA.

Online-Plattformen unterliegen demnach gegenüber „normalen" Host-Providern verschärften Anforderungen an Beschwerdemanagementsystemen: Das Beschwerdemanagementsystem nach Art. 17 DSA richtet sich aber im Gegensatz zu dem notice-and-action System nach Art. 14 DSA allein auf Beschwerden von Nutzern, deren Inhalte durch entsprechende Entscheidungen der Online-Plattformbetreiber entfernt oder gesperrt wurden oder deren Zugang zur Plattform bzw. deren Benutzerkonto gesperrt wurde, Art. 17 Abs. 1 DSA. Die Entscheidung über die Beschwerde darf nicht allein durch automatisierte Verfahren getroffen werden, Art. 17 Abs. 5 DSA, aber offenbar mit ihrer Unterstützung. Eigenartigerweise enthält Art. 17 DSA keine Hinweise darauf, dass die betroffenen Dritten in dem Verfahren gehört werden – wie es etwa der EuGH in der UPC Teleka-

137 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung), ABl. L 321 vom 17.12.2018, S. 36-214.

138 Wiederum Langenbucher/Bliesener/Spindler/*Spindler*, Bankenrecht-Kommentar, WpHG § 63 Rn. 8 ff.; *Kasper*, WM 2021, 60; vgl. *Mülbert*, ZHR 172 (2008), 170, 176, 183; MüKoBGB/*Lehmann*, Band 13, Teil 12 A. Rn. 181.

bel-Entscheidung zur Wahrung der Grundrechte der Betroffenen deutlich gefordert hatte, auch wenn diese Entscheidung eine Sperrverfügung gegenüber Access-Provider betraf.[139] Ebenso wenig enthält Art. 17 DSA einen ausdrücklichen Anspruch der Nutzer auf Wiederherstellung der Inhalte.

(i) Streitschlichtungssysteme

Eine der größten Herausforderungen für die Wahrung von Persönlichkeitsrechten auf Online-Plattformen besteht mit Sicherheit in der Gewährleistung effektiven und schnellen Rechtsschutzes.[140] Denn ein Provider ist in aller Regel nicht geeignet, um in die Rolle eines Richters zu schlüpfen, zumal gerade Auseinandersetzungen um rechtswidrige Inhalte bei Persönlichkeitsrechten kaum einer Automatisierung zugänglich sein dürften. Daher ist der Vorschlag des Art. 18 DSA zu begrüßen, der Provider von Online-Plattformen dazu verpflichtet, mit nach Art. 18 Abs. 2 DSA zertifizierten außergerichtlichen Streitschlichtungsstellen zu kooperieren und sich ihren Entscheidungen zu unterwerfen. Allerdings haben nur Nutzer, deren Inhalte nach Art. 17 Abs. 1 DSA blockiert, gelöscht oder deren Benutzerkonten gesperrt wurden, nach Art. 18 Abs. 1 DSA Zugang zu diesen außergerichtlichen Streitschlichtungsstellen (unter denen sie aber auswählen können); warum diese Möglichkeit nicht anderen Betroffenen, z.B. in ihren Persönlichkeitsrechten Verletzten zur Verfügung steht, bleibt unklar.

In zivilrechtlicher Hinsicht ist wiederum fraglich, inwiefern Art. 18 DSA auch die Pflichten aus dem Teilnahmevertrag mit den Nutzern konkretisieren kann – was uneingeschränkt zu bejahen ist, da gerade die Bereitstellung solcher Streitschlichtungsmechanismen essentiell für die Nutzer sein kann, um Abhilfe gegenüber entsprechenden Entscheidungen der Provider zu erhalten. Allerdings stellt sich wiederum die Frage, welche Sanktion zivilrechtlich bei einer Pflichtverletzung offen stünde: Hier kann zwar ein Erfüllungsanspruch theoretisch zur Verfügung stehen, doch steht es nach wie vor im Ermessen des Providers, mit welcher Streitschlichtungsstelle er kooperieren will. Denkbar ist aber auch ein Schadensersatzan-

139 EuGH Urt. v. 27.3.2014 – C-314/12 Rn. 54, 57 = GRUR 2014, 468, 471 – *UPC Telekabel/Constantin Film*; zum rechtlichen Gehör auch *Spindler*, GRUR 2014, 826, 833.

140 S. dazu bereits in diese Richtung *Spindler*, Gutachten F zum 69. Deutschen Juristentag, „Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung“, 2012, S. 56 ff.; ebenso jetzt *Wagner*, GRUR 2020, 447, 455.

spruch durch den Nutzer, der von einer ungerechtfertigten Sperre betroffen ist und erst durch ein gerichtliches Verfahren Rechtsschutz erhält, was schneller durch ein außergerichtliches Verfahren hätte realisiert werden können. In der Praxis wird daher wohl eher die öffentlich-rechtliche Durchsetzung der Normalfall sein.

Hinsichtlich der Anforderungen an die Zertifizierung solcher außergerichtlichen Streitschlichtungsstellen durch den Digitale Dienste Koordinator verlangt Art. 18 Abs. 2 DSA, dass diese unparteiisch und unabhängig vom Plattformbetreiber und von den Nutzern sein müssen, ferner, dass sie über die nötige Expertise in einer oder mehrerer der betroffenen Fragen der rechtswidrigen Inhalte oder der Verletzung der Vertragsbedingungen des Providers verfügen, sowie dass sie einfach elektronisch erreichbar sind, schnell und kosteneffizient in einer der Sprachen der EU-Mitgliedstaaten handeln können und über klare und faire Verfahrensregeln verfügen – ohne dass diese näher von Art. 18 Abs. 2 DSA spezifiziert würden. Der Charakter des nur zugunsten des Nutzers installierten außergerichtlichen Streitschlichtungsverfahrens, das nicht dem Provider selbst offensteht,[141] zeigt sich nicht zuletzt anhand der aus zivilprozessualer Sicht eigenartig anmutenden Kostentragungsregelung des Art. 18 Abs. 3 DSA: So muss der Provider zwar im Falle, dass er unterliegt, die Kosten des Nutzers tragen, aber nicht umgekehrt, wenn der Nutzer unterliegt. Hinsichtlich der Kosten der Streitschlichtungsstelle selbst präzisiert Art. 18 Abs. 3 UAbs. 2 DSA diese nicht weiter, sondern begnügt sich damit, dass diese „vernünftig" sein müssen und nicht die Kosten des Verfahrens selbst übersteigen dürfen. Die zertifizierten Streitschlichtungsstellen müssen vom Digitale Dienste Koordinator an die Kommission übermittelt werden, die eine Liste der verfügbaren Stellen veröffentlicht. Unberührt von diesen Verfahren bleiben die von der Richtlinie 2013/11/EU[142] vorgesehenen alternativen Streitschlichtungsmechanismen für Verbraucher; Art. 18 DSA ist vielmehr für alle Nutzer einer Online-Plattform anwendbar, damit auch für kommerzielle Nutzer, wie z.B. Händler.

141 *Rössel*, ITRB 2021, 35, 40.

142 Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten), ABl. L 165 vom 18.6.2013, S. 63.

(ii) Trusted flaggers

Abweichend von den Regelungen für alle Host-Provider sieht Art. 19 DSA die Einführung eines „trusted flagger“-Verfahrens für Beschwerdeführer vor, die sich in der Vergangenheit als vertrauenswürdig erwiesen haben. Nachrichten bzw. Beschwerden, die von diesen Personen kommen, sollen von den Providern der Online-Plattformen mit Priorität und ohne Verzögerung behandelt werden – allerdings sieht schon Art. 14 DSA vor, dass Nachrichten bzw. Beschwerden ohne Verzögerung bearbeitet werden sollen, so dass sich hieraus eine gewisse zeitliche Hierarchie ergibt. Wer als „trusted flagger“ gelten kann, wird wiederum vom Digitale Dienste Koordinator festgelegt, wobei nach Art. 19 Abs. 2 DSA nur diejenigen Unternehmen („entities“) in Betracht kommen,[143] die über besondere Erfahrung in der Entdeckung, Identifizierung und Benachrichtigung von rechtswidrigen Inhalte verfügen und diese auch zeitnahe und objektiv ausführen, ferner die kollektive Interessen vertreten und unabhängig von jeder Online-Plattform sind. ErwGr 46 S. 3 DSA führt als Beispiele Europol oder nicht-Regierungsorganisationen wie das Netzwerk INHOPE an, das sich um Kindesmissbrauch kümmert. Aber auch im Urheberrecht sollen Verbände oder Organisationen der Industrie und der Rechteinhaber den „trusted flagger“-Status erhalten – was einmal mehr zeigt, dass der DSA hier durchaus Art. 17 DSM-RL flankieren will, obwohl prima vista Art. 1 Abs. 5 c) DSA das Urheberrecht nicht tangieren soll.[144]

Quasi die Kehrseite sind die Pflichten der Provider, um gegen Missbrauch sowohl seitens der Nutzer als auch von Beschwerdeführern vorzugehen. Art. 20 Abs. 1 DSA hält fest, dass Betreiber von Online-Plattformen für eine angemessene Zeit und nach vorheriger Warnung ihre Dienste für Nutzer sperren sollen, die zuvor in erheblicher Weise rechtswidrige Inhalte eingestellt haben. Gleiches gilt nach Art. 20 Abs. 2 DSA für die Behandlung von Beschwerden von Unternehmen bzw. Organisationen („entities“) und Einzelpersonen, die öfters Nachrichten oder Beschwerden eingereicht haben, die offensichtlich unbegründet waren.

---

143 Nach ErwGr 46 S. 2 DSA soll der Status als „trusted flagger“ nicht individuellen Personen zukommen.

144 Zu trusted flaggern unter Art. 17 DSM-RL schon Erklärung der Bundesregierung bei der Abstimmung im Ministerrat vom 15.4.2019, Pkt 8, Interinstitutional File: 2016/0280(COD), 7986/19 ADD 1 REV 2; dazu *Spindler*, CR 2020, 50, 55 Rn. 36 f.; *Spindler*, CR 2019, 277, 286 Rn. 55; *Hofmann*, GRUR 2019, 1219, 1228; *Raue/Steinebach*, ZUM 2020, 355, 363; mit einem eigenen Entwurfsvorschlag *Leistner*, ZUM 2020, 505, 512 ff.

(iii) Mitteilungs- und Publizitätspflichten

Für die Pflichten nach Art. 21 Abs. 1 DSA hat offenbar das deutsche NetzDG Pate gestanden: Denn Art. 21 DSA verpflichtet die Online-Plattform Betreiber zur Mitteilung von Informationen an die Aufsichts- bzw. Strafverfolgungsbehörden,[145] die den Verdacht auf eine erhebliche Straftat mit Gefahr für Leib und Leben nahelegen, insbesondere Straftaten wie sie in der Kinderpornografie-Bekämpfungs-RL[146] aufgeführt werden, ErwGr 48 DSA.[147] Auch die Publizitätspflichten, die für alle Provider bereits nach Art. 13 gelten, werden für Online-Plattformen nochmals durch Art. 23 Abs. 1 DSA ausgeweitet.

(c) Vierte Stufe: Pflichten für besonders große Online-Plattformen

Neben den wesentlich erweiterten Pflichten für Online-Plattformen treten als weiteres Herzstück des DSA die Anforderungen an besonders große Online-Plattformen, für die der DSA an den Begriff der systemischen Risiken anknüpft, wie sie aus der Finanzmarkt-Regulierung bekannt sind (Art. 2 c) Europäischer Ausschuss für Systemrisiken-VO[148]). Denn die besonders großen Online-Plattformen werden als potentielle Verursacher von gesellschaftlichen Risiken und Gatekeeper (ErwGr 56 DSA), insbesondere für die demokratische Meinungsbildung angesehen.[149] Neben den Regelungen zu systemischen Risiken in Art. 25 – 28 DSA, zu denen auch die Pflicht zur Einführung eines Compliance-Beauftragten (Art. 32 DSA) gehört, führt der DSA auch spezielle Anforderungen für Systeme zu Empfeh-

145 Zur Zuständigkeit des jeweiligen Mitgliedstaates s. Art. 21 Abs. 2 DSA.

146 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates, ABl. L 335 vom 17.12.2011, S. 1-14.

147 Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 über die Umweltverträglichkeitsprüfung bei bestimmten öffentlichen und privaten Projekten, Abl. L 26 vom 28.1.2012, S. 1-21.

148 Verordnung (EU) Nr. 1092/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 über die Finanzaufsicht der Europäischen Union auf Makroebene und zur Errichtung eines Europäischen Ausschusses für Systemrisiken, ABl. L 331 vom 15.12.2010, S. 1-11.

149 Umfassend *Bauer*, WRP 2020, 171; *Stark*, MMR 2017, 721; schon *Holznagel*, NordÖR 2011, 205.

lungen oder zur online Werbung ein; ferner werden die Transparenz- und Publizitätspflichten nochmals verschärft, Art. 33 DSA.

Speziell für die auf systemische Risiken ausgerichteten Pflichten des DSA kommt nur die Qualifizierung als öffentlich-rechtliche Pflichten in Betracht, was sich nicht zuletzt in den zahlreichen Ermächtigungsbefugnissen der EU-Kommission sowie der Digitale Dienste Koordinatoren in Art. 23 Abs. 4, 25, 31, 33 Abs. 2, 34 ff DSA äußert. Es handelt sich im Wesentlichen – vergleichbar den finanzmarktrechtlichen Pflichten – um Corporate Governance-Vorschriften, die im Wege der Aufsicht durch Behörden, hier dem Digitale Dienste Koordinator, durchgesetzt werden müssen, und nur in Ausnahmefällen zivilrechtliche Pflichten auslösen.

Art. 25 DSA definiert den Anwendungsbereich besonders großer Online-Plattformen als solche, bei denen monatlich durchschnittlich mindestens 45 Millionen Teilnehmer in der EU aktiv sind. Demgemäß soll es nicht auf die registrierten Nutzer ankommen, sondern nur auf die „aktiven“; vergleichbare Probleme der Berechnung der Nutzerzahl sind auch aus dem NetzDG bekannt.[150]

Nach Art. 26 Abs. 1 DSA haben die Plattformbetreiber zunächst mindestens einmal jährlich die systemischen Risiken durch ihre Plattformen zu analysieren, worunter Art. 26 Abs. 1 S. 2 DSA die Verbreitung rechtswidriger Inhalte versteht, einschließlich des Vertriebs von Piraterie-Produkten (ErwGr 57 S. 1 DSA). Ferner fallen unter die systemischen Risiken negative Auswirkungen auf die Ausübung von Grundrechten hinsichtlich der Meinungs- und Informationsfreiheit, dem Schutz der Privat- und Familiensphäre, der Rechte von Kindern sowie der Verhinderung von Diskriminierung, wobei die Kommission hier vor allem an den Einsatz von Algorithmen durch die Plattformbetreiber oder Dritte denkt, die etwa die Meinungsfreiheit gefährden können (ErwGr 57 S. 5 DSA). Schließlich umfassen die systemischen Risiken Manipulationen der Dienste, einschließlich der automatischen Nutzung der Dienste, die negative Effekte auf den Schutz der öffentlichen Gesundheit, Minderjährige, aber auch auf Wahlen sowie die öffentliche Sicherheit haben können. Damit zielt Art. 26 Abs. 1 DSA neben der Verhinderung von Desinformationskampagnen auch auf Phänomene wie „hate speech“ oder die Beeinflussung von Wahlen ab, wie etwa durch falsche Nutzerkonten, den Einsatz von social bots etc. (ErwGr 57 S. 7 DSA).

150 Spindler/Schmitz/*Liesching*, TMG, § 1 NetzDG Rn. 70; ähnlich schon *Guggenberger*, ZRP 2017, 98; *Spindler*, K&R 2017, 533, 543; dagegen BeckOK InfoMedienR/*Hoven/Gersdorf*, 34. Ed. 1.5.2021, NetzDG § 1 Rn. 30.

Im Rahmen dieser Risikoanalyse müssen die Plattformbetreiber nach Art. 26 Abs. 2 DSA die Auswirkungen ihrer Systeme zur Moderation und zur Empfehlung von Inhalten, einschließlich der Werbung, auf die Verbreitung von rechtswidrigen Inhalten oder solchen, die nicht mit den Vertragsbedingungen der Plattformbetreiber vereinbar sind, berücksichtigen. Aufbauend auf dieser Risikoanalyse müssen die Plattformen Risikomanagementsysteme einrichten, die unter anderem nach Art. 27 Abs. 1 DSA Anpassungen in den Systemen zur Moderation und zur Empfehlung von Inhalten enthalten, ferner Maßnahmen zur Begrenzung von Werbung in Verbindung mit den angebotenen Diensten, die Stärkung der internen Überwachung der Plattformen im Hinblick auf die systemischen Risiken, die Initiierung einer Zusammenarbeit mit „trusted flaggers" nach Art. 19 DSA, bis hin zur Zusammenarbeit mit anderen Online-Plattformen (ohne Beschränkung auf besonders große Online-Plattformen) hinsichtlich der Codes of Conduct (Art. 35 DSA) und Krisenprotokollen nach Art. 37 DSA.

Bei der Erfassung der systemischen Risiken und der Maßnahmen sollen nach ErwGr 59 DSA Repräsentanten von Nutzern und von etwaig betroffenen Gruppen sowie unabhängige Experten und Organisationen der Zivilgesellschaft beteiligt werden – ohne dass der DSA hierfür ein besonderes Format oder gar einen Anspruch dieser genannten Gruppen vorsähe. Deutlich wird aber das Anliegen der EU-Kommission, einen möglichst umfassenden Ansatz für sehr große Online Plattformen vorzusehen, der eben auch die Gefahren für die demokratisch verfassten Ordnungen der EU und der Meinungsfreiheit umfasst – wobei die Balance zwischen den verschiedenen Grundrechten und erfassten Zielen offen bleibt, was wiederum Kritik hinsichtlich der Verlagerung von staatlichen Pflichten auf Private hervorruft.

Ebenfalls aus der Regulierung systemischer Risiken von Finanzmärkten (vgl. Art. 69 Abs. 2 i) MIFID II) ist die Verkoppelung der Pflichten mit regelmäßigen Auditierungen bekannt: So müssen auf Kosten der Provider von besonders großen Plattformen diese mindestens einmal jährlich unabhängige Audits durchführen, um die Erfüllung der Pflichten des gesamten Kapitels III des DSA zu überprüfen, mithin der Pflichten der Provider über diejenigen der Host-Provider und der Online-Plattformen bis hin zu den intensivsten Pflichten nach Art. 26 ff. DSA zum Riskmanagement. Aber auch die Einhaltung von Pflichten auf der Grundlage der Codes of Conduct oder von Krisenprotokollen nach Art. 37 DSA werden vom Audit umfasst. Indes sind die Provider nicht an die Empfehlungen des Audit-Berichts gebunden, indem sie zwar innerhalb eines Monats nach Erhalt des Berichts nach Art. 28 Abs. 4 S. 2 DSA Stellung dazu beziehen müssen, ihnen aber Art. 28 Abs 4 S. 3 DSA erlaubt, die Vorschläge nicht umzusetzen,

was die Provider allerdings begründen und alternative Maßnahmen erläutern müssen.

c) Der Vorschlag für eine KI-Verordnung

KI findet gerade im Bereich von meinungsbildenden Plattformen Einsatz, die bestimmte Inhalte bewerten, sortieren und sie dann entsprechend „zubereitet“ dem Nutzer darbieten (sog. „*content curation*“), so dass das berühmte Phänomen der „*echo chambers*“[151] entsteht. Die Risiken für die Ausübung von Grundrechten im Netz sind daher vielfältig und reichen vom Datenschutz über das Recht der freien Meinungsäußerung bis hin zu möglicher Diskriminierung, etwa durch verzerrte Trainingsdaten. Die *EU-Kommission* verfolgt mit dem Vorschlag einer KI-VO einen *risikobasierten horizontalen Ansatz* im Bereich des Produktsicherheitsrechts, der sich auf den Einsatz von KI generell bezieht und nicht sektorspezifisch (wie etwa in den Produktsicherheitsrechts-Verordnungen oder -Richtlinien) vorgeht. Der Vorschlag der KI-VO soll ausdrücklich zukunftsoffen und in der Lage sein, neue Entwicklungen zu berücksichtigen.[152]

(1) Der grundlegende Ansatz: Risikobasiert mit Regulierung für hoch-riskante KI

Die *EU-Kommission* hat sich unter verschiedenen Möglichkeiten dezidiert für einen *risikobasierten Ansatz* ausgesprochen,[153] der zwingende Regelungen nur für hoch-riskante KI-Systeme enthält, es für andere KI-Systeme aber bei moderaten Pflichten sowie einem *code-of-conduct-Konzept* belässt.[154] Dabei erstreckt der KI-VO-E seinen Anwendungsbereich ausdrück-

151 Grundsätzlich zu „echo chambers“ siehe *Paal/Hennemann*, JZ 2017, 641; instruktiv zu ihrem Entstehen: *Drexl*, „Economic Efficiency Versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics“, 2016, S. 5, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881191_(zuletzt abgerufen am 17. Mai 2021); ausf. zu den mit ihnen verbundenen Gefahren für die Meinungsvielfalt: *Drexl*, ZUM 2017, 529.

152 Explanatory Memorandum, COM(2021) 206 final vom 21.4.2021, S. 3.

153 In diese Richtung bereits *Martini*, „Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz“, 2019, S. 226 ff.

154 Explanatory Memorandum, COM(2021) 206 final vom 21.4.2021, S. 9.

lich auch auf Anbieter bzw. Betreiber mit Sitz außerhalb der EU.[155] Erklärtes Ziel der Regulierung der hoch-riskanten KI ist die Gewährleistung der Grundrechte der betroffenen Nutzer, insbesondere das Recht auf Meinungsfreiheit, die Nichtdiskriminierung sowie die datenschutzrechtlichen Grundrechte.[156] Zentrales Element der Überwachung der Anforderungen an hoch-riskante KI-Systeme ist dabei der produktsicherheitsrechtliche Ansatz der Konformitätsbewertung anhand *technischer Standards*, einhergehend mit einer *Vermutungswirkung*, die aber auch andere Alternativen zulässt, womit die *EU-Kommission* einerseits die nötige Flexibilität gewährleisten, andererseits eine Überlastung der Aufsichtsbehörden verhindern will.[157]

Zur Durchsetzung der Pflichten von hoch-riskanten KI will die *EU-Kommission* eine Registrierungspflicht für sog. *stand-alone KI* und damit eine EU-weite Datenbank schaffen, mit deren Hilfe durch Überwachungsbehörden oder sonstige Dritte die Aktivitäten der KI im Hinblick auf die Einhaltung der Pflichten, insbesondere die Wahrung der betroffenen Grundrechte, überwacht werden können.[158] Gleichzeitig wird damit der Forderung nach einer vorhergehenden öffentlich-rechtlichen Genehmigung[159] eine Absage erteilt.

Flankiert wird dieser Ansatz durch Pflichten der KI-Betreiber, die Überwachungsbehörden über ernsthafte Vorfälle oder Fehlfunktionen der KI mit Gefährdung der Grundrechte zu unterrichten; die entsprechenden Informationen der Überwachungsbehörden sollen dann von der *EU-Kommission* zur Marktanalyse und -bewertung ausgewertet werden.[160]

Für die Definition der hoch-riskanten KI-Anwendungen verwendet der KI-VO-E einen zweifachen Ansatz: zum einen stellt der KI-VO-E auf die Verwendung von KI-Systemen als sicherheitsrelevante Elemente in

155 S. dazu sogleich unter III.C.

156 Explanatory Memorandum, COM(2021) 206 final vom 21.4.2021, S. 11. Das Memorandum führt noch zahlreiche weitere betroffene Grundrechte auf, bis hin zum Umweltschutz.

157 Explanatory Memorandum, COM(2021) 206 final vom 21.4.2021, S. 14.

158 Explanatory Memorandum, COM(2021) 206 final vom 21.4.2021, S. 11.

159 S. dazu etwa Datenethikkommission, „Gutachten der Datenethikkommission der Bundesregierung", 2019, S. 195, 207 f., abrufbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html;jsessionid=FF71C19934371EB93FE4A14E4C67E962.1_cid334?nn=11678504 (zuletzt abgerufen am 17. Mai 2021).

160 Explanatory Memorandum, COM(2021) 206 final vom 21.4.2021, S. 11.

Produkten ab,[161] die dem Produktsicherheitsrecht, insbesondere Konformitätsbewertungsverfahren, unterfallen, und zum anderen für stand-alone KI-Systeme auf einen umfangreichen Annex II.[162] Für beide Fallgruppen kommt es auf die beabsichtigte Verwendung an, nicht nur auf die konkrete Funktion, in der das KI-System verwendet wird.

Die erste Gruppe von produktsicherheitsrechtlichen Anforderungen nach Art. 6 Abs. 1 b) Annex II KI-VO-E zeichnet sich durch ein breites Spektrum von Richtlinien und Verordnungen aus, die allesamt auf dem *New Legislative Framework*, mithin den Konformitätsbewertungsverfahren beruhen, beginnend mit der (ebenfalls überarbeiteten) Maschinen-VO[163] über die Aufzugs-RL[164] bis hin zu den medizinproduktrechtlichen Verordnungen[165]. Daneben werden aber auch KI-Anwendungen als Sicherheitskomponenten in Produktsicherheitsvorschriften, die nicht dem Konformitätsbewertungsverfahren folgen, nach Art. 6 Abs. 1 a), Annex II, Section B KI-VO-E erfasst, darunter vor allem Kfz-Typengenehmigungsverfahren.

Die zweite Gruppe erfasst nach Art. 6 Abs. 2, Annex III KI-VO-E *stand-alone KI-Systeme*, die im Wesentlichen wichtige Sicherheitsaspekte, wie deren Einsatz im Bereich kritischer Infrastrukturen, oder auch Grundrechte betreffen können, wie KI-Systeme zur Bewertung von Schülern und Studen-

---

161 Dies u.a., um zu gewährleisten, dass nur sichere Produkte auf dem Binnenmarkt im Umlauf sind; wobei diese Sicherheit im digitalen Zeitalter auch bezüglich aller digitaler Komponenten wie KI gewährleistet sein soll, vgl. ErwGr 28 KI-VO-E.

162 Für ihre Einstufung als High-Risk-KI ist besonders relevant, ob sie angesichts ihres Verwendungszwecks ein hohes Risiko für die Gesundheit, Sicherheit oder die Grundrechte der Unionsbürger darstellen, wobei sowohl die Schwere des möglichen Schadens als auch die Wahrscheinlichkeit seines Eintretens zu berücksichtigen sind, vgl. ErwGr 32 KI-VO-E.

163 Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG, ABl. Nr. L 157/24 vom 9.6.2006, S. 24-86.

164 Richtlinie 2014/33/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Aufzüge und Sicherheitsbauteile für Aufzüge, ABl. Nr. L 96/251 vom 29.3.2014, S. 251-308.

165 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl. Nr. 117/1 vom 5.5.2017, S. 1-175; Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission, ABl. Nr. L 117/176 vom 5.5.2017, S. 176-332.

ten, zur Auswahl und Beförderung von Arbeitnehmern oder dem Einsatz von *Scoring*-Systemen im Bereich essentieller privater oder öffentlicher Dienste, einschließlich des *Kreditscoring*-Systems (Annex III Nr. 5 b) KI-VO-E). Als hoch-riskante KI-Systeme besonders hervorgehoben werden vom Annex III Nr. 6 KI-VO-E solche Systeme, die im Bereich der strafrechtlichen Rechtspflege und Verfolgung von Straftaten eingesetzt werden, etwa des predictive policing[166], aber auch der Verwendung von KI-Systemen zur Aufdeckung von Straftaten.

(2) Anforderungen an hochriskante KI-Systeme

Der KI-VO-E folgt in seinem risikobasierten, im Produktsicherheitsrecht verankerten Ansatz letztlich ähnlichen Mustern, wie der jüngst vorgelegte Entwurf eines Digital Services Acts zu besonders großen Online-Plattformen oder wie schon früher finanzmarktrechtliche Regulierungen, indem abgestuft nach Risiken Risk- und Qualitätsmanagementsysteme sowie Transparenz- und Publizitätspflichten eingeführt werden. Der produktsicherheitsrechtliche Ansatz schlägt sich auch in den Vermutungswirkungen bei Einhaltung akzeptierter technischer Standards und den entsprechenden Konformitätsbewertungsverfahren nieder, mit denen die *EU-Kommission* hofft, einen flexiblen Ansatz realisieren zu können.

Nach Art. 9 KI-VO-E müssen alle hochriskanten KI-Systeme von einem Riskmanagementsystem flankiert werden, dessen Details durch Art. 9 Abs. 2 KI-VO-E vorgegeben werden. Zu den Elementen zählen nach Art. 9 Abs. 2 S. 2 KI-VO-E die bekannten Bestandteile eines Riskmanagementsystems, wie die Identifizierung und Einschätzung von möglichen Risiken sowie die Festlegung von Maßnahmen. Dabei soll das Riskmanagementsystem auch vorhersehbaren Missbrauch der KI-Systeme ebenso wie Daten aus der Produktbeobachtung nach Art. 61 KI-VO-E über zusätzliche Risiken einbeziehen. Hinsichtlich der erforderlichen Maßnahmen nach Art. 9 Abs. 2 S. 2 d) KI-VO-E macht Art. 9 Abs. 4 S. 1 KI-VO-E deutlich, dass keine hundertprozentige Sicherheit gefordert wird, sondern dass Restrisiken als „akzeptabel" eingestuft werden können. Dies wird durch Art. 9 Abs. 4 S. 3 b) KI-VO-E bekräftigt, wenn ausreichende Kontrollmöglichkeiten für Risiken gefordert werden, die nicht vollständig eliminiert werden können,

166 Zum Predictive Policing siehe *Sommerer*, „Personenbezogenes Predictive Policing, Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose", 2020; *Härtel*, LKV 2019, 49; *Singelnstein*, NStZ 2018, 1.

flankiert durch entsprechende Informationspflichten über solche Risiken und Training für Nutzer, Art. 9 Abs. 4 S. 3 c) KI-VO-E.

Art. 9 Abs. 4 S. 4 KI-VO-E hebt schließlich den Wissens-, Trainings- und Erfahrungshorizont der Nutzer einschließlich der Umgebung, in der die KI eingesetzt werden soll, hervor, um die Risiken zu eliminieren bzw. zu reduzieren. Besonderes Augenmerk schenkt der KI-VO-E zudem dem Testen der KI-Systeme, die nach Art. 9 Abs. 7 KI-VO-E spätestens vor der Markteinführung durchgeführt werden sollten; allerdings beschränkt Art. 9 Abs. 6 KI-VO-E die Testanforderungen auf den beabsichtigten Einsatzbereich der KI – Missbräuche etc. brauchen demnach nicht einbezogen werden.

KI-Systeme bedürfen des Trainings an Daten; daher ist es nicht verwunderlich, dass Art. 10 KI-VO-E sich ausdrücklich mit den Daten als Voraussetzung für KI-Systeme auseinandersetzt, insbesondere der *„Data Governance“*. Dazu gehören nach Art. 10 Abs. 2 KI-VO-E unter anderem die Wahl der Datensätze, der relevanten Annahmen, mögliche Voreinstellungen bzw. Ausrichtungen (*bias*) sowie die Identifizierung von möglichen Datenlücken und -mängeln. Art. 10 Abs. 3 und Abs. 4 KI-VO-E stellen eigentlich selbstverständliche Anforderungen an die Daten auf, wie ihre Repräsentativität, Vollständigkeit und Richtigkeit, ebenso wie die Berücksichtigung von örtlichen oder funktionalen Zusammenhängen, in deren Rahmen die KI-Systeme eingesetzt werden sollen.

Eine zentrale Rolle im gesamten Konzept der *EU-Kommission* spielen dabei die harmonisierten *technischen Standards*, die von der *EU-Kommission* in Auftrag gegeben werden, bei denen der Betreiber aber auch gleichwertige Lösungen entsprechend dem *New Legislative Framework* nachweisen kann, um die Konformität mit den Anforderungen einzuhalten. Damit will die *EU-Kommission* die erforderliche Flexibilität zur Bewältigung der Risiken erreichen, was naturgemäß davon abhängen wird, ob, wann und unter welchen Bedingungen derartige Standards entwickelt werden können.

Bekanntlich zeichnen sich KI-Systeme ferner durch das sog. Black-box-Problem[167] aus, indem die Nachvollziehbarkeit der von der KI erzeugten Ergebnisse unklar bleibt.[168] Um diesem Problem Rechnung zu tragen, ver-

---

167 Die AI High Level Expert Group, “A definition of AI: Main capabilities and scientific disciplines”, 18.12.2018, S. 6 definiert das Problem wie folgt: “The notion of black-box AI refers to such scenarios, where it is not possible to trace back to the reason for certain decisions”.

168 Ebers/Heinze/Krügel/Steinrötter/*Niederée/Nejdl*, Künstliche Intelligenz und Robotik, Rechtshandbuch, 1. Aufl. 2020, § 2 Rn. 123; *Steege*, SVR 2021, 1, 4; *Zech*, ZfPW 2019, 198, 202; *ders.*, DJT 2020 Band I Gutachten, Teil A 11, A 33; *Dett-*

langt Art. 12 Abs. 1 KI-VO-E die Verwendung von Mechanismen zur Nachvollziehbarkeit, sog. *logging devices*. Insbesondere sollen die *logging devices* die Überwachung von Tätigkeiten der KI ermöglichen, aus denen Risiken nach Art. 65 Abs. 1 KI-VO-E resultieren können; auch sollen diese Mechanismen die Produktbeobachtungspflichten erleichtern, Art. 12 Abs 3 KI-VO-E iVm Art. 61 KI-VO-E. Besondere Anforderungen werden schließlich an biometrische Erkennungssysteme gestellt, Art. 12 Abs. 4 KI-VO-E.

Art. 14 KI-VO-E verlangt von hochriskanten KI-Systemen, dass sie ausreichend durch Menschen beaufsichtigt werden können, wenn die KI in Gebrauch ist, wobei die Aufsicht auf die Verhinderung oder Verringerung von Risiken für Gesundheit, Sicherheit oder die Grundrechte ausgerichtet ist und auch vorhersehbarer Missbrauch umfasst wird, Art. 14 Abs. 2 KI-VO-E. Dazu muss das KI-System entsprechende Maßnahmen vorsehen, etwa durch Mensch-Maschine-Schnittstellen, die entweder vom Betreiber von vornherein eingebaut oder für Nutzer zur Implementierung vorgesehen werden müssen. Art. 13 Abs. 4 KI-VO-E präzisiert die Anforderungen, indem verlangt wird, dass der menschliche Aufseher in der Lage sein muss, die Fähigkeiten und Grenzen des KI-Systems zu verstehen und dieses angemessen zu beaufsichtigen, insbesondere auf Fehlfunktionen unverzüglich zu reagieren. Ferner gehört dazu, dass der Mensch sich bewusst sein muss, dass die Gefahr einer *"automation bias"* besteht, mithin Empfehlungen der KI blind zu übernehmen. Auch soll der menschliche Aufseher in die Lage versetzt werden, jederzeit die Ergebnisse der KI-Systeme zu relativieren, ebenso wie den Betrieb der KI zu unterbrechen (panic button).

Art. 15 KI-VO-E verlangt ferner eine ausreichende Sicherheit und Genauigkeit der KI-Systeme. Hinsichtlich der Robustheit der Systeme lässt die KI-VO-E die genauen Anforderungen weitgehend offen, weist aber darauf hin, dass diese durch technische Maßnahmen wie Back-Up-Systeme oder *"fail-safe-plans"* erreicht werden können, Art. 15 Abs. 3 KI-VO-E. Bemerkenswert ist in diesem Zusammenhang, dass Art. 15 Abs. 3 S. 3 KI-VO-E auch die sog. *"feedback loops"* erfasst, in denen das selbstlernende System anhand seiner eigenen Ergebnisse praktisch auf eine Pfadabhängigkeit seiner Bewertungen gelangt; diese sollen durch geeignete Maßnahmen abgemildert (und damit nicht unbedingt verhindert) werden. Bezüglich der Cybersicherheit verlangt Art. 15 Abs. 4 KI-VO-E, dass KI-Systeme gegen Attacken unautorisierter Dritter gesichert sind, wobei auch die Manipula-

---

ling/Krüger, MMR 2019, 211, 212; *Kainer/Förster*, ZfPW 2020, 275, 279; *Linardatos*, ZIP 2019, 504, 504; *Borges*, NJW 2018, 977, 978, der allerdings von „autonomen Systemen" anstelle von „KI" spricht.

tionen von *Trainingsdaten* oder die Verfälschung von Lernmodellen erfasst werden; im Rahmen der Konformitätsbewertungen bezieht die KI-VO-E dabei auch Zertifizierungen nach dem Cybersecurity Act ein, für die dann nach Art. 42 Abs. 2 KI-VO-E ebenfalls eine Vermutungswirkung eingreift.[169]

Art. 13 KI-VO-E enthält schließlich Instruktionspflichten und sieht zunächst in Art 13 Abs. 1 KI-VO-E vor, dass KI-Systeme so zu gestalten sind, dass sie ausreichend transparent sind, damit die Nutzer das System richtig verwenden und die Ergebnisse interpretieren können. Der eigentliche Schwerpunkt liegt indes auf den Instruktionen, die ein KI-System enthalten muss: Neben einer Generalklausel in Art. 13 Abs. 2 KI-VO-E enthält Art. 13 Abs. 3 KI-VO-E einen Katalog an nötigen Instruktionen, die sich vor allem auf den Grad an *Robustheit*, *Genauigkeit* und *Sicherheit*, auf den die KI hin getestet wurde, bezieht, ebenso wie auf Umstände, die darauf Einfluss haben können. Ferner müssen Informationen über Risiken für Gesundheit, Sicherheit oder Beeinträchtigungen von Grundrechten gegeben werden, die durch vorhersehbare Ereignisse im Rahmen des Zwecks der KI oder zu erwartendem Missbrauch eintreten können; bemerkenswert ist hier, dass Art. 13 Abs. 3 b) iii) KI-VO-E nicht zwischen den verschiedenen Grundrechten unterscheidet. Wichtig sind ferner die geforderten Informationen über die *Trainings*-, *Validations*- und *Testdaten*, die für die KI genutzt wurden, Art. 13 Abs. 3 b) v) KI-VO-E; nur so kann der Nutzer ermessen, auf welcher Grundlage die KI tatsächlich trainiert wurde. Schließlich muss auch über die Maßnahmen zur menschlichen Überwachung nach Art. 14 KI-VO-E informiert werden, Art. 13 Abs. 3 d) KI-VO-E.

B. Alternative: Soft Law und Selbstregulierungen?

Wie schon in einigen Rechtsakten anklang, etwa der AVMD-RL, wird oftmals auf Selbstregulierungen[170] und Kodices oder Einrichtungen der

169 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. Nr. L 151/15 vom 7.6.2019, S. 15-69.

170 Ausf. zu den Facetten privater Regelsetzung durch Plattformen s. *Schweitzer*, ZEuP 2019, 1, 4 f.; *Mendelsohn*, MMR 2021, 857, 859 f.; in Bezug auf die (Selbst-) Regulierung von Influencern s. auch *Heins/Lefeldt*, MMR 2021, 126.

„regulierten Selbstregulierung" (etwa im NetzDG) verwiesen, die sich die jeweiligen Branchen geben sollen. Die Vorteile eines solchen Ansatzes liegen auf der Hand, kann doch durch Selbstregulierung kosteneffizient[171] eine wesentlich höhere Akzeptanz[172] der gesetzten Regeln bei den Beteiligten erreicht werden, ebenso wie eine höhere Passgenauigkeit[173], da branchenspezifische Kodices auf die Besonderheiten der Betroffenen Rücksicht nehmen können – im Gegensatz zu einem notwendigerweise auf einer gewissen Abstraktionshöhe angesiedelten Gesetz. Gleichzeitig ist aber die Freiwilligkeit der Kodices ihre „Achillesferse": So wie das Beispiel der von der EU-Kommission 2016 angeregten Selbstverpflichtungserklärungen[174] gegenüber sozialen Netzwerkbetreibern gezeigt hat, die nur eine äußerst geringe Befolgungsquote[175] aufwiesen, hängt es gerade von den Anreizen in einer Branche ab (und ihren aus ihrer Perspektive bestehenden „Widerstandspotentialen" gegenüber staatlichen Regulierungen), ob derartige Kodices eine Chance auf Befolgung haben. So weit unmittelbare marktwirksame Anreize fehlen, etwa in Gestalt einer höheren Kundenzufriedenheit etc., sind die Anreize, derartige Kodices zu befolgen, eher gering oder nur auf die Erwartung angewiesen, damit härtere Eingriffe seitens staatlicher Stellen zu vermeiden.

171 *Buck-Heeb/Dieckmann*, „Selbstregulierung im Privatrecht", 2010, S. 224 ff.; *Hobt*, ZHR 161 (1997), 368, 398; *Lehmann*, GRUR Int. 2006, 123, 128.

172 *Buck-Heeb/Dieckmann*, „Selbstregulierung im Privatrecht", 2010, S. 223; *Brunner*, „Rechtsetzung durch Private: Private Organisationen als Verordnungsgeber", 1982, S. 116 f.; *Lehmann*, GRUR Int. 2006, 123, 125 f.

173 *Buck-Heeb/Dieckmann*, „Selbstregulierung im Privatrecht", 2010, S. 222 f.; *Eidenmüller*, ZGE 2007, 484, 488 f.; *Voegeli-Wenzl*, GRUR Int. 2007, 807, 812; aA. *Kirchhof*, ZGR 2000, 681, 689, der darauf abstellt, dass den Parlamenten als legitimierten Gesetzgeber entsprechendes Fachwissen zugänglich wäre.

174 „The EU Code of Conduct on countering illegal hate speech online", abrufbar unter https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (zuletzt abgerufen am 20. Dezember 2021).

175 Begr. RegE BT-Drs. 18/12356, S. 1 f., 11; S. auch den aktuellen Report von Jugendschutz.net, abrufbar unter https://www.jugendschutz.net/fileadmin/daten/publikationen/praxisinfos_reports/report_hate_speech_ein_europaeischer_vergleich.pdf (zuletzt abgerufen am 20. Dezember 2021); *Hoffmann-Riem*, AöR 142 (2017), 1, 39; *Wagner*, GRUR 2020, 329, 332; *ders.*, GRUR 2020, 447, 452.

V. Vor- und Nachteile der verschiedenen Ansätze zur Regulierung

Zivilrechtliche Regulierungen setzen auf individuelle Anreize durch Klagen von Geschädigten, teilweise modifiziert durch die Möglichkeit von Verbands- und Sammelklagen. Allerdings sind diese Anreize bei sog. „small claims“, also geringfügigen Ansprüchen angesichts der prohibitiv hohen Kosten, um eine Klage einzureichen, eher gering, so dass gerade selbst bei massenhaften Verstößen „kleinerer Natur“ sich kaum ein Kläger finden wird, für den es sich lohnen würde, einen Schädiger vor Gericht zu bringen.[176] Zwar kann diesem Phänomen teilweise durch Sammelklagen oder Verbandsklagen Rechnung getragen werden, doch unterliegen auch Verbände wiederum ihren eigenen Anreizen, indem sie primär publikumswirksame Verfahren anstoßen werden.[177]

Zudem setzen zivilrechtliche Regulierungen immer auf die individuelle Schädigung des „Betroffenen“; oftmals beziehen sich aber Risiken für demokratische Prozesse und die Meinungsbildung auf Vorgänge, die nicht mit einer individuellen Schädigung einhergehen, sondern kollektive Interessen betreffen, etwa bei der Verbreitung von „fake news“ oder der Kuratierung von Inhalten und Meinungen mit Hilfe von KI-Systemen.

Hier vermögen grundsätzlich nur öffentlich-rechtliche Regulierungen Abhilfe zu schaffen, die eben keine individuelle Schädigung bzw. Aktion voraussetzen, sondern vielmehr quasi aus einer Makroperspektive systemische Risiken zum Gegenstand haben. Auch ist es dann nicht erforderlich, zunächst eine (drohende) Schädigung abzuwarten; vielmehr greift die öffentlich-rechtliche Regulierung schon im Vorfeld quasi „pro-aktiv“ ein und kann Missständen vorbeugend entgegenwirken.

Öffentlich-rechtliche (und auch strafrechtliche) Ansätze leiden dagegen vor allem unter dem Manko des nötigen Personaleinsatzes und der nur beschränkt verfügbaren Ressourcen, so dass die Wahrscheinlichkeit einer engmaschigen Überwachung entsprechend gering ausfällt. So ist etwa kaum anzunehmen, dass eine Aufsichtsbehörde ohne ein entsprechend sehr hohes Budget in der Lage sein wird, komplexe Algorithmen, erst recht gar selbst lernende KI-Systeme mit Hilfe von geeigneten Fachpersonal wird untersuchen können, wenn dieses ein Vielfaches an Gehalt auf der „Gegenseite“ geboten bekommt. Dieses Phänomen ist etwa aus der

176 BeckOK ZPO/*Lutz*, 42. Ed. 1.9.2021, ZPO § 606 Rn. 5.1; *Schaub*, JZ 2011, 13, 14 f.; *Weber*, VuR 2013, 323, 325; *Balke/Liebscher/Steinbrück*, ZIP 2018, 1321, 1323; *Gsell*, BKR 2021, 521, 522 f.

177 *Koch*, JZ 2011, 438, 442 f.; *Koch*, WuW 2013, 1059, 1069; *Stadler*, JZ 2018, 793, 801 f.

Finanzmarktbranche als Asymmetrie zwischen Finanzaufsichtsbehörden und Finanzmarktteilnehmern hinlänglich bekannt.[178]

Einher damit geht die Gefahr, dass eine Behörde „politisch gefangen" genommen wird (capture of agency-Theorie[179]), in dem Sinne, dass sie nur besonders öffentlichkeitswirksame Fragen bzw. Verfahren betreiben wird.

VI. Fazit

Das Bild der Verantwortlichkeit von Informations-Intermediären hat sich in den letzten zehn Jahren fundamental verändert: Standen zunächst noch die weitgehende Befreiung von jeder Verantwortlichkeit für Plattformen im Vordergrund, hat sich die Einstellung der Gesetzgeber gegenüber den Intermediären dahingehend entwickelt, dass diese als Gatekeeper und Schlüsselinstanzen in der Meinungsbildung wesentlich stärker in die Pflicht genommen werden. Ausdruck dieser neuen Regulierungsansätze sind aus nationaler Sicht das NetzDG und aus europäischer Sicht der Digital Services Act. Beiden Ansätzen ist gemein, dass sie auf die Bewältigung systemischer Risiken abzielen. Allerdings wird dies nicht allein durch das öffentliche Recht bzw. Aufsichtsbehörden gelingen, da diese nur punktuell Pflichten der Plattformbetreiber durchsetzen können; vielmehr bedarf es eines Steuerungsmix aus öffentlich-rechtlichen und zivilrechtlichen Instrumentarien, für die die Rechtsprechung bereits erste Ansätze bereitgestellt hat. In dieser Hinsicht bedürfen die europäischen Vorschläge des Digital Services Act und des AI Acts noch der zivilrechtlichen Ergänzung, auch wenn sie prinzipiell in die richtige Richtung weisen.

178 *Baur/Boegl*, BKR 2011, 177, 186; *Volz*, VW 2020, 74, 75; *Langenbucher*, EuZW 2020, 681, 682.

179 *Livermore/Revesz*, "Regulatory Review, Capture, and Agency Inaction", Georgetown Law Journal, Band 101 (2013), 1337; *Rose/Walker*, "Dodd-Frank Regulators, Cost-Benefit Analysis, and Agency Capture", Stanford Law Review Online, Band 66 (2013), 9.

Big Data in einer digitalisierten, datengestützten Demokratie

Ruben Bach, Frauke Kreuter

1. Einleitung

Big Data und die daraus gewonnen Informationen wirken in weite Teile moderner Demokratien hinein. Anbieter großer Internetplattformen nutzen Daten oder Datenspuren ihrer Mitglieder, um Informationsströme zu optimieren (Foster et al. 2020). Politische Entscheidungsträger nutzen Daten, um gesellschaftliche Prozesse besser zu steuern, sei das bei der Bekämpfung von Kriminalität (Lynch 2018), bei der Verbesserung der Gesundheitsversorgung (Pan et al. 2017) oder in der modernen Stadtplanung (Glaeser 2019), um nur ein paar Beispiele zu nennen. Parteien, Politikerinnen und Politiker nutzen Daten, um den Erfolg ihrer Wahlkampagnen zu maximieren (Nickerson und Rogers 2014).

Die Nutzung von Daten in diesen Kontexten ist nicht neu. Was sich verändert sind die Datentypen, die für diese Aktivitäten verwendet werden und die Art und Weise, wie sie verwendet werden. Traditionelle Datenquellen, wie ein Zensus der Bevölkerung oder andere groß aufgesetzte Bevölkerungsbefragungen, erscheinen oft zu langsam in einer Welt, in der Entscheidungen schnell getroffen werden müssen und sich soziale Gegebenheiten schnell ändern (Lane 2020). Immer häufiger werden deshalb sogenannte digitale Datenspuren verwendet.[1]

Als digitale Datenspuren werden Daten bezeichnet, die sich aus der Interaktion von Individuen mit digitalen Geräten oder Online-Informationssystemen ergeben (Howison et al. 2011, S. 769). Dazu gehören Transaktionsdaten von Zahlungssystemen, Telekommunikationsnetzen, Webseiten, Smartphone-Apps und Sensoren (Stier et al. 2020). Die Begeisterung für digitale Datenspuren rührt vor allem von der Feinkörnigkeit der Daten her, die es ermöglichen, individuelle und soziale Verhaltensweisen und Verhaltensänderungen in hoher Frequenz und in Echtzeit zu beobachten. Darüber hinaus handelt es sich um nicht-teilnehmende Messungen, d.h. die

1 Einen Überblick über digitale Datenspuren liefern Keusch und Kreuter (2021), wir verwenden in diesem Beitrag einige der dort präsentierten Materialien.

Datenerhebung erfolgt, ohne dass die beobachtete Person aktiv dazu etwas beitragen muss.[2]

In diesem Beitrag zeichnen wir nach, wo digitale Datenspuren entstehen, wenn sich Nutzerinnen und Nutzer im Internet und auf sozialen Medien bewegen und wie diese verarbeitet und genutzt werden, um Inhalte gezielt und personalisiert zu verbreiten und zu bewerben. Ein grundlegendes Verständnis der Funktionsweise und der Prozesse um die Erhebung und Nutzung von digitalen Datenspuren ist notwendig, um aktuelle politische und soziale Entwicklungen etwa zur Personalisierung von Inhalten verschiedener Art nachvollziehen und kritisch beurteilen zu können. Als praktisches Beispiel der Nutzung digitaler Verhaltensspuren wollen wir dabei einen Blick auf die gezielte Ansprache von Bürgerinnen und Bürgern mittels politischem Microtargeting werfen. Die hier diskutierten Datenquellen können selbstverständlich auch in anderen Kontexten verwendet werden.

2. *Politisches Microtargeting*

Das wohl bekannteste Beispiel der Nutzung digitaler Verhaltensdaten ist für Werbezwecke mittels *Microtargeting*, d.h. der zielgruppenbasierten Ansprache etwa auf Webseiten oder auf Social Media Plattformen wie Facebook, Instagram, Twitter und TikTok.[3] Ziele hierbei sind zum Beispiel, Werbung passgenau denjenigen Personen oder Gruppen von Personen auszuspielen, für die ein Produkt entworfen wurde, bei denen eine hohe Kaufbereitschaft vermutet wird, die eine große Reichweite besitzen, um ein Produkt in ihren Netzwerken weiter zu verbreiten, oder bei denen der größte Absatz erwartet wird. Zunehmend etabliert sich Microtargeting aber auch im politischen Raum. Politisches Microtargeting bezeichnet die Segmentierung von Personen in immer feiner definierte Gruppen anhand von Interessen, Präferenzen und Verhaltensweisen, die beispielsweise aus den digitalen Verhaltensspuren der Individuen abgeleitet werden (Kruschinski und Haller 2017). Diese Gruppen können dann mit speziell auf sie zugeschnittenen Inhalten gezielt angesprochen werden.

Leitgedanke des politischen Microtargetings ist zum einen, dass Ressourcen wie Wahlkampfmittel effizient eingesetzt werden, etwa indem politische Werbung verstärkt an die Personen ausgespielt wird, bei denen

2 Von informierter Einwilligung einmal abgesehen, dazu kommen wir später.
3 Siehe hierzu auch den Beitrag von Kelber und Leopold in diesem Sammelband.

noch keine gefestigte Wahlabsicht vermutet wird (Nickerson und Rogers 2014; Kruschinski und Haller 2017). Zum anderen können Inhalte effektiv eingesetzt werden, das heißt, dass diese an die Zusammensetzung der Zielgruppe angepasst werden, in der Hoffnung so eine größere Wirkung zu erzielen als mit allgemein gehaltenen Inhalten. Beispielsweise könnten Zielgruppen, die vor allem junge Familien beinhalten, mit Inhalten zu Familien- und Bildungspolitik beworben werden, während Zielgruppen, die primär aus Rentnerinnen und Rentnern bestehen, verstärkt mit Inhalten zum Ausbau der Rentenversorgung angesprochen werden. Die Hoffnung hier ist, dass speziell auf einzelne Individuen oder Gruppen von Individuen mit ähnlichen Eigenschaften zugeschnittene Inhalte (etwa Wahlwerbung für die eigene Partei) deutlich effektiver sind als allgemeine Maßnahmen (Nickerson und Rogers 2014). Darauf basierend, entwickeln Datenanalystinnen und Datenanalysten mithilfe digitaler Verhaltensdaten und neuer Analyseverfahren immer detailliertere Werkzeuge zur Segmentierung von Individuen in einzelne Gruppen.

Insgesamt ist die gezielte Ansprache von (potentiellen) Wählerinnen und Wählern in Deutschland zwar noch weit weniger verbreitet als etwa in den USA. Allerdings lässt sich auch für Deutschland beobachten, dass insbesondere der Einsatz von digitalen Verhaltensspuren stetig zunimmt (Jungherr 2016). Insbesondere Social Media Plattformen wie Instagram, TikTok, Facebook und andere stellen hierfür ideale Bedingungen bereit, da ihre algorithmen- und datengetriebenen Businessmodelle auf die zielgenaue und personalisierte Ansprache ihrer Nutzerinnen und Nutzer ausgerichtet sind (Kruschinski und Bene 2021).[4]

Zu den führenden Plattformen, auf denen in Deutschland (politische) Werbung im Internet geschaltet wird, gehören YouTube, Facebook und Instagram (Kemp 2021). Die Nutzungshäufigkeit dieser Plattformen unterscheidet sich zwischen einzelnen Bevölkerungsgruppen deutlich. Das heißt auch, dass auf verschiedenen Plattformen verschiedene Bevölkerungsgruppen erreicht werden. Zudem verschiebt sich die Popularität der Plattformen regelmäßig mit der Entwicklung neuer Technologien (Beisch und Schäfer 2020). So spielen etwa insbesondere für jüngere Erwachsene Plattformen wie TikTok, Snapchat und Twitch eine deutlich größere Rolle als für ältere Generationen. Ebenso verschieben sich die selbst auferlegten Regeln einzelner Plattformen zur Schaltung politischer Werbung. Beispielsweise ist derzeit (2021) Werbung zu politischen Zwecken auf Twitter nicht

4 Siehe hierzu auch den Beitrag von Djeffal in diesem Sammelband.

mehr erlaubt (Twitter ohne Datum)[5]. Google hingegen erlaubt politische Werbung als kontextuelle Werbung, d.h. zum Beispiel im Zusammenhang mit thematisch ähnlichen Videos auf YouTube. Ebenso möglich ist das Targeting von Personengruppen aufgrund von Alter, Geschlecht und Region mit politischer Werbung bei Google (Google 2019). Ohne größere Einschränkungen hinsichtlich der Targetingmerkmale ist politisches Microtargeting derzeit bei Facebook[6] möglich, wobei sich dies auch in naher Zukunft ändern soll (Bovermann 2021). Aufgrund der stetigen Veränderungen erläutern wir die Nutzung von digitalen Verhaltensdaten zum Zweck von Microtargeting deshalb weitestgehend unabhängig von einer bestimmten Plattform und bringen nur gelegentlich Beispiele, die sich auf einzelne Plattformen beziehen. Die Sammlung und Auswertung von digitalen Verhaltensdaten für zielgruppengenaue Werbe- und Personalisierungszwecke ist generell weit verbreitet und kann im Prinzip auf jeder Webseite, nicht nur in sozialen Medien, vorgenommen werden.

3. Daten

Die für die Entwicklung und Anwendung der für Algorithmen notwendigen digitalen Verhaltensdaten stammen in der Regel entweder von den Plattformen selbst (*Plattform-Online-Daten*), oder werden über Trackingnetzwerke erhoben (*Off-Plattform-Online-Daten*). Mitunter werden auch Offline-Daten hinzugezogen, die wir hier nur am Rande streifen.

3.1. Plattform-Online-Daten

Unter Plattform-Online-Daten verstehen wir hier alle Daten, die Nutzerinnen und Nutzer in ihrer Interaktion mit der Plattform erzeugen oder angeben. Dazu gehören etwa soziodemographische Informationen, die bei einer Registrierung angegeben werden. Verpflichtend ist bei vielen Plattformen eine Altersangabe, etwa um Volljährigkeit festzustellen oder um Kinder von der Nutzung auszuschließen. Freiwillige Angaben umfassen je nach Ausrichtung der Plattform z.B. Bildungsabschlüsse, Beziehungsstatus,

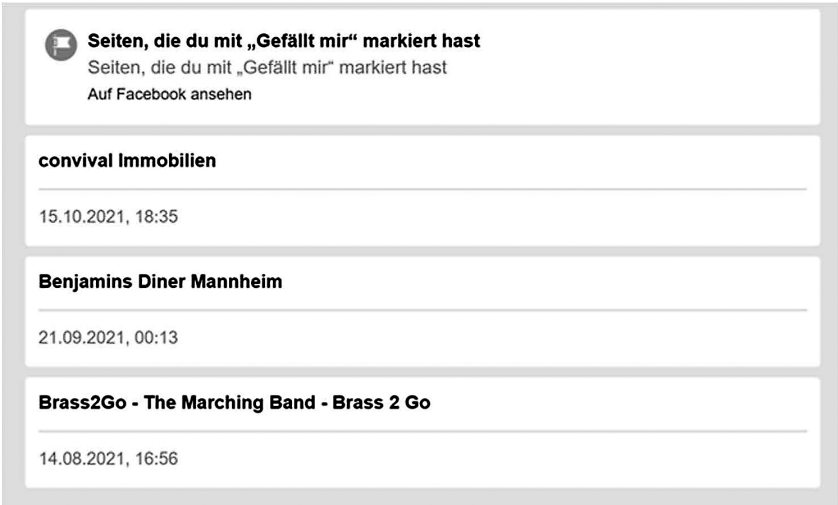
5 Das bedeutet allerdings nicht, dass Politikerinnen und Politiker und ihre Parteien nicht mit Accounts auf Twitter vertreten sein können.

6 Wir sprechen hier von der Plattform Facebook als ein Beispiel und nicht über alle Angebote des jetzt in Meta umbenannten Unternehmens.

Geschlecht oder Informationen zum Arbeitgeber. Der Füllgrad dieser Variablen, d.h., die Anzahl der Personen, die diese Merkmale angeben, ist typischerweise eher gering (Salganik 2018, S. 24). Auch geografische Merkmale, die mit Erlaubnis der Nutzerinnen und Nutzer zu Fotos, Tweets oder Posts hinzugefügt werden, fehlen häufig. Rieder und Kühne (2018, S. 427) sprechen in ihrer Literaturübersicht beispielsweise von etwa 20% geo-getaggter Fotos auf Instagram, 10% geo-getaggten Tweets auf Twitter und etwa 10% mit Ortsangaben markierten Fotos auf Facebook.

Eher verfügbar, weil sie direkt aus der Interaktion mit der Plattform entstehen, sind Informationen zu Interaktionen mit anderen Nutzerinnen und Nutzern und deren Inhalten. Hierzu gehören Likes, Retweets, das Teilen von eigenen Inhalten, besuchte Events und Gruppenmitgliedschaften, sowie Informationen über die mit einem "Gefällt mir" versehenen oder geteilten Inhalte selbst, aber auch Interaktionen mit Unternehmensseiten und deren Produkten wie etwa Bewertungen. Auch Datum und Uhrzeit des Logins auf die Plattform können gespeichert werden. Außerdem können Informationen zum Besuch einer Seite (innerhalb von z.B. Facebook) gemeinsam mit Datum und Uhrzeit abgespeichert und über diese Merkmale mit anderen Aktivitäten zum gleichen oder ähnlichen Zeitpunkten verlinkt werden. Wie Abbildung 1 zeigt, lassen sich aus den reinen Besuchs- und Aktivitätsdaten zunächst nur sehr wenig Informationen direkt ableiten.

Abb 1. Beispieldaten von Facebook-Seiten, die mit "Gefällt mir" markiert wurden



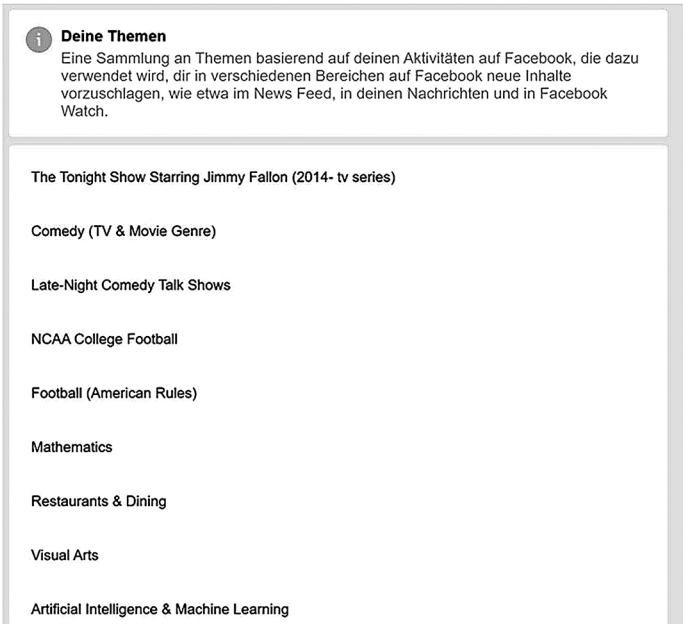
Weitere wichtige Informationen lassen sich beispielsweise über den *user agent string* auslesen, den Nutzerinnen und Nutzer beim Aufrufen einer Webseite an den Server, der die Webseite hostet, übermitteln. Das können etwa Informationen über den genutzten Browser, das Betriebssystem, den Hersteller des Computers, den Typ des digitalen Endgeräts (PC, Smartphone, Tablet) und weitere im Browser installierte Software sein (siehe Abb. 2). Auch die IP-Adresse eines Endgeräts wird beim Besuch einer Webseite übermittelt. Über diese lassen sich Rückschlüsse auf die geografische Region ziehen, an dem sich ein Gerät und somit die das Gerät nutzende Person aufhalten. Informationen zum Betriebssystem, der Bildschirmgröße etc. werden genutzt, um zu steuern, wie die Informationen auf dem Browser angezeigt werden, z.B. ob eine für mobile Endgeräte freundliche Version der Webseite angezeigt werden muss. Forscherinnen und Forscher oder Organisationen, die Werbung schalten wollen, können Informationen über das Betriebssystem mitunter als Proxy für den sozio-ökonomischen Status der Nutzerinnen und Nutzer verwenden.

Abb 2. Beispiel eines User-Agent String

```
Your user agent: Mozilla/5.0 (iPhone; CPU iPhone OS
14_8 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1
Other HTTP headers
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Encoding: gzip, deflate, br
Accept-Language: en-us
Host: duckduckgo.com
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_8
like Mac OS X) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1
```

Durch die Häufung von bestimmten besuchten Seiten oder die Korrelation der Häufigkeit mehrerer besuchter Seiten lassen sich thematische Präferenzen zusammenfassen. Besucht z.B. jemand innerhalb von Facebook Seiten von Restaurants, kann Dining als interessierendes Thema abgelegt werden (Abb. 3). Aufwendigere statistische Verfahren erlauben die Bildung von sogenannten Clustern ähnlicher Themen. Hierzu werden Seiten anhand möglichst vieler Merkmale kodiert (Kleidung, Art der Kleidung, Preis der Kleidung, Designerkleidung etc.) und anhand statistisch geschätzter Ähnlichkeiten andere Seiten oder Themen gefunden, die interessant sein könnten.

Abb 3. Beispielliste für eine Person auf Facebook ermittelte Themen



Ähnlich zu der Gruppierung von Seiten lassen sich auch Nutzer und Nutzerinnen anhand beobachteter Daten mittels Clustering, einem Verfahren des sogenannten *unsupervised machine learnings* in Gruppen einteilen. Ziel hierbei ist es, Cluster von Personen zu bilden, sodass die Individuen innerhalb eines Clusters möglichst ähnlich sind, zwischen den Clustern jedoch möglichst verschieden. Als Ähnlichkeitsmerkmale könnten alle oben genannten Informationen wie Alter, Einkommen, Weltanschauung aber auch Social Media Aktivität, Interessen und Präferenzen genutzt werden. Die Inhalte können dann spezifisch auf die Personen in einem Cluster zugeschnitten werden. Ein bekanntes Beispiel aus der Markt- und Sozialforschung für unsupervised machine learning sind die Sinus Milieus. Diese fassen Menschen mit ähnlichen Wertvorstellungen und einer vergleichbaren sozialen Lage in zehn Cluster, sogenannte Milieus, zusammen (Flaig und Barth 2018). Die resultierenden Milieus sind sowohl durch soziale Lage (Unterschicht bis Oberschicht) als auch Grundorientierung (Tradition bis Neuorientierung) definiert.

Fehlen für manche Nutzerinnen und Nutzer Informationen, die bei anderen vorhanden sind, so lassen diese sich mit Techniken wie dem *supervised machine learning* ergänzen oder imputieren. Hierbei wird z.B.

geschätzt, wie wahrscheinlich eine Person, die ihr Alter, Geschlecht, ihre Bildung und ihren Beziehungsstatus angegeben hat, eine bestimmte Partei präferiert (fehlende Information), basierend auf den politischen Präferenzen anderer, ihr ähnlicher Personen, die neben ihrer Parteipräferenz demographische Angaben hinterlegt haben.

Wenn Plattform-Online-Daten mit anderen Informationen verknüpft werden, z.B. mit Antworten zu einem Persönlichkeitstest, dann kann auf diese Weise auch gelernt werden, welche Merkmale und Merkmalskombinationen welchen Persönlichkeitstyp vorhersagt. Ein Beispiel aus der akademischen Forschung für Vorhersagen solcher unbeobachteter Merkmale (wie Persönlichkeiten) anhand beobachteter Merkmale (z.B. Likes) ist die Studie von Kosinski et al. (2013). Die Autoren konnten zeigen, dass die in der psychologischen Persönlichkeitsforschung weit verbreiteten *Big Five Persönlichkeitsmerkmale* (Offenheit für Erfahrungen, Gewissenhaftigkeit, Extraversion, Verträglichkeit und Neurotizismus) mittels statistischer Vorhersagemethoden aus nur wenigen Likes, die auf Facebook abgegeben wurden, vorhergesagt werden können. Die Erkenntnisse aus dieser Studie wurden später unter anderem von der Datenanalysefirma Cambridge Analytica in ihrem datengetriebenen Modell der gezielten Ansprache von Wählerinnen und Wählern aufgegriffen.

Auch sensible Informationen wie sexuelle Orientierung, politische Ansichten oder Gesundheitsinformationen lassen sich auf diese Weise potentiell aus beobachteten Informationen abschätzen (Cabañas et al. 2018). Solange für einen Teil der Nutzerinnen und Nutzer sowohl die Merkmale, die zur Vorhersage genutzt werden (die *predictors* oder *inputs*) als auch die Merkmale, die vorhergesagt werden sollen (die *outcomes* oder *outputs*), beobachtet werden, lässt sich ein statistisches Modell für jegliche beobachteten Outcomes trainieren. Wie *genau* diese Vorhersagen sind, hängt jedoch von einer Reihe von Faktoren ab.

In anderen Worten heißt das, nur weil sich ein Vorhersagemodell trainieren lässt, bedeutet dies noch lange nicht, dass die Vorhersagen auch zutreffen. Kosinski et al. (2013) berichten beispielsweise, dass das Geschlecht, Ethnizität und ob ein Mann homosexuell ist, vereinfacht gesprochen, anhand von Social Media Likes in den ihnen zur Verfügung stehenden Daten in etwa 90% der Fälle korrekt vorhergesagt werden könne. Merkmale wie Konsum von Alkohol oder Drogen, Homosexualität von Frauen und politische Einstellungen lassen sich mit ihren Modellen jedoch deutlich schlechter vorhersagen. Das heißt, es lässt sich zwar anhand der beobachteten statistischen Zusammenhänge eine Vorhersage treffen, diese trifft aber möglicherweise in vielen Fällen nicht zu. Eine Studie des Pew Research Centers in den USA kam zum Beispiel zu dem Schluss, dass die von Face-

book für US-Nutzerinnen und Nutzer abgeschätzte politische "Affinität" für mehr als ein Viertel der Personen *nicht* zutrifft (Hitlin und Raine 2019). Um dies zu zeigen, wurden Teilnehmerinnen und Teilnehmer der Pew-Studie gebeten, die ihnen von Facebook zugeschriebene politische Affinität in den Einstellungen ihres Accounts abzulesen und anzugeben, ob diese ihre tatsächlichen politischen Ansichten trifft oder nicht. Da die statistischen Modelle und Algorithmen als Betriebsgeheimnis der Öffentlichkeit verborgen bleiben, liegen insgesamt wenige Erkenntnisse vor, wie präzise die Algorithmen Vorhersagen treffen können. Die Frage etwa, ob die Vorhersagemodelle der ehemaligen Datenanalysefirma Cambridge Analytica besonders präzise waren, wurde von verschiedenen Seiten angezweifelt (siehe z.B. Chen und Potenza 2018). Wie wichtig die Präzision der Vorhersage ist, hängt aber davon ab, was im Nachgang mit den gewonnenen Informationen geschieht.

Insgesamt bleibt festzuhalten, dass sich unter Verwendung einer Vielzahl an Daten, die zum Beispiel auf Social Media und auf anderen Onlineplattformen anfallen, auch nicht direkt beobachtete Informationen abschätzen lassen. Oft ist für Außenstehende jedoch nicht klar, wie zutreffend diese geschätzten Informationen sind. Der Fundus an Daten, die für die gezielte Ansprache einzelner Personen oder Gruppen von Personen genutzt werden können, kann durch die Kombination von direkt beobachteten und mittels statistischer Verfahren abgeschätzter Informationen gerade bei Plattform-Online-Daten schnell groß werden. Einen Einblick in die Informationen, die zum Beispiel Facebook über seine Nutzerinnen und Nutzer bereithält, lässt sich unter www.facebook.com/dyi gewinnen.

3.2 Off-Plattform-Online-Daten

Besonders ergiebig und nützlich werden Daten aus digitalen Verhaltensquellen, wenn Plattform-Online-Daten mit weiteren Daten aus anderen (Online-)Quellen verknüpft werden können. Wir wollen letztere hier als *Off-Plattform-Online-Daten* bezeichnen. Ein Kerninstrument der Off-Plattform-Online-Daten sind Cookies, die sich zur Sammlung von digitalen Verhaltensdaten über einzelne Plattformen und Webseiten hinaus eignen. Weitere Techniken des Trackings von Nutzerinnen und Nutzern sind z.B. Browser und Canvas Fingerprinting (Libert 2015) und die Nutzung von Advertising Identifiers, insbesondere auf mobilen Geräten wie Smartphones und Tablets (Kollnig et al. 2021). Fingerprinting-Techniken arbeiten durch das Wiedererkennen von Nutzerinnen und Nutzern anhand von (nahezu einzigartigen) Kombinationen etwa aus Gerät (Marke, Her-

steller, Modell und weitere Merkmale), dem genutzten Browser und der auf einem Gerät installierten Schriftarten. Advertising Identifiers (Ad-IDs) sind Identifikationsnummern, die auf Android- und iOS-Geräten genutzt werden, um Nutzerinnen und Nutzer beispielsweise über Apps hinweg verfolgen zu können und Werbepartnern die Möglichkeit zu geben, personalisierte Werbung zu schalten. Aufgrund der Omnipräsenz und Bekanntheit von Cookies fokussieren wir uns diesem Beitrag auf diese.

Cookies sind kleine Textdateien, die bei Besuchen von Webseiten von den Betreibern der Webseiten auf digitalen Endgeräten wie Computern und Smartphones der Besucherinnen und Besucher abgelegt werden (Gomer et al. 2013; Urban et al. 2018). Cookies erlauben die Re-Identifikation von Nutzerinnen und Nutzern bei wiederholten Website-Besuchen, aber auch das Sammeln von Nutzeraktivitäten über verschiedene Webseiten hinweg. Sogenannte *first-party cookies* werden genutzt, um das Browsen auf Webseiten angenehmer zu gestalten. Sie werden von der besuchten Website (der *first-party*) gesetzt und ermöglichen beispielsweise, dass Nutzerinnen und Nutzer Spracheinstellungen nicht bei jedem Websitebesuch neu konfigurieren müssen, oder dass sie bei einem erneuten Aufruf einer Website automatisch in ihren Account eingeloggt sind. *Third-party cookies* hingegen werden zwar durch die first-party gesetzt, laden jedoch Informationen, die außerhalb der besuchten Website, also bei einer third-party, liegen. Durch diese externe Referenz können Informationen über den Besuch der first-party Website mit einer third-party Webseite ausgetauscht werden.

Die third-parties sind dabei oft Werbeunternehmen, die Cookies auf sehr vielen Webseiten im Internet als third-party cookies einbinden lassen. Besucht eine Nutzerin oder ein Nutzer nun beispielsweise eine zweite Website, auf der das gleiche third-party cookie eingebunden ist, so ist die Information, dass ein und dieselbe Person beide Websites besucht hat, für das third-party Werbeunternehmen ersichtlich. Sind die Cookies einer third-party nun auf sehr vielen Webseiten eingebunden, lassen sich detaillierte Informationen über die Onlineaktivitäten einzelner Personen sammeln. Da jedoch nicht immer cookies von allen third-parties auf einer Webseite eingebunden sind, tauschen gelegentlich third-parties die in Cookies genutzten Informationen zur Wiedererkennung einzelner Nutzerinnen und Nutzer auch untereinander aus (Urban et al. 2018). So lassen sich auch dann Onlineaktivitäten für eine third-party beobachten, wenn diese selbst kein entsprechendes Cookie eingebunden hat, aber eine andere. Ist z.B. ein Cookie einer anderen third-party eingebunden und die beiden third-parties tauschen die von ihnen genutzten Informationen zur Identifikation einer Person untereinander aus, so können verschiedene

third-parties durch *Cookie Synchronisierung* die beobachteten Onlineaktivitäten untereinander teilen und vervollständigen. So lässt sich sicherstellen, dass die beobachteten Daten ein möglichst vollständiges Bild der Onlineaktivitäten einer Person zeichnen, auch wenn ihre eigenen Cookies nicht zwingend auf jeder Website eingebunden sind.

Schätzungen bezüglich der Verbreitung von Cookies zum Zweck der Sammlung von Onlineaktivitäten von Nutzerinnen und Nutzern gehen davon aus, dass bis zu 99% der populärsten Webseiten im Internet potentielle third-party cookies einsetzen (Kontaxis und Chew 2015; Libert 2015). Anhand der durch Cookies gesammelten Daten können Trackingunternehmen schätzungsweise bis zu 73% der Internetaktivitäten von durchschnittlichen Nutzerinnen und Nutzern beobachten (Englehardt et al. 2015; Yu et al. 2016). Die Sammlung von Nutzerverhalten durch Cookies wird dabei dominiert von einigen wenigen Unternehmen, allen voran Alphabet, der Mutterfirma von Google, sowie Meta/Facebook (Binns et al. 2018; Brandtzaeg et al. 2019; Englehardt und Narayanan 2016). Diese Unternehmen sind zugleich auch diejenigen, die einen enormen Datenfundus aus Nutzungsaktivitäten innerhalb der eigenen Plattformen generieren können, wie wir weiter oben beschrieben haben.

Sind Nutzerinnen und Nutzer in ihren Account eingeloggt oder haben nach dem Ausloggen aus ihrem Account die entsprechenden Cookies nicht gelöscht, so lassen sich die Daten aus Off-Plattform-Aktivitäten und Online-Plattform-Aktivitäten, also das Besuchen von Websites außerhalb der eigenen Plattform, leicht verknüpfen. Durch diese Kombination der Daten entstehen für Plattformen große Datenpools, die, insbesondere in Kombination mit (un)supervised machine learning Algorithmen gut für die zielgenaue und personalisierte Ansprache von Individuen genutzt werden können.

Die Fülle von Unternehmen, die third-party Cookies setzen und über Webseiten hinweg Daten sammeln geht weit über die genannten Unternehmen hinaus und das Verfolgen von Nutzeraktivitäten ist nahezu ubiquitär (Christl 2017). Normativ kritisch kann dies werden, wenn die Datensammlung in Kontexten passiert, in denen dies nicht erwartet wird. Die Philosophin Helen Nissenbaum hat auf diese Problem in dem von ihr konzipierten Framework der *Contextual Integrity* hingewiesen (Nissenbaum 2019). Zur Veranschaulichung ziehen wir die Plattform ResearchGate, eine europäischen Plattform zur Netzwerkbildung von Wissenschaftlerinnen und Wissenschaftlern, heran. Mit Stand März 2020 hat eine Nutzerin von ResearchGate, die der Voreinstellung zum Setzen von Cookies zustimmt, mit einem Schlag dem Setzen von 500 third-party cookies zugestimmt. Zudem wird durch die Zustimmung zum Setzen von Google

Cookies rund weiteren 1500 Firmen, den Technology-Partnern von Google, Zustimmung zur Nutzung ihrer so gewonnenen Daten erteilt.

Abbildung 4: Auszug der ersten 100 third-party Cookiebetreiber, deren Cookies auf der Plattform ResearchGate eingebunden sind und so digitalen Verhaltensdaten aufzeichnen. Stand März 2020. Eine volle Liste inklusive der Technologypartner von Google befindet sich unter https://github.com/rubac/cookies_RG

1020, Inc. dba Placecast and Ericsson Emodo	Adform A/S	Adssets AB	Audience Trading Platform Ltd.
1plusX AG	Adhese	AdsWizz Inc.	AudienceProject Aps
2KDirect, Inc. (dba iPromote)	adhood.com	Adtelligent Inc.	Audiens S.r.l.
33Across	Adikteev / Emoteev	AdTheorent, Inc	AuDigent
7Hops.com Inc. (ZergNet)	ADITION technologies AG	AdTiming Technology Company Limited	audio content & control GmbH
: Tappx	Adkernel LLC	ADUX	Automattic Inc.
A Million Ads Ltd	Adledge	advanced store GmbH	Avazu Inc.
A.Mob	Adloox SA	ADventori SAS	Avid Media Ltd
Accelerize Inc.	Adludio Ltd	Adverline	Avocet Systems Limited
Accorp Sp. z o.o.	ADMAN - Phaistos Networks, S.A.	ADWAYS SAS	Axel Springer Teaser Ad GmbH
Active Agent AG	ADman Interactive SL	ADYOULIKE SA	Azerion Holding B.V.
Acuityads Inc.	adMarketplace, Inc.	Aerserv LLC	Bandsintown Amplified LLC
adé media	AdMaxim Inc.	Affectv Ltd	Bannerflow AB
Adacado Technologies Inc. (DBA Adacado)	Admedo Ltd	Affle International	Beachfront Media LLC
adality GmbH	admetrics GmbH	Alive & Kicking Global Limited	Beemray Oy
ADARA MEDIA UNLIMITED	Admixer EU GmbH	Alliance Gravity Data Media	BeeswaxIO Corporation
AdClear GmbH	Adnami Aps	Amobee, Inc.	BEINTOO SPA
AdColony, Inc.	Adobe Advertising Cloud	AntVoice	BeOp
AddApptr GmbH	Adobe Audience Manager	Apester Ltd	Better Banners A/S
AdDefend GmbH	Adprime Media Inc.	AppNexus Inc.	BidBerry SRL
AdElement Media Solutions Pvt Ltd	adrule mobile GmbH	Arcspire Limited	Bidmanagement GmbH
Adello Group AG	Adserve.zone / Artworx AS	Arkeero	Bidstack Limited
Adelphic LLC	Adsolutions BV	ARMIS SAS	BIDSWITCH GmbH
Adevinta Spain S.L.U.	AdSpirit GmbH	Arrivalist Co.	Bidtellect, Inc
Adform A/S	adsquare GmbH	ATG Ad Tech Group GmbH	BidTheatre AB

Durch die Kombination der so erhobenen Daten mit Befragungen (eines Teils) der Nutzerinnen und Nutzer einer Webseite lassen sich zum Beispiel mit den zuvor beschriebenen Methoden des supervised machine learnings auch Modelle trainieren, die die Inhalte der Befragung dann für alle Webseiten-Nutzerinnen und -Nutzer vorhersagen können. So könnte man beispielsweise einige Personen etwa in einer Onlinebefragung nach verschiedenen Merkmalen wie soziodemographischen Informationen, Parteipräferenzen und Wahlabsicht befragen und die so gewonnenen Daten mit ihren Onlineaktivitäten verknüpfen. Anhand dieser Daten ließe sich dann ein statistisches Modell trainieren, das später angewandt werden könnte, um allein anhand der z.B. aus Cookies gesammelten Onlineaktvitäten Informationen zu soziodemographischen Informationen, Parteipräferenzen und Wahlabsicht der Onlinenutzerinnen und -nutzer zu generieren. In der Praxis zeigt sich, dass die Vorhersage basierend auf Onlineaktivitäten in der Regel für einige Merkmale wie Alter, Geschlecht, Bildung, Beruf und Einkommensgruppen gut funktioniert, für andere Merkmale jedoch keine sehr genauen Vorhersagen getroffen werden können (siehe z.B. Hinds und Joinson 2018 und Kapitel 3.1).

Unsere eigene Forschung zu digitalen Verhaltensspuren hat gezeigt, dass Merkmale wie politische Einstellungen oder Wahlverhalten sich für Internetnutzerinnen und -nutzer in Deutschland nur mit verhältnismäßig geringer Genauigkeit aus reinen Off-Plattform-Online-Daten abschätzen lassen (Bach et al. 2021). Abbildung 5 verdeutlicht dies anhand eines Vergleichs der Vorhersagegenauigkeit verschiedener supervised machine learning Modelle. Vorhergesagt wird dabei, ob eine Person die Partei *Bündnis 90/Die Grünen* bei der Bundestagswahl 2017 gewählt hat oder nicht (linke Abbildung) bzw. die Partei *Alternative für Deutschland* gewählt hat oder nicht (rechte Abbildung). Unsere Modelle sind dabei inspiriert von Datensammlungs- und -auswertungspraktiken wie man sie auch in der Praxis vorfindet. Die Boxplots fassen die Güte der Vorhersagen anhand verschiedener Prädiktorengruppen zusammen. Die Vorhersagegüte wird dabei über die ROC-AUCs[7] der Crossvalidierungssets[8] abgebildet. Vereinfacht gesagt ist die Genauigkeit der Vorhersagen dann hoch, wenn die Werte möglichst nah an den Wert eins reichen.

In der ersten Zeile ("Soz.dem.") haben wir für die Vorhersage der Wahlentscheidung nur soziodemographische Merkmale genutzt, also etwa Alter, Geschlecht und Bildung. In der zweiten Zeile ("Websites/Apps") hingegen haben wir Informationen über die von einer Person während der vier Monate vor der Wahl besuchten Websites und auf ihrem Smartphone genutzten Apps als Prädiktoren genutzt.[9] In der dritten Zeile ("Soz.dem. + Tracking allg.") haben wir sowohl soziodemographische Informationen als auch allgemeine Informationen über das Onlineverhalten der letzten Monate einer Person genutzt, etwa die durchschnittliche Länge und die am häufigsten beobachteten Wochentage und Uhrzeiten der Internetnutzung. In der vierten Zeile ("Soz.dem. + Nachrichtenkonsum") war dagegen insbesondere der Nachrichtenkonsum von Interesse, ausgehend von der Annahme, dass der Nachrichtenkonsum einer Person Aufschluss über ihre politischen Präferenz geben könnte. In der letzten Zeile schließlich ("Soz.dem. + Websites/Apps") haben wir alle in den anderen Modellen

7 Area under the Receiver Operating Curve. Würde man für jede Person eine Münze werfen, um die Wahlentscheidung zu bestimmen, so würde sich ein ROC-AUC Wert von 0,5 ergeben. Ein Vorhersagemodell, das viele richtige Vorhersagen macht (also etwa für tatsächliche AfD-Wählerinnen und -Wähler die AfD-Wahlentscheidung auch vorhersagt), weist ROC-AUCs größer 0,5 und nahe eins auf.

8 Datenpunkte, die während des Trainings unserer machine learning Modelle genutzt werden, um aus einer Fülle von möglichen Modellen das Beste auszuwählen.

9 Für Informationen zur Sammlung dieser Daten verweisen wir aus Platzgründen auf das Papier (Bach et al. 2021).

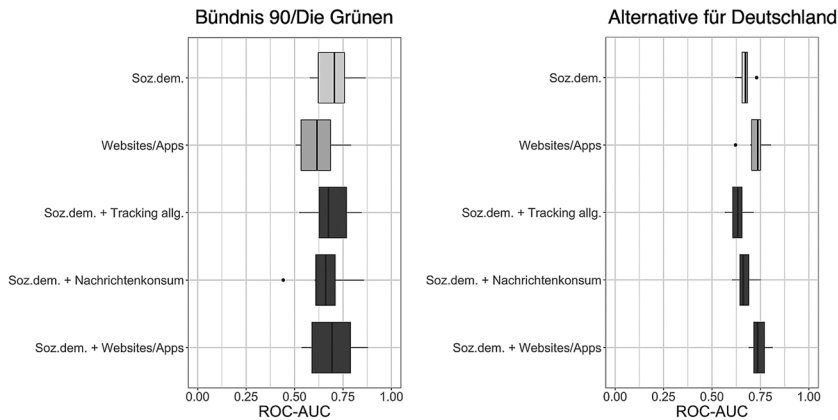
enthaltenen Prädiktoren, die wir aus digitalen Verhaltensspuren abgeleitet haben, mit soziodemographischen Informationen kombiniert. Wie oben erwähnt, lassen sich jedoch mit keinem der Modelle besonders genaue Vorhersagen erzielen. Das heißt, die von uns trainierten Modelle erlauben es uns nicht, aus den digitalen Verhaltensspuren die politischen Präferenzen einer Person, gemessen über ihre Wahlentscheidung, treffgenau nachzuvollziehen. Interessanterweise zeigt sich jedoch, dass die Vorhersagen für die Wahl der AfD weniger Varianz über die verschiedenen Crossvalidierungssets aufweisen. Vereinfacht gesagt können wir daraus schließen, dass es Unterschiede in der Vorhersagegüte für die einzelnen Parteien gibt. Zwar lassen sich für keine der beiden Parteien besonders genaue Vorhersagen treffen, für die AfD funktioniert es jedoch etwas besser als für die Grünen.

Wie oben schon angeschnitten sind die Unterschiede in der Vorhersagegüte der Modelle je nach Nutzung der Daten mehr oder weniger relevant. Kampagnen, die sich darauf konzentrieren Leute an die Wahlurnen zu bringen, können durchaus Erfolge verzeichnen und sind mitunter effektiver als solche, die versuchen Meinungen zu verändern (siehe zum Beispiel Nickerson und Rogers 2014 und Baldwin-Philippi 2019, zum Unterschied zwischen persuasion und mobilisation). Das heißt, selbst wenn die Vorhersagegüte von Modellen variiert und nicht immer zutrifft, so können sie dennoch in politischen Kampagnen hilfreich sein, um Ressourcen effektiver einzusetzen, etwa wenn für einen Teil der Personen korrekte Vorhersagen gemacht werden und diese dann etwa zur Wahl mobilisiert werden können.

Zusammenfassend lässt sich also festhalten, dass durch nahezu omnipräsentes Verfolgen von Nutzeraktivitäten im Internet große Mengen an Daten und Informationen anfallen und gesammelt werden. Diese könnten dann unter anderem zum Trainieren eines statistischen Vorhersagealgorithmus genutzt werden, der die gezielte Wählerinnen- und Wähleransprache ermöglicht. Wenn etwa für einen Teil der Nutzerinnen und Nutzer sowohl Wahlabsicht und Onlineaktivitäten beobachtet werden, könnte mit diesem Algorithmus für all die, bei denen nur Onlineaktivitäten beobachtet werden, eine Vorhersage gemacht werden, etwa ob sie unentschlossen sind, welche Partei sie wählen werden. Die so identifizierten unentschlossenen Wählerinnen und Wähler könnten dann mit gezielt auf ihre Präferenzen zugeschnittenen Inhalten angesprochen werden. Solange der Algorithmus jedoch nicht selbst trainiert wird oder offen einsehbar ist, wie gut die Identifikation der unentschlossenen Wählerinnen und Wähler ist, bleibt die Qualität der Vorhersagen offen. Die bisherige Forschung, die sich dieser Frage widmet, deutet daraufhin, dass für einige Merkmale

genaue Vorhersagen getroffen werden können, während sich für andere Merkmale nur unscharfe Vorhersagen machen lassen.

Abbildung 5: Die Boxplots fassen die Güte der Vorhersagen bezüglich der Wahlentscheidung einer Person für oder gegen die genannte Partei anhand verschiedener Prädiktorengruppen zusammen. Die Vorhersagegüte wird dabei über die ROC-AUCs der Crossvalidierungssets abgebildet. Vereinfacht gesagt ist die Genauigkeit der Vorhersagen dann hoch, wenn die Werte möglichst nah an den Wert eins reichen.



3.3 Offline-Daten

Abschließend wollen wir noch Offline-Daten erwähnen. Eine detaillierte Behandlung dieser Datenquellen würde den Rahmen dieses Kapitels sprengen. Wir wollen sie dennoch hier erwähnen, um aufzuzeigen, welche weiteren Daten sich mit den hier genannten verknüpft lassen und beispielsweise in den USA häufig auch im politischen Microtargeting Verwendung finden (Nickerson und Rogers 2014).

Ein gutes Beispiel sind Informationen, die über Kundenkarten oder Kundenbindungsprogramme gewonnen werden. Die Verknüpfung kann zum Beispiel über Adressen, Telefonnummern oder E-Mail-Adressen, die bei der Registrierung einer Kundenkarte oder eines Kundenkontos angegeben werden, stattfinden. Wird die gleiche Adresse, Telefonnummer oder E-Mail-Adresse bei der Nutzung von Onlineplattformen angegeben, so können die Datenquellen problemlos zusammengefügt werden. Auch

wenn keine eindeutigen Informationen zur Verknüpfung von Informationen aus verschiedenen Quellen vorhanden sind, lassen sich Informationen mittels Record-Linkage-Verfahren, die auf statistischen Wahrscheinlichkeiten basieren, verknüpfen (siehe z.B. Tokle und Bender 2020).

Als Lieferant von Offline-Daten werden häufig Data Broker wie das Unternehmen Acxiom (https://www.acxiom.de) genutzt. Data Broker sind Unternehmen, die auf die Sammlung von Daten über Individuen aus verschiedensten Quellen sowie das Handeln und Lizenzieren dieser Daten an Dritte spezialisiert sind. Auch wenn Data-Broker in öffentlichen Debatten um Daten und Demokratie im digitalen Zeitalter oft nicht so stark im Rampenlicht stehen wie Betreiber sozialer Medien, so sind sie doch ein integraler Bestandteil von Datenströmen in modernen digitalisierten Demokratien.

4. Zusammenfassung und Diskussion

Dieses Kapitel gibt einen kurzen Einblick in die wesentlichen Datenströme und zeigt, dass aus unstrukturierten Daten mit Hilfe statistischer oder datengetriebener Verfahren strukturierte Informationen über Individuen generiert werden können. Motiviert haben wir dabei die Nutzung der Daten im Kontext von Wahlwerbung, aber selbstverständlich können diese Daten auch zu anderen Zwecken genutzt werden.

Wie eingangs erwähnt sind digitale Datenströme, egal aus welchen Quellen sie kommen, für viele von Interesse. Auch evidenzbasierte Politik ist auf Daten angewiesen, um den Zustand einer Gesellschaft zu erfassen und Veränderungen in einer Gesellschaft zu erkennen. Deshalb ist es bei der Generierung neuer Regularien besonders wichtig, die Verwendungszwecke der Daten im Auge zu behalten und nicht Datenströme per se abzuschneiden.[10] So fließen automatisiert erhobene Datenströme etwa von Kassensystemen und aus Onlinequellen mitunter in die Berechnung von Inflationsindizes ein (Leclair et al. 2019). Spätestens seit der Coronapandemie wird zudem an zahlreichen Stellen deutlich, dass Datenströme von Plattformen oder Transaktionen Informationslücken schließen konnten, etwa bei der Vorhersage der Pandemieentwicklung selbst (Salomon et al. 2021).

Derzeit liegt die Verantwortung der Datenweitergabe bei den einzelnen Nutzerinnen und Nutzern. Die Informationsdichte über die möglichen

10 Siehe hierzu auch den Beitrag von Buchmann in diesem Sammelband.

Verwendungen ist allerdings sehr hoch und selbst solche Nutzerinnen und Nutzer, die sich der verhaltensorientierten Online-Werbung bewusst sind und maßgeschneiderte Werbung und personalisierte Suchergebnisse als hilfreich empfinden, wissen oft nicht, wie und was Unternehmen aus ihren Daten lernen können (Dolin et al. 2018; Hitlin und Raine 2019; Ur et al. 2012). Auch wenn im Kleingedruckten der Einwilligungen im Prinzip nachvollzogen werden kann, mit wem die Daten geteilt werden und für welche Analysen die Daten verwendet werden, bleibt die gesamte Daten- und Analysekette häufig doch undurchsichtig (z. B. Christl 2017). Ein Grund dafür ist, dass die Details der Algorithmen, die zur Analyse der Daten verwendet werden, oft nicht bekannt sind, wodurch eine Prüfung der Angemessenheit des Informationsflusses (Nissenbaum 2019) unmöglich wird. Ob hier mehr Transparenz hilft, oder eine Verlagerung der Verantwortung ein besseres Instrument wäre, ist eine offene Debatte. Denkbar wäre zum Beispiel, dass schadhafte Nutzung von Daten nicht nur zivilrechtlich sondern auch strafrechtlich zu verfolgen, ganz unabhängig davon woher Datenströme kommen und welcher Nutzung zugestimmt wurde.

Diese Fokussierung auf die Verwendung ist vor allem auch im Hinblick darauf sinnvoll, dass die einzelnen Nutzerinnen und Nutzer ohnehin nur begrenzt Kontrolle darüber haben, welche Vorhersagen für sie getroffen werden. Selbst wenn sich Einzelne gezielt dafür entscheiden, Informationen über sich zurückzuhalten, erlauben moderne mathematische und statistische Verfahren das Imputieren fehlender Werte, und Algorithmen können darauf trainiert werden, bestimmte Informationen vorherzusagen (Bischoff et al. 2018; Christl 2017; Lecuyer et al. 2015). Wenn also genügend andere ihre Informationen teilen, können sich einzelne nicht gegen eine Inferenz auf ihre eigenen Informationen schützen. Es ist deshalb durchaus überlegenswert, die Verantwortung stärker auf die Seite der Datennutzer zu verlagern. Nissenbaums Leitgedanken zur *Contextual Integrety* können hier ein Ansatz sein, der auf einen normgerechten Umgang mit Daten plädiert.

Eine Regulierung der Verwendung anstatt einer Regulierung der einzelnen Datentypen oder Datenströme wäre auch deshalb überlegenswert, da sich derzeit ohnehin nicht absehen lässt, welche zusätzlichen Datenströme auftauchen werden, welche Verlinkungen von Datenquellen in der Zukunft denkbar sind und welche Rechenleistung zukünftig vorhanden sein wird, um Vorhersagen zu beschleunigen oder zu verbessern. Wichtig wäre es deshalb einen Rahmen zu schaffen, der flexibel genug ist Individuen vor Schaden zu schützen ohne die positive Nutzen von Daten zu blockieren.

Literaturverzeichnis

Bach, Ruben L.; Kern, Christoph; Amaya, Ashley; Keusch, Florian; Kreuter, Frauke; Hecht, Jan; Heinemann, Jonathan (2021): Predicting Voting Behavior Using Digital Trace Data. In: *Social Science Computer Review* 39 (5), S. 862–883. DOI: 10.1177/0894439319882896.

Baldwin-Philippi, Jessica (2019): Data campaigning: between empirics and assumptions. In: *Internet Policy Review* 8 (4), S. 1–18. DOI: 10.14763/2019.4.1437.

Beisch, Natalie; Schäfer, Carmen (2020): Ergebnisse der ARD/ZDF-Onlinestudie 2020. Internetnutzung mit großer Dynamik. Medien, Kommunikation, Social Media. In: *Media Perspektiven* 9, S. 462–481.

Binns, Reuben; Lyngs, Ulrik; van Kleek, Max; Zhao, Jun; Libert, Timothy; Shadbolt, Nigel (2018): Third Party Tracking in the Mobile Ecosystem. In: Proceedings of the 10th ACM Conference on Web Science. Amsterdam, the Netherlands, 27–30 May 2018. New York: ACM, S. 23–31.

Bischoff, J.; Cygan, S.; Münkel, J.; Schindler, W. (2018): Auf Datensuche in der Welt der Datenhändler. In: *mdr*, 2018. Online verfügbar unter https://www.mdr.de/datenspuren/datenspuren-138.html, zuletzt geprüft am 12.07.2019.

Bovermann, P. (2021): Facebook dreht am Anzeigenalgorithmus. In: *SZ Online*, 10.11.2021. Online verfügbar unter https://www.sueddeutsche.de/wirtschaft/facebook-targeting-werbung-abschalten-1.5461094, zuletzt geprüft am 10.11.2021.

Brandtzaeg, P. B.; Pultier, A.; Moen, G. M. (2019): Losing control to data-hungry apps: A mixed-methods approach to mobile app privacy. In: *Social Science Computer Review* 37, S. 466–488.

Cabañas, José González; Cuevas, Ángel; Cuevas, Rubén (2018): Unveiling and Quantifying Facebook Exploitation of Sensitive Personal Data for Advertising Purposes. In: Proceedings of the 27th USENIX Security Symposium. 27th USENIX Security Symposium (USENIX Security 18), S. 479–495. Online verfügbar unter https://www.usenix.org/conference/usenixsecurity18/presentation/cabanas.

Chen, A.; Potenza, A. (2018): Cambridge Analytica's Facebook data abuse shouldn't get credit for trump: 'I think Cambridge Analytica is a better marketing company than a targeting company.'. In: *The Verge*, 2018. Online verfügbar unter https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting, zuletzt geprüft am 28.10.2021.

Christl, W. (2017): Corporate surveillance in everyday life: How companies collect, combine, analyze, trade, and use personal data on billions. Cracked Labs. Vienna, Austria. Online verfügbar unter https://crackedlabs.org/en/corporate-surveillance, zuletzt geprüft am 28.10.2021.

Dolin, Claire; Weinshel, Ben; Shan, Shawn; Hahn, Chang Min; Choi, Euirim; Mazurek, Michelle L.; Ur, Blase (2018): Unpacking Perceptions of Data-Driven Inferences Underlying Online Targeting and Personalization. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. New York, NY, USA. New York, NY, USA: ACM.

Englehardt, S.; Narayanan, A. (2016): Online tracking: A 1-million-site measurement and analysis. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. Vienna, Austria, 24 - 28th October. New York: ACM, S. 1388–1401.

Englehardt, S.; Reisman, D.; Eubank, C.; Zimmermann, P.; Mayer, J.; Narayanan, A.; Felten, E. W. (2015): Cookies that give you away: The surveillance implications of web tracking. In: Proceedings of the 24th International Conference on World Wide Web. Florence, Italy, 18 - 22 May. NY: ACM, S. 289–299.

Flaig, B. B.; Barth, B. (2018): Hoher Nutzwert und vielfältige Anwendung: Entstehung und Entfaltung des Informationssystems Sinus-Milieus®. In: B. Barth, B. B. Flaig, N. Schäuble und M. Tautscher (Hg.): Praxis der Sinus-Milieus®: Springer VS, Wiesbaden, S. 3–21. Online verfügbar unter https://link.springer.com/chapter/10.1007/978-3-658-19335-5_1.

Foster, Ian; Ghani, Rayid; Jarmin, Ron S.; Kreuter, Frauke; Lane, Julia (Hg.) (2020): Big Data and Social Science: A Practical Guide to Methods and Tools. London: CRC Press.

Glaeser, Edward (2019): Urban Management in the 21st Century: Ten Insights from Professor Ed Glaeser: Centre for Development and Enterprise (CDE). Online verfügbar unter https://www.africaportal.org/publications/urban-management-21st-century-ten-insights-professor-ed-glaeser/.

Gomer, Richard; Rodrigues, Eduarda Mendes; Milic-Frayling, Natasa; Schraefel, M. C. (2013): Network Analysis of Third Party Tracking: User Exposure to Tracking Cookies through Search. In: 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT). Atlanta, GA, 17 - 20 November. New York: IEEE, S. 549–566.

Google (2019): An update on our political ads policy. Online verfügbar unter https://www.blog.google/technology/ads/update-our-political-ads-policy/, zuletzt geprüft am 28.10.2021.

Hinds, J.; Joinson, A. N. (2018): What demographic attributes do our digital footprints reveal? A systematic review. In: *PLoS One* 13 (11), S. 1–40.

Hitlin, Paul; Raine, Lee (2019): Facebook Algorithms and Personal Data. In: *Pew Research Center*. Online verfügbar unter https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/, zuletzt geprüft am 28.10.2021.

Howison, James; Wiggins, Andrea; Crowston, Kevin (2011): Validity Issues in the Use of Social Network Analysis with Digital Trace Data. In: *Journal of the Association for Information Systems* 12 (12), S. 768–797. DOI: 10.17705/1jais.00282.

Jungherr, A. (2016): Four Functions of Digital Tools in Election Campaigns: The German Case. In: *International Journal of Press/Politics* 3, S. 358–377.

Kemp, S. (2021): Digital 2021: Germany. Online verfügbar unter https://datareportal.com/reports/digital-2021-germany, zuletzt geprüft am 28.10.2021.

Keusch, Florian; Kreuter, Frauke (2021): Chapter 7 Digital Trace Data. In: Uwe Engel, Anabel Quan-Haase, Sunny Xun Liu und Lars Lyberg (Hg.): Handbook of Computational Social Science, Vol 1: Taylor & Francis. Online verfügbar unter https://library.oapen.org/handle/20.500.12657/51412.

Kollnig, Konrad; Shuba, Anastasia; Binns, Reuben; van Kleek, Max; Shadbolt, Nigel (2021): Are iPhones Really Better for Privacy? Comparative Study of iOS and Android Apps. In: *arXiv preprint* (arXiv:2109.13722). Online verfügbar unter https://arxiv.org/abs/2109.13722.

Kontaxis, Georgios; Chew, Monica (2015): Tracking Protection in Firefox For Privacy and Performance. In: Abigail Goldsteen, Tyrone Grandison, Mike Just, Larry Koved, Rohan Malcolm und Sean Thorpe (Hg.): Proceedings of the 9th Workshop on Web 2.0 Security and Privacy (W2SP) 2015. San Jose, CA, 21.05. Online verfügbar unter https://arxiv.org/abs/1506.04104.

Kosinski, Michal; Stillwell, David; Graepel, Thore (2013): Private traits and attributes are predictable from digital records of human behavior. In: *Proceedings of the National Academy of Sciences* 110 (15), S. 5802–5805. DOI: 10.1073/pnas.1218772110.

Kruschinski, Simon; Bene, Márton (2021): In varietate concordia?! Political parties' digital political marketing in the 2019 European Parliament election campaign. In: *European Union Politics* 23 (1), S. 43–65. DOI: 10.1177/14651165211040728.

Kruschinski, Simon; Haller, André (2017): Restrictions on data-driven political micro-targeting in Germany. In: *Internet Policy Review* 6 (4), S. 1–23. DOI: 10.14763/2017.4.780.

Lane, Julia (2020): Democratizing our data. A manifesto. Cambridge, Massachusetts: The MIT Press.

Leclair, Marie; Léonard, Isabelle; Rateau, Guillaume; Sillard, Patrick; Varlet, Gaëtan; Vernédal, Pierre (2019): Scanner Data: Advances in Methodology and New Challenges for Computing Consumer Price Indices. In: *Economie et Statistique / Economics and Statistics* 509, S. 13–29. DOI: 10.24187/ecostat.2019.509.1981.

Lecuyer, Mathias; Spahn, Riley; Spiliopolous, Yannis; Chaintreau, Augustin; Geambasu, Roxana; Hsu, Daniel (2015): Sunlight. In: Indrajit Ray, Ninghui Li und Christopher Kruegel (Hg.): Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. CCS'15: The 22nd ACM Conference on Computer and Communications Security. Denver Colorado USA, 12.10.2015 - 16.10.2015. New York, NY, USA: ACM, S. 554–566.

Libert, T. (2015): Exposing the hidden Web: An analysis of third-party HTTP requests on 1 million websites. In: *International Journal of Communication* 9, S. 1–10. Online verfügbar unter https://arxiv.org/abs/1511.00619.

Lynch, James (2018): Not Even our Own Facts: Criminology in the Era of Big Data. In: *Criminology* 56 (3), S. 437–454. DOI: 10.1111/1745-9125.12182.

Nickerson, David W.; Rogers, Todd (2014): Political Campaigns and Big Data. In: *Journal of Economic Perspectives* 28 (2), S. 51–74. DOI: 10.1257/jep.28.2.51.

Nissenbaum, H. (2019): Contextual Integrity Up and Down the Data Food Chain. In: *Theoretical Inquiries in Law* 20 (1), S. 221–256. Online verfügbar unter https://www.degruyter.com/document/doi/10.1515/til-2019-0008/html.

Pan, Ian; Nolan, Laura B.; Brown, Rashida R.; Khan, Romana; van der Boor, Paul; Harris, Daniel G.; Ghani, Rayid (2017): Machine Learning for Social Services: A Study of Prenatal Case Management in Illinois. In: *American journal of public health* 107 (6), S. 938–944. DOI: 10.2105/AJPH.2017.303711.

Rieder, Y.; Kühne, S. (2018): Geospatial Analysis of Social Media Data - A Practical Framework and Applications. In: Stuetzer, C.M., Welker, M. und M. Egger (Hg.): Computational Social Science in the Age of Big Data. Concepts, Methodologies, Tools, and Applications. Köln: Herbert van Halem Verlag (DGOF Schriftenreihe), S. 417–440.

Salganik, M. (2018): Bit By Bit. Social Research in the Digital Age. Princeton, NJ: Princenton University Press.

Salomon, Joshua A.; Reinhart, Alex; Bilinski, Alyssa; Chua, Eu Jing; La Motte-Kerr, Wichada; Rönn, Minttu M. et al. (2021): The US COVID-19 Trends and Impact Survey: Continuous real-time measurement of COVID-19 symptoms, risks, protective behaviors, testing, and vaccination. In: *Proceedings of the National Academy of Sciences* 118 (51). DOI: 10.1073/pnas.2111454118.

Stier, Sebastian; Breuer, Johannes; Siegers, Pascal; Thorson, Kjerstin (2020): Integrating Survey Data and Digital Trace Data: Key Issues in Developing an Emerging Field. In: *Social Science Computer Review* 38 (5), S. 503–516. DOI: 10.1177/0894439319843669.

Tokle, J.; Bender, S. (2020): Big Data and Social Science. Data Science Methods and Tools for Research and Practice. In: Ian Foster, Rayid Ghani, Ron S. Jarmin, Frauke Kreuter und Julia Lane (Hg.): Big Data and Social Science: A Practical Guide to Methods and Tools. London: CRC Press.

Twitter (ohne Datum): Political content. Online verfügbar unter https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html, zuletzt geprüft am 28.10.2021.

Ur, Blase; Leon, Pedro Giovanni; Cranor, Lorrie Faith; Shay, Richard; Wang, Yang (2012): Smart, useful, scary, creepy. In: Lorrie Faith Cranor (Hg.): Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12. the Eighth Symposium. Washington, D.C, 11.07.2012 - 13.07.2012. New York, New York, USA: ACM Press, S. 1.

Urban, T.; Tatang, D.; Degeling, M.; Holz, T.; Pohlmann, N. (2018): The unwanted sharing economy: An analysis of cookie syncing and user transparency under GDPR. In: *arXiv preprint* (arXiv:1811.08660), https://arxiv.org/pdf/1811.08660.

Yu, Z.; Macbeth, S.; Modi, K.; Pujol, J. M. (2016): Tracking the trackers. In: Proceedings of the 25th international conference on World Wide Web. Montreal, Cananda, 11 - 15 April. New York, NY: ACM, S. 121–132.

Personalisierung durch Profiling, Scoring, Microtargeting und mögliche Folgen für Demokratie – Funktionsweisen und Risiken aus datenschutzrechtlicher Sicht

Ulrich Kelber, Nils Leopold

1. Einleitung

Dass die weitgehende kommerzielle Datenausspähung der großen Internetunternehmen nicht allein ein Problem der davon betroffenen Bürgerinnen und Bürger ist, sondern letztlich auch weitreichende gesellschaftliche Folgen hat, wurde mit dem Aufkommen des Rechtspopulismus in den USA, Brasilien und Europa zum Thema mindestens der Diskussion in Fachkreisen. Hass und Hetze im Netz, Fake News, politische Wahlwerbung und Manipulation in Social Media sind als Bedrohung für die freiheitlichen Demokratien westlicher Ausprägung unübersehbar geworden.

Wenn es einen maßgeblichen Wendepunkt zu benennen gälte, der das Zusammenspiel aus Digitalisierung und der Furcht vor der Bedrohung der Demokratie ins kollektive Bewusstsein gehoben hat, so war es der Cambridge Analytica-Facebook-Fall. Vergleichbar den Snowden-Enthüllungen und dem folgenden weltweiten Geheimdienstskandal, wurden wie unter einem Brennglas gravierende negative Konsequenzen der rapiden globalen Digitalisierung deutlich. Als wenn ein Vorhang weggezogen wurde und den Blick freigibt auf die Hintergründe einer eigentlich bekannt-vertrauten Social Media-Szenerie: das gemütliche digitale Wohnzimmer, dem Millionen sich täglich so sehr anvertrauen, lag ausgebreitet vor uns, nur dieses Mal schauten überall die Drähte der Maschinen heraus. Es wurde klar, dass es eine sorgfältig gestellte digitale Kulisse war.

Genau diesen Vorhang immer wieder einen Stück weit zur Seite ziehen, um den Blick auf komplexe Mechanismen freizugeben, bewusst und sichtbar[1] zu machen, in welchem Umfang wir Menschen uns bereits in einem komplexen Zusammenspiel mit IT-Systemen befinden, stellt eine enorme Herausforderung dar. Charakteristisch für die digitale Entwicklung im

1 Vgl. Wischmeyer, AöR 2018 S. 20.

Umfeld gerade der Social Media Plattformen ist es, dass unser Selbstverständnis von Autonomie durch die Art der Behandlung der Nutzerinnen und Nutzer als Quasi-Objekte ihnen unbewusster Steuerung weitgehend in Frage gestellt wird. Während der Umfang der kommerziellen Interessen der Plattformbetreiber und die eigentlichen Funktionsweisen der eingesetzten Techniken und Verfahren weitgehend im Dunklen bleiben, wird das Verhalten der Nutzer für Zwecke der Unternehmen umso transparenter gemacht, detailliert analysiert, kategorisiert, zum Teil vorhersagbar und damit manipulierbar. Eine solche Entwicklung ist bedeutsam sowohl für Gemeinwohlziele wie Datenschutz als auch für die Demokratie selbst. Die Sorge um die Zukunft der Demokratie[2] im Kontext der Digitalisierung hat inzwischen den Blick geschärft für diese gesellschaftlichen Zusammenhänge und Gefährdungen, die bis dahin allenfalls in Fachkreisen andiskutiert waren. Die Frage, inwieweit die Spezifika von Internetkommunikation und Social Media Plattformen unsere politische Öffentlichkeit verändern, und inwieweit der Schutz demokratischer Strukturen und Verfahren womöglich Anpassungen bedarf, wird zumeist nicht vorrangig dem Datenschutz zur Beantwortung angetragen. Zu sehr wird die Aufgabe des Datenschutzes allein mit dem „Schutz der Einzelnen vor der Preisgabe ihrer persönlichen Daten“ assoziiert. Allerdings werden Erscheinungsformen, Funktionsweisen und auch bestimmte Auswirkungen von personalisierten digitalen Diensten im Rahmen datenschutzrechtlicher Vorgaben bereits seit Jahren diskutiert und bearbeitet.

Privatheit und Datenschutz erfüllen im Digitalen, natürlich neben zahlreichen anderen Regelungsgebieten, schon heute eine Vielzahl von Funktionen. In der Digitalisierung sind Datenschutz und Privatheit dabei auch nicht nur für die Rechte Einzelner von großer Bedeutung. Schon das Bundesverfassungsgericht hatte in seinem bis heute prägenden Volkszählungsurteil zwar mit der „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ den individualrechtlichen Charakter des Rechts auf informationelle Selbstbestimmung hervorgehoben. Es hatte andererseits aber auch die Beeinträchtigung individueller Selbstbestimmung als Beeinträchtigung des Gemeinwohls betont, “weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[3] Und es

2 Letztlich hat vor allem der furchterregende weltweite Aufstieg rechtspopulistischer und rechtsextremer Parteien die diskutierte Fragestellung befördert.

3 BVerfGE 65, Rdnr. 146.

zählt zu den Grundlagen des Datenschutzverständnisses, dass gerade der Schutz der Privatheit zu einer pluralistischen Gesellschaft beiträgt.[4]

Digitalisierung bedeutet heute im Verhältnis von Unternehmen zu Bürgern bzw. deren Rolle als Verbraucherinnen und Verbraucher vor allem eines, nämlich Personalisierung: die mit dem Ziel der Personalisierung geschaffenen Geschäftsmodelle, Instrumente und Praktiken zielen auf die personengenaue Erfassung, Auswertung, Ansprache und Beeinflussung/Manipulation der Bürgerinnen und Bürger. Die dabei entstehenden Risiken für die Privatheit sind, je nach Kontext und Ausgestaltung, massiv und bedrohen, zumindest bei Bekanntwerden im Rahmen von Skandalen, das Vertrauen in die Entwicklung der Digitalisierung.

In den letzten Jahren ins Blickfeld gerückt ist die umfassende Diffusion des Einsatzes von Techniken und Verfahren der Personalisierung in die gesamte Erlebniswelt der Online-Nutzerinnen und Nutzer, bei Recherche, Spielen, Kommunizieren, Mobilität und durch die Erfassung von Körperwerten. Oftmals werden sämtliche Informationen als auch Kommunikationen individuell auf die mutmaßlichen Präferenzen zugeschnitten. Nachrichtenfeeds, Kontakte als auch Suchmaschinentreffer sind zunehmend individuell vorselektiert. Einen Sonderfall bildet die politische Ansprache und Werbung über kommerzielle Plattformen auf der Grundlage der Personalisierungsmöglichkeiten.

Der vorliegende Artikel zeigt die Funktionsweisen der bekannten Verfahren und ihre datenschutzrechtlichen Implikationen auf. Das dabei entstehende Bild gibt zumindest Hinweise auf nicht weniger als signifikante Einschränkungen von Öffentlichkeiten klassischen Typs und wirft auch aus datenschutzrechtlicher Sicht Fragen nach weiteren gesetzgeberischen Anstrengungen zum Schutz demokratischer Öffentlichkeiten auf.

Der Fall Cambridge Analytica und die Debatte um den Einfluss von Facebook auf die US-Präsidentenwahl im Jahr 2016 sowie die Abstimmung im Vereinigten Königreich über den Austritt aus der Europäischen Union („Brexit") zeigen als schon oft untersuchte Beispiele die Bedeutung insbesondere algorithmengesteuerter Meinungs- und Willensbildung bei Online-Angeboten wie Suchmaschinen und sozialen Netzwerken.

4 Vgl. Albers DVBl. 2010, S. 1062.

2. Digital unterwegs sein bedeutet personalisiert werden

a. Grundlagen

Wer digitale Technik nutzt und keine aktiven und zumeist zumindest für Durchschnittsnutzer aufwändig herzustellende Gegenmaßnahmen trifft, verliert seine Anonymität. An die Stelle der aus dem Alltag bekannten relativen Anonymität des Alltages tritt die allgegenwärtige Datenerfassung durch die Anbieter digitaler Dienste. Aus den Datenspuren und Datenteppichen der Vergangenheit wird so die Datenwolke, die sich mit jeder Handlung oder Nichthandlung verändert, durch eigenes Zutun, durch Interaktion oder durch die Ableitung der Handlung Dritter.

Aus der Perspektive des Datenschutzes rückte bei der Entwicklung der Informationstechnik zunächst die automatisierte rechnergestützte Datenverarbeitung der einzelne Personen betreffenden Informationen und Daten in den Mittelpunkt. Die Verarbeitung auch von personenbezogenen Daten in Computersystemen, die beliebig lange Speicherung, Rekombination, Bewertung, multifunktionelle Nutzung und schließlich die Übermittlung dieser Informationen zwischen verschiedenen Rechnersystemen schuf neue Risiken der Auswertbarkeit, Überwachbarkeit und, auf der Grundlage des generierten Wissens, auch der Beeinflussung/Manipulierbarkeit von Menschen. Mit der Entstehung von neuen Informations- und Kommunikationstechnologien, insbesondere des Internets als eines digitalen Netzwerks der Netzwerke, also einer Verschaltung von Rechnernetzwerken und einzelnen Rechnern wurde die eindeutige Identifizierbarkeit von Informationsaustausch und von Kommunikationshandlungen ermöglicht und auf eine neue Stufe gehoben.

Die Funktionsweise des Datenaustausches über die technisch normierten Internetprotokolle erzwingt die zumindest temporäre Zuteilung von eindeutigen Rechneradressen und den Abgleich von Informationen zumindest zur Erreichbarkeit von sendenden und empfangenden Rechnerstellen. So wird etwa mittels der IP-Adresse eine eindeutige Übermittlung von Datenpaketen innerhalb des Internet ermöglicht, mittels dieser in Servern für den Weitertransport zwingend laufend erfassten IP-Adresse aber auch die Rückverfolgbarkeit von Personen/ Beteiligten einer Kommunikation oder Handlung ermöglicht. Schon für den bloßen Aufruf einer Webseite erfolgen entsprechende Datenerfassungen entlang der gesamten digitalen Infrastruktur. Welcher Rechner, wann, wie lange auf welche Inhalte zugegriffen hat wird damit vollständig erfassbar und gespeichert. Aus diesen technischen Gegebenheiten folgt die grundsätzlich stets bestehende Identifizierbarkeit der Nutzerinnen und Nutzer. Wollen Nutzer des

Internets ihre Identität vor Anderen, etwa wie im wirklichen Leben beim Bummel durch ein Kaufhaus, verborgen halten, müssen Sie schon selbst aktive Maßnahmen für den Erhalt ihrer Anonymität ergreifen. Denn die Default-Einstellung online ist Rückverfolgbarkeit und potentielle Identifizierbarkeit. Und neben die IP-Adresse sind längst zahlreiche andere Technologien der Identifikation von Nutzerinnen und Nutzer getreten. So gesehen stellt die Personalisierung, hier verstanden als allgemeine Erfassbarkeit und Personenbeziehbarkeit von digitalen Informationshandlungen, schon sehr früh den maßgeblichen Risikokontext des Datenschutzes dar.

Heute müssen Nutzerinnen und Nutzer für zahlreiche Dienste des Internet keine Gebühr bezahlen. Viele Unternehmen finanzieren Ihren Aufwand durch Werbung, die auf den entsprechenden Plattformen und Websites geschaltet wird oder mit dem Sammeln und Verkaufen von Informationen ihrer Nutzerinnen und Nutzer. Jeder Mensch hinterlässt beim Browsen im Internet unzählige Daten (z.B. durch Online-Einkäufe, Social Media Posts, Suchmaschinen-Eingaben, Verweildauer, Interaktion etc.) und wird zusätzlich gezielt getrackt (etwa mit der sog. Cookie-Technologie). Mit Hilfe dieser Daten können Unternehmen das Verhalten von Konsumenten analysieren, kategorisieren und vorhersehen (Grundlage ist das Profiling, darunter auch das Scoring, zunehmend unter Zuhilfenahme intelligenter Systeme) und so u.a. Werbekampagnen gezielt aussteuern (das sog. Targeting), aber auch zu entscheiden, wer für Angebote z.B. von Verträgen überhaupt in Frage kommt und wer ausgeschlossen bleibt.

Je mehr man über die Nutzerinnen und Nutzer weiß, desto (vermeintlich) genauer können Werbekampagnen adressiert werden. Die Hoffnung besteht dann in höheren Erlösen für Werbeeinblendungen als bei konventionellen Maßnahmen wie z.B. kontextbasierter Werbung. Die mitunter hohe Präzision der kommerziellen Werbekampagnen zeigt, dass dieses Targeting durchaus funktioniert und auch auf andere Einsatzbereiche angewendet werden kann. Untersuchungen legen nahe, dass auch im politischen Wahlkampf datenbasierte Werbemodelle zunehmend genutzt werden, um mit politischer Werbung den Wahlausgang aktiv zu beeinflussen.

Zur Macht der digitalen Plattformbetreiber gehören demnach eine Vielzahl technischer Verfahren vorrangig mit dem Einsatzziel, das Verhalten von Personen in statistisch relevanter Weise annähernd genau vorherzusagen, und damit für die Platzierung von Werbebotschaften und das Setzen von Kaufanreizen zu nutzen. Für die Verfahren der Online-Personalisierung können regelmäßig grob drei verschiedene Stadien im Prozess der Informationsgenerierung unterschieden werden: 1. Die Datengewinnung, 2. Die Datenanalyse und Datenbewertung, 3. Die gezielte Ansprache der Nutzer.

b. Data Warehousing und Data Mining als Vorläufer von Big Data

Fortschreitende Digitalisierung und globale Vernetzung haben bereits seit einigen Jahrzehnten die immer weitere Erfassung von Lebensbereichen zur Folge. Wer Internetdienste, Mobiltelefone und Kundenkarten nutzte, musste schon früh die weitgehende Preisgabe vielfältiger persönlicher Daten an die beteiligten Unternehmen gewärtigen. Während Erfassung und Speicherung von anfallenden Daten für die Unternehmen immer einfacher und kostengünstiger wurden, wuchs das Interesse an der Auswertung und Verwertung der anfallenden Datenmengen. Die Kommerzialisierung der Datenverarbeitung war bereits Mitte der 90er Jahre in vollem Gange. Das Verständnis von Datenbeständen als weitgehend ungenutzt bleibendes Informationskapital der Unternehmen setzte sich langsam durch. Vor diesem Hintergrund entstanden IT-Strategien des sog. Data Warehousing und die damit verbundenen IT-Technologien, um unterschiedlichste Datenbestände von Unternehmen in einheitlichen, von den operativen Daten getrennten Datenbanken für unterschiedlichste Zwecke der Unternehmen verfügbar machen zu können.[5]Daten verschiedenster Geschäftsbereiche werden danach gesondert gebündelt, aggregiert und in einheitlichen Datenbanken gespeichert und aufbereitet, um auf diesen Datenbeständen möglichst genaue Auswertungen, etwa nach Produktionsartikeln, Kunden, Regionen oder Zeiträumen händisch oder mit unterstützenden Tools durchführen zu können. Diese gezielte Nutzung von zu anderen Zwecken erlangten Informationen und Daten zur gezielten Beobachtung und Analyse von Kundenpräferenzen und Kundenverhalten stellt die Grundlage für die Bildung von Kundenprofilen, das sog. Profiling[6] dar.

Im Mittelpunkt datenschutzrechtlicher Bewertung standen und stehen dabei Geschäftsmodelle des Customer Relationship Management, bei denen Kundendaten gezielt zur Kundenbindung einschließlich der gezielten Kundenansprache ausgewertet werden. Typischerweise können dabei auch weitere, die Kunden betreffende Daten von außen einbezogen und zur Anreicherung der Datensätze genutzt werden. Es entstehen umfangreiche Datensammlungen mit aussagekräftigen Kundenprofilen. Auch wenn dabei automatisierte Tools zur Verfügung stehen, bleibt es bei der Auswertung auf der Basis von Analysten und deren erstellten Hypothesen. Oft bilden

5 Vgl. hierzu insgesamt Scholz in : Roßnagel, Handbuch Datenschutzrecht 2000, 9.2, S. 1837.

6 Vgl. dazu die Legaldefinition in Art. 4 Abs. 4 DSGVO sowie Art. 22 DSGVO zu speziellen Anforderungen, näher dazu unten.

die enormen Datenmengen des Data Warehousing die Grundlage für auf diese Datenmengen zum Einsatz kommende automatisierte Analyseverfahren.

Unter dem Schlagwort Data Mining etwa werden schon seit 20 Jahren diverse Methoden und Verfahren bezeichnet, mit denen eine automatisierte Analyse von großen Datenbeständen mit Hilfe von Algorithmen erfolgt. Dabei geht es um die Suche nach Mustern und Zusammenhängen in den Daten mittels Datenanalysen, zunehmend auch, um neue, bislang unbekannte Wissenszusammenhänge aufzudecken. Die Suche nach typischen Verhaltensmustern von konkreten Kunden und die automatische Erstellung von ganzen Kundenklassen nach den so auffindbaren Mustern rückte damit weiter in den Vordergrund. So können Kunden z.B. aus den Unternehmensinteressen heraus als unsichere Schuldner oder als potentiell wechselwillige Vertragsnehmer identifiziert und rechtzeitig entsprechend angesprochen/ behandelt werden. Grundlage für diese Auswertungen des Data Warehouse sind wiederum Kundenprofile, seien sie nun individualbezogen (etwa aufgrund der Einkaufshistorie) oder als nach bestimmten Merkmalen typisierte Kundenklassen, die Einzelnen zugeordnet werden.

So bedeutsam diese Entwicklung aus der Sicht der Unternehmen etwa für die Effektivierung der Kundenansprache und damit für die Erreichung ihrer geschäftlichen Ziele auch geworden ist, für den Datenschutz der Betroffenen bedeutet diese Entwicklung eine erhebliche Verschlechterung: besonders das wichtige Schutzkonzept der Zweckbindung von personenbezogenen Daten gerät unter Druck, mit dem der Dekontextualisierung von aus unterschiedlichsten Lebenszusammenhängen stammenden Informationen und Daten entgegengewirkt werden soll. Die Betroffenen werden damit für die Unternehmen umfänglicher durchleuchtbar und letztlich potentiell auch leichter manipulierbar. Es entsteht ein zunehmendes Machtungleichgewicht zwischen datensammelnden und –verarbeitenden Unternehmen auf der einen Seite sowie den Bürgerinnen und Bürgern auf der anderen Seite.

c. Konzepte des Scoring

Zu den bereits älteren Verfahren der Personalisierung zählt auch das sog. Scoring. Scores oder Kundenwerte bilden einen Unterfall des rechtlich geregelten Profiling. Mit Kreditscoring bezeichnet werden etwa mathema-

tisch-wissenschaftlich nachvollziehbare[7] Bewertungsmodelle[8], bei denen Bürgerinnen und Bürger nach bestimmten Merkmalen klassifiziert werden, so etwa im Hinblick auf ihre Bonität oder ihre Profitabilität für das Unternehmen. Eingesetzt werden auch hier seit langem algorithmengestützte Verfahren. Fragwürdig sind häufig die Qualität der verwendeten Datenbasis sowie die Kriterien, die sich häufig nach bloßen Ähnlichkeiten bestimmen, ohne notwendig mit der Lage der Person übereinzustimmen, wie z.B. Zugehörigkeit zu einer bestimmten Gruppe in der Bevölkerung im Hinblick auf Wohnort, Alter, Migrationshintergrund, Beruf oder Hobby. Der zu Personen ermittelte Scorewert stellt somit einen Wahrscheinlichkeitswert über ein bestimmtes zukünftiges Verhalten einer natürlichen Person dar und wird entweder inhouse oder bei einem externen Dienstleister erstellt. Das bekannteste Scoring-Verfahren ist das Kreditscoring der Auskunfteien wie der SCHUFA. Ein anderes Beispiel ist das sog. Geoscoring, also die Bestimmung von Scorewerten nach dem örtlichen Umfeld wie etwa der Zahlungsfähigkeit der Wohngegend/ Nachbarschaft unter Außerachtlassung der individuellen Situation der Betroffenen genießt ebenfalls einen schlechten Ruf, nicht zuletzt auch mit Blick auf die gesellschaftlichen Auswirkungen, wenn entsprechende Bewertungen Vorurteile gegenüber ganzen Stadtteilen erst schaffen oder vorhandene Vorurteile praktisch validieren und perpetuieren. Bekannt ist der Einsatz von Scoreverfahren den Bürgerinnen und Bürgern auch aus dem Online-Versandhandel: nur wer die erforderlichen Scorewerte erreicht, erhält die gewünschte Ware bzw. Dienstleistung per Rechnung, bekommt die Gelegenheit, über das elektronische Lastschriftverfahren zu bezahlen oder darf kostenfrei zurücksenden.[9]

Die quantitative und qualitative Zunahme von Distanzgeschäften, insbesondere per Internet, steigert die praktische Bedeutung der Verfahren für die Betroffenen. Scores bestimmen inzwischen auch seit langem, mit welcher Werbung man konfrontiert wird, ob überhaupt, und wenn ja welche Verträge mit welchen Bedingungen angeboten werden, ob eine Information bereitgestellt oder eine Zugangserlaubnis erteilt wird.[10] Das Grundproblem dieser Verhaltensbewertung auf der Grundlage von blei-

7 Zu den Anforderungen an die Wissenschaftlichkeit vgl. Ehmann in: Simitis, Kommentar zur DSGVO, 2019, Anh. 2 zu Art. 6, Rdnr. 39.

8 Bloße statistische Korrelationen werden daher nicht als Scoring eingestuft, vgl. Ehmann in: Simitis, Kommentar zur DSGVO, 2019, Anh. 2 zu Art. 6, Rdnr. 29.

9 Vgl. etwa Moos/Rothkegel ZD 2016, S. 561.

10 So Weichert, ZRP 2014, 168 mit Verweis auf eine schon damals vom BMJV in Auftrag gegebene Forschungsstudie.

benden statistischen Verfahren liegt darin, dass relevante, das Leben zum Teil ganz erheblich beschränkende Entscheidungen über Personen getroffen werden, die primär auf der Basis eines statistischen Urteils getroffen werden, welches zumeist auch noch intransparent bleibt. Statistiken können im Einzelfall jedoch durchaus danebenliegen, bestimmte Personen oder Personengruppen ungerechtfertigt diskriminieren und ihre Marginalisierung zementieren. Zur Behebung von Machtasymmetrien im Wirtschaftsleben hat unsere Rechtsordnung aufwändige Regelungen geschaffen. Sie zielen durchweg auf Mitsprache und Stärkung der wirtschaftlich Schwächeren, um ihnen eine gerechte Teilhabe am Wirtschaftsleben zu ermöglichen. Transparenz und Beteiligungsrechte sichern dieses Menschenbild etwa der mündigen Verbraucher ab. Scoringverfahren ohne ausreichende Transparenz, Qualitätskontrolle, menschliche Aufsicht und Mitsprache der davon Betroffenen stehen tendenziell im Widerspruch zu diesen Maßstäben unserer Rechtsordnung.

d. Big Data, Algorithmen und Künstliche Intelligenz

Unter Big Data werden begrifflich Konzepte und technische Verfahren zusammengefasst, bei denen große Mengen an Daten gesammelt, verfügbar gemacht und für sog. Big Data-Analysen u.a. mit dem Ziel der Mustererkennung ausgewertet werden. Das, was heute „Big Data" genannt wird, ist nichts völlig Neues, sondern hat sich aus bestehenden Instrumenten wie eben den oben beschriebenen Data Warehousing-Praktiken weiterentwickelt.[11]Große Datenmengen fallen insbesondere bei der Nutzung des Internets und der Beobachtung von Internetaktivitäten an, bei Nutzung von Wearables, bei Vorhandensein von Sensoren oder bei altbekannten Produkten, die nun vernetzt sind, wie z.B. Fahrzeugen. Ihre Erzeugung ist inzwischen in allen Bereichen der Wirtschaft Ziel einer sog. Datenpolitik bzw. Datenökonomie und Gegenstand von zahlreichen Regulierungsanstrengungen.[12]

Big Data-Verfahren zeichnen sich u.a. durch Weiterentwicklungen bei den Faktoren Menge an Daten, Geschwindigkeit der Bereitstellung sowie der Breite der erfassbaren Datenformate aus. Das Versprechen für die Unternehmen bleibt wie bei den Vorläufern des Data Warehousing das-

11 Ebenso vgl. Weichert ZD 2013, 251.

12 So etwa beim Entwurf der EU-Kommission für einen Data-Governance-Act, ferner bei den Datenstrategien der EU sowie der Bundesregierung von 2020.

selbe: die Entdeckung von bislang verborgenen Zusammenhängen in Datenmengen, mit deren Hilfe Geschäftsmodelle effektiviert und Innovationen ermöglicht werden sollen. Unterschieden[13] werden etwa Verfahren nicht personalisierter Musterkennung für Verhaltensmodelle (predictive analytics), Simulationen oder intelligente Stromnetze, ferner datenschutzrechtlich wesentlich problematischere Verfahren der Kumulation von Daten zur Identifikation und Selektion von Personen im Wege der Erkennung von Mustern aus einer unstrukturierten Datensammlung. Ziel dabei ist gerade, konkrete Individuen zu isolieren und zu erkennen wie z.B. bei Betrugspräventionsverfahren oder bei Formen des völlig zu Recht heftig umstrittenen Predictive Policing. Schließlich unterschieden werden Verfahren, bei denen durch laufende Kumulation, Aggregation und Auswertung vorhandener Daten bzw. unter Hinzuspeichern weiterer Daten zu einem bereits existierenden Datensatz neue, spezifischere Informationen zu einer bereits zuvor individualisierten natürlichen Person generiert werden, so etwa beim Tracking und Targeting oder etwa speziellen Versicherungstarifen wie den sog. Pay-as-you-Drive-Angeboten.[14]

Grundlage sind auch hier zunächst die zum Teil mit dem Begriff der Künstlichen Intelligenz gleichgesetzten Algorithmen. Unter einem Algorithmus kann eine eindeutige, ausführbare Folge von klar definierten Handlungsanweisungen endlicher Länge zur Lösung eines Problems verstanden werden.[15] Algorithmen können zum Zweck der Datenauswertung, Wissensgenerierung und damit Ermittlung von Entscheidungskriterien eingesetzt werden. Algorithmen, die zur Entscheidung selbst eingesetzt werden, stellen eine Weiterentwicklung dar und werden oft unspezifisch als „intelligente Systeme“ bezeichnet. Diese intelligenten Systeme sind im Wesentlichen durch drei Elemente gekennzeichnet: Sie setzen große, hochqualitative Datenmengen für ihren Erfolg voraus, sind als eigenständig lernende Algorithmen konstruiert (also nicht mehr vollständig vorab durch Menschen programmiert) und sind nach wie vor in gewissem Umfang von menschlicher Begleitung bei Entwicklung und Einsatz abhängig.[16] Sie gelten als Schlüsselressource des 21. Jahrhunderts und sollen in praktisch allen Lebensbereichen die digitale Entscheidungsautomatisierung bis hin zu autonomen Systemen (zum Beispiel selbstfahrende Autos)

13 Vgl. Schulz in Gola, DSGVO, 2018, Art. 6 Rdnr. 254.
14 Gola, a.a.O., Rdnr. 258.
15 Ernst, JZ 2017, 2019.
16 Vgl. dazu im Einzelnen Wischmeyer, AöR 2018, S. 10 ff.

vorantreiben und damit die Wettbewerbsfähigkeit der Wirtschaft sichern helfen.

In der Praxis der Online-Welt hingegen sieht ihr Einsatz so aus: der News Feed[17] von Facebook und der den Nachrichten zugrundeliegende Algorithmus ist weitgehend intransparent.[18] Soweit bekannt, vermischt er politische und soziale News mit kommerzieller Werbung und dürfte entsprechend der kommerziellen Zielsetzungen des Unternehmens im Ganzen hochgradig personalisiert sein. Es liegt nahe, dass der Algorithmus allein oder vorrangig darauf ausgerichtet ist, Informationen einzuspielen, für welche eine Person zu bezahlen bereit sein wird und sie außerdem möglichst lange auf der Plattform zu binden. Dementsprechend wird der Algorithmus auch entscheiden, dieser Person andere, womöglich unter Vielfaltsgesichtspunkten oder Nachrichtenwert bedeutsame Informationen ggf. vorzuenthalten. Denn datenbasierte algorithmische Auswertungssysteme „erkennen" nicht wirklich, ob es sich um neutrale Inhalte (z.B. Kuchenrezept) oder um meinungsrelevante Inhalte (z.B. Tagesgeschehen, politische Äußerungen usw.) handelt und nicht, ab wann ein zunächst neutraler Inhalt meinungsrelevant wird. Das System differenziert technisch bedingt individualisiert nach zahlreichen Interessen und Informationen, die sich bei der Interaktion zwischen Nutzer, Werbetreibenden und Intermediär ermitteln lassen.[19]Eine ausgewogene Meinungsvielfalt, wie sie etwa nach der Rundfunkfreiheit des Grundgesetzes als Zielvorstellung besteht, dürfte mit zahlreichen Angeboten der bestehenden Plattformen von kommerziellen Informationsintermediären daher schon aus technischen Gründen kaum vereinbar sein. Im Gegenteil: Fast zwangsläufig „wählen" die Algorithmen die emotionale Zuspitzung aus, weil diese die Interaktionen der Nutzerinnen und Nutzer mit der Plattform und anderen erhöht.

Zutreffend ist längst erkannt, dass die nunmehr der Digitalisierung zugrundeliegenden Algorithmen und zunehmend intelligenten Systeme selbst eine Art der Regulierung darstellen, allerdings eine, der sich die Betroffenen, anders als bei der demokratisch erzeugten Regulierung durch Recht, nicht entziehen können. Die derart ausgeübte faktische Macht fordert die Demokratie heraus und erfordert Antworten zugunsten von Recht (als Freiheitsordnung), Selbstbestimmung und demokratischen Struktu-

17 Dass der Newsfeed von Facebook je nach Einspielung von eher positiven oder negativen Nachrichten die Stimmungen der Nutzerinnen und Nutzer wirkungsvoll und gezielt emotional beeinflussen kann gilt als wissenschaftlich gesichert, vgl. Böhme-Neßler, GewA 2019, S. 219 m.w.N.

18 Gillespie Fn. 6, zitiert bei Boehme-Neßler, GewA 2019, 129.

19 Schwartmann/Hermann/Mühlenbeck, MMR 2019, 498, 501.

ren. Mit einer bloßen Ethik allein der Programmierer und der von diesen in Algorithmen eingeschriebenen, häufig eher technodeterministischen Weltbilder ist es nicht getan.

Die rechtlichen Konsequenzen des Einsatzes von intelligenten Systemen bei der Personalisierung von Online-Diensten sind schon für sich betrachtet, also ohne das Zusammenspiel mit den Personalisierungsverfahren selbst, vielfältig. Ihre auf Korrelationen basierende, nicht-deterministische Funktionsweise und ihre dynamisch sich laufend ändernden Systemzustände machen sie für Laien praktisch kaum noch verstehbar bzw. intransparent und auch für herkömmliche externe Beaufsichtigung kaum zugänglich. Der aufwändige Prozess der Entwicklung und Anlernung der Systeme wirft schwierige Fragen danach auf, wie z.B. der tatsächliche Erfolg bzw. die Geeignetheit ihres Einsatzes gemessen/nachgewiesen und mögliche Diskriminierungen bestimmter Personengruppen verhindert werden können. Aus datenschutzrechtlicher Perspektive potenzieren sich damit die auch bereits beim Einsatz der deterministischen Vorläuferprogramme aufgeworfenen Fragen insbesondere der Transparenz bzw. schon der Nachvollziehbarkeit der Funktionsweise der Programme.

e. Targeting und Microtargeting

Microtargeting stellt eine besondere Form und Weiterentwicklung des gewöhnlichen Targeting dar.

Mit Targeting bezeichnet man im Marketing die zielgruppenorientierte und gezielte (Timing; Ort; Art der Darstellung etc.) Platzierung von Ansprache und Werbung, u.a. auf der Grundlage der zuvor beschriebenen Schritte der Sammlung und Analyse von Profilen. Die individuelle Ansprache mit Werbung richtet sich nach bestimmten unterschiedlichen Kriterien und Vorgehensweisen. Je nach verwendeten Kriterien unterscheidet man etwa Keyword Advertising, Geotargeting, Semantisches Targeting und etwa auch das Predictive Behavioral Targeting. Das Keyword Advertising und Semantisches Targeting kommt insbesondere bei Suchmaschinen sowie bei der Auswertung von geschriebenen Texten/aufgerufenen Webseiten zum Einsatz, die etwa beim Auftauchen eines bestimmten Begriffs in der Suchmaske dieses Keyword in einem vollautomatischen Prozess und nahezu in Echtzeit an Werbetreibende als potentielles Werbeziel melden

und die Schaltung der Werbung versteigern.[20] Bei Geotargeting hingegen geht es um die Schaltung regionaler, standortabhängiger Werbung in Abhängigkeit vom Vorliegen etwaiger hinreichend brauchbarer Standortinformationen. Diese können etwa über die IP-Adressen von Computern, aber inzwischen bei Mobilfunkgeräten auch über die Erfassung der Einwahldaten in TK-Netze ermittelbar werden.

Beim Predictive Behavioural Targeting werden zunächst, gewissermaßen im Kleinen, Interessengruppen durch gezielte Auswertung von soziodemografischen Angaben, Surfverhalten, Vorlieben und Abneigungen und z.B. auch Befragungen ermittelt. Diese in ihrem Verhalten und bei Vorliegen der Merkmale relativ gesichert vorhersehbaren Gruppen werden nun mit Hilfe von komplexeren algorithmischen Verfahren auf alle Nutzerinnen und Nutzer im Wege statistischer Verfahren erweitert.

In Social Media Plattformen kommen alle der bekannten Formen des Targeting nebeneinander zum Einsatz.[21] Dabei ist davon auszugehen, dass diese Plattformen vollständig geloggt und für Zwecke der Werbung und Kundenbindung ausgewertet werden d.h. praktisch jede unterscheidbare Interaktion der Nutzerinnen und Nutzer mit diesen Plattformen kann der Auswertung für personalisierte Werbung oder Bindungsmaßnahmen zugeführt werden. Wie im Fall von Facebook kann die Zusammenführung und Verknüpfung der Daten unterschiedlichster datensammelnder Dienste des Unternehmens für das Targeting eingesetzt werden.[22]

Das sog. Microtargeting stellt im Wesentlichen eine Weiterentwicklung des Behavioural Targeting auf der Grundlage von Big Data-Analysen und dem Einsatz von intelligenten Systemen dar. Genutzt werden psychometrische Verfahren, um Vorhersagen über Persönlichkeit und emotionale und motivationale Lebenslagen zu machen. Auf dieser noch feiner granulierten Basis soll Werbung gezielter ausspielbar werden. Es werden nicht nur die Inhalte, sondern auch die Art und Weise der Ansprache individualisiert. Microtargeting nutzt dazu Kundendaten und demografische Daten, um die Interessen einzelner oder kleiner Gruppen ähnlich denkender Personen zu identifizieren.[23] Der Kreis der Kunden wird dann auf der Grundlage dieser Gruppen kategorisiert. Ziel ist, das Verhalten der Nutzer auf der Grundlage des Wissens über sie in Richtung der eigenen kommerziellen

20 Vgl. zu diesem unübersichtlichen Feld statt aller Christl/Spiekermann, Networks of Control, Wien 2016 (auch online abrufbar).

21 Zur datenschutzrechtlichen Bewertung liegt eine aktuelle Stellungnahme des Europäischen Datenschutzausschusses.

22 Vgl. NZKart 2020, 473-483.

23 Vgl. TAB-Bericht Kind/Weide, Themenkurzprofil Nr. 18 Mai 2017.

Interessen und der der eigenen Werbekunden zu beeinflussen. Entscheidend ist nun, dass in der Summe der zur Anwendung kommenden Verfahren durchgehend alle angezeigten oder eben auch die überhaupt nicht auftauchenden Inhalte der technischen Kuratierung durch Algorithmen und damit auch der individualisierten Sortierung unterliegen. Im Ergebnis erleben die Nutzer der großen Plattformangebote alle ein unterschiedliches Facebook, Google usw. Im Hinblick auf die Schaltung von Werbung wird dieses Vorgehen gerechtfertigt mit dem unterstellten Wunsch auch der Nutzer, möglichst passgenaue Angebote zu erhalten.

Das politische Microtargeting im Fall des Unternehmens Cambridge Analytica wurde zunächst ermöglicht durch Bereitstellung einer App („thisisyourdigitallife"), mit der Umfragen geschaltet wurden. Über eine Programmierschnittstelle von Facebook konnten problemlos auch die Daten der Kontakte der App-Nutzer hinzugezogen und verknüpft werden. Auf diese Weise waren die Daten von mehr als 50 Millionen Menschen weltweit erfasst und für Zwecke politischer Wahlwerbung verfügbar.[24] Zu den Kennzeichen dieser psychometrisch unterstützten Ausspielung politischer Werbung zählt, dass sie in bislang nicht erreichter Datendichte arbeitet. Facebook etwa bietet Anzeigenkunden –und damit auch politischen Parteienwährend des Wahlkampfs – die Möglichkeit den Kreis der Empfänger mittels psychografischer Eigenschaften zu bestimmen und anhand von Geschlecht, Alter, Aufenthaltsort, besuchten Webseiten, politischer Einstellung und anderen Datenpunkten die Zielgruppe einer Anzeige zu bestimmen.[25] Für die Öffentlichkeit werden diese Kampagnen praktisch nicht sichtbar, denn sie sind nur für den bestellten Zeitraum und nur für den ausgewählten Empfängerkreis sichtbar. So erlaubt dieses Instrument Parteien potentiell nicht nur, zeitgleich widersprüchliche politische Aussagen je nach Zielgruppe zu treffen oder Kampagnen gezielt auf die Hinderung bestimmter Gruppen an der Teilnahme an Wahlen auszurichten. Es verhindert insbesondere, dass der Rest der demokratischen Öffentlichkeit von den Aussagen Kenntnis nehmen, diese auf den Wahrheitsgehalt der Aussagen hin zu prüfen und sie bei der eigenen Willensbildung auf die eine oder andere Weise zu berücksichtigen vermag.[26]

---

24 Zum Fall insgesamt Wolfie Christl, in APuZ 24-26/2019, https://www.bpb.de/apuz/292335/datenoekonomie.

25 Sehr detailliert beschrieben und erläutert bei Christl, APUZ 24/26, 2019, abrufbar unter https://www.bpb.de/apuz/292349/microtargeting-persoenliche-daten-als-politische-waehrung.

26 Schemmel, Der Staat 2018, 501–527.

Während es zutrifft, dass womöglich auch mit Hilfe des Microtargeting sich wieder mehr Bürgerinnen und Bürger für Politik und Demokratie interessieren und die nach Art. 21 Grundgesetz geschützten politischen Parteien auch mit diesem Instrument ihrem Auftrag womöglich besonders effektiv nachgehen könnten, liegen die Risiken für die Meinungsbildung als auch für die demokratische Kultur insgesamt auf der Hand: der Einsatz von politischem Microtargeting erlaubt zumindest bei bestimmten Vorgehensweisen nicht weniger als die gezielte Manipulationen der öffentlichen Meinung (nicht nur bei anstehenden Wahlen), ohne dass dieses von den nicht adressierten Teilen der Öffentlichkeit wahrgenommen werden können. Dass selbst einige Plattformen die Auswirkungen zunehmend mit einer gewissen Angst wahrzunehmen scheinen, zeigt sich in den Versuchen, mehr Transparenz in die geschalteten Anzeigenkampagnen zu schaffen, in dem es Übersichtsseiten für eine Überprüfung geben soll.

3. Folgerungen für Öffentlichkeit und Demokratie

a. Beitrag zur Fragmentierung der Öffentlichkeit

Auch das Phänomen der Öffentlichkeit und dessen Verbindung mit den Funktionsweisen von Demokratie ist wesentlich medial bedingt. Anders gesagt: Entwicklungen bei Informations- und Kommunikationstechniken fungieren als Medienfaktoren und können den Wandel von Legitimations- bzw. Demokratieprozessen befeuern.[27]

Das Gesamtbild des Einsatzes von Personalisierungstechniken bei bekannten digitalen Angeboten gerade im Bereich Social Media belegt eine schon heute hohe Dichte von mit modernster Technik individualisierten Oberflächen und Funktionen. Die zum Einsatz kommenden Verfahren und Technologien erzeugen eine digitale Erfahrung, die mit der Erfahrung von anderen Nutzern derselben Plattform kaum vergleichbar, jedenfalls praktisch kaum jemals identisch sein dürfte. Die damit einhergehende Individualisierung der online erlebten Wirklichkeit vermag so, spätestens mit der sich abzeichnenden weiteren Zunahme[28] der Nutzung digitaler Medienöffentlichkeiten, wohl auch gesamtgesellschaftliche Wirkungen er-

27 Ingold, Der Staat 56 (2017), 491–533.

28 Bislang nutzt die deutliche Mehrheit der bundesdeutschen Bevölkerung noch die etablierten Kanäle von Funk, Fernsehen und Druckpresse zur Information und Meinungsbildung.

zeugen, etwa zu einer weiteren Fragmentierung[29] von Öffentlichkeit als Bühne und zentralem Element der Meinungsbildung beizutragen. Die medienwissenschaftliche Wirkungsforschung gilt dazu bis heute allerdings als noch zu wenig aussagekräftig.[30] Die mit Medien wie Facebook oder etwa auch Twitter geschaffenen, besonderen Formen von selektiven Teil-Öffentlichkeiten sind von vornherein und jeweils individuell vorgefiltert und bestätigen eher die kritische Vermutung der Entstehung von sog. Filterblasen,[31] in denen gleichförmige Aussagen und Gleichgesinnte überwiegen und die Konfrontation mit der Lebenswirklichkeit und der tatsächlich bestehenden Vielfalt von Auffassungen, aber auch mit hochwertigen und gesicherten Inhalten stark herabgesetzt sein kann. Die Konfrontation sowie die inhaltliche Auseinandersetzung mit anderen Meinungen, aber auch die Gewöhnung an den Umgang etwa mit wissenschaftlich belegten bzw. objektivierten, qualitätsgesicherten Inhalten kann dann vermindert sein.

Es ist bezeichnend, dass das Bundesverfassungsgericht kürzlich in einer Entscheidung zum öffentlich-rechtlichen Rundfunk (unter Bezugnahme auf die Arbeiten des Deutschen Bundestages in der Enquete Internet und Digitale Gesellschaft) hervorgehoben hat, dass die Gefahr hinzukomme, „dass – auch mit Hilfe von Algorithmen – Inhalte gezielt auf Interessen und Neigungen der Nutzerinnen und Nutzer zugeschnitten werden, was wiederum zur Verstärkung gleichgerichteter Meinungen führt. Solche Angebote sind nicht auf Meinungsvielfalt gerichtet, sondern werden durch einseitige Interessen oder die wirtschaftliche Rationalität eines Geschäftsmodells bestimmt, nämlich die Verweildauer der Nutzer auf den Seiten möglichst zu maximieren und dadurch den Werbewert der Plattform für die Kunden zu erhöhen. Insoweit sind auch Ergebnisse in Suchmaschinen vorgefiltert und teils werbefinanziert, teils von „Klickzahlen" abhängig."[32]

---

29 Vgl. dazu Spiecker gen. Döhmann, Kontexte der Demokratie: Parteien – Medien – Sozialstrukturen, VVDStRL 77 (2018); Schemmel, a.a.O.; kritisch differenzierend mit Blick auf den Begriff der Öffentlichkeit Ingold, Der Staat, 2017, S. 509.

30 So etwa Ingold, a.a.O.; Neuere Hinweise bei EU Kommission, COM(2021) 262 final.

31 Zu dem von Eli Pariser geprägten Begriff der Filter Bubble als einer Art kommunikativer Komfortzone vgl. bestätigend Hoffmann-Riem, AöR 2017, S. 13, der auch gesamtgesellschaftliche Wirkungen wie die Fragmentierungsthese für möglich hält. Zur Diskussion insgesamt vgl. auch Lischka/ Stöcker, Digitale Öffentlichkeit, Bertelsmann-Stiftung 2017; ferner die Nachweise unter Fn. 21.

32 Vgl. BVerfG, Beschluss des Ersten Senats vom 20. Juli 2021 - 1 BvR 2756/20 -, Rn. 1-119.

Der These von der auf diese Weise einfachen Manipulierbarkeit politischer Meinungen könnte zwar entgegengehalten werden, dass es derartige Filterblasen doch schon immer (etwa in Gestalt der selektiv präsentierten Inhalte einer Tageszeitung) gegeben habe und doch die Verbreitung etwa von politischer Werbung über digitale Plattformen insoweit ein Wahlkampfinstrument wie jedes andere darstelle. Doch dies verkennt, neben den bereits genannten Möglichkeiten gezielter missbräuchlicher Nutzung, schon die mangelnde Vergleichbarkeit qua hybrider Aufmachung und interaktiver Form der Kommunikation als Grundlage. Soziale Netzwerke kommen öffentlich nicht als Werbeunternehmen daher, die sie ihrem Unternehmensziel nach sind. Das Bewusstsein der Nutzerinnen und Nutzer über die auch bei Funktionen wie Newsfeeds durchweg nach kommerziellen Interessen präsentierte und „ge-nudgte" Realität dürfte weithin nach wie vor zu gering sein.

Der Vollständigkeit halber sei hier gesagt, dass auch andere Auswirkungen des Micro-Targeting verheerend sein können, so z.B. Verwirrungsstrategien gegenüber entstehenden sozialen Bewegungen durch Fake-Profile mit gezielten Ansprachen. Die Fragmentierungsgefahr, die von mancher Seite bestritten wird, steht also keineswegs allein, sondern ist nur die am meisten untersuchte bzw. diskutierte potenzielle Auswirkung.

b. Addiction by Design – Engführung von Aufmerksamkeit auch per Oberflächengestaltung

Datenverarbeitungstechnik wirkt sich stets auf die Datenbasis und die gewinnbaren Informationen aus. Und ihr Einsatz und ihre Anwendungen wirken auf soziale Zusammenhänge zurück und prägen letztendlich, als sog. soziotechnisches System, auch soziale Systeme und deren Abläufe. In datenschutzrechtlicher Hinsicht bestimmen vor allem diese sozialen Auswirkungen die rechtliche Bewertung, nicht die Technik selbst.

In komplexen soziotechnischen Systemen hilft damit der alleinige Blick auf die eingesetzten Technologien nicht weiter. Auch das weitere Setting des Technikeinsatzes muss betrachtet werden. Eigentlich bieten im Onlinebereich gerade die Mensch-Maschine-Schnittstelle der Angebotsoberflächen und die damit bestehenden Interaktionsmöglichkeiten reichlich Platz für Reflexion, Selbstbestimmung und Demokratie stärkende Elemente. Konkret angelegt sind solche Elemente etwa in den gesetzlichen datenschutzrechtlichen Regelungen für mehr Transparenz und die Absicherung der Zustimmung der Nutzerinnen und Nutzer. Dagegen stehen freilich die auf Automatisierung und eher Unhinterfragbarkeit angelegten

Geschäftsmodelle. Gerungen wird seitens der Unternehmen deshalb mit Gesetzgeber und Aufsichtsbehörden gerade bei diesen Fragen um jeden Millimeter dieser Oberfläche. Ein gutes Beispiel dafür bieten die endlosen Debatten und rechtlichen Entscheidungen zu Opt-In/ Opt out bei Cookie-Bannern im Internet, zur Ausgestaltung von online abrufbaren AGB, der Anzahl der zu setzenden Häkchen der User usw.[33]

In der Realität bleiben Social-Media-Umgebungen auf weitgehend automatisierte Abläufe und Entscheidungsentlastung angelegt. Dieses im Design angelegte, gezielte Unterlaufen bewusster Reflexion scheint durchweg in Abläufe und Funktionen eingebaut, worauf etwa die wachsende auch datenschutzrechtliche Debatte um Designelemente digitaler Oberflächen wie die sog. dark patterns und auch das sog. Nudging, also das gezielte kommerzielle Ausnutzen von angeborenem bzw. erlernten menschlichen Verhaltensmuster wie Heuristiken und Biases hinweisen.[34] Dazu zählt z.B. auch die gezielt auf Abhängigkeiten (Addiction by Design) setzende Steuerung der Newsfeeds mit laufend neuen emotionalen Inhalten, um die Aufenthalts- und Nutzungszeit der Nutzer gezielt auszudehnen. Als Grundeinstellung sind viele Feeds auf automatische Einspielung des nächsten Beitrags als eines endlosen Streams ausgerichtet. Die Sorge um den Menschen als „Digital Unconscious", also als Objekt unbewusster Steuerung, erhält damit auf gleich mehreren Ebenen Nahrung. Das Postulat individueller Autonomie aus Artikel 2 Abs. 1 Grundgesetz droht faktisch durch technisch fundierte, als solche nicht oder eben nur schwer erkennbare Fremdsteuerungen unterlaufen zu werden.[35]

4. Antworten des Datenschutzes und Grenzen

Für die meisten der hier im Einzelnen und beispielhaft vorgestellten Techniken und Verfahren gibt es im Datenschutzrecht bereits relativ etablierte rechtliche Maßstäbe und es gilt die Datenschutzgrundverordnung. Die Frage nach den Auswirkungen der digitalen Personalisierung insbesondere

33 Vgl. EuGH, Urteil v. 1. Oktober 2019 – C-673/17 und auch BGH, Urteil v. 28. Mai 2020 – I ZR 7/16.

34 Aus der juristischen Literatur etwa Weinzierl, NVwZ 2020,1087. Instruktiv dazu sind die Untersuchungen von VZBV und Stiftung Neue Verantwortung, vgl. https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste/dark-patterns-so-wollen-websites-und-apps-sie-manipulieren-58082 mit weiteren Nachweisen.

35 Hoffmann-Riem, AöR 2017, S. 6.

bei den genannten Plattformen als sogenannte „Informationsintermediäre" für Öffentlichkeit und Demokratie berührt auch den Datenschutz, kann aber sicher mit diesem allein angesichts der überindividuell angelegten Problematik der Wahrung von Meinungsvielfalt nicht beantwortet werden.

Auf die Grenzen der Bearbeitbarkeit der mit Big Data und intelligenten Systemen einhergehenden strukturellen Machfragen durch ein vorrangig auf den Schutz individueller Persönlichkeitsrechte ausgerichtetes Datenschutzrecht wird denn auch durch eine Reihe von Autoren zutreffend hingewiesen.[36]

Das Grundrecht auf Datenschutz nach Art. 8 der Grundrechtecharta (und Art. 16 AEUV) statuiert das Recht jeder Person auf den Schutz der sie betreffenden personenbezogenen Daten. Datenschutz soll nicht etwa die Daten schützen, sondern gegen Gefährdungen durch die automatisierte Datenverarbeitung. Im Mittelpunkt steht, wie schon unter der alleinigen Geltung des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 Grundgesetz, der Schutz der Persönlichkeit und auch der Erhalt des Würdeschutzes. Der Datenschutz dient insoweit dem Schutz der Bürgerinnen und Bürger vor der Herabwürdigung zu einem bloßen Objekt der Entscheidung, Ausspähung oder auch der Manipulation. Er zielt auf Transparenz und die Mitbestimmung und Beteiligung der von Datenverarbeitung Betroffenen. Die Bausteine seines Schutzprogramms werden bei den genannten Verfahren und Datenverarbeitungen der Personalisierung auf Plattformen der Informationsintermediäre in unterschiedlichem Umfang relevant.

Nach dem grundgesetzlichen Datenschutzkonzept findet auch die Demokratie als Schutzgut insoweit regelmäßig mit Erwähnung, weil das Bundesverfassungsgericht die Demokratie als auf der selbstbestimmten Entfaltung seiner Bürgerinnen und Bürger basierend versteht: Ohne selbstbestimmten Informationsaustausch ist jede Verwirklichung von Grundrechten durch Kommunikation gefährdet.[37] Zugleich ist informationelle Selbstbestimmung die Grundlage einer demokratischen Kommunikationsverfassung. Denn Selbstbestimmung ist „eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens.[38] Auch individuel-

36 Hoffmann-Riem, a.a.O., S. 7; ferner Wischmeyer a.a.O., S. 31.

37 Roßnagel, ZD 2013, S. 562, mit umfänglichen Erwägungen zu den konzeptionellen Herausforderungen von Big Data.

38 BVerfGE 1, 43.

le Entwicklung und Entfaltung kann nur gelingen, wenn grundlegende Schutzmuster des Datenschutzes die Betroffenen und damit auch die Demokratie selbst wirkungsvoll zu schützen vermögen.

Angesicht dieses eher weiten Schutzkonzepts des Datenschutzes mit einer Vielzahl von Schutzgütern erscheint es nicht ausgeschlossen, dass mögliche Auswirkungen der Personalisierung auf die Demokratie und die Wechselwirkungen zwischen technisch enggeführten digitalen Öffentlichkeiten einerseits und den zu schützenden individuellen Entwicklungsmöglichkeiten der Bürgerinnen und Bürger andererseits schon de lege lata unter gewissen Umständen datenschutzaufsichtsbehördliche Berücksichtigung finden. Denn Umfang und Tiefe der Personalisierung sowie die weitgehende Intransparenz der Datenverarbeitung ermöglichen tiefgreifende Beeinflussungs-/Manipulationsmöglichkeiten auch im Hinblick auf öffentliche Diskurse und damit demokratische Verfahren, die auf die informationelle Selbstbestimmung zurückwirken. Je mehr valide Hinweise auf demokratie- als auch persönlichkeitsrelevante manipulative Vorgehensweisen wie Desinformation, Aufstachelung zum Hass und gezielte gesellschaftliche Spaltung bis hin zu politischem Microtargeting demokratiegefährdender Prägung bekannt werden, desto eher können solche Praktiken einschränkende Entscheidungen gerechtfertigt sein.

Der Datenschutz befasst sich wie bereits gezeigt seit langem mit Social Media, Big Data und KI. Im Mittelpunkt stand und steht dabei die mögliche Beeinträchtigung der Persönlichkeitsrechte der Bürgerinnen und Bürger durch die mit diesen Geschäftsmodellen und Verarbeitungspraktiken verbundenen Methoden und Verfahren. Im Rahmen einer aufsichtsbehördlichen Prüfung wird deren Einsatz je gesondert auf Zulässigkeit geprüft und bewertet.

Die DSGVO als rechtlicher Rahmen

Nach der Datenschutzgrundverordnung (DSGVO) bedarf es für die von Webplattformen eingesetzten Verfahren der Personalisierung einer eindeutigen Rechtsgrundlage nach Artikel 6 DSGVO. In der Regel bleibt den Unternehmen angesichts der hier in Rede stehenden weitgehenden Datenverarbeitung nichts anderes als die Einwilligung nach Art. 6 Abs. 1 a. samt der Anforderungen für die Einwilligung nach Art. 7 DSGVO. Was zunächst als eine die Selbstbestimmung der Nutzerinnen und Nutzer bestmöglich berücksichtigende Lösung und als Königsweg einer freiheitlichen Gesellschaft angesehen wurde, hat sich in der Praxis gerade der großen On-

line-Plattformen allerdings längst in sein Gegenteil verkehrt.[39] Die Einwilligungslösung nach der DSGVO bietet den Informationsintermediären Raum für weitreichende Alles-oder-Nichts-Vertragslösungen. In der Kombination mit umfänglichen AGB und zumeist vage formuliert, nutzen die zu ihren Gunsten laufende völlige Asymmetrie der Informationsverteilung und die Überforderung der Nutzerinnen und Nutzer für ihre Zwecke aus und erhalten Einwilligungen als vermeintlichen Freibrief mindestens für den impliziten Einsatz aller genannten Personalisierungsverfahren. Die datenschutzrechtlichen Prinzipien der Zweckbindung und Datenminimierung laufen weitgehend leer, wenn und weil auf Grundlage der so eingeholten Einwilligung die Daten bei Einbindung in Big-Data-Analysen laufend und für höchst unterschiedliche Zwecke eingesetzt werden.

Auf diese fragwürdige datenschutzrechtlich vielfältig angreifbare Praxis der Webunternehmen haben auch die Datenschutzaufsichtsbehörden bislang leider noch keine durchgreifende Antwort finden können. Das hat, neben weiteren Gründen[40], mit praktischen Mängeln des europäischen Abstimmungsverfahrens der Aufsichtsbehörden zu tun. Denn die Mehrzahl der großen Plattformunternehmen haben ihre europäischen Hauptniederlassung in nur wenigen EU-Mitgliedsstaaten wie Irland und unterliegen nach dem sog. One-Stop-Shop-Verfahren zunächst der alleinigen Aufsicht der bisher äußerst langsam agierenden dortigen Behörde.[41]

Weitere Aspekte der Datenschutzgrundverordnung betreffen die Regelung des Profiling in Art. 4 Nr. 4 DSGVO und die automatisierte Entscheidung im Einzelfall nach § 22 DSGVO.

Profiling nach Art. 4 Nr. 4 ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Deutlich wird, dass die Definition die weiteren hier getroffenen Unterscheidungen nach technischen Verfahren wie Tracking, Scoring oder Tar-

39 Vgl. statt vieler: Hoffmann-Riem, a.a.O., S. 23.

40 Dazu zählen etwa die Unbestimmtheit und zum Teil zu enge Fassung potentiell einschlägiger Bestimmungen der DSGVO dar, siehe nachfolgend.

41 Und das Kooperations- und Kohärenzverfahren zur Klärung von Streitigkeiten über die mehrere Aufsichtsbehörden erlaubt es bislang nicht hinlänglich, insoweit gegen das Nichthandeln einzelner Aufsichtsbehörden wirksam vorzugehen, vgl. Weber/Dehnhardt ZD 2021, S. 63.

geting nicht kennt, sondern allein nach dem Ziel der Verarbeitung einordnet. Die weit gehaltene Definition und Einordnung bleibt im Hinblick auf das grundsätzliche Verbot der ausschließlich automatisierten Verarbeitung (einschließlich Profiling) in Artikel 22 DSGVO folgenlos, denn für die Rechtfertigung gelten wie bereits erläutert die allgemeinen Zulässigkeitsbestimmungen des Artikel 6 DSGVO, womit pauschal der Weg zur Einwilligung eröffnet bleibt.

Es ist besonders misslich, dass der europäische Gesetzgeber sich im Hinblick auf die Personalisierungsverfahren auf keine differenzierenden und den Datenschutz der Betroffenen in den Mittelpunkt stellenden Regelungen einigen konnte. Hier muss dringend nachgebessert werden.[42]

In ihrem nicht verfügenden Teil gibt die DS-GVO ferner vor, Betroffenen „aussagekräftige Informationen über die involvierte Logik" mitzugeben (Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h) sowie „geeignete mathematische oder statistische Verfahren für das Profiling" sowie Korrekturmechanismen zu verwenden, um die Risiken für die Persönlichkeit sowie Diskriminierungsgefahren zu minimieren (ErwGr 71 UAbs. 2 S. 1). Umfang und Inhalt dieser Bestimmungen sind umstritten, böten allerdings durchaus ebenfalls Möglichkeiten, etwa mit Blick auf den Einsatz intelligenter Systeme und deren derzeitig ungelöstes Transparenz- bzw. Nachvollziehbarkeitsproblem grundlegendere Fragen an die Plattformbetreiber zu stellen.

Insgesamt sollte deutlich geworden sein, dass auch der jetzige, wenn bereits in Teilen reformbedürftige datenschutzrechtliche Rahmen durchaus Anknüpfungspunkte für das Einschreiten von Aufsichtsbehörden gegen aktuelle Praktiken bei den Personalisierungsverfahren der Plattformen bietet. Dabei handelt es sich allerdings um zeitlich wie inhaltlich aufwändige Verfahren, die schlussendlich auch nicht primär das gewünschte Ziel der Sicherstellung von Meinungsvielfalt auf Plattformen als zunehmend relevante Teilöffentlichkeiten der Demokratie verfolgen, sondern am Schutz der Datenschutzrechte der betroffenen Nutzerinnen und Nutzer ausgerichtet sind.

42 Vgl. die Forderungen der Datenschutzbehörden aus Anlass der ersten Evaluation der DSGVO im Erfahrungsbericht der Datenschutzkonferenz vom 6.11.2019, abrufbar unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/20191113_Erfahrungsbericht_DS-GVO.pdf.

5. Elemente der rechtspolitischen Debatte

a. EU-Vorschläge zur Regulierung des digitalen Sektors

Das Thema der Auswirkungen der Digitalisierung auf die Demokratie, etwa wie hier in Gestalt der Fragmentierung durch Personalisierung, führt direkt in die zentrale und strittige Debatte um Plattform- und Algorithmenregulierung. Die Digitalisierung der Medien und insbesondere die Netz- und Plattformökonomie des Internet einschließlich der sozialen Netzwerke begünstigen Konzentrations- und Monopolisierungstendenzen bei Anbietern, Verbreitern und Vermittlern von Inhalten. So ist schon deshalb klar, dass weit über das Datenschutzrecht hinaus Bereiche wie etwa das Wettbewerbs- und Kartellrecht betroffen sind.

Der digitale Wandel fordert die Diskussion über Umfang und Inhalt des Datenschutzes und erforderliche Weiterentwicklungen auf vielen Feldern heraus. Über den weiteren Umgang mit den auch in diesem Kontext maßgeblichen, die Verfahren und Technologien prägenden und steuernden Algorithmen bei Online-Plattformen scheint zumindest in Brüssel derzeit die Grundentscheidung getroffen. Mit der Vorlage des weltweit ersten Gesetzentwurfs zur KI-Regulierung, dem sog. Artificial Intelligence Act[43], hat die EU-Kommission ihren Anspruch unterstrichen, wertegeleitete Regulierung auch bei dieser als wirtschaftlich besonders schützenswerten Innovation in Anschlag zu bringen. Im Hinblick auf den Einsatz von intelligenten Systemen für die hier gegenständlichen Personalisierungsverfahren erscheint es durchaus sachgerecht, im Rahmen dieses Gesetzgebungsverfahrens rote Linien etwa für die Zulässigkeit des Microtargeting für Werbezwecke zu ziehen.

Mehr Regulierung soll ferner sowohl europäische Datensouveränität als auch den Schutz der Persönlichkeitsrechte und die Datenschutzrechte der Bürgerinnen und Bürger stärken und die Markt- und Meinungsmacht der bestehenden großen Plattformen einhegen.[44] Zutreffend wird die Verantwortung und auch Schutzpflicht für einen effektiven Schutz der Grund-

---

43 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.

44 Vgl. etwa die EU-Datenagenda und die inzwischen vorliegenden Gesetzentwürfe der EU-Kommission insbesondere zum sog. Digital Markets Act sowie zum Digital Services Act.

rechte und die Umsetzbarkeit bestehender gesetzlicher Schutzprogramme beim Staat verortet. Im Detail enthalten diese Gesetzentwürfe allerdings allesamt deutliche Schwächen und auch Regelungslücken. Was von den Plänen letztlich im politischen Prozess umsetzbar sein wird bleibt abzuwarten.

Von Datenschutzbehörden[45] bereits gefordert und unterstützungswürdig erscheint die Initiative von einer Reihe Abgeordneten aus dem Europäischen Parlament zum Digital Services Act für eine erhebliche Beschränkung und letztlich das Ende des feingranulierten Online-Microtargeting, wie es gerade von den großen Plattformunternehmen praktiziert wird.[46]

Von grundlegender Bedeutung ist auch der im Entwurf für den Digital Services Act vorgesehene Datenzugang gerade für Behörden, aber auch für Forscher in Art. 31 DSA-E. Er könnte, datenschutzrechtlich sauber geregelt, tatsächlich dabei unterstützen, die Phänomene von Hassrede und Falschnachrichten einschließlich der etwaigen Beschleunigung durch die Systemfunktionalitäten der großen Plattformen besser zu verstehen, Wirkungsweisen zu validieren und auf dieser Basis sachgerechte Problemlösungen zu entwickeln[47]. In diese Richtung geht auch die Bestimmung des § 5a des Netzwerkdurchsetzungsgesetzes (NetzDG), der Forschungsinstitutionen Zugang zu den Nutzungsdaten der Intermediäre einräumt, um die Wirkungsweise des Einsatzes von Algorithmen zu untersuchen und besser zu verstehen.

b. Privacy-by-Design als weiterhin möglicher Ausweg

Die umfassende Personalisierung der Nutzererfahrung und die damit ermöglichte Ausspähung und Manipulation im Online-Bereich mag einen Ausblick darauf geben, was erst mit den erwartbaren Angeboten des Internet of Things (IoT)[48] und dem sog. Ubiquitous Computing auf der

45 Vgl .Stellungnahme 1/2021 zum Data Services Act des Europäischen Datenschutzbeauftragten, abrufbar unter https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf.

46 Tracking-Free-Ads-Coalition, vgl. etws den Bericht unter https://www.heise.de/news/Targeting-EU-Abgeordnete-fordern-Aus-fuer-spionierende-Werbung-5041368.html. Die Forderung der entsprechende Initiative hat bislang nicht Eingang in die Position des federführenden EU-Ausschusses gefunden.

47 Vgl. dazu sowie zu DMA und DSA insgesamt etwa Gielen/Uphues EuZW 21, 627.

48 Vgl. aktuell zu Entwicklungen des IoT Kreye, SZ vom 2.10.2021.

Grundlage allgegenwärtiger Sensorik des Alltages insgesamt auf unsere Gesellschaften zukommt.

Statt angesichts der weitreichenden Folgen der Personalisierungen nun das Recht, den Datenschutz oder auch die Demokratie gleich ganz neu zu erfinden, mag es angesichts der bedeutenden Veränderungen der Online-Kommunikationen, die ja nur Vorboten sehr viel weiter gehender Veränderungen aller unser Lebensbereiche sind, darauf ankommen, erst einmal das bestehende Recht innovativ weiter zu entwickeln. Hierzu liegen inzwischen eine Fülle von Vorschlägen vor, die auch die Regulierung der hier gegenständlichen Personalisierung der Angebote von Informationsintermediären bzw. großen Informations- und Kommunikationsplattformen zumindest in ihren Teilaspekten angehen. Die größte Aufmerksamkeit erfährt dabei die Regulierung der Künstlichen Intelligenz.

An erster Stelle wird im Datenschutz seit langem die Kooperation von Technik und Recht genannt, konzeptionell im Datenschutz bekannt als Privacy-By-Design.[49] Erst mit einem eingebauten Datenschutz ab Werk (auch als sog. Privacy-By-Default) würde es dem Datenschutz gelingen, gewissermaßen vor die Lage zu kommen und bereits im Entwicklungsprozess Berücksichtigung bei Unternehmen und Programmierern zu finden, die noch auf absehbare Zeit die Hoheit über den Entstehungsprozess behalten werden. Dazu müsste die Anwendung dieses weiterhin wichtigen Konzeptes, auch wenn es jahrelang lediglich als wenig schlagkräftiges Soft Law behandelt wurde, allerdings auch verpflichtend auf die Hersteller von IT-Systemen erstreckt werden.

Im Rahmen der Debatte um Künstliche Intelligenz wird dies als Eingriff in die Algorithmenentwicklung diskutiert, um bestimmte rechtliche Zielsetzungen zu gewährleisten. In dieselbe Richtung gehen Vorschläge, KI selbst für die Durchsetzung von rechtlichen Zielen einzusetzen, eine wachsende Debatte in vielen Bereichen. So wird im Verbraucherschutzrecht die Idee personalisierter Verbraucherinformationen diskutiert.[50]

---

49 Geregelt in der DSGVO in Art. 25 Abs. 1. Als technische und organisatorische Maßnahmen, die proaktiv einzurichten und aktiv zu betreiben sind, gelten insbesondere Datenminimierung, Pseudonymisierung, Schnittstellen zur Transparenz für Information, Intervention und Audit, sowie die Überwachung durch Verantwortliche. Eine Grundlage zur Planung von „Privacy by Design" ist die Datenschutz-Folgenabschätzung mit einer zugehörigen Risiko-Analyse für die Privatheit der Anwender des Systems in Art. 35 DS-GVO.

50 Vgl. zur noch jungen Debatte die Gutachten unter https://www.svr-verbraucherfragen.de/2021/09/21/personalisierte-verbraucherinformation-ein-werkstattbericht/.

Schließlich hat die EU-Kommission in ihrem Democracy Action Plan[51] weitere Maßnahmen zum Erhalt der Medienfreiheit und des Pluralismus angekündigt und dabei konkret unter dem Gesichtspunkt der Gefahr von Desinformation angekündigt, etwa das Problem der politischen Werbung regulierend aufgreifen zu wollen.[52]

6. *Das Gutachten der Datenethikkommission*

Das Gutachten der Datenthikkommission (DEK)[53] hat die Wahrung und Förderung von Demokratie und gesellschaftlichem Zusammenhalt als einen der Leitgedanken ihrer umfänglichen Studie zur Digitalisierung formuliert. Hervorgehoben werden Digitale Technologien als systemrelevant für die Entfaltung der Demokratie. Sie ermöglichen neue Formen der politischen Beteiligung, können aber auch Gefahren im Hinblick auf Manipulation und Radikalisierung mit sich bringen. Die DEK empfiehlt Maßnahmen gegen ethisch nichtvertretbare Datennutzungen, darunter auch gegen die Integrität der Persönlichkeit verletzende Profilbildung, gezielte Ausnutzung von Vulnerabilitäten, sog. Addictive Designs und Dark Patterns, und dem Demokratieprinzip zuwiderlaufende Beeinflussung politischer Wahlen.[54]

Mit Blick auf Künstliche Intelligenz und die besonderen Gefahren von Medienintermediären mit Torwächterfunktion für die Demokratie empfiehlt die DEK der Bundesregierung umfängliche ex-ante-Verfahren der Zulassung zu prüfen. Der EU-Gesetzgeber hat diese Vorschläge in seinem bisherigen Vorschlag allenfalls unzureichend aufgegriffen und setzt eher auf eine Selbstregulierung der Anbieter. Die DEK empfiehlt allerdings auch, die Anbieter in diesem engen Bereich zum Einsatz solcher algorithmischer Systeme zu verpflichten, die den Nutzern zumindest als zusätzliches Angebot auch einen Zugriff auf eine tendenzfreie, ausgewogene und die plurale Meinungsvielfalt abbildende Zusammenstellung von Beiträgen

51 Aktionsplan für die Demokratie, vgl. https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_de.

52 Vgl. dazu die aktuelle Mitteilung der EU-Kommission COM(2021) 262 final, abrufbar unter.

53 Gutachten von 2018, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.

54 Vgl. S. 18.

und Informationen verschaffen.[55] Eine entsprechende Pflicht zur Statuierung von Neutralitätsgeboten und Vielfaltsvorgaben erscheint der DEK etwa auch mit Blick auf den Schutz Minderjähriger vor Beeinflussung durch und über soziale Netzwerke geboten.[56]

7. Ausblick

Eine generelle Zurückdrängung personalisierter Angebote in digitalen Angeboten erscheint mit Blick auf die langjährige Praxis und Akzeptanz durch Nutzerinnen und Nutzer weder erreichbar noch sonderlich sinnvoll. Schließlich werden Funktionen der auf persönliche Präferenzen setzenden Unterstützung angesichts der wachsenden Auswahl an Informationen immer relevanter. Gleichwohl gilt es, auch mit deutlichen, schon auf die Erhebung von Daten beschränkenden Vorgaben dort zu reagieren, wo Demokratie und persönliche Selbstentfaltung gravierend beeinträchtigt werden.

Im Einklang mit dem Europäischen Datenschutzbeauftragten fordert auch der BfDI deshalb langfristig ein Verbot von gezielter Online-Werbung, die auf durchdringenden Formen des Tracking basiert sowie eine Einschränkung sensibler Datenkategorien, die für solche Werbemethoden verarbeitet werden können. Mit der wirkungsvollen Beschränkung von zumindest einzelnen Elementen der Personalisierung kann der Datenschutz, wenn auch mittelbar, einen Beitrag auch zum Erhalt pluraler Meinungsvielfalt und demokratischen Strukturen leisten. Darüber hinausgehende Anstrengungen insbesondere des europäischen Gesetzgebers sind erforderlich, um dem Menschenbild der europäischen Grundrechtecharta als auch dem Grundgesetz entsprechend Demokratie und Selbstbestimmung auch in der beschleunigten Digitalisierung zu gewährleiten.

55 Vgl. S. 30.
56 Vgl. S. 230.

Soziale Medien und Kuratierung von Inhalten. Regulative Antworten auf eine demokratische Schlüsselfrage

Christian Djeffal

Dieser Beitrag erläutert die sozio-technische Funktionsweise der Kuratierung von Inhalten in sozialen Medien. Er zeigt, wie die der öffentlichen Debatte durch künstliche Intelligenz strukturiert wird und diskutiert mögliche regulatorische Antworten. An verschiedenen Beispielen der vergangenen Jahre lässt sich zeigen, dass Dynamiken in sozialen Medien sowohl Menschenrechte als auch demokratische Werte gefährden können. Um diesen Entwicklungen zu begegnen, gibt es unterschiedliche regulatorischen Ansätzen auf verschiedenen Ebenen. Der vorliegende Beitrag erörtert aktuelle Gesetzgebungsvorhaben und gibt einen Ausblick auf neue Möglichkeiten, den Fragen der Kuratierung von Inhalten zu begegnen.

I. Die Kuratierung von Inhalten in der Entwicklung des Internets

A. Auf dem Weg zu sozialen Medien

In den frühen Tagen des Internets waren Interaktionen unmittelbar und die Kommunikation auf Kenntnisnahme von Inhalten ausgerichtet.[1] Das Aufrufen von Seiten setzte Adressen voraus, die man oft über Verzeichnisse organisierte. Die Kommunikation über E-Mail oder Chats bezog sich ebenfalls auf Personen mit Adressen oder Namen, die man bereits kannte oder auf Listen fand. In dieser Zeit kuratierte jeder Nutzer sein eigenes Internet über Adressbücher und Linklisten.[2] Damals wuchs aber die Zahl der Inhalte und der Nutzer so stark, dass es kaum möglich war, einen Überblick über alle relevanten Informationen und Personen zu behalten. Verschiedene Trends befeuerten diesen Wandel. Zum einen war es die rasante Kommerzialisierung des Internets, die auch zu einer stetigen Suche

1 Bernstein, William J.: Masters of the word. How media shaped history from the alphabet to the internet, London 2013, S. 224.

2 van Dijck, José: The culture of connectivity. A critical history of social media, Oxford 2013a, 5.

nach Innovationen und neuen Anwendungsmöglichkeiten führte. Zum anderen erlaubten Trends wie Open-Source-Software oder das Bloggen immer mehr Menschen, online gestalterisch aktiv zu werden.[3] In dieser Situation schlug die Stunde der Intermediäre. Sie haben in unterschiedlichen Konstellationen Vermittlungsdienste wahrgenommen und Angebot und Nachfrage zueinander gebracht, ohne selbst Teil von Dienstleistungen oder Konversationen zu sein. Suchmaschinen vermitteln Inhalte im Netz an Suchende, e-Commerce-Portale vermitteln Angebote für bestimmte Waren, soziale Netzwerke vermitteln Kommunikationsinhalte. Aufgrund der schieren Menge der Informationen haben sich besonders automatisierte Ansätze bewährt, die das Interesse der Nutzer adäquat erfassen. So erlaubte etwa die Suchmaschinentechnologie eine völlig andere Erschließung des Internets. Sie machte Inhalte auffindbar, deren Ort oder Autor man zuvor nicht kannte oder die man an dieser Stelle nicht vermutet hätte. Ein ähnlicher Effekt stellte sich mit sozialen Medien ein. Sie erlauben es, mit ganz unterschiedlichen Menschen in Kontakt zu treten und Informationen auszutauschen. Diese sozialen Medien beschränken sich aber nicht nur auf die Tätigkeit als Intermediäre, sie sind auch Plattformen, auf denen Menschen Profile anlegen und Interaktionen kreieren können.[4] Auf diesen Plattformen gewinnt die Kommunikation eine neue Qualität, weil sie gleichsam persönlich als auch in größeren Gruppen stattfinden kann. Ein Nutzer kann selbst Inhalte kreieren und sie einer unbegrenzten Anzahl von Nutzern zugänglich machen. Diese können die Inhalte weiterverbreiten oder wieder darauf Bezug nehmen. Dieses Generieren und Teilen von Inhalten ist mittlerweile zum wesentlichen Begriffsinhalt sozialer Medien geworden.[5] Gleichzeitig sorgen Empfehlungsalgorithmen und Filter dafür, dass jeder Nutzer nach bestimmten Kriterien einen persönlichen

3 Stevenson, Michael: From Hypertext to Hype and Back Again. Exploring the Roots of Social Media in Early Web Culture, in: Burgess, Jean, Alice E. Marwick, Thomas Poell (Hrsg.): The sage handbook of social media, London 2018, hier: S. 80–81.

4 Siehe zum Plattformbegriff aus unterschiedlichen Perspektiven van Dijck, José: The culture of connectivity. A critical history of social media, Oxford 2013b, S. 31–48.

5 Aichner, Thomas, Matthias Grünfelder, Oswin Maurer, Deni Jegeni: Twenty-Five Years of Social Media. A Review of Social Media Applications and Definitions from 1994 to 2019, in: Cyberpsychol Behav Soc Netw, Bd. 24, 2021, S. 215–222, hier: S. 220.

Ausschnitt der Inhalte sieht. So werden soziale Medien als neue Iteration des Internets angesehen, die auch als Web 2.0 bezeichnet wird.[6]

Es ist vielfach anerkannt worden, dass soziale Medien zu einem „Strukturwandel der Öffentlichkeit" geführt und damit grundlegend verändert haben, was öffentliche Kommunikation bedeutet.[7] Soziale Medien sind heute Teil des Alltags, sie gehen aber tatsächlich auf eine Reihe von Innovationen zurück, die auf algorithmischen Automatisierungen basieren. Diese betreffen die Frage, welche Inhalte einzelnen Nutzern angezeigt werden. Die Kuratierung und der Vorschlag von Inhalten wirken auf den ersten Blick unwichtig und trivial. Weil sich aber die Aufmerksamkeit von Nutzern nur auf bestimmte Stellen reduziert und im Übrigen flüchtig ist, liegt im Kuratieren von Informationen eine bedeutsame Gestaltungsmacht. Denn durch die Kuratierung wird das geformt, was die Nutzer überhaupt an Informationen wahrnehmen können. Das Kuratieren von Inhalten beeinflusst also die wahrgenommene Realität der Nutzer.[8] Plattformen im Web 2.0 haben dazu geführt, dass der Internetnutzer nicht nur Suchender ist, sondern auch gefunden werden kann. Dadurch, dass Inhalte vermittelt werden, ist der Einzelne adressierbar und erreichbar geworden. Dies wurde möglich, weil Einzelne ein Profil anlegen und als Person in Erscheinung treten. Dadurch ergaben sich ganz neue Möglichkeiten, aber auch Notwendigkeiten Inhalte zu kuratieren.

Sowohl die Ereignisse der letzten Jahre als auch mögliche Entwicklungen sozialer Medien erfordern eine genauere Befassung mit dem Thema der Kuratierung, ihren Konsequenzen und ihrer rechtlichen Regelung. Bereits lange werden problematische Konsequenzen der Kuratierung diskutiert und kritisiert, darunter die Konsequenzen von Falschnachrichten, Hassrede und jugendgefährdenden Inhalten. Radikalisierungstendenzen während der Pandemie und die Stürmung des Kapitols machen diese Frage umso dringender. Die vertiefte journalistische und zivilgesellschaftliche Auseinandersetzung mit dem Thema kulminierte in der Berichterstattung um die Facebook Files bzw. Facebook Papers, die die Debatte um die Neu-

---

6 Jenkins, Henry, Sam Ford, Joshua Green: Spreadable media. Creating value and meaning in a networked culture (Postmillennial pop), New York, London 2013, S. 49.

7 So jüngst mit Rückgriff auf seine eigene Theorie Jürgen Habermas: Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit, in: Seeliger, Martin, Sebastian Sevignani (Hrsg.): Ein neuer Strukturwandel der Öffentlichkeit? (Leviathan Sonderband), Baden-Baden 2021, S. 470–500.

8 Milano, Silvia, Mariarosaria Taddeo, Luciano Floridi: Recommender systems and their ethical challenges, in: AI & Soc, Bd. 35, 2020, S. 957–967, hier: S. 957.

gestaltung sozialer Medien befeuert haben. Währenddessen verlagern sich Teile der Kommunikation in Messengerdienste. Man spricht in diesen Fällen, in denen Inhalte weder Vermessen noch nachverfolgt werden können, von „dark social media". Gleichzeitig bereiten sich viele Unternehmen auf eine weitere Welle der Virtualisierung vor, die als Metaverse bezeichnet wird. Vor diesem Hintergrund wird die Befassung mit Fragen der Kuratierung von Inhalten noch dringender.

B. Bedeutung und Sinn der Kuratierung

Kuratieren soll hier in einem umfassenden Sinn verstanden werden. Im Kontext von sozialen Medien kann es sich um verschiedene Inhalte handeln, insbesondere um Texte, Bilder, Videos und Tondateien.[9] Die Komplexität der Aufgabe wird dadurch gesteigert, dass die Formate auch kombiniert werden, etwa Bilder und Texte in sog. Memes.[10] Unter Kuratierung fasst man verschiedene Handlungen.[11] Zum einen geht es um den Ausschluss von Inhalten. Durch Filter werden Inhalte blockiert und können nicht erscheinen, durch Löschprozesse werden sie nach ihrem Erscheinen entfernt.[12] Ein weiteres Verständnis von Kuratierung schließt allerdings auch Empfehlungssysteme (recommender systems) mit ein. Diese Empfehlungsmechanismen lenken die Aufmerksamkeit der Nutzer. Sie steuern, welche Inhalte den Nutzern so präsentiert werden, dass sie mit höherer Wahrscheinlichkeit wahrgenommen werden. In erster Linie wird dies über die Reihenfolge der Inhalte gewährleistet. In der Regel werden dabei insbesondere die Inhalte wahrgenommen, die der Nutzer auf den ersten Blick erfassen kann. Ferner können Inhalte durch das Layout hervorgehoben werden. Im Falle von Videos werden die besonders wahrgenommen, die automatisch abgespielt werden. Auch durch das Weblayout kann die Aufmerksamkeit gesteuert werden, wenn Inhalte etwa farblich hervorgehoben oder aber mit einem Zusatz wie „Werbung" versehen werden. Andere Inhalte werden damit nicht ausgeschlossen, die Wahrschein-

9 Cambridge Consultants: Use of AI in online content moderation 2019 (im Folgenden: Cambridge Consultants, Use of AI in online content moderation), S. 4.

10 ebda., 30ff.

11 Grimmelmann, James: The Virtues of Moderation, in: Yale Journal of Law and Technology, Bd. 17, 2015, hier: 56ff. Dieser sieht 5 Tätigkeiten von Kuratierung umfasst, nämlich Ausschluss, Bepreisung, Organisation, und Normierung.

12 Roberts, Sarah T.: Behind the screen. Content moderation in the shadows of social media, New Haven 2019b, S. 33.

lichkeit ihrer Kenntnisnahme schwindet allerdings. In den Worten „content moderation" kommt deutlicher zum Ausdruck, dass Kuratierung auch einen kommunikativen Aspekt hat, der ebenfalls die Inhalte beeinflusst.

Die Kuratierung von Inhalten reagiert damit auf verschiedene gesellschaftliche Bedürfnisse, die aus der Perspektive von Akteuren verständlich werden. Auf der Seite der Plattformbetreiber ist die Kuratierung von Inhalten die Grundlage eines neuen Geschäftsmodells. Dieses besteht bei den meisten sozialen Medien daraus, dass Nutzern auf Plattformen ein Interaktionsraum geboten wird, der anziehend wirkt. Neben der Kuratierung von Nutzerinhalten treten die Betreiber sozialer Medien auch als Vermittler von Werbung auf. Die Betreiber bilden Profile auf der Grundlage der Daten, die Nutzer auf der Plattform hinterlassen.[13] Das erlaubt Werbetreibenden, zielgerichtet Werbung für bestimmte Profilgruppen zu schalten. So sind Betreiber sozialer Medien zu wichtigen Akteuren im Internet-Werbemarkt geworden, der nach Schätzungen im Jahr 2023 weltweit über 60% des Umsatzes mit Werbungen ausmachen wird.[14] Nach Prognosen werden soziale Medien 2023 erstmals zum umsatzstärksten Werbemedium werden und das Fernsehen überholen.[15] Aus der Möglichkeit des Schaltens von Werbungen ergibt sich auch ein zentrales Ziel für soziale Medien: Die Kuratierung der Inhalte soll so ausgestaltet werden, dass Nutzer möglichst viel Zeit auf der Plattform verbringen und möglichst intensiv involviert werden. Daraus kann man auf das Interesse von Plattformen schließen, Inhalte zu filtern, die vom Verweilen auf der Plattform abhalten.

Auf der Seite der Nutzer geht es um die Organisation von Informationen und um den Schutz ihrer Rechte und Interessen. Der oben erwähnte Überfluss an Informationen im Internet führt dazu, dass Nutzer auf eine Vorauswahl angewiesen sind, um Dienste überhaupt nutzen zu können. Durch die Kollektivierung der Kommunikation ist ein neuer Diskursraum entstanden, in dem unterschiedliche Nutzerinteressen berührt sein können. Zum einen haben Nutzer die Möglichkeit, ihre Meinungsfreiheit auf eine neue Weise auszuüben, sich Gehör zu verschaffen und gleichzeitig andere Stimmen als zuvor wahrzunehmen. Die Praxis der sozialen Medien führte aber dazu, dass auch Inhalte geteilt werden können, die zu erheb-

13 Siehe dazu in diesem Band: Bach, Ruben, Frauke Kreuter: Big Data in einer digitalisierten, datengestützten Demokratie, S. 119ff.

14 Zenith: Digital advertising to exceed 60% of global adspend in 2022 2021, https://www.zenithmedia.com/digital-advertising-to-exceed-60-of-global-adspend-in-2022/, 09.12.2021 (im Folgenden: Zenith, Digital advertising to exceed 60% of global adspend in 2022).

15 ebda.

lichen Rechtsverletzungen von Nutzern führen. Dazu zählen Bilder, die Persönlichkeitsrechte oder das Urheberrecht verletzen, oder Hassrede.[16] Mittlerweile ist davon auszugehen, dass die Nutzung von sozialen Medien mit einer Vielzahl von nachteiligen Konsequenzen für die Nutzer einhergehen kann, die unmittelbar oder mittelbar mit der Kuratierung von Inhalten zusammenhängen. Bereits seit einiger Zeit wird über Nachteile für das Wohlbefinden und die psychische Gesundheit insbesondere von Heranwachsenden debattiert. Ein sprechendes Beispiel ist der Fall Molly Russel, der im Vereinigten Königreich für viel Aufsehen sorgte. Molly Russel nahm sich kurz vor ihrem 14. Geburtstag das Leben. Ihre suizidalen Tendenzen wurden durch die sozialen Medien verstärkt. Dabei wurden Inhalte so kuratiert, dass sie einer großen Anzahl von suizidalen Inhalten ausgesetzt war.[17]

Es liegt im Interesse der betroffenen Nutzer, dass diese Inhalte gelöscht oder blockiert werden. Staat und Verwaltung verfolgen öffentliche Interessen und wollen vor entsprechenden Inhalten schützen. Dazu gehört etwa das Verbreiten terroristischer Werbung oder volksverhetzender Inhalte. Nicht verschwiegen werden darf, dass die Kuratierung von Inhalten auch die Interessen derer betrifft, die diese Aufgabe zu ihrem Beruf gemacht haben. Viele Menschen arbeiten als Dienstleister für Plattformen oder Dritte und helfen bei der Bewertung der Inhalte. Seit langem ist aber bekannt, dass ihre psychische Gesundheit beeinträchtigt werden kann, wenn sie in hohem Maße belastenden Inhalten einschließlich Gewaltvideos oder Kinderpornographie ausgesetzt sind.[18]

Aus dieser kurzen Kartierung der Interessen ergibt sich, dass sich die Interessen verschiedener Akteure decken, aber auch widersprechen können. In den vergangenen Jahren ist dabei deutlich erkennbar geworden, dass aktuelle Kuratierungspraktiken die angesprochenen Probleme wie Falschnachrichten, Hassrede oder das Verbreiten von Inhalten mit ehrverletzendem Inhalt nicht in den Griff bekommen haben. Vielmehr sind die vielfältigen Konsequenzen zu Tage getreten, die soziale Medien haben

16 Gillespie, Tarleton: Custodians of the internet. Platforms, content moderation, and the hidden decisions that shape social media, New Haven 2018 (im Folgenden: Gillespie, Custodians of the internet), 24ff.

17 Molly Russell entered ‘dark rabbit hole of suicidal content’ online, says father, in: The National, 28.10.2019; Urwin, Rosamund, Sian Griffiths: Pinterest emailed suicide tips after Molly Russell’s death, in: The Sunday Times, 27.01.2019.

18 Roberts, Sarah T.: Behind the screen. Content moderation in the shadows of social media, New Haven 2019a, S. 21.

können. Das wirft die Frage auf, wie man soziale Medien regulieren und besser kuratieren kann.

II. Die Kuratierung von Inhalten als sozio-technisches System

Eine zentrale Erkenntnis der Technikтheorie ist, dass Technik nie alleine wirkt, sondern in ihrer gesellschaftlichen Einbettung wirksam wird. So verändern angewandte Technologien die Gesellschaft, die Art und Weise ihrer Wirksamkeit ist aber gleichzeitig auch gesellschaftlich determiniert. Technik „wird in der Gesellschaft gemacht". Ebenso lässt sich eine Gesellschaft, die auf gewissen Technologien fußt, nur mehr vor dem Hintergrund dieser Technologien erklären. Aufgrund dieser Wechselbezüglichkeit sind Technologien in ihrem sozio-technischen Kontext darzustellen. So kann auch die Kuratierung von Inhalten jedenfalls nicht allein durch die Analyse der zugrundeliegenden Technik erfasst werden, vielmehr müssen auch die sozio-technische Sphäre und die Governance-Sphäre analysiert werden. Diese Gliederung erlaubt ein Strukturieren der verschiedenen Aspekte.[19] Die technische Sphäre konzentriert sich dabei auf die unmittelbare technische Wirkweise und die entsprechenden Mechanismen. In der sozio-technischen Sphäre nimmt man die unmittelbare Interaktion von Technik und Gesellschaft in den Blick. In der Governance-Sphäre geht es demgegenüber um generelle Absichten der Steuerung und Beeinflussung. In diesem Sinne soll auch die Kuratierung von Inhalten in zusammengehörigen Sphären verstanden werden.

A. Technische Sphäre

Wie oben beschrieben tragen verschiedene Handlungen zur Kuratierung von Inhalten bei. Jede dieser Handlungen kann auch maschinell unterstützt oder sogar ausgeführt werden, wobei künstliche Intelligenz in der jeweiligen Ausgestaltung eine wichtige Rolle spielen kann. Der Ausschluss von Inhalten wird insbesondere unter dem Stichwort Filtertechnologien diskutiert. Hier kamen ursprünglich einfache Technologien zum Einsatz

19 Djeffal, Christian: Sustainable AI Development (SAID). On the Road to More Access to Justice, in: Souza, Siddarth Peter de, Maximilian Spohr (Hrsg.): Technology, Innovation and Access to Justice. Dialogues on the Future of Law, Edinburgh 2020, 112-130, hier: 118-120.

wie etwa der Abgleich von Wörtern bei Text oder von hash-Werten bei Bildern und Videos.[20] Durch Technologien der künstlichen Intelligenz, die hier nicht ausführlich beschrieben werden können, werden zunehmend bessere Ergebnisse erreicht, die den Kontext immer besser erfassen können. Dennoch bringen auch diese Systeme gewisse Probleme mit sich. In der Regel hängt ihre Genauigkeit (accuracy) vom Vorliegen ausreichender Trainingsdaten ab. Das kann auf der einen Seite zu Diskriminierungen führen, wenn eine bestimmte Gruppe so repräsentiert ist, dass sie stigmatisiert wird, weil sie etwa mit einem bestimmten Vergehen in Verbindung gebracht wird. Eine Unterrepräsentation kann demgegenüber zu mangelndem Schutz führen. Fehleranfälligkeit kann problematisch sein, wenn durch fehlende Kontextsensitivität falsche Inhalte unterdrückt werden. So wurden Inhalte eines berühmten Schachkanals gesperrt, weil die ständige Erwähnung von Schwarz und Weiß als diskriminierend gewertet wurde.[21]

Empfehlungssysteme können allgemein definiert werden als „Software-Tools und -Techniken, die Vorschläge für Artikel liefern, die für einen bestimmten Benutzer höchstwahrscheinlich von Interesse sind".[22] Die grundlegendsten Methoden dafür sind entweder inhalts- oder wissensbasiert.[23] Inhaltsbasierte Ansätze untersuchen den Inhalt eines Artikels und das Profil eines Nutzers und versuchen, passende Kriterien zu ermitteln. Wissensbasierte Ansätze nutzen zusätzliches Wissen, um brauchbare Informationen zu finden. Neuere Systeme kombinieren diese Merkmale. Der Begriff kollaboratives Filtern spielt darauf an, dass das Verhalten vieler Teilnehmer in ein Empfehlungssystem einbezogen werden kann. Empfehlungssysteme beruhen auf der Erstellung von Nutzerprofilen und der Verwendung dieser Profile für Empfehlungen. Sie sammeln, speichern und analysieren Daten, die es ihnen ermöglichen, Informationen für die Nutzer zu filtern. Empfehlungssysteme prägen unsere Online-Erfahrung. Sie haben zwar allgemeine Stärken und Schwächen, enthalten aber oft auch spezifische Auswahlmöglichkeiten und sogar Kompromisse. Empfehlungssysteme können auf unterschiedliche Weise gestaltet werden. Durch die Weiterentwicklung der künstlichen Intelligenz und insbesondere durch

20 Cambridge Consultants, Use of AI in online content moderation, S. 48.

21 Knight, Will: Why a YouTube Chat About Chess Got Flagged for Hate Speech. AI programs that analyze language have difficulty gauging context. Words such as "black," "white," and "attack" can have different meanings., in: wired, 01.03.2021.

22 Ricci, Francesco, Lior Rokach, Bracha Shapira (Hrsg.): Recommender Systems Handbook, Second edition, Boston, MA 2015, S. 1.

23 Jannach, Dietmar: Recommender Systems. An introduction, Cambridge 2011, S. 1–5.

das maschinelle Lernen haben Empfehlungsalgorithmen die Möglichkeit erhalten, sich ständig zu verbessern und zunehmend granular zu werden. Sie können sehr spezifische Aspekte von Personen und Inhalten miteinander in Beziehung setzen und möglicherweise neue Verbindungen vorschlagen, die noch nicht entdeckt wurden. Die kontinuierliche Optimierung hat diese Systeme auch effektiver gemacht, da sie in vielen Fällen aus dem aufeinanderfolgenden Verhalten der Person lernen können.

Im Hinblick auf das Design sind Big-Data Methoden insbesondere wichtig, um zu verstehen, welche Auswirkungen bestimmte Ausgestaltungen haben. Intensiv diskutiert wird derzeit über Reaktions-Knöpfe (reaction buttons). So wird davon ausgegangen, dass negative Buttons dazu führen, dass Diskussionen eine negative Wendung nehmen und so u.a. Hassrede und Beleidigungen Vorschub geleistet wird. In diesem Sinne hat etwa Youtube seinen „dislike-button" aus genau diesen Gründen abgeschafft.[24]

B. Sozio-technische Sphäre

Die Kuratierung von Inhalten ist eingebunden in ein enges Netz von Maßnahmen und organisatorischen Aspekten. Zum einen findet an verschiedenen Stellen eine unmittelbare menschliche Beteiligung an den Prozessen statt. Wie bereits erwähnt gibt es zahlreiche Menschen, die unmittelbar mit der Kuratierung von Inhalten befasst sind.[25] In manchen Bereichen sind sie allein für diese Arbeiten verantwortlich, in anderen Bereichen werden schwierige Fälle an sie ausgesteuert. Ferner werden ihre Handlungen auch als Trainingsdaten für künstliche Intelligenz verwendet. Diese Personen können entweder direkt bei den Betreibern der sozialen Medien angestellt sein, sie können ferner für spezialisierte Dienstleister oder selbstständig über sogenannte Micro-Worker-Plattformen arbeiten. Auch den Nutzern kann eine Rolle zukommen, wenn sie etwa in die Kuratierung von Inhalten eingebunden werden. Ein weiterer sozio-technischer Aspekt sind Reaktionsmöglichkeiten für Nutzer, oft „flaggen" genannt. Hierbei können Nutzer Inhalte melden, die nach ihrem Dafürhalten rechtswidrig sind.

---

24 Barrabi, Thomas: YouTube CEO says removing 'dislike' button prevents harmful 'attacks', in: New York Post, 26.01.2022; Meineck, Sebastian: Der Sinn von Dislike-Buttons – das sagt die Wissenschaft, in: netzpolitik.org, 27.01.2022.

25 Gillespie, Custodians of the internet, S. 115.

Ferner bestehen auch jenseits der Trainingsdaten zahlreiche Möglichkeiten, KI-Systeme zur Kuratierung von Inhalten menschlich zu beeinflussen und zu ändern. Denn Menschen treffen zahlreiche Gestaltungsentscheidungen und können auch bei sogenannten lernenden Systemen auf verschiedenen Wegen Einfluss auf die Ergebnisse nehmen. Änderungen in Kuratierungsalgorithmen werden fortlaufend vorgenommen und oft auch genau von kommerziellen Nutzern beobachtet.

C. Governance-Sphäre

Jenseits der unmittelbaren Steuerung gibt es verschiedene allgemeine Instrumente, die zur Steuerung der Kuratierung von Inhalten herangezogen werden können. Diese können in allgemeinen Geschäftsbedingungen oder auch Gesetzen festgehalten werden. Diese Instrumente können unterschiedliche Ziele verfolgen. Es ist von essentieller Bedeutung, dass die Steuerungsziele sich unterscheiden können und sich tatsächlich auch widersprechen. Entscheidend ist der oben erwähnte Konflikt zwischen der Verweildauer der Nutzer und wertsensitiven Entscheidungen.

III. Pfade von Regulierung und Verantwortlichkeit

Vor dem Hintergrund der bereits geschilderten Probleme, aber auch der großen Möglichkeiten und Verheißungen von sozialen Medien stellt sich die Frage, wie man auf die Kuratierung von Inhalten so einwirken kann, dass die schweren Verletzungen individueller und kollektiver Güter abgestellt werden. Als Rahmen für diese Diskussion dienen herkömmlicherweise drei Idealtypen der Regulierung, nämlich Selbstregulierung, Regulierung, und Ko-Regulierung. Anhand dieser Bezugspunkte soll die aktuelle Regulierungsdebatte nachgezeichnet werden.

Im Rahmen der Selbstregulierung sollen Betreiber der Technik selbst für die Schaffung von Regeln und ihre Durchsetzung sorgen. Im Kontext von sozialen Medien funktioniert dies rechtlich durch die Nutzung von allgemeinen Geschäftsbedingungen.[26] Sie werden zwischen den Betreibern und allen Nutzern vereinbart und legen fest, welche Inhalte auf der Plattform erlaubt bzw. verboten sind. So können die Plattformbetreiber zum

26 Belli, Luca, Jamila Venturini: Private ordering and the rise of terms of service as cyber-regulation, in: Internet Policy Review, Bd. 5, 2016, S. 1–17.

Beispiel bestimmte Inhalte definieren, wie etwa Nacktheit oder Gewalt, die nicht auf der Plattform gezeigt werden dürfen. Dabei müssen die Plattformbetreiber die Regeln selbst durchsetzen. Die Sperrung und Löschung der Accounts von Donald Trump im Kontext der Stürmung des Kapitols haben diese Möglichkeiten in den Fokus gerückt.[27] Regelungsmöglichkeiten bestehen aber für die Betreiber sozialer Medien insbesondere auch darin, durch technische Möglichkeiten auf das Verhalten von Nutzern Einfluss zu nehmen. Die Ko-Regulierung kombiniert Selbstregulierung und Regulierung und setzt einen staatlichen Rahmen, innerhalb dessen private Akteure verantwortlich handeln sollen.[28] Der Staat nimmt hier keinen direkten Einfluss auf private Akteure, sondern beeinflusst private Akteure indirekt.

Im Hinblick auf die Betreiber sozialer Medien stellen sich aus regulatorischer Sicht zwei große Fragen: einerseits, wie die Kuratierung von Inhalten selbst geregelt ist, was also etwa im Hinblick auf Transparenzpflichten gelten soll. Anderseits bedarf es der Klärung, wie die Verantwortlichkeit der Betreiber sozialer Medien für Inhalte auf den Plattformen ausgestaltet werden soll. Dabei handelt es sich um eine mittelbare oder sekundäre Verantwortlichkeit, weil die Inhalte selbst von Nutzern erstellt werden und zu fragen ist, unter welchen Umständen das Fehlverhalten der Nutzer den Plattformbetreibern zugerechnet werden kann.[29]

In den Vereinigten Staaten, wo viele der weltweit tätigen Plattformbetreiber ansässig sind, wurden beide Fragen bereits früh im Sinne der Selbstregulierung der Plattformen beantwortet. Es gab keine direkte Technikregulierung, ferner sorgte die berühmte Section 230 des Communication Decency Act (CDA) dafür, dass die Betreiber sozialer Medien grundsätzlich nicht für Nutzerinhalte verantwortlich waren.[30] Insofern oblag es grundsätzlich den Betreibern sozialer Medien, für Ordnung auf ihren

---

27 Fischer, Sara, Ashley Gold: All the platforms that have banned or restricted Trump so far 2011, https://www.axios.com/platforms-social-media-ban-restrict-trump-d9e44f3c-8366-4ba9-a8a1-7f3114f920f1.html, 08.01.2022.

28 Schulz, Wolfgang, Thorsten Held: Regulierte Selbstregulierung als Form modernen Regierens. Endbericht Mai 2002 (Arbeitspapiere des Hans-Bredow-Instituts 10), Hamburg 2002.

29 Riordan, Jaani: A Theoretical Taxonomy of Intermediary Liability, in: Frosio, Giancarlo (Hrsg.): The Oxford handbook of online intermediary liability, First edition (Oxford handbooks in law), Oxford 2020, S. 56–89, hier: 65ff.

30 Goldman, Eric: An Overview of the United States' Section 230 Internet Immunity, in: Frosio, Giancarlo (Hrsg.): The Oxford handbook of online intermediary liability, First edition (Oxford handbooks in law), Oxford 2020, S. 153–171. Zur Rechtslage in Deutschland siehe dazu in diesem Band den Beitrag von Spindler,

Plattformen zu sorgen, ohne dass sie dazu gezwungen wurden. Besonders in der Folge des Sturms auf das Kapitol ist die Diskussion um Regulierung in vollem Gange.[31] Sieben Vorschläge betreffen allein die Änderung von Section 230 CDA.[32]

Nicht nur in den Vereinigten Staaten findet ein reger Diskurs über die Regulierung sozialer Medien statt. Das chinesische Gesetz „Regelung zur Verwaltung algorithmischer Empfehlungssysteme für Internet-Informati-

---

Gerald: „Funktion und Verantwortung von Plattformen als Informations-Intermediäre", S. 73ff.

31 Anti-Defamation League, Avaaz, Decode Democracy, Mozilla, New America's Open Technology Institute: Trained for Deception: How Artificial Intelligence Fuels Online Disinformation. Relevant Legislation 2021, https://foundation.mozilla.org/en/campaigns/trained-for-deception-how-artificial-intelligence-fuels-online-disinformation/relevant-legislation/, 22-02-2022; McCabe, David: Lawmakers Target Big Tech 'Amplification.' What Does That Mean? 2021, https://www-nytimes-com.eaccess.ub.tum.de/2021/12/01/technology/big-tech-amplification.html?searchResultPosition=7, 22-02-2022; Singh, Spandana: Regulating Platform Algorithms. Approaches for EU and U.S. Policymakers 2021, https://www.newamerica.org/oti/briefs/regulating-platform-algorithms/, 22-02-2022; Reardon, Marguerite: Regulating the tech giants may finally be within reach 2022, https://www.cnet.com/news/regulating-tech-giants-may-finally-be-within-reach/, 22-02-2022.

32 Rep. Clarke, Yvette D. (D-NY-9) (2021): Civil Rights Modernization Act of 2021. House - Energy and Commerce. H.R. 3184. Online verfügbar unter https://www.congress.gov/bill/117th-congress/house-bill/3184/text?q=%7B%22search%22%3A%5B%223184%22%5D%7D&r=3&s=2. Rep. Malinowski, Tom (D-NJ-7) (2021): Protecting Americans from Dangerous Algorithms Act. House - Energy and Commerce. H.R. 2154. Online verfügbar unter https://www.congress.gov/bill/117th-congress/house-bill/2154/text. Rep. Pallone, Frank Jr. (D-NJ-6) (2021): Justice Against Malicious Algorithms Act of 2021. House - Energy and Commerce. H.R. 5596. Online verfügbar unter https://www.congress.gov/bill/117th-congress/house-bill/5596. Sen. Graham, Lindsey (R-SC) (2021): A bill to repeal section 230 of the Communications Act of 1934. Senate - Commerce, Science, and Transportation. S. 2972. Online verfügbar unter https://www.congress.gov/bill/117th-congress/senate-bill/2972/text. Sen. Klobuchar, Amy (D-MN) (2021): Health Misinformation Act of 2021. Senate - Commerce, Science, and Transportation. S. 2448. Online verfügbar unter https://www.congress.gov/bill/117th-congress/senate-bill/2448/allinfo. Sen. Rubio, Marco (R-FL) (2021): DISCOURSE Act. Senate - Commerce, Science, and Transportation. S. 2228. Online verfügbar unter https://www.congress.gov/bill/117th-congress/senate-bill/2228/text?q=%7B%22search%22%3A%5B%22marco+rubio+disincentivizing+internet+service+censorship%22%2C%22marco%22%2C%22rubio%22%2C%22disincentivizing%22%2C%22internet%22%2C%22service%22%2C%22censorship%22%5D%7D&r=1&s=2. Sen. Warner, Mark R. (D-VA) (2021): SAFE TECH Act. Senate - Commerce, Science, and Transportation. S. 299. Online verfügbar unter https://www.congress.gov/bill/117th-congress/senate-bill/299.

onsdienste“[33] wurde am 04.01.2022 verabschiedet und ist am 01.03.2022 in Kraft getreten. Das Gesetz zeichnet sich dadurch aus, dass es direkte Vorgaben für die Kuratierung von Inhalten macht. Diese reichen von allgemeinen Zielen für die Optimierung der Empfehlungssysteme in Art. 6 bis hin zu detaillierten Vorgaben über Nutzermodellierung in Art. 10 oder IT-Sicherheit in Art. 9. Ersten Reaktionen zufolge handelt es sich bei dem Vorhaben um einen ambitionierten Entwurf, der sich erstmals direkt der Frage von Empfehlungssystemen widmet.[34] Es wird zu beobachten sein, wie offene Rechtsbegriffe wie die Pflicht von Diensteanbietern zur Orientierung an den „allgemeinen Wertvorstellungen“ (Art. 6) ausgelegt werden. Ferner liegt der Rahmen der angedrohten Bußgelder mit einer Obergrenze von 100 000 Yuan, was ca. 13 000 € entspricht, im niedrigen Bereich.

Auch die Institutionen der Europäischen Union verhandeln gerade intensiv über die Regulierung von sozialen Medien. Nachdem die Europäische Kommission den Entwurf eines Gesetzes über Digitale Dienste (EGDD)[35] vorgelegt hat, haben das europäische Parlament und der Rat der Europäischen Union ihre Änderungswünsche formuliert. Obwohl die interinstitutionellen Verhandlungen noch ausstehen und die endgültige Annahme des Gesetzes noch unsicher ist, lassen sich bereits jetzt übereinstimmende Aspekte feststellen. Der EGDD schließt regelungstechnisch grundsätzlich die Verantwortlichkeit von Plattformanbietern bei Unkenntnis gemäß Art. 5 EDGG aus, belegt sie aber nach einem gestuften Modell mit bestimmten Sorgfaltspflichten. Unterschieden wird hierbei innerhalb von Dienstleistern zwischen allen Anbietern von Vermittlungsdiensten (Art. 10ff. EGDD), Hosting-Dienstanbietern einschließlich Plattformen (Art. 14ff. EGDD), Online-Plattformen (Art. 16 EGDD) und sehr großen

33 Das Gesetz ist abrufbar unter: http://www.cac.gov.cn/2022-01/04/c_1642894606258238.htm. Die folgenden Betrachtungen basieren auf einer eigenen nicht-autoritativen Übersetzung. Eine Übersetzung eines vorhergehenden Gesetzesentwurfs findet sich hier: https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/.

34 Toner, Helen, Paul Triolo, Rogier Creemers: Experts Examine China’s Pioneering Draft Algorithm Regulations 2022, https://digichina.stanford.edu/work/experts-examine-chinas-pioneering-draft-algorithm-regulations/, 08.01.2022.

35 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final. Siehe dazu ausführlich in diesem Band den Beitrag von Buchheim, Johannes: Der Kommissionsentwurf eines Digital Services Act – Regelungsinhalte, Regelungsansatz, Leerstellen und Konfliktpotential, S. 239ff.

Online-Plattformen (Art. 25ff. EGDD). Die Kuratierung oder Moderation von Inhalten wird legal definiert als

> *die Tätigkeiten der Anbieter von Vermittlungsdiensten, mit denen illegale Inhalte oder Informationen, die von Nutzern bereitgestellt werden und mit den allgemeinen Geschäftsbedingungen des Anbieters unvereinbar sind, erkannt, festgestellt und bekämpft werden sollen, darunter auch Maßnahmen in Bezug auf die Verfügbarkeit, Sichtbarkeit und Zugänglichkeit der illegalen Inhalte oder Informationen, z. B. Herabstufung, Sperrung des Zugangs oder Entfernung, oder in Bezug auf die Möglichkeit der Nutzer, solche Informationen bereitzustellen, z. B. Schließung oder Aussetzung des Kontos eines Nutzers[…]*

Aus der Definition ergibt sich, dass der EGDD die Kuratierung nur im Hinblick auf illegale Inhalte in den Blick nimmt. Die Kuratierung von Inhalten ist dabei ein Querschnittsthema, das für verschiedene Sorgfaltspflichten eine Rolle spielt. Gemäß Art. 12 EGDD müssen die allgemeinen Geschäftsbedingungen des Plattformanbieters „alle Richtlinien, Verfahren, Maßnahmen und Werkzeuge, die zur Moderation von Inhalten eingesetzt werden, einschließlich algorithmischer Entscheidungsfindung und menschlicher Überprüfung" umfassen. Die Kuratierung steht auch im Zentrum der Transparenzpflichten, die gestuft für Vermittlungsdienste (Art. 13 EGDD), Online-Plattformen (Art. 23, 24 EGDD), online Werbung (Art. 24 EGDD) und sehr große Online-Plattformen (Art. 30, 33 EGDD) geregelt ist. Ferner werden für das Verfahren der Kuratierung insbesondere durch die Entfernung von Inhalten detaillierte Vorgaben gemacht. Geregelt werden u.a. ein Melde- und Abhilfeverfahren (Art. 14 EGDD), eine Begründungspflicht bei der Entfernung von Inhalten (Art. 15 EGDD), für Onlineplattformen ein internes Beschwerdemanagement (Art. 17 EGDD) und besondere Konsequenzen für einzelne Nutzer (Art. 20 EGDD). Der EGDD sieht einen direkten Einfluss auf die Technik insbesondere im Rahmen sehr großer Online-Plattformen vor. Im Rahmen der Risikobewertung neuer Dienste in Art. 26 EGDD müssen gemäß Absatz 2 Moderationssysteme als Maßnahme mitgedacht werden. Noch deutlicher wird dies in Art. 27 Abs. 1 a) EGDD, der Risikominderungsmaßnahmen beschreibt und dabei als erstes Beispiel die „Anpassung der Systeme zur Moderation von Inhalten oder der Empfehlungssysteme, ihrer Entscheidungsprozesse, der Merkmale oder der Funktionsweise ihrer Dienste oder ihrer allgemeinen Geschäftsbedingungen" nennt. Der EGDD greift also tief in die technische, sozio-technische und die Governance-Sphäre von Plattformanbietern ein.

IV. Neue Pfade der Regulierung?

Die Regulierung von Inhalten ist eine Operation am offenen Herzen der Demokratie. Man kann diese Frage weder allein den Unternehmen überlassen, die diese Dienste anbieten, noch staatlichen Stellen. Die Zivilgesellschaft muss eine Rolle spielen. Denn obwohl beide Akteure auch das öffentliche Wohl im Blick haben, besteht jeweils die Gefahr, die Macht, die von einer Kontrolle des öffentlichen Diskurses ausgeht, für kommerzielle oder politische Zwecke zu missbrauchen. Der Befund in diesem Band ist insofern eindeutig, als dass eine demokratische Neuerung der Öffentlichkeit gefordert wird,[36] die Bürgerinnen ebenfalls mit einbezieht und sich den sozio-technischen Realtitäten anpasst.[37]

Daher möchte ich an dieser Stelle dafür streiten, auch den Nutzern und mithin Bürgern unmittelbar und mittelbar größere Einflussmöglichkeiten auf die Kuratierung von Inhalten zu geben. Ansätze dazu sind sowohl in der Informatik als auch in der Wissenschafts- und Technikforschung über Jahrzehnte entwickelt worden.[38] Um sie aber für das Recht fruchtbar zu machen, muss die althergebrachte Dialektik von Selbstregulierung, staatlicher Regulierung und Ko-Regulierung durchbrochen werden.[39] Dies kann nur durch eine aktivierende Regulierung gelingen, die nicht nur den Rahmen für Unternehmen und Verbände setzt, sondern deutlich darüber hinausgreift. Welche Elemente zu einer solchen aktivierenden und gestal-

---

36 Siehe dazu in diesem Band die Beiträge von Thiel, Thorsten: Der digitale Strukturwandel von Öffentlichkeit: Demokratietheoretische Anmerkungen, S. 46-47 sowie von Vesting, Thomas: Direkt zu den Leuten. Die funktionale Interpretation der Rundfunkfreiheit und die neuartige Environmentalität intelligenter Computernetzwerke, S. 217ff.

37 Vgl. hierzu in diesem Band die Beiträge von Ochs, Carsten: The Digital Public and its Problems: Komplexität, Verfahren und Trägerschaft als rekursive Konstitutionsprobleme einer digitalen Problemöffentlichkeit, S. 61-62 sowie von Vesting (Fn. 35), S. 217ff.

38 Stilgoe, Jack, David H. Guston: Responsible Research and Innovation, in: Felt, Ulrike, Rayvon Fouché, Clark A. Miller, Laurel Smith-Doerr (Hrsg.): The handbook of science and technology studies, Fourth edition, Cambridge, Massachusetts, London, England 2017, S. 853–880; Bødker, Keld, Finn Kensing, Jesper Simonsen: Participatory IT design. Designing for business and workplace realities, Cambridge, Mass 2004.

39 Der Begriff der Selbstregulierung ist leider bereits durch die Selbstregulierung des Marktes belegt, obwohl man durchaus daran denken könnte, dass es auch hier um eine Selbstregulierung geht, nämlich der Gesellschaft, die Bürger und wirtschaftliche Akteure einschließt, und der staatlichen Gemeinschaft.

tungsbezogenen Regulierung beitragen können, soll im Folgenden kurz skizziert werden.

Ein Element einer aktivierenden Regulierung ist, dass sie den Gemeinwohlbezug bestimmter Technologien herstellt und in unterschiedlichen Graden fördert und verankert. Im technikwissenschaftlichen Diskurs in den Vereinigten Staaten wurde kürzlich das Konzept von „public interest technologies" geprägt.[40] Eine Verknüpfung von Technik und verfassungsrechtlichen Zielvorstellungen kann die Technik in einen bestimmten Bezug setzen und die Beteiligten bei ihrer Gestaltung beeinflussen. Im Datenschutzrecht hat dies sogar zu einer Rechtspflicht der Verwirklichung des Datenschutzes durch (sozio-)technische Gestaltung geführt, wie sich aus Art. 25 der Datenschutzgrundverordnung ergibt.[41] Diese Möglichkeit der Regulierung kann weitergedacht werden und auch implizit in Normen verankert sein.[42] Der erste Schritt einer Kuratierung von Inhalten sollte sie mit demokratischen Zielvorstellungen, aber auch mit Persönlichkeitsrechten in Verbindung bringen. Die entsprechenden Algorithmen und ihr sozio-technisches Umfeld müssen jedenfalls auch aus diesen Perspektiven gedacht werden.

Verbunden damit schafft eine aktivierende Regulierung konkrete Anreize zur Verwirklichung dieser Ziele. Bereits heute wird die Forschungsförderung rechtlich gesteuert, so lassen sich auch gesellschaftliche Belange in Ausschreibungen einbringen und in diesen berücksichtigen. Über die Forschungsförderung kann das Recht bewusst Innovationen beeinflussen und so den Grundstein für die Erweiterung der Möglichkeiten der Technik legen. Es geht hier nicht nur darum, gewisse Praktiken auszuschließen oder sich auf einen gemeinsamen Mindeststandard zu einigen. Vielmehr will eine aktivierende Regulierung etwas zur dynamischen Entwicklung der Technik beitragen. Allein die Verfügbarkeit besserer Methoden kann bereits eine Wirkung entfalten, wie Konzepte des „Critical Design" oder der Metagovernance herausgestellt haben.[43] Diese Wirkung kann durch

40 https://pitcases.org/.

41 Bygrave, Lee A.: Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, in: Oslo Law Review, Bd. 1, 2017, S. 105–120.

42 Djeffal, Christian: The Normative Potential of the European Rule on Automated Decisions. A New Reading for Art. 22 GDPR, in: ZaöRV, Bd. 81, 2020, S. 847–879, hier: S. 857–860.

43 Gjaltema, Jonna, Robbert Biesbroek, Katrien Termeer: From government to governance…to meta-governance: a systematic literature review, in: Public Management Review, 2019, S. 1–21.

das Recht aber noch verstärkt werden, wenn etwa Konzepte wie der Stand der Technik eingesetzt werden.

Auch im Hinblick auf die Kuratierung von Inhalten gibt es durchaus Ansätze, wie Zielvorstellungen hinsichtlich Selbstbestimmung und Demokratie in die sozio-technische Gestaltung der entsprechenden Systeme miteinbezogen werden können.[44] Tatsächlich gibt es z.B. vielversprechende Ansätze, die Nutzern erlauben sollen, Algorithmen zu beeinflussen.[45] Sie reichen vom Feedback der Nutzer bis hin zur Gestaltung oder zur Auswahl der jeweiligen Algorithmen.[46] Diese Ansätze wurden bereits im Rahmen der US-amerikanischen Debatte um die Regulierung sozialer Medien erwähnt und später sogar in einem Projekt zur Umsetzung der Forschung durch Twitter aufgegriffen.[47] Die technische Selbstregulierung von Nutzern könnte ein Weg sein, die Kuratierung von Inhalten ganz neu zu organisieren. Das Nutzerverhalten in sozialen Medien zeigt allerdings, dass mehr Möglichkeiten für Nutzer kein Allheilmittel sind. Im gleichen Maße, in dem man mehr Verantwortung in ihre Hände legt, muss man auch die Grundlagen für die Ausübung ihrer Selbstbestimmung schaffen und

---

44 Djeffal, Christian, Eduardo Magrani, Christina Hitrova: Recommender systems and autonomy: A role for regulation of design, rights, and transparency (forthcoming), in: Indian Journal of Law and Technology, 2022, im Erscheinen.

45 Diese werden unter dem Schlagwort Nutzerkontrolle (user control) verhandelt. Hierzu etwa Steck, Harald, Roelof van Zwol, Chris Johnson: Interactive Recommender Systems, in: ACM Recommender Systems Conference (Hrsg.): RecSys'15. Proceedings of the 9th ACM Conference on Recommender Systems, September 16-20, 2015, Vienna, Austria (RecSys '15), New York, NY 2015, S. 359–360; He, Chen, Denis Parra, Katrien Verbert: Interactive recommender systems: A survey of the state of the art and future research challenges and opportunities, in: Expert Systems with Applications, Bd. 56, 2016, S. 9–27.

46 Jin, Yucheng, Bruno Cardoso, Katrien Verbert: How do different levels of user control affect cognitive load and acceptance of recommendations?, in: CEUR Workshop Proceedings (Bd. 1884) 2017, S. 35–42; Ekstrand, Michael D., Daniel Kluver, F. Maxwell Harper, Joseph A. Konstan: Letting Users Choose Recommender Algorithms: An Experimental Study, in: Proceedings of the 9th ACM Conference on Recommender Systems (RecSys '15), New York, NY, USA 2015, S. 11–18.

47 Seeking Alpha: Twitter, Inc.'s (TWTR) CEO Jack Dorsey on Q4 2020 Results. Earnings Call Transcript 2021, https://seekingalpha.com/article/4404806-twitter-inc-s-twtr-ceo-jack-dorsey-on-q4-2020-results-earnings-call-transcript, 16.04.2021; Wolfram, Stephen: Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms. Testimony before the Senate Subcommittee on Communications, Technology, Innovation, and the Internet Hearing on 2019, https://www.commerce.senate.gov/services/files/7A162A13-9F30-4F4F-89A1-91601DA485EE.

sie über Handlungsmöglichkeiten und Konsequenzen aufklären. Anreize zur Förderung von algorithmischer Nutzerkontrolle sind also weder ein schneller technischer Fix noch eine einfache juristische Lösung. Es ist vielmehr ein langer und voraussetzungsreicher Weg. Nutzer und damit Bürger aktiv am Prozess zu beteiligen folgt einem dynamischen Verständnis von Demokratie als sich fortlaufend verbessernden Prozess, der an seinen Herausforderungen wächst und der sich durch die Bewältigung teilweise auch schwerer Irritationen unter Beweis stellt.

V. Schlussbetrachtung

Die Entwicklung des Web 2.0 stellt zentrale Werte unseres Zusammenlebens und unserer Verfassung auf die Probe. Das Phänomen der Hassrede zeigt, welche großen Auswirkungen soziale Medien auf Persönlichkeitsrechte haben können: Falschnachrichten stellen demokratische Verfahren auf die Probe, die Reaktionen auf diese Entwicklungen und das Zusammenspiel von Plattformbetreibern und staatlichen Stellen werfen grundsätzliche Fragen der Rechtsstaatlichkeit auf. Diese Fragen beziehen sich heute nicht mehr nur auf eine vorgestellte virtuelle Welt. Soziale Medien zeitigen solche gravierenden Wirkungen, dass vielmehr bereits über eine Mitverantwortlichkeit von Betreibern selbst für Genozid gestritten.[48] Wie oft bei sozio-technischen Artefakten kann die Kuratierung von Inhalten sowohl als Teil des Problems als auch als Teil der Lösung angesehen werden. Es stellt sich die Frage nach ihrer Ausgestaltung. Diese ist alles andere als einfach zu bewältigen. In unterschiedlichen Rechtsordnungen gibt es bedeutende Regulierungsversuche. Dieser Beitrag hat die Frage aufgeworfen, inwiefern ein aktivierender Regulierungsansatz wichtige Ergänzungsmöglichkeiten einbringen könnte, die insbesondere die Zwecksetzung in der Technik beeinflussen und den Kreis der beteiligten Akteure erweitern. In dem Maße, in dem Technik in der Gesellschaft an Bedeutung gewinnt, muss ihre Regulierung überdacht werden. Ansätze der Ko-Regulierung zeichnen sich dadurch aus, dass sie Steuerung möglich machen und Wissensprobleme überwinden. Soziale Medien zeigen aber, dass der Einsatz von Technik noch ganz andere und tiefergehende Fragen aufwerfen kann, denen man nicht anders als mit Anpassungen und Innovationen begegnen kann. Dies ist eine Aufgabe für alle Bereiche der Gesellschaft.

48 Chandran, Rina, Avi Asher-Schapiro: Analysis: Rohingya lawsuit against Facebook a 'wake-up call' for social media, in: Reuters, 10.12.2021.

Literaturverzeichnis

Aichner, Thomas, Matthias Grünfelder, Oswin Maurer, Deni Jegeni: Twenty-Five Years of Social Media. A Review of Social Media Applications and Definitions from 1994 to 2019, in: Cyberpsychol Behav Soc Netw, Bd. 24, 2021, S. 215–222.

Anti-Defamation League, Avaaz, Decode Democracy, Mozilla, New America's Open Technology Institute: Trained for Deception: How Artificial Intelligence Fuels Online Disinformation. Relevant Legislation 2021, https://foundation.mozilla.org/en/campaigns/trained-for-deception-how-artificial-intelligence-fuels-online-disinformation/relevant-legislation/, 22-02-2022.

Barrabi, Thomas: YouTube CEO says removing 'dislike' button prevents harmful 'attacks', in: New York Post, 26.01.2022.

Belli, Luca, Jamila Venturini: Private ordering and the rise of terms of service as cyber-regulation, in: Internet Policy Review, Bd. 5, 2016, S. 1–17.

Bernstein, William J.: Masters of the word. How media shaped history from the alphabet to the internet, London 2013.

Bødker, Keld, Finn Kensing, Jesper Simonsen: Participatory IT design. Designing for business and workplace realities, Cambridge, Mass 2004.

Bygrave, Lee A.: Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements, in: Oslo Law Review, Bd. 1, 2017, S. 105–120.

Cambridge Consultants: Use of AI in online content moderation 2019.

Chandran, Rina, Avi Asher-schapiro: Analysis: Rohingya lawsuit against Facebook a 'wake-up call' for social media, in: Reuters, 10.12.2021.

Djeffal, Christian: Sustainable AI Development (SAID). On the Road to More Access to Justice, in: Souza, Siddarth Peter de, Maximilian Spohr (Hrsg.): Technology, Innovation and Access to Justice. Dialogues on the Future of Law, Edinburgh 2020, 112-130.

Djeffal, Christian: The Normative Potential of the European Rule on Automated Decisions. A New Reading for Art. 22 GDPR, in: ZaöRV, Bd. 81, 2020, S. 847–879.

Djeffal, Christian, Eduardo Magrani, Christina Hitrova: Recommender systems and autonomy: A role for regulation of design, rights, and transparency (forthcoming), in: Indian Journal of Law and Technology, 2022, im Erscheinen.

Ekstrand, Michael D., Daniel Kluver, F. Maxwell Harper, Joseph A. Konstan: Letting Users Choose Recommender Algorithms: An Experimental Study, in: Proceedings of the 9th ACM Conference on Recommender Systems (RecSys '15), New York, NY, USA 2015, S. 11–18.

Fischer, Sara, Ashley Gold: All the platforms that have banned or restricted Trump so far 2011, https://www.axios.com/platforms-social-media-ban-restrict-trump-d9e44f3c-8366-4ba9-a8a1-7f3114f920f1.html, 08.01.2022.

Gillespie, Tarleton: Custodians of the internet. Platforms, content moderation, and the hidden decisions that shape social media, New Haven 2018.

Gjaltema, Jonna, Robbert Biesbroek, Katrien Termeer: From government to governance…to meta-governance: a systematic literature review, in: Public Management Review, 2019, S. 1–21.

Goldman, Eric: An Overview of the United States' Section 230 Internet Immunity, in: Frosio, Giancarlo (Hrsg.): The Oxford handbook of online intermediary liability, First edition (Oxford handbooks in law), Oxford 2020, S. 153–171.

Grimmelmann, James: The Virtues of Moderation, in: Yale Journal of Law and Technology, Bd. 17, 2015.

He, Chen, Denis Parra, Katrien Verbert: Interactive recommender systems: A survey of the state of the art and future research challenges and opportunities, in: Expert Systems with Applications, Bd. 56, 2016, S. 9–27.

Jannach, Dietmar: Recommender Systems. An introduction, Cambridge 2011.

Jenkins, Henry, Sam Ford, Joshua Green: Spreadable media. Creating value and meaning in a networked culture (Postmillennial pop), New York, London 2013.

Jin, Yucheng, Bruno Cardoso, Katrien Verbert: How do different levels of user control affect cognitive load and acceptance of recommendations?, in: CEUR Workshop Proceedings (Bd. 1884) 2017, S. 35–42.

Jürgen Habermas: Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit, in: Seeliger, Martin, Sebastian Sevignani (Hrsg.): Ein neuer Strukturwandel der Öffentlichkeit? (Leviathan Sonderband), Baden-Baden 2021, S. 470–500.

Knight, Will: Why a YouTube Chat About Chess Got Flagged for Hate Speech. AI programs that analyze language have difficulty gauging context. Words such as "black," "white," and "attack" can have different meanings., in: wired, 01.03.2021.

McCabe, David: Lawmakers Target Big Tech 'Amplification.' What Does That Mean? 2021, https://www-nytimes-com.eaccess.ub.tum.de/2021/12/01/technology/big-tech-amplification.html?searchResultPosition=7, 22-02-2022.

Meineck, Sebastian: Der Sinn von Dislike-Buttons – das sagt die Wissenschaft, in: netzpolitik.org, 27.01.2022.

Milano, Silvia, Mariarosaria Taddeo, Luciano Floridi: Recommender systems and their ethical challenges, in: AI & Soc, Bd. 35, 2020, S. 957–967.

Molly Russell entered 'dark rabbit hole of suicidal content' online, says father, in: The National, 28.10.2019.

Reardon, Marguerite: Regulating the tech giants may finally be within reach 2022, https://www.cnet.com/news/regulating-tech-giants-may-finally-be-within-reach/, 22-02-2022.

Ricci, Francesco, Lior Rokach, Bracha Shapira (Hrsg.): Recommender Systems Handbook, Second edition, Boston, MA 2015.

Riordan, Jaani: A Theoretical Taxonomy of Intermediary Liability, in: Frosio, Giancarlo (Hrsg.): The Oxford handbook of online intermediary liability, First edition (Oxford handbooks in law), Oxford 2020, S. 56–89.

Roberts, Sarah T.: Behind the screen. Content moderation in the shadows of social media, New Haven 2019a.

Roberts, Sarah T.: Behind the screen. Content moderation in the shadows of social media, New Haven 2019b.

Schulz, Wolfgang, Thorsten Held: Regulierte Selbstregulierung als Form modernen Regierens. Endbericht Mai 2002 (Arbeitspapiere des Hans-Bredow-Instituts 10), Hamburg 2002.

Seeking Alpha: Twitter, Inc.'s (TWTR) CEO Jack Dorsey on Q4 2020 Results. Earnings Call Transcript 2021, https://seekingalpha.com/article/4404806-twitter-inc-s-twtr-ceo-jack-dorsey-on-q4-2020-results-earnings-call-transcript, 16.04.2021.

Singh, Spandana: Regulating Platform Algorithms. Approaches for EU and U.S. Policymakers 2021, https://www.newamerica.org/oti/briefs/regulating-platform-algorithms/, 22-02-2022.

Steck, Harald, Roelof van Zwol, Chris Johnson: Interactive Recommender Systems, in: ACM Recommender Systems Conference (Hrsg.): RecSys'15. Proceedings of the 9th ACM Conference on Recommender Systems, September 16-20, 2015, Vienna, Austria (RecSys '15), New York, NY 2015, S. 359–360.

Stevenson, Michael: From Hypertext to Hype and Back Again. Exploring the Roots of Social Media in Early Web Culture, in: Burgess, Jean, Alice E. Marwick, Thomas Poell (Hrsg.): The sage handbook of social media, London 2018.

Stilgoe, Jack, David H. Guston: Responsible Research and Innovation, in: Felt, Ulrike, Rayvon Fouché, Clark A. Miller, Laurel Smith-Doerr (Hrsg.): The handbook of science and technology studies, Fourth edition, Cambridge, Massachusetts, London, England 2017, S. 853–880.

Toner, Helen, Paul Triolo, Rogier Creemers: Experts Examine China's Pioneering Draft Algorithm Regulations 2022, https://digichina.stanford.edu/work/experts-examine-chinas-pioneering-draft-algorithm-regulations/, 08.01.2022.

Urwin, Rosamund, Sian Griffiths: Pinterest emailed suicide tips after Molly Russell's death, in: The Sunday Times, 27.01.2019.

van Dijck, José: The culture of connectivity. A critical history of social media, Oxford 2013a.

van Dijck, José: The culture of connectivity. A critical history of social media, Oxford 2013b.

Wolfram, Stephen: Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms. Testimony before the Senate Subcommittee on Communications, Technology, Innovation, and the Internet Hearing on 2019, https://www.commerce.senate.gov/services/files/7A162A13-9F30-4F4F-89A1-91601DA485EE.

Zenith: Digital advertising to exceed 60% of global adspend in 2022 2021, https://www.zenithmedia.com/digital-advertising-to-exceed-60-of-global-adspend-in-2022/, 09.12.2021.

Demokratie und Rechtsstaat im digitalen Zeitalter im Spiegel der verfassungsrechtlichen Vorgaben

Astrid Epiney

Die Digitalisierung beeinflusst nicht nur praktisch alle Bereiche des gesellschaftlichen, wirtschaftlichen und politischen Lebens, sondern stellt auch eine Herausforderung für die Rechtsordnung im Allgemeinen und die Verfassungsrechtsordnung sowie das Funktionieren der Demokratie im Besonderen dar. Zurückzuführen sein dürfte dies in erster Linie auf mit zwei Faktoren:

- Erstens führt die Digitalisierung zu einer beeindruckenden Beschleunigung, die sehr verschiedene Bereiche betrifft. Zu erwähnen ist beispielhaft die im Zusammenhang mit der Thematik dieses Bandes eine besondere Rolle spielende Geschwindigkeit der Verbreitung von Informationen.
- Zweitens fördert die Digitalisierung eine gewisse Fragmentierung der Gesellschaft, gerade soweit die politische Öffentlichkeit betroffen ist, führen doch insbesondere die sozialen Netzwerke dazu, dass sich zahlreiche Personen nur noch in geschlossenen Kreisen bewegen, was eine gesamtgesellschaftliche Debatte, welche für eine funktionierende Demokratie von großer Bedeutung ist, erschwert.

Diese Phänomene der Beschleunigung und Fragmentierung – die sehr vielschichtig sind und hier nicht im Einzelnen beschrieben und analysiert werden können – bringen auch Gefährdungen verfassungsrechtlich geschützter Rechte mit sich und können gewisse öffentliche Interessen gefährden. So implizieren die sehr leistungsfähigen Möglichkeiten der Datenverarbeitung und insbesondere der Datenverknüpfung Gefährdungen des Rechts auf Persönlichkeitsschutz bzw. des Rechts auf «informationelle Selbstbestimmung» bzw. führen zu Eingriffen in diese grundrechtlich geschützten Rechte. Die durch die Digitalisierung ermöglichte rasche und insbesondere sehr weite Kommunikation von Informationen kann auch der Verbreitung sog. *Fake News* und von «Verschwörungstheorien» Vorschub leisten, welche diverse Bereiche betreffen und durchaus sehr konkrete, wenn auch mitunter nur schwer nachweisbare bzw. quantifizierbare

Auswirkungen entfalten können, wie Beeinflussungen von politischen Entscheidungen.

Auf der anderen Seite eröffnet die Digitalisierung selbstverständlich zahlreiche Möglichkeiten, sowohl für den Staat als auch für Wirtschaft und Gesellschaft sowie die Einzelnen. Stichworte sind hier die Vereinfachung und grössere Effizienz der Verwaltung, die Beteiligungsmöglichkeiten der Bürger, aber auch die Förderung wissenschaftlichen und technologischen Fortschritts. Und selbstredend kann es keinesfalls darum gehen, einem «Rückbau» der Digitalisierung das Wort zu reden oder die entsprechende Entwicklung als solche aufhalten zu wollen, ganz abgesehen davon, dass ein solcher Versuch nicht von Erfolg gekrönt wäre.

Vielmehr geht die zentrale und sehr bedeutende Frage dahin, wie Politik, Wirtschaft und Gesellschaft die Digitalisierung gestalten werden und wollen und auf welche Weise den zweifellos bestehenden Spannungsfeldern Rechnung getragen werden kann. Aufgeworfen wird damit auch die Frage nach dem Ob und Wie einer rechtlichen Regulierung verschiedener Aspekte. Diese Problematik muss selbstredend für die verschiedenen Bereiche angegangen werden. Allerdings sind jedenfalls die verfassungsrechtlichen Vorgaben zu beachten, deren Wirkungsweise gewissen strukturellen Gesetzmässigkeiten gehorcht, und es lohnt sich, sich diese immer wieder in Erinnerung zu rufen, auch in Anbetracht eher neuer Herausforderungen.

Ausgangspunkt ist dabei in vorliegendem Zusammenhang, dass die Chancen und Risiken der Digitalisierung in einem demokratischen Rechtsstaat eine Reihe von Spannungsfeldern zu Tage treten lassen. Beispielhaft seien folgende Konstellationen erwähnt:

- Anliegen des Persönlichkeitsschutzes und der informationellen Selbstbestimmung können in Konflikt mit der Wirtschaftsfreiheit sowie der Meinungsfreiheit stehen.
- Die freie Meinungsbildung in einer Demokratie und ihre Funktionsweise kann durch *Fake News* oder «Verschwörungstheorien», aber auch *shitstorms* aller Art beeinträchtigt werden, wobei auf der anderen Seite die Meinungsfreiheit einen sehr weiten Anwendungsbereich hat und auch nicht genehme oder (vermeintlich) «falsche» Aussagen geschützt sind.
- Aber auch die Meinungsfreiheit selbst kann im Konflikt mit der Meinungsfreiheit anderer geraten.
- Schließlich sei auf das Interesse des Staates und der Bürger, die Chancen der Digitalisierung für eine effiziente und effektive Verwaltung und leistungsfähige sowie attraktive Dienstleistungen zu nutzen, hinge-

wiesen, das aber in einem gewissen Konflikt mit Anliegen des Persönlichkeits- und Datenschutzes stehen kann.

Diese wenigen Beispiele und Spannungsfelder illustrieren gleichzeitig, dass es aus verfassungsrechtlicher Sicht bei den Fragen nach den Herausforderungen der Digitalisierung für die Funktionsweise von Demokratie und Rechtsstaat aus struktureller und dogmatischer Perspektive keineswegs um neue Themata geht. Vielmehr handelt es sich letztlich um klassische Problemfelder, welche aber freilich aufgrund der Digitalisierung eine mitunter völlig neue Dimension erlangen. Insofern geht es weniger um «qualitativ», denn um «quantitativ» neue Fragestellungen.

Diese verlangen jedenfalls teilweise nach neuen und originellen regulatorischen Ansätzen; hingegen drängt es sich nach der hier vertretenen Ansicht nicht auf, den verfassungsrechtlichen Rahmen bzw. die verfassungsrechtlichen Instrumente und Vorgaben, welche bei derartigen Spannungsfeldern zum Zuge kommen, grundsätzlich zu modifizieren. Vielmehr stellen die demokratischen und rechtsstaatlichen Verfahren, welche freilich in den verschiedenen Staaten unterschiedlich ausgeprägt sein können, Instrumente und Mechanismen zur Verfügung, um den Spannungsfeldern Rechnung tragen und zu ausgewogenen sowie insbesondere (demokratisch) legitimierten Entscheidungen gelangen zu können.

Erinnert sei in diesem Zusammenhang daran, dass die auch auf der Grundlage des EU-Rechts und der EMRK zu beachtenden Grundwerte einer demokratischen und rechtsstaatlichen Ordnung m.E. eine der wichtigsten Errungenschaften der Zivilisation darstellen. Sie garantieren auf der einen Seite die Beachtung der Grundrechte der Bürger, ohne auf der anderen Seite die Verfolgung öffentlicher Interessen zu verunmöglichen. Durch die Zurverfügungstellung von demokratisch legitimierten Verfahren mit Blick auf das Treffen politischer Entscheidungen und die Verbindlichkeit auf diese Weise erlassener Gesetze sowie die Gewährleistung einer unabhängigen Justiz wird letztlich ein friedliches Zusammenleben unter Wahrung der Grundrechte der Bürger ermöglicht. Diese zentrale Errungenschaft ist keineswegs selbstverständlich, wie verschiedene Entwicklungen auch in EU-Mitgliedstaaten zeigen.

Mit Blick auf die Digitalisierung und ihre Chancen und Risiken auch in der und für die demokratische und rechtsstaatliche Gesellschaft sind die sich stellenden Fragen und Herausforderungen daher auf der Basis dieser Grundwerte anzugehen. Bei der Frage, ob und welche regulatorischen Massnahmen vom Gesetzgeber getroffen werden sollen, dürften folgende Aspekte von besonderer Bedeutung sein:

- In einem ersten Schritt sind jeweils die relevanten Rechte und (öffentlichen oder privaten) Interessen zu identifizieren, unter Einschluss der genauen Zielsetzung einer (möglichen) Regelung oder Regulierung. Dabei ist insbesondere auch danach zu fragen, ob die betroffenen Rechte und Interessen verfassungsrechtlich geschützt sind und in welchem Verhältnis sie zu einander stehen. Von Bedeutung ist hierbei auch, dass dem Staat (oder auch der Europäischen Union) auch Pflichten zum Tätigwerden obliegen, so insbesondere, wenn es um den Schutz von Grundrechten – wobei im Zusammenhang mit der Digitalisierung nicht nur der Persönlichkeitsschutz, sondern auch die Meinungsfreiheit von besonderer Bedeutung sind – oder den Schutz politischer Rechte geht. Diese Schutzpflichten verpflichten den Staat oder / und die Europäische Union, die sich nach den Umständen als notwendig erweisenden Massnahmen zu ergreifen, um die Beeinträchtigung dieser Rechte adäquat zu schützen (seien die Ursachen im Verhalten anderer Privater oder in sonstigen Umständen, wie zum Beispiel technische Unzulänglichkeiten, zu sehen).
- Auf dieser Grundlage sind die verschiedenen Rechte und Interessen in Beziehung zu einander zu setzen, was eine Evaluation ihres (verfassungsrechtlichen) Gewichts impliziert. Relevant ist dabei auch, ob «Kerngehalte» in Frage stehen, also ob es um eine eigentliche «Aushöhlung» eines Rechts oder auch eines öffentlichen Interesses geht. Die Frage, unter welchen Voraussetzungen eine Verletzung des Kerngehalts insbesondere eines Grundrechts vorliegt, ist freilich schwierig zu beantworten; Rechtsprechung und Lehre liefern aber gewisse Anhaltspunkte. So dürfte z.B. das Recht auf Persönlichkeitsschutz bzw. auf Datenschutz dann in seinem Kerngehalt betroffen sein, wenn eine ständige und anlasslose Überwachung der Bürger ermöglicht wird.
- Sodann sind Erwägungen der Verhältnismässigkeit und der praktischen Konkordanz zu berücksichtigen: Es ist also zu eruieren, auf welche Weise bestmöglich verschiedene, mitunter widerstreitende Rechte und Interessen zum Ausgleich gebracht werden können.

Ausgehend von dieser Analyse sind letztlich durch die zuständigen gesetzgebenden Organe nach den hierfür vorgesehenen Verfahren und unter Beachtung ihrer Zuständigkeiten Regulierungsansätze zu entwickeln, wobei die Frage, ob diese auch die hier nur sehr grob skizzierten verfassungsrechtlichen Vorgaben beachten, grundsätzlich gerichtlich überprüft werden kann.

Dabei steht das Gemeinwesen (sowohl die einzelnen Staaten als auch supranationale Organisationen wie insbesondere die EU) in der übrigens

auch aufgrund der erwähnten Schutzpflichten rechtlich begründeten Verantwortung, gewisse Regulierungen betreffend die Digitalisierung tatsächlich an die Hand zu nehmen, spricht doch sehr Vieles dafür, dass im Falle fehlender Regulierungen sowohl Rechte Einzelner als auch gewichtige öffentliche Interessen – wie das Funktionieren der Meinungsbildung in einer demokratischen und offenen Gesellschaft – über Gebühr beeinträchtigt würden. M.a.W. sollten bzw. müssten die zuständigen politischen Akteure die sich aufdrängenden Entscheidungen treffen und ihrer Verantwortung bzw. ihren verfassungsrechtlichen Verpflichtungen – es dürften gute Gründe dafür sprechen, dass im Zuge der sich aus der Verfassung ergebenden insbesondere grundrechtlichen Schutzpflichten zumindest in gewissen Bereichen Handlungspflichten des Gesetzgebers bestehen – gerecht werden. Eine zentrale Herausforderung im Zusammenhang mit der Digitalisierung dürfte dabei die Frage nach den zur Verfolgung der angestrebten Zielsetzungen adäquaten Regulierung sein, geht es doch auch um aus «technischer» Sicht komplexe Fragen. Interdisziplinäre Zusammenarbeiten erscheinen hier ebenso sinnvoll wie notwendig, kann doch nur so zumindest versucht werden, die Steuerungsfähigkeit des Rechts zu gewährleisten.

Zentral dürfte aber in diesem Zusammenhang der dem Gesetzgeber einzuräumende Gestaltungsspielraum sein: Letztlich geht es bei der Regelung von Spannungsfeldern und dem Ausgleich von Interessen immer auch um politische (Wert-) Entscheidungen, über welche man sich in aller Regel trefflich streiten kann und sollte (und in Bezug auf welche es häufig keine «richtige» oder «falsche» Antwort gibt, ganz abgesehen davon, dass sich die Abwägungsentscheidungen und -grundlagen mit der Zeit auch ändern können). Dass eine solche offene Debatte auch in Zukunft konstruktiv möglich sein kann, sollte ein zentrales Anliegen aller politischen und gesellschaftlichen Akteure sowie der Bürger sein, wobei gleichzeitig die Anerkennung und Legitimität demokratisch nach den massgeblichen Verfahren getroffener Entscheidungen sicherzustellen ist. Und möglicherweise könnten gerade diese für das Funktionieren unseres demokratischen Rechtsstaates essentiellen Interessen ein Leitmotiv für die in den verschiedenen Sektoren zu entwickelnden Lösungsansätze sein. Denn das Funktionieren des demokratischen Rechtsstaats sieht sich immer wieder mit vielfältigen Herausforderungen konfrontiert, zu denen auch gewisse Implikationen der Digitalisierung gehören. Es lohnt sich aber, ihm adäquat Sorge zu tragen und diese Herausforderungen auf der Grundlage seiner Errungenschaften anzugehen.

Direkt zu den Leuten. Die funktionale Interpretation der Rundfunkfreiheit und die neuartige Environmentalität intelligenter Computernetzwerke*

Thomas Vesting

I. Einleitung

Mein Beitrag entwickelt die These, dass das Medienrecht der Bundesrepublik Deutschland ursprünglich – auch als Verfassungsrecht – auf einer normativen Modellbildung basierte, die eine spezifisch sozio-politische Voraussetzung hatte: eine industrielle Massengesellschaft samt einer dazu gehörenden stabilen Kultur großer Gruppen – Volksparteien, Gewerkschaften und Wirtschaftsverbände –, die ihrerseits fest in den verschiedenen kulturellen Milieus der Industriegesellschaft verankert waren. Das zeigt eine genauere Analyse von Konrad Hesses verfassungsrechtlichem Modell öffentlicher Meinungsbildung, an der sich die funktionale Interpretation der Rundfunkfreiheit lange Zeit orientiert hat. Die Voraussetzungen dieses Modells verlieren jedoch heute, in einer von Computernetzwerken geprägten intelligenten informationstechnologischen Umwelt des Menschen, ihre Gültigkeit. Es kann daher im Medienrecht kein Weiter-So geben. Vielmehr bedarf es einer Diskussion über ein neues netzwerkadäquates Medienrecht, auch über eine neue Medienverfassung, die die freie Entwicklung digitaler Technologien in gerechter Weise abstützt und nicht zu Gunsten überkommener Strukturen blockiert.

---

* Der vorliegende Text ist eine überabeitete und ergänzte Version eines von mir – unter dem Titel „Die Rundfunkfreiheit und die neue Logik der „Content-Curation“ in elektronischen Netzwerken“ – in der Juristenzeitung publizierten Artikels (JZ 20/2020), 975 - 982.

II. Konrad Hesses Modell öffentlicher Meinungsbildung

In seinen *Grundzügen des Verfassungsrechts der Bundesrepublik Deutschland*, die 1966 zum ersten Mal erscheinen und zwanzig Auflagen erleben, bemerkt Konrad Hesse, dass „politische Antriebe (heute) nur noch in geringem Maße von Einzelpersonen ausgehen".[1]

Konrad Hesse gehörte mit Horst Ehmke, Peter von Oertzen, Wilhelm Hennis, Ernst Gottfried Mahrenholz und anderen zu einer Gruppe von Staatsrechtslehrern und Politikwissenschaftlern, die in den staats- und kirchenrechtlichen Seminaren Rudolf Smends im Göttingen der 1950er und 1960er Jahre ihr geistiges Zentrum hatte. Diese Gruppe war der Ort einer intellektuellen Verdichtung für vieles, was die alte Bundesrepublik ausgemacht hat. Ihre Bedeutung bestand vor allem darin, dass sie – mehr als jede andere staats- und verfassungsrechtliche Bewegung ihrer Zeit – eine für eine prosperierende Industriegesellschaft angemessene Sprache entwickelt hat. Sie hat das verfassungsrechtliche Denken nicht länger auf die staatliche Ordnung beschränkt, sondern den Verfassungsbegriff um die Grundlagen des gesellschaftlichen (nicht-staatlichen) Lebens erweitert; und hat damit, wenn auch eher unbewusst, Anschluss an den anglo-amerikanischen Typus einer heterarchisch-dezentralen Gesellschaftsbildung gesucht. Das gilt auch und gerade für Konrad Hesse.[2] Bei Hesse geht es um eine Öffnung des Verfassungsrecht für gesellschaftliche Institutionen wie Ehe und Familie, Eigentum, Bildung, Kunst und Wissenschaft – und nicht zuletzt um ein Verfassungsdenken, das für das „Wirken sozialer Gruppen" Platz hat.[3] Hesse konzipierte mit anderen Worten ein Verfassungsrecht, dass die sozio-politischen Kräfte einschloss, die die junge Bundesrepublik bestimmten, wie etwa die politischen Parteien, die noch große Volksparteien waren, die Gewerkschaften und andere einflussreiche Verbände. Weil es diese großen Gruppen und Organisationen waren, die die Industriegesellschaft, ihre kulturellen Milieus und damit auch die verfassungsrechtliche Wirklichkeit prägten,[4] konnte Konrad Hesse sagen, dass

1 *Konrad Hesse*, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland (1966), Neudruck 20. Aufl. 1999, Rn. 151.

2 *Hesse* (Fn. 1), Rn. 18; *Dieter Grimm*, Offenheit als Leitmotiv im Verfassungsverständnis von Konrad Hesse, AöR 144 (2019) / Heft 3, S. 457, 461; vgl. auch *Michael Stolleis*, Geschichte des öffentlichen Rechts, Bd. IV.: Staats- und Verwaltungsrechtswissenschaft in West und Ost 1945-1990, 2012, 356 ff.

3 *Hesse* (Fn. 1), Rn. 18.

4 Zur Wirklichkeitsbezogenheit der rechtlichen Verfassung vgl. *Hesse*, Die normative Kraft der Verfassung, in: *Krüper/Payandeh/Sauer* (Hrsg.), Konrad Hesse. Die norma-

„politische Antriebe (heute) nur noch in geringem Maße von Einzelpersonen ausgehen".[5]

In der Industriegesellschaft der alten Bundesrepublik bestimmten diese großen Gruppen und Organisationen nicht nur die Prozesse politischer Willensbildung im engeren Sinn des Art. 20 Abs. 2 Grundgesetz (GG), d.h. Wahlen und Abstimmungen, den politischen Kampf um parlamentarische Mehrheiten und die Regierungsbildung. Sie prägten vielmehr auch die der politischen Willensbildung im engeren Sinne vorgelagerte öffentliche Meinungsbildung im gesellschaftlich-kommunikativen Raum. Wie Wahlen und Abstimmungen in der Massendemokratie nicht ohne Parteien und Verbände gedacht werden konnten, so war die Öffentlichkeit ebenfalls durch in der Gesellschaft vorfindliche „organisierte Gruppeninteressen"[6] bestimmt – und nicht länger als ein System privater Meinungen vorstellbar, das von Einzelpersonen getragen wurde und das liberale Individuum, das Teil einer in nachbarschaftlichen Netzwerken zu denkenden Gesellschaft und gerade kein isolierter Einzelner war, mit hervorbrachte.[7] Hesses Ausgangspunkt war also die Wahrnehmung einer grundlegenden strukturellen Veränderung der modernen Gesellschaft - der oft beschriebene Übergang von der liberalen Gesellschaft zur industriellen Massengesellschaft, den man in einer medientheoretischen Perspektive auch als Übergang vom Paradigma der „Medien in der Gesellschaft der Individuen" zu den „Medien" der „Gesellschaft der Organisationen" fassen kann.[8]

Vor diesem Hintergrund entwirft Konrad Hesse in den Randnummern 149–152 seiner Grundzüge des Verfassungsrechts ein Modell der öffentlichen Meinungsbildung, das unter den Bedingungen der modernen Massenkommunikation Gültigkeit beanspruchen kann. Diese Formulierung – „unter den Bedingungen der modernen Massenkommunikation" – ist schon eine der Rechtsprechung des Bundesverfassungsgerichts,[9] dessen Mitglied Konrad Hesse 1975 auf Vorschlag von SPD und FDP wurde. Hesse war im Bundesverfassungsgericht nicht nur maßgeblich am Urteil zur

---

tive Kraft des Faktischen, 2019, 1, 4 ff.; dazu auch *Rainer Wahl*, Die normative Kraft der Verfassung. Die Antrittsvorlesung Konrad Hesses in ihrem historischen Kontext, ebd., 19; kritisch *Matthias Jestaedt*, „Die normative Kraft der Verfassung." Eine zeitgebundene Gründungsschrift der Bonner Staatsrechtslehre, ebd., 63.

5 *Hesse* (Fn. 1), Rn. 151.

6 *Hesse* (Fn. 1), ebd.

7 Vgl. *Kirk Wetters*, The Opinion System. Impasses of the Public Sphere from Hobbes to Habermas, New York 2008, 123 ff.

8 *Karl-Heinz Ladeur*, Die Zukunft der Medienverfassung, in: Ladeur/Ingold/Graber/Wielsch, 2021, S. 17, 24.

9 BVerfGE 57, 295, 320.

Mitbestimmung beteiligt,[10] sondern hat als Berichterstatter seit den 1980er Jahren auch mehrere Urteile zum Rundfunkrecht in Verfahren vorbereitet, die durch den lange Zeit umstrittenen Übergang vom öffentlich-rechtlichen Rundfunkmonopol zu der so genannten dualen Rundfunkordnung ausgelöst wurden. Ich will hier keine Verfassungsrechtsprechungsgeschichte betreiben, aber ich denke, dass man mit Fug und Recht sagen kann, dass Konrad Hesse die Rechtsprechung des Bundesverfassungsgerichts zum Rundfunkrecht stark geprägt hat.[11] Wie also sah sein Modell öffentlicher Meinungsbildung genauer aus?

In diesem Öffentlichkeitsmodell werden Grundrechte und Staatsorganisationsrecht eng aufeinander bezogen. Das Grundrecht der Meinungsfreiheit (Art. 5 GG) wird als wichtiges Korrektiv zur Mediatisierung der politischen Willensbildung durch die besonderen Organe des Art. 20 Abs. 2 GG in Stellung gebracht. Hesses Öffentlichkeit, die sich etwa im Hinblick auf anstehende Wahlen in der gesellschaftsweiten Kommunikation immer wieder Geltung zu verschaffen sucht, ist also sehr viel umfassender angelegt als die Sphären von amtlichen Meinungen in Parlament, Regierung und Verwaltung. Hesse konzentriert sich vor allem auf die politisch relevante Massenkommunikation, die mehr als je zuvor von den Meinungsströmungen organisierter Gruppeninteressen abhängig wird. Hier kommt es zu einer die Entscheidungen in Parlament und Regierung, die Amtskommunikation, vorbereitenden „Vorformung des politischen Willens".[12] Es ist dies das Feld der „intermediären Kräfte",[13] in dessen Zentrum Hesse neben den politischen Parteien und Verbänden auch die wichtigsten (politischen) Massenmedien seiner Zeit, Presse und Rundfunk, verortet; wobei die Freiheit der Presse noch in der 20. Auflage der Grundzüge (1995) als die „wichtigste Voraussetzung der Meinungsbildung" angesehen wird.[14] Mit Hilfe der Massenmedien werden die unterschiedlichen Meinungen gebündelt – in Hesses Sprache „vorgeformt" –, um so einerseits politische Entscheidungen in Regierung und Parlament und andererseits Wahlen und Abstimmungen zu ermöglichen.

Daher liegt der Akzent bei Hesse von vornherein auf der „Bildung einer *öffentlichen Meinung*".[15] Bildung einer öffentlichen Meinung ist eine durch-

10 BVerfGE 50, 290.
11 Vgl. auch *Voßkuhle/Schemmel*, Der Staatsrechtler Konrad Hesse als Richter des Bundesverfassungsgerichts, AöR 144 (2019) / Heft 3, S. 425, 433 ff.
12 *Hesse* (Fn. 1), Rn. 151, 387.
13 *Hesse* (Fn. 1), Rn. 151.
14 *Hesse* (Fn. 1), Rn. 394 ff.
15 *Hesse* (Fn. 1), Rn. 150.

aus nicht unproblematische Formel, weil in einer liberalen Gesellschaft letztlich jede Form öffentlicher Meinungsbildung auf Beiträgen privater, in der Gesellschaft zerstreuter Meinungsäußerungen aufbauen muss, jedenfalls die private und öffentliche Meinungsbildung voneinander abhängig bleiben und die individuelle Seite der Meinungsbildung nicht einseitig gegenüber ihrer kollektiven Seite vernachlässigt werden darf. Hesse qualifiziert die Meinungsfreiheit zwar als „geistige Freiheit" und notwendiges Element des Rechtsstaates und platziert sie – mit Rudolf Smend – als „Stück sittlicher notwendiger Lebensluft" ganz in der Nähe des Art. 4 GG;[16] außerdem betont er, dass im Fall der Meinungsäußerungs- und Informationsfreiheit die subjektiv-rechtlichen Momente des Art. 5 Abs. 1 GG stärker hervorträten als etwa im Fall der Rundfunkfreiheit. Die Vernachlässigung der privaten Seite des spontanen Austausches von Meinungen, des „Meinungen-Systems",[17] wie Georg Christoph Lichtenberg den Prozess der freien Meinungsbildung in der Mitte des 18. Jahrhunderts nannte (dessen praktisches Vorbild das freiheitliche England war), ist in Hesses Modell öffentlicher Meinungsbildung aber insofern angelegt, als dieses unterstellt, dass die öffentliche Meinung unter den Bedingungen der Massenkommunikation nur in seltenen Fällen spontan vorhanden sei, „sondern in aller Regel Ergebnis organisierten Zusammenwirkens, oft etwas Gelenktes und darum kein unfehlbarer Maßstab der Richtigkeit."[18]

Das frühbürgerliche Subjekt, das im Medium der Öffentlichkeit an der Konstruktion eines säkularen und experimentellen Weltverständnisses sowie an seiner Fähigkeit zur ständigen Selbstveränderung arbeitet,[19] wobei die Meinungsäußerung dabei als neuartige Suche nach dem Wahrscheinlichen an die Stelle der Wahrheit tritt, weicht bei Konrad Hesse einem mehr oder weniger passiven Rezipienten, der durch die organisierten Mächte der Massenkommunikation hergebracht wird. Diese Sicht berührt sich an manchen Stellen mit Jürgen Habermas' *Strukturwandel der Öffentlichkeit*, in dessen Zentrum die Vorstellung einer Überlagerung und Verdrängung des frühbürgerlichen Ideals rationaler Meinungsbildung durch eine kommerzielle Dynamik steht, die aus dem kulturräsonierenden ein kulturkon-

16 *Hesse* (Fn. 1), Rn. 388.
17 *Wetters* (Fn. 7), 188 ff.
18 *Hesse* (Fn. 1), Rn. 150.
19 *Wetters* (Fn. 7), 137 („self-reformation"); *Karl-Heinz Ladeur*, Helmut Ridders Konzeption der Meinungsfreiheit als Prozessgrundrecht, KJ 52/2 (2020), S. 172, 176, 178.

sumierendes Publikum macht.[20] Zwar wird der Aufstieg des Gruppenpluralismus und der Massenmedien bei Hesse keineswegs so negativ bewertet wie bei Habermas,[21] aber beide sind doch Vertreter eines Öffentlichkeitsdenkens, in dem ein politisches Verständnis von Meinungsbildung dominiert, die Verständigung der Bürger oder Gruppen über gemeinsame staatspolitische Ziele. Dieses Denken sieht die Öffentlichkeit nicht, wie es für die liberale Ordnung allein angemessen wäre, mit Prozessen der spontanen gesellschaftlichen Selbstorganisation und des „poetic making" verknüpft,[22] der Konstruktion einer von Menschen selbst gemachten Wissensordnung, eines „maker's knowledge",[23] von der die politische Meinungsbildung und die Entscheidungsöffentlichkeit des Staates nur ein Teil sind. Vielmehr bindet es die Öffentlichkeit von vornherein an eine Vorstellung *politischer* Einheitsbildung (Hesse) oder an einen von kommerziellen Verzerrungen und Organisationen befreiten rationalen Diskurs zwischen Individuen, die lediglich deliberieren, sich aber anscheinend nicht um ihre materielle Selbsterhaltung kümmern müssen (Habermas).

III. Der Organisationsmensch als Paradigma funktionaler Grundrechtsinterpretation

Aus dem gruppenpluralistischen Öffentlichkeitsmodell ergibt sich die Notwendigkeit, Art. 5 GG anders zu verstehen und anders zu interpretieren als andere Grundrechte. Während nach herrschender Auffassung grundsätzlich natürliche oder juristische Personen im Zentrum des Grundrechtschutzes stehen, das heißt Individuen oder Organisationen, nimmt Hesse eine sich von ihrem personalen Substrat tendenziell lösende funktionale Freiheit in den Blick, die im 3. Rundfunkkurteil als „dienende Freiheit" bezeichnet wird.[24] Andreas Voßkuhle und Jakob Schemmel haben in jüngerer Zeit zu recht bemerkt, dass diese funktionalistische Interpretation der Rundfunkfreiheit durchaus über die bis zu diesem Zeitpunkt vorlie-

20 Vgl. *Jürgen Habermas*, Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft (1962), 1990, 248 ff., 261, 267 ff.
21 Vgl. *Habermas* (Fn. 20), 293 ff., 326 ff., 340.
22 *Victoria Kahn*, The Trouble with Literature, Oxford 2020, 2.
23 *Kahn* (Fn. 22), 25, 120.
24 BVerfGE 57, 295, 320 (im Original kursiv). Dazu *Martin Stock*, Medienfreiheit als Funktionsgrundrecht. Die journalistische Freiheit des Rundfunks als Voraussetzung allg. Kommunikationsfreiheit, 1985.

gende Rechtsprechung hinausgeht:[25] Danach gewährleistet Art. 5 Abs. 1 GG die Bildung einer öffentlichen Meinung, der sowohl die Kommunikationsgrundrechte des Abs. 1 (Meinungs- und Informationsfreiheit) wie die Mediengrundrechte des Abs. 2 (Presse, Rundfunk, Film) zugeordnet sind. Allerdings wird dieser fruchtbare Gedanke, der auf eine Art Prozeduralisierung der Kommunikations- und Mediengrundrechte hinauslaufen müsste, weder in der Rechtsprechung des Bundesverfassungsgerichts noch bei Konrad Hesse selbst näher ausgearbeitet. An die Stelle der Idee des grundrechtlichen Schutzes eines unpersönlichen Prozesses der Meinungsbildung, eines transsubjektiven Phänomens „des ‚organizing intelligence'", der „Herstellung einer ‚creative, progressive, exciting and intellectually robust community'",[26] tritt bei Hesse letztlich doch wieder eine mit ihrem personalen Substrat verknüpfte Rundfunkfreiheit, die Freiheit der Verlagshäuser, Zeitungsverleger oder der öffentlich-rechtlichen Rundfunkanstalten, die als juristische Personen als die primären Träger der Presse- und Rundfunkfreiheit angesehen werden, während natürliche Personen vor allem als Mediennutzer, als Rezipienten, als Träger der Informationsfreiheit ins Spiel kommen.[27]

Die funktionale Interpretation der Rundfunkfreiheit hat also eine ganz klare Botschaft: Das Zentrum des Prozesses der freien Meinungsbildung und der Medienverfassung bilden die großen Organisationen und die Organisationsmenschen. Davon geht Hesse aus und kann das in gewisser Weise auch, weil in der prosperierenden Industriegesellschaft der Bundesrepublik Deutschland nicht nur die Volkparteien Großorganisationen waren. Auch die großen Tageszeitungen und Wochenmagazine waren in der Hand großer deutscher Verlagshäuser, gehörten privatrechtlich verfasster Medienunternehmen oder Presseverlagen wie dem Axel Springer Verlag oder der WAZ-Mediengruppe. Auch der Rundfunk operierte in der Form der Großorganisation, zunächst als ausschließlich öffentlich-rechtlich organisierte Rundfunkanstalt wie der WDR oder das ZDF und später auch als privates Medienunternehmen wie RTL oder Pro-Sieben/Sat 1. Und weil es unter den Bedingungen der Massenkommunikation keine andere politisch auch nur annähernd gleich relevante Öffentlichkeit als die Öffentlichkeit

25 *Voßkuhle/Schemmel* (Fn. 11), S. 425 (Fn. 58).

26 *Ladeur* (Fn. 19), S. 172, 176; vgl. auch *Dan Wielsch*, Medienregulierung durch Persönlichkeits- und Datenschutzrechte, JZ 75 (2020) / Heft 3, S. 105; *Gunther Teubner*, Zum transsubjektiven Potential subjektiver Rechte. Gegenrechte in ihrer kommunikativen, kollektiven und institutionellen Dimension, in: Franzki/Horst/Fischer-Lescano (Hrsg.), Gegenrechte: Recht jenseits des Subjekts, 2018, 357.

27 *Hesse* (Fn. 1), Rn. 393.

der großen Organisationen gab, konnte Konrad Hesse sagen, dass die „politischen Antriebe" in Prozessen öffentlicher Meinungsbildung heute „nur noch in geringem Maße von Einzelpersonen" ausgehen.

IV. Die Garantie der Rundfunkfreiheit und die liberale Ordnung des Grundgesetzes

Wenn also die Mediengrundrechte primär die die öffentliche Meinungsbildung prägenden großen Organisationen schützen, weil das Organisationsmenschentum die Bedingung politischer Macht ist und die einzelnen Mediennutzer sich nur aus von Organisationsmenschen gemachten Medien informieren können, warum können Radio und Fernsehen dann nicht wie Presseunternehmen und Filmproduktionsunternehmen privatrechtlich und marktwirtschaftlich organisiert sein? Warum öffentlich-rechtliche Rundfunkanstalten oder jedenfalls eine Mischung aus öffentlich-rechtlichen Anstalten und privaten Medienunternehmen?

Eine überzeugende Beantwortung dieser Frage ist für das Verfassungsrecht unabdingbar. Die Errichtung von öffentlich-rechtlichen Rundfunkanstalten ist eine politische Lösung zur Gewährleistung der Rundfunkfreiheit, die den Kern liberaler Ordnung, dem das Grundgesetz verpflichtet ist, tangiert. Dieser Kern besteht darin, dass jeder Eingriff des Staates in die Selbstorganisation der Gesellschaft und ihrer Wissensordnung einer besonderen Legitimation bedarf, da politisches Handeln im Unterschied zu wirtschaftlichem Handeln letztlich immer mit dem Einsatz oder der Drohung staatlicher Gewalt verbunden ist. Natürlich wird niemand gezwungen, die Programme von ARD und ZDF zu konsumieren, aber alle müssen Rundfunkbeiträge bezahlen, wohingegen niemand gezwungen wird, eine FAZ oder eine TAZ zu kaufen, die er nicht lesen will; alles, was private Medienunternehmen einsetzen können, ist „sweet talk",[28] die Qualität des Produkts, Rhetorik, Verführung, Werbung usw. Hinter der privaten Presse steht aber kein „Beitragsservice". Das ist ein Unterschied ums Ganze, über den das Verfassungsrecht nicht einfach hinweggehen kann, auch nicht mit dem Argument, dass „große Konzerne" heute eine dem Staat vergleichbare Handlungsmacht hätten.

Konrad Hesse gibt auf diese Frage nach der Notwendigkeit öffentlich-rechtlicher Rundfunkanstalten folgende Antwort: Der Gesetzgeber ist

28 *Deirdre N. McCloskey*, Why Liberalism Works. How True Liberal Values Produce a Freer, More Equal, Prosperous World for All, New Haven/London 2019, 27.

im Fall der Rundfunkordnung aufgrund besonderer Umstände nicht zu marktwirtschaftlichen Lösungen verpflichtet. Er darf eine „positive Ordnung" etwa in Form einer gruppenpluralistischen Medienverfassung schaffen.[29] Diese muss aber sicherstellen, dass die Vielfalt der in der Gesellschaft vorhandenen Meinungen, also die gebündelten Meinungen der großen Gruppen, in der durch den Gesetzgeber geschaffenen positiven Ordnung repräsentiert sind. Die gesellschaftlichen Ströme freier Meinungsbildung müssen durch die Rundfunkorganisation hindurchfließen, und das Programm muss die in der Gruppenöffentlichkeit vorhandene Vielfalt der Meinungen abbilden.[30] Alle großen gesellschaftlichen Gruppen, alle gesellschaftlich relevanten Kräfte, müssen, wie es bereits im ersten Rundfunkurteil heißt, im Gesamtprogramm – nicht in jeder einzelnen Sendung – „zu Wort kommen".[31] Wie dann auch in der weiteren Rechtsprechung des Bundesverfassungsgerichts herausgearbeitet worden ist, ist es vor allem die Aufgabe der Rundfunkräte der öffentlich-rechtlichen Sender, diese Vielfalt der Meinungen im Programm sicherzustellen,[32] also Aufgabe jener Minirepubliken im Körper der Anstalten, in der die sozio-politische Landschaft und die kulturellen Milieus der großen Republik gespiegelt werden und sich effektiv artikulieren können sollen.

Die am Gruppenpluralismus der alten Bundesrepublik abgelesene Vielfaltsvorstellung gilt zunächst für die binnenpluralistische Organisation des öffentlich-rechtlichen Rundfunks und sein darauf abgestimmtes Programm. Aber auch die außenpluralistische Struktur des privaten Rundfunks wird von Hesse in die positive Ordnung integriert. Der Gesetzgeber muss, wenn er dem privaten Rundfunk einen Entfaltungsraum geben will, dafür einen gesetzlichen Rahmen zur Verfügung stellen (der heutige Medienstaatsvertrag), zu dem eine begrenzte Staatsaufsicht gehört (die heutigen Landesmedienanstalten). Umgekehrt bedürfen private Rundfunkveranstalter einer staatlichen Zulassung, sie unterfallen, im Unterschied zur Presse (und den Telemedien), dem verwaltungsrechtlichen Verbot mit Erlaubnisvorbehalt. Und zu guter Letzt muss die bestehende Meinungsvielfalt auch im außenpluralistischen System des privaten Rundfunks zur Darstellung gelangen.[33] Daher muss der private Rundfunk gesetzlich etwa auf ein Mindestmaß an inhaltlicher Ausgewogenheit, Sachlichkeit und gegenseitiger Achtung in seinem Programm verpflichtet werden (jetzt §§ 59 ff. MStV).

---

29 BVerfGE 57, 295, 320.
30 *Hesse* (Fn. 1), Rn. 396; BVerfGE 57, 295, 319 ff.
31 BVerfGE 12, 205, 262.
32 BVerfGE 136, 9 (Rn. 38 ff.).
33 *Hesse* (Fn. 1), Rn. 396; BVerfGE 74, 297, 325 ff.

Auch wenn die Darstellung des von Konrad Hesse entworfenen Modells der öffentlichen Meinungsbildung und ihrer Fortführung in der Rechtsprechung des Bundesverfassungsgerichts hier lückenhaft bleiben müssen, dürften die Grundzüge der funktionalen Interpretation der Rundfunkfreiheit und die daraus hervorgehende Vorstellung einer gruppenpluralistischen Medienverfassung doch hinreichend klar geworden sein: Die Einzelperson ist nur in der spontanen, gesellschaftlichen Alltagskommunikation unmittelbar an der öffentlichen Meinungsbildung beteiligt. Ansonsten kann sie sich nur als Organisationsmensch, als Teil einer politischen Partei oder eines anderen gesellschaftlichen Verbandes in die Prozesse politischer Willensbildung einbringen. Sofern aber die sozio-politische Realität der tragenden Gruppen der Gesellschaft und ihre kulturellen Weltbilder im Gesamtprogramm des Rundfunks zu Wort kommt und die Mediennutzer die unterschiedlichen, in der Gesellschaft fließenden Meinungsströme im Programm wiederfinden, bleibt die Freiheit der Berichtserstattung gewahrt, einschließlich der Freiheit der Einzelperson, sich aus unterschiedlichen Quellen zum Zweck der Meinungsbildung informieren zu können.

V. Direkt zu den Leuten

Wir machen jetzt einen räumlichen und zeitlichen Sprung. Vom Freiburg und Karlsruhe der 1970er bis 1990er Jahre geht es nun in den vorletzten amerikanischen Präsidentschaftswahlkampf. Im Januar 2016 sagt der republikanische Präsidentschaftskandidat Ted Cruz in einem Interview mit Fox News: „Die Reporter wollen, dass Hillary gewinnt. Die Antwort darauf ist das zu tun, was Reagan getan hat, über die Köpfe der Medien hinweg zu gehen."[34] Aber wie Cruz zugleich klarstellt, sei das heute viel einfacher als zu Reagans Zeiten. Denn die Zeit, in der drei Fernsehsender den Informationsfluss mit einer Art Würgegriff hätten steuern können, liege hinter uns. „Wir haben das Internet. [...] Wir haben die sozialen Medien. Wir haben die Möglichkeit direkt herumzugehen, direkt zu den Leuten."[35]

Die Tragweite dieser Beobachtung kann man kaum überschätzen. Mit dem Aufstieg einer technologischen Umwelt intelligenter Computernetz-

34 Zitiert nach *Jill Lepore*, The New Yorker, Februar 2016 https://www.newyorker.com/magazine/2016/02/22/did-social-media-produce-the-new-populism (meine Übersetzung, Thomas Vesting).

35 *Lepore* (Fn. 34): „We have got the Internet. ... We have got talk radio. We have got social media. We've got the ability to go directly around, and directly to the people."

werke haben die Prozesse öffentlicher Meinungsbildung neue Informationskanäle und neuartige Intermediäre bekommen. Man braucht keine Presseverlage oder Rundfunkanstalten mehr, um zu den Leuten gehen zu können. Man kann sie direkt adressieren; und dazu benötigt man nicht mehr als ein Smartphone. Mit Hilfe entsprechender Algorithmen kann diese Ansprache sogar personalisiert und dadurch bis zu einem gewissen Grad auf die kulturellen oder politischen Präferenzen von Einzelpersonen zugeschnitten werden. Und umgekehrt können die Menschen jetzt über Twitter, Facebook, Instagram, TikTok oder WhatsApp ihre Meinungen zu jedem beliebigen Thema ohne die herkömmlichen intermediären Organisationen kundtun. Das gilt insbesondere für Personen, die ohnehin schon in der Öffentlichkeit stehen und prominent sind. Nicht nur Popstars wie Rihanna oder Katy Perry haben mehr als 120 Millionen Follower auf Twitter. Auch ein früherer Politiker wie Barack Obama kann in dieser Liga mitspielen. Selbst eine nicht übermäßig prominente brasilianische Abgeordnete wie Carla Zambelli hat über Facebook, Instagram und Twitter im Februar 2020 nach eigenen Angaben ca. 90 Millionen Personen erreicht, eine unglaubliche Zahl, wenn man bedenkt, dass die neun größten brasilianischen Tageszeitungen zusammen nur knapp 1,5 Millionen Leser haben. In Deutschland ist die Entwicklung noch weit hinter solchen Zahlen zurück. Christian Lindner hat aber immerhin ca. 1.300.000 Follower auf Twitter, Facebook und Instagram, und Rezo hat mit seinem Video über „Die Zerstörung der CDU" im Jahr 2019 immerhin zehnmal so viele Zuschauer erreicht wie Markus Lanz im Schnitt mit einer Sendung.

Der Aufstieg intelligenter Computernetzwerke hat das allgemein zugängliche Medienangebot auf ein noch vor wenigen Jahrzehnten unvorstellbares Niveau gehoben und sowohl zur Ausdifferenzierung des Medienangebots wie zu neuen Formen und Wegen seiner Verbreitung geführt. Diese Entwicklung führt ökonomisch und medial gesehen dazu, dass die Einschaltquoten der großen Fernsehsender in allen westlichen Ländern bestenfalls stagnieren, aber jedenfalls bei jungen Leuten zurückgehen. Ebenso sinken die Auflagen von Tageszeitungen und Wochenzeitschriften. Es gibt Variationen dieses Bildes, aber der Trend ist eindeutig: Die herkömmlichen (national orientierten) Massenmedien, Rundfunk und Presse, verlieren an Einfluss und Bedeutung. Gewinner sind (international agierende) soziale Netzwerke, Suchmaschinenbetreiber, Streaming-Dienste und Plattformen aller Art wie Apple, Amazon, Google, Facebook, Twitter, Netflix usw. Das zwingt die herkömmlichen Medienanbieter, sich auf die neue Situation einzustellen – und es ist allgemein bekannt, wie schwierig das ist. Besonders der öffentlich-rechtliche Rundfunk kann aufgrund sei-

ner Geschichte und seiner Organisationsstruktur nur sehr eingeschränkt und nur sehr langsam auf die neue mediale Lage reagieren.

VI. Eine neuartige mediale Environmentalität

Der Aufstieg datengetriebener und umweltsensibler Computernetzwerke ist das Resultat eines tiefen medientechnologischen Einschnitts, der den Bifurkationen der Evolutionsbiologie gleichkommt.[36] Dadurch ist ein neuartiger umweltlicher Sinnhorizont entstanden, der hier, in Anknüpfung an eine von Michel Foucault benutzte Terminologie, als mediale „Environmentalität" beschrieben wird,[37] und mit dem sich die Gesellschaft, die Kultur und die Subjektivierungsprozesse verändern. Das hat auch Konsequenzen für die Medienverfassung: Der herkömmliche Rundfunk als Medium der „Gesellschaft der Organisationen" wird jetzt mit den Medien der „Gesellschaft der Netzwerke" konfrontiert,[38] mit sozialen Netzwerken, Suchmaschinen und Streaming-Diensten, die über neuartige multifunktionale Endgeräte wie Smartphones oder Tablets individuell genutzt werden können. In diesen Kontext gehört auch der im letzten Abschnitt schon angedeutete Bedeutungszuwachs einer neuartigen Plattformökonomie,[39] deren Geschäftsmodelle sich in vielfacher Hinsicht von denjenigen der klassischen Massenmedien unterscheiden.

Schon seit einiger Zeit wird die Medienverfassung durch die informationstechnologische Entwicklung herausgefordert. Die massenmediale Kultur wird mehr und mehr durch eine informationstechnologische Kultur überlagert. Diese ist durch ein ständiges Fluktuieren der Muster der kommunikativen Beziehungen zwischen Individuen gekennzeichnet, die sich keiner vorab gegebenen Allgemeinheit mehr fügen und der keine mit der gruppenpluralistischen Medienverfassung noch verbundene Ein-

---

36 Vgl. *Mark B. N. Hansen*, Feed Forward – On the Future of Twenty-First-Century Media, Chicago/London 2015; *Thomas Vesting*, Die Medien des Rechts IV: Computernetzwerke, 2015.

37 Vgl. *Michel Foucault*, Die Geburt der Biopolitik. Geschichte der Gouvernementalität II. Vorlesungen am Collège de France 1978/1979. Berlin: Suhrkamp, 2006, 361; vgl. auch *Hansen* (Fn. 36); und *Erich Hörl*, Die environmentalitäre Situation. Überlegungen zum Umweltlich-Werden von Denken, Macht und Kapital, in: Internationales Jahrbuch für Medienphilosophie 4 (2018), 221 ff.

38 *Ladeur* (Fn. 8), 24 ff., 30 ff.

39 Vgl. *Julie E. Cohen*, Law for the Platform Economy, 51 U.C. Davis L. Rev. 133-2014 (2017), S. 136 ff.

heitserwartung mehr unterlegt werden kann.[40] Es entsteht vielmehr eine Welt jenseits weniger gesellschaftlich tonangebender großer Gruppen. In der Kultursoziologie ist diese neuartige Lage in jüngerer Zeit als labile Aggregation von Singularitäten beschrieben worden, von Einzelnen, die ständig daran arbeiten, ihre Einzigartigkeit durch die Selbststilisierung von Verhaltensmustern – vom Konsum bis zur sexuellen Orientierung – zu dokumentieren.[41] Man könnte auch von einer Kultur ohne festes Zentrum sprechen, die sich, wie die Parteienlandschaft nach dem Bedeutungsverlust der großen Volksparteien,[42] durch kurzfristige Schwankungen und größere Disparitäten auszeichnet. Im Focus einer solchen Perspektive stünde dann eine dynamische, auf ständige Selbstveränderung angelegte Kultur, in der die digitalen Computernetzwerke eine neuartige Environmentalität generieren, von dem sich das Medienrecht – auch als Verfassungsrecht – künftig leiten lassen müsste.[43]

Nimmt man die Entwicklung von sozialen Netzwerken stellvertretend für die Emergenz digitaler Medien liegt der entscheidende Unterschied zwischen diesen und dem herkömmlichen Rundfunk in der grundlegenden Veränderung des Charakters der Medienproduktion und Medienrezeption. Die plattformvermittelte Kommunikation der sozialen Netzwerke sprengt die Form der passiven Rezeption zeitlich genau fixierter Programme durch wiederkehrende stabile Publika. Das einstige Programm wird hier zum gemeinsamen Produkt einer Vielzahl von Nutzern, beispielsweise in Form von schnell aufeinander reagierenden Meinungsäußerungen in einem Chat, der sich zu jeder beliebigen Zeit bilden, aber genauso schnell auch wieder verschwinden kann. Das bringt einerseits „ein starkes Ansteigen im Reichweitenpotential für Jedermann-Kommunikationen mit sich“[44] und andererseits die Auflösung stabiler Programmformen in einer eher episodenhaften Prozessrealität, die durch ständige Updates angereichert wird und phänomenologisch unruhig bleibt. Soziale Netzwerke werden zwar als kommerzielle Unternehmen betrieben und sind in diesem Sinn handelnde Organisation, ihr Geschäftsmodell beruht aber nicht auf der Herstellung fix und fertiger Medienprodukte wie Filmen, Sport- oder Nachrichtensendungen. Das Unternehmen stellt vielmehr die

40 *Albert Ingold*, Digitalisierte Öffentlichkeiten und ihre Regulative, in: Kruse/Müller-Mall (Hrsg.), Digitale Transformation der Öffentlichkeit, Weilerswist 2020, 163 ff., 169.
41 Vgl. *Andreas Reckwitz*, Die Gesellschaft der Singularitäten, 2017.
42 Ausführlicher *Thomas Vesting*, Staatstheorie, 2018, 173 ff.
43 *Ladeur* (Fn. 8), 30.
44 *Ingold* (Fn. 40), 163 ff., 168.

technologischen Mittel – die Plattform – für den Aufbau kommunikativer Beziehungsnetzwerke bereit, die jetzt selbst als „neue(r) Quasi-Akteur" auftreten und rechtlich auch so behandelt werden müssen.[45] Die sozialen Netzwerke werden auch nicht dadurch zu herkömmlichen Massenmedien, dass die nutzergenerierten Inhalte teilweise mit herkömmlichen Medienangeboten wie zum Beispiel Nachrichtenfeeds kombiniert werden. Denn diese werden, wie die Kommunikation in sozialen Netzwerken, im Allgemeinen ebenfalls nicht redaktionell aufbereitet, sondern mit Hilfe von Algorithmen gefiltert und für die Nutzer personalisiert.

Die digitale Transformation der Medien verändert die Prozesse der freien Meinungsbildung daher ebenso grundlegend wie die in der Öffentlichkeit vorherrschenden Kommunikationsmuster. Das Hauptmerkmal der neuen digitalen (postmassendemokratischen) Öffentlichkeit liegt in einer gesellschaftlichen, sich selbst über Netzwerke organisierenden zerstreuten Kommunikation und nicht mehr in einer Form, die über repräsentative Gruppen und ihre Sinnwelten gebündelt wird. Die Veränderung besteht anders gesagt darin, dass an die Stelle „hochselektiver Medienfilter" einer formierten und organisierten Gesellschaft eine „Vielzahl von Filtermedien" in distribuierten interaktiven Kommunikationsformen in einer stärker permissiven Gesellschaft tritt.[46]

VII. Was heißt das für das deutsche Medienrecht?

Kann man an der für die Industriegesellschaft und ihre Gruppenkultur entwickelten funktionalen Interpretation der Rundfunkfreiheit festhalten? Und sollte man das aus dieser Rechtsprechung hervorgegangene Regulierungsregime, wie es seit 1991 zunächst im Rundfunkstaatsvertrag der Länder seinen Ausdruck gefunden hat, auf Computernetzwerke übertragen und die großen global agierenden Plattformen der US-amerikanischen Unternehmen wie die privaten Rundfunkunternehmen einer medienrechtlichen Regulierung unterwerfen, wie es der neue Medienstaatsvertrag und die europäische Regulierung nun erstmals vorsehen? Diese Fragen sind

45 *Karl-Heinz Ladeur*, Netzwerkrecht als neues Ordnungsmodell des Rechts. – nach dem Recht der Gesellschaft der Individuen und dem Recht der Gesellschaft der Organisationen, in: Eifert/Gostomzyk (Hrsg.), Netzwerkrecht: Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, Baden-Baden 2018, 169 ff., 171.

46 *Jens Kersten*, Schwarmdemokratie. Der digitale Wandel des liberalen Verfassungsstaates, 2017, 127, 133, 134.

von so großer Komplexität, dass sie im Rahmen eines Beitrags zu einem Sammelband nicht adäquat beantwortet werden können. Ich möchte aber eine Richtung markieren, in der künftig über diese und vergleichbare Fragen diskutiert werden sollte. Dazu zunächst eine These, die ich nur kurz begründen werde.

Für eine liberale Verfassung wie die des Grundgesetzes ist das normative Modell einer freien Meinungsbildung unverzichtbar. Zwar löst Konrad Hesses Modell der Bildung einer öffentlichen Meinung die politische Seite der Öffentlichkeit zu sehr von der gesellschaftlichen und privaten Meinungsbildung trennt. Aber bei Hesse geht es doch auch um die ständige *Bildung* einer öffentlichen Meinung, um den prozesshaften Charakter der publizistischen Auseinandersetzung um die politische Macht, die sich bei ihm letztlich an der Presse orientiert. Und dieses prozesshafte Moment gilt für alle Grundrechte des Art. 5 Abs. 1 GG, sowohl für die Interpretation der Kommunikationsgrundrechte des Satzes 1 wie der Mediengrundrechte des Satzes 2; sie alle schützen den Prozess der freien Meinungsbildung. Dieser Ausgangspunkt kann beibehalten werden und sollte, wie im dritten Abschnitt schon angedeutet, in einem Konzept des prozeduralen, prozesshaften und impersonalen Grundrechtsschutzes genauer ausgearbeitet werden. Die Meinungsfreiheit und die Medienfreiheiten würden dann nicht primär die Subjektivität und Persönlichkeit des Einzelnen schützen, sondern einen Prozess der freien Meinungsbildung in einer beweglichen kulturellen Matrix. Meinungsbildung wäre dann als ein transsubjektives Phänomen „des ‚organizing intelligence'" zu konzipieren, als Mittel zur „Herstellung einer ‚creative, progressive, exciting and intellectually robust community'",[47] bei dem das Subjekt – wie schon das grammatische Subjekt Wittgensteins – zu einem Teilhaber an einem Geschehen wird, das nicht aus ihm selbst – aus seinem Höchstpersönlichen – kommt.[48] Subjektivität ist folglich keine zentrale oder letzte Instanz mehr, im Gegenteil, die teilhabende oder relationale Subjektivität wird durch die digitalen Technologien künftig noch mehr an Bedeutung gewinnen, weil diese eine intelligente sensorische Umwelt schaffen, an die sich das menschliche Subjekt nicht mehr nur anpasst, sondern die dem menschlichen Subjekt etwas anbietet, „zur Verfügung stellt, was sie ihm beibringt".[49]

---

47 *Ladeur* (Fn 19), S. 172, 176.

48 Vgl. *Sandra Markewitz*, Das grammatische Subjekt. Konstitutionsformen von Subjektivität in der Moderne, in *dies*. (Hrsg.), Grammatische Subjektivität, Wittgenstein und die moderne Kultur, 2019, 23, 46.

49 Vgl. *Erich Hörl*, Internationales Jahrbuch für Medienphilosophie 4 (2018), 221, 235. Das ließe sich auch auf unterschiedliche historische Erscheinungsformen me-

Im Ergebnis können also wichtige Komponenten von Hesses Modell der öffentlichen Meinungsbildung weitergeführt werden. Was aber heute auf den Prüfstand muss, ist die Frage, ob es Sinn macht oder gar verfassungsrechtlich geboten sein könnte, der neuartigen medialen Environmentalität der elektronischen Netzwerke und ihrer Sinnwelten mit der Logik eines Rechtsregimes zu begegnen, das aus der industriellen Massengesellschaft und der zu ihr gehörenden Kultur politischer Gruppierung stammt. Sollen also auch die neuen digitalen Medien – die sozialen Netzwerke, die Suchmaschinen, die Streaming-Dienste – und ihre Plattformen, soweit sie die öffentliche Meinungsbildung tangieren, dem Regime des Rundfunkrechts mit seiner treuhänderischen Lösung eines Binnen- oder Außenpluralismus und damit einer staatlichen Verantwortung unterworfen werden? Oder wäre nicht das Modell der Presseregulierung vorzugswürdig? Oder wäre nicht sogar eine allgemeine (nicht medienspezifische) Regulierung der neuen Situation allein angemessen, also eher eine Deregulierung der Medien, statt immer mehr Medienregulierung?

Hesses verfassungsrechtliche Modellbildung, die die gesetzgeberische Möglichkeit legitimiert, eine positive Rundfunkordnung zu schaffen, baute darauf auf, dass die Produktion von Fernseh- und Hörfunksendungen kostenintensiv und Sendefrequenzen ursprünglich knapp waren und der marktwirtschaftliche Wettbewerb zwischen privaten Unternehmen kein vergleichbar vielfältiges Gesamtprogramm erzeugen konnte. Insbesondere die zuletzt genannte Überzeugung des Berichterstatters Hesse, die den politischen Streit um die duale Rundfunkordnung lange beherrscht hat, hat auch immer wieder Einfluss auf die Urteile des Bundesverfassungsgerichts gehabt. An eine derartige Vielfaltsvorstellung, jetzt als Vorstellung einer Vielfaltverengung durch die Konzentrationstendenzen innerhalb der Plattformökonomie, knüpft die medienpolitische Diskussion heute wieder an, wenn sie den Aufstieg intelligenter Computernetzwerke wie zuvor den Rundfunk unter Vielfaltsgesichtspunkten beobachtet und diese Beobachtung mit der Unterstellung verbindet, dass die elektronischen Netzwerke zu einer zunehmenden Monopolisierung der Verfügung über Inhalte durch wenige „große Konzerne“ sowie zu „Filterblasen“ und zu „Fake News“ führten.

---

dialer Infrastrukturen beziehen, die bestimmte kulturelle und gesellschaftliche Entwicklungen ermöglichen oder eben nicht ermöglichen; vgl. *Mireille Hildebrandt*, Smart Technologies and the End(s) of Law, Cheltenham U.K. 2016, 47 ff. (zu Möglichkeitsbedingungen der Oralität, der Schrift, des Buchdrucks, des Films usw.); vgl. auch *Christoph B. Graber*, Washington University Jurisprudence Review 10 (2017), S. 221, 226 f.

In der medienpolitischen Diskussion wird aber nie gefragt, ob die Medienöffentlichkeit heute noch so funktioniert, wie Konrad Hesse sie beschrieben hat: als organisationsbasierte Öffentlichkeit. Das muss aber vorausgesetzt werden können, wenn von Vielfaltsverengung oder Gefahren für die Meinungsfreiheit gesprochen wird und damit normativ an die Idee der Sicherung einer auf den Prinzipen des politischen Gruppenpluralismus beruhenden Rundfunkfreiheit angeknüpft werden soll. Es muss vor allem vorausgesetzt werden können, dass es große Organisationen sind, die die disperse Kommunikation in der Gesellschaft bündeln und konturieren, sie als linke oder rechte, grüne oder liberale politische Position erkennbar machen – und dass diese, über große Organisationen und einen professionellen Journalismus vermittelte Öffentlichkeit eine Monopolstellung hat oder zumindest die öffentliche Meinungsbildung maßgeblich prägt. Genau diese Voraussetzung ist aber entfallen, wie nicht erst die letzten US-Wahlkämpfe um die Präsidentschaft deutlich gemacht haben. Um es allgemeiner zu sagen: Wir leben längst mit den Medien der „Gesellschaft der Netzwerke".[50] In dieser Umwelt bildet nicht mehr der Organisationsmensch das dominierende Paradigma, sondern der sich selbst vernetzende Homo Digitalis. Die technologische Kreativität des Silicon Valley hat neue Kommunikationskanäle geschaffen, die beispielsweise über die sozialen Netzwerke eine direkte Kommunikation von Einzelpersonen an beliebig viele andere Einzelpersonen ermöglichen. Damit wird Konrad Hesses These, dass „politische Antriebe nur noch in geringem Maße von Einzelpersonen ausgehen" hinfällig – hinfällig allerdings nur insofern, als die Antriebe heute eben nicht mehr allein von Organisation, sondern mehr und mehr von einer neuartigen informationstechnologische Environmentalität ausgehen.

An diesen Befund lässt sich eine verfassungsrechtliche These anschließen. Hesses organisationsbezogenes Modell der Bildung einer öffentlichen Meinung mag bis in die 1990er Jahre eine gewisse Schlüssigkeit gehabt haben. Je mehr die darin implizit eingeflossene Unterstellung, die lebensweltliche Selbstverständlichkeit, von der Hesse zu seiner Zeit zweifellos noch ausgehen konnte, nämlich dass die Bildung einer Öffentlichkeit primär im Feld der organisierten Gruppeninteressen angesiedelt ist, entfallen, umso mehr verliert dieses Modell an verfassungsrechtlicher Evidenz. Es ist vor diesem Hintergrund erstaunlich, dass das Bundesverfassungsgericht in seinem Urteil zum Rundfunkbeitrag aus dem Jahr 2018 das in der medienpolitischen Diskussion kursierende Bild von der Vielfaltsverengung

50 *Ladeur* (Fn. 8), 30 ff.

durch digitale Medien mehr oder weniger eins zu eins in seine Urteilsbegründung übernommen und in seinem jüngsten Beschluss zum Rundfunkfinanzierung wiederholt hat. Ohne eine tiefere Auseinandersetzung mit dem Stand der wissenschaftlichen Diskussion behauptet das Bundesverfassungsgericht, dass die Digitalisierung der Medien und insbesondere die Netz- und Plattformökonomie des Internets einschließlich der sozialen Netzwerke Konzentrations- und Monopolisierungstendenzen bei Anbietern, Verbreitern und Vermittlern von Inhalten begünstigten.[51] Das Bundesverfassungsgericht will mit dieser Behauptung belegen, dass die neuartige Environmentalität der elektronischen Netzwerke nicht mit einem Freiheitsgewinn und mehr Möglichkeiten für die öffentliche Meinungsbildung einhergeht, sondern mit neuartigen Gefahren der Vielfaltsverengung, wie sie etwa durch die Verstärkung gleichgerichteter Meinungen, durch den Einsatz von Algorithmen oder die allein auf Klickzahlen ausgerichtete wirtschaftliche Rationalität von Geschäftsmodellen verbunden seien.[52] Daher, so der juristische Schluss, könne auf den die Rundfunkfreiheit sichernden öffentlich-rechtlichen Rundfunk und die Beitragspflicht heute weniger denn je verzichtet werden.[53]

VIII. Begünstigt Google eine Verstärkung gleichgerichteter Meinungen?

Das Problem, das sich eine solche Argumentationsführung einhandelt, besteht darin, dass sie zum Beispiel eine Suchmaschine wie Google, die für den Nutzer die Funktion eines Kurators in einem Meer von Daten und Informationen einnimmt,[54] juristisch wie ein klassisches Medienunternehmen unter Vielfaltsgesichtspunkten betrachtet. Damit wird eine der faszinierendsten Erfindungen des 20. Jahrhunderts (und ein Beispiel für die überlegene technologische Kreativität des Silicon Valley) an einem Maßstab gemessen bzw. auf eine Funktion verengt, die allenfalls einen Teilaspekt des für einen Beobachter letztlich unüberschaubaren Leistungsspektrums der Suchmaschine herausgreift. Damit verfehlt diese Argumentationsführung aber gerade den universalen, nicht auf einen Zweck (wie

51 BVerfGE 149, 222 (Rn. 79); 158, 389 (Rn. 80).
52 BVerfGE 149, 222 (Rn. 79); 158, 389 (Rn. 80).
53 BVerfGE 149, 222 (Rn. 81); 158, 389 (Rn. 81).
54 Vgl. *Albert Ingold*, Governance of Algorithms. Kommunikationskontrolle durch ‚Content Curation' in sozialen Netzwerken, in: Unger/Unger-Sternberg (Hrsg.), Demokratie und künstliche Intelligenz, 2019, 183.

die Bereitstellung von Rundfunkprogrammen) begrenzten Charakter von Google als Plattform. Ich möchte das an einem Beispiel erläutern.

Google ermöglicht jedem Nutzer, der mit der Suchmaschine arbeitet, Zugang zu Daten und Informationswelten, die vor ihrer Erfindung gar nicht oder jedenfalls nur mit sehr viel mehr Aufwand zugänglich waren. So hat Google unter anderem begonnen, den Traum einer universalen Bibliothek zu realisieren, von dem französische Aufklärer wie Condorcet geträumt haben. Google Books hat inzwischen 25 Millionen Bände digitalisiert, mehr als doppelt so viele Bücher, wie die Berliner Staatsbibliothek, die größte deutsche wissenschaftliche Universalbibliothek, in Papierform im Bestand hat. Die deutsche digitale Bibliothek, die Antwort der deutschen Kulturpolitik auf Google, stellt demgegenüber jährlich 1,3 Millionen € für die Digitalisierung des deutschen Buchbestandes zur Verfügung, so dass die Staatsbibliothek Berlin von ihren 10 Millionen Büchern immerhin schon 400.000 digitalisiert hat. Google tut also nicht nur viel für die mediale Vielfalt, sondern ist im Feld der Digitalisierung von Buchbeständen auch erheblich leistungsfähiger als der deutsche Staat. Man kann Martin Schallbruch daher nur zustimmen: „Google Books ist eine Privatinitiative, von der wir dankbar sein können, dass es sie gibt."[55]

Google ist heute aber nicht nur ein gigantisches digitales kulturelles Archiv. Es erweitert auch die Möglichkeiten der politischen Meinungsbildung eines jeden Einzelnen. Google ermöglicht jedem Nutzer, nahezu jede beliebige Zeitung dieser Welt zu finden und in Ausschnitten zu lesen oder nach interessanten Meinungen abzusuchen, etwa die kostenlosen Webseiten der New York Times, der NZZ, von La Repubblica oder die des Economist. Hier stoßen wir auf ein durchaus konflikthaftes Feld, auf das der deutsche Gesetzgeber bereits 2013 mit einem (letztlich nicht erfolgreichen) Leistungsschutzrecht für Presseverlage zu antworten versucht hat.[56] Aber in unserem Kontext geht es nicht um eine Kollisionsordnung zwischen Presse und Suchmaschinenbetreiber wie Google, sondern allein und ausschließlich um die Frage, was es angesichts dieser faszinierenden Erweiterung von Möglichkeiten der Meinungsbildung bedeuten kann, mehr oder weniger pauschal zu behaupten, die Digitalisierung der Medien begünstige Konzentrations- und Monopolisierungstendenzen bei Vermittlern von Inhalten? Die publizistischen Inhalte werden durch die neuen

55 Vgl. *Martin Schallbruch*, Schwacher Staat im Netz: wie die Digitalisierung den Staat in Frage stellt, 2018, 110 ff., 112.

56 Der EuGH hat das Leistungsschutzrecht für Presseverlage am 12.9.2019 (C-299/17) wegen Verstoßes gegen die europarechtliche Notifizierungspflicht für nicht anwendbar erklärt.

digitalen Medien nicht monopolisiert, sondern sie explodieren ins Unendliche.

IX. Regulierung von Medienintermediären – ohne Grundrechte?

Es kann nicht zweifelhaft sein, dass die neuen digitalen Medien und eine Suchmaschine wie Google der *rule of law* unterworfen sind, also etwa den für die freie Meinungsbildung relevanten Schrankengesetzen wie etwa dem Strafrecht (und in Deutschland auch dem Netzwerkdurchsetzungsgesetz), dem Persönlichkeitsschutz, dem Datenschutz oder dem Wettbewerbsrecht usw. Es erscheint aber sehr fraglich, ob ein organisationsbasiertes Modell der Öffentlichkeit und eine von gruppenpluralistischer Vielfalt ausgehende Medienregulierung es wahrscheinlich machen, der neuen Logik der elektronischen Netzwerke adäquat zu begegnen – und beispielsweise mit einer universalen Suchmaschine wie Google und der sich um sie herum bildenden Drittanbieter so umzugehen, dass die Entwicklungsoffenheit der informationstechnologischen Dynamik auch in Zukunft gewährleistet werden kann.

Zu Recht stuft der neue Medienstaatsvertrag im Unterschied zu einer jüngeren Entscheidung des Bundesverfassungsgerichts Google als Medienintermediär ein und reduziert dessen Dienstleistungen damit nicht auf rein wirtschaftliches Handeln.[57] Aber die dazu beabsichtigte Regulierung ist diffus. Sie zielt im Kern auf Diskriminierungsfreiheit und Transparenz. Aber was soll es beispielsweise bedeuten, wenn Google künftig zu Zwecken der Sicherung der Meinungsvielfalt die zentralen Kriterien einer Aggregation, Selektion und Präsentation von Inhalten und ihre Gewichtung unter Einschluss von Informationen über die Funktionsweise der eingesetzten Algorithmen in verständlicher Sprache leicht wahrnehmbar, unmittelbar erreichbar und ständig zur Verfügung halten soll (§ 93 MStV)? Soll sich das auf jeden Einzelfall beziehen? Googles Marktmacht resultiert doch gerade daraus, dass Google als Plattform riesige Datenmengen aggregiert, verarbeitet und immer wieder neu zusammensetzen kann – und deren konkrete Zweckverwendungen vorab selbst gar nicht kennt. Unstrittig dürfte zumindest sein, dass Google auch als ausländische juristische Person selbst Grundrechtsträger ist und die neuen Vorschriften des Medienstaatsvertrages tief in die europäischen und nationalen Grundrechte von Google eingreifen. Das gilt allerdings nicht nur im Hinblick auf die unternehmeri-

57 Vgl. BVerfGE 152, 216 (Rn. 105).

sche Freiheit der Europäischen Grundrechtecharta (Art. 16) und die Wirtschaftsfreiheiten des Grundgesetzes (Art. 12, 14, 2 Abs. 1). Darüber hinaus erbringt Google als Kurator von Inhalten – als neuartiger Medienintermediär – auch eine mediale Leistung für den Nutzer und muss daher als Träger der Pressefreiheit,[58] zumindest aber als Träger der Meinungsfreiheit anerkannt werden.

X. Schluss: Ein neue Medienverfassung für intelligente Computernetzwerke

Je länger man über das hier diskutierte Problem nachdenkt und sich dabei von klaren juristischen Gedanken und nicht von plakativen politischen Formeln leiten lässt, umso deutlicher wird, dass eine universale Suchmaschine wie Google nichts mit der institutionellen (organisationsbezogenen) Ordnung des Rundfunks zu tun hat. Die erweiterte Regulierung des Medienstaatsvertrages hinterlässt einen wenig durchdachten Eindruck, und sie wird in der Praxis wohl eher zu einer Überforderung der Landesmedienanstalten führen und die unproduktive Regulierungsvielfalt von staatsvertraglichem Medienrecht, Telekommunikationsregulierung und Bundeskartellrecht, in dem sich das mediale Deutschland schon lange befindet, noch weiter steigern. Es spricht deshalb alles dafür, für die neuartige mediale Environmentalität intelligenter Computernetzwerke ein neues „Sozialverfassungsrecht der digitalen Medien“[59] zu entwerfen und für dieses netzwerkadäquate Institutionen und eine entsprechende Regulierung zu schaffen.

Es müsste um eine Medienverfassung gehen, das die Stelle des organisationsbasierten Modells der Bildung einer öffentlichen Meinung besetzen könnte. Die normative Funktion der Öffentlichkeit liegt in einem liberalen Verfassungsstaat darin, durch die Beobachtung des Selbst im Spiegel der anderen eine relationale, bewegliche, zukunftsoffene Kultur zu schaffen und die darin angelegte Möglichkeit zur Selbstveränderung des Einzelnen durch Freiheitsreche abzustützen und zu ermöglichen. Das darin ein-

---

58 Davon ist das OLG Hamburg unter Rückgriff auf Überlegungen von Hoffmann-Riem bereits in einer Entscheidung aus dem Jahr 2011 ausgegangen, OLG Hamburg MMR 2011, 685; anders BVerfGE 152, 216 (Rn. 102–105); kritisch dazu *Karl-Heinz Ladeur*, Grundrechtsschutz im europäischen Mehrebenensystem durch das BVerfG, insbesondere der Grundrechtsschutz der Betreiber von Suchmaschinen, WRP (2020) / Heft 2, S. 139, 141 f.

59 *Dan Wielsch*, Funktion und Verantwortung. Zur Haftung im Netzwerk, RW 10 (2019) / Heft 1, S. 84, 88.

geschlossene Moment der Allgemeingültigkeit der universalen Ordnung wird auch im gruppenpluralistischen Öffentlichkeitsmodell als „Aufgabe" beibehalten, indem dort unterstellt wird, dass die „Vorformung des politischen Willens" nur „in öffentlicher Auseinandersetzung der unterschiedlichen Meinungen und Interessen" möglich sei.[60] Der Umbau von einer unterstellten zu einer immer erst herzustellenden Allgemeinheit wird zwar bei Konrad Hesse, wie gezeigt, zu sehr auf das Feld der formal institutionalisierten Politik und ihrer Gruppen verengt. Aber an seiner Art. 5 Abs. 1 GG unterlegten Idee der Bildung einer öffentlichen Meinung ist doch richtig, dass das Allgemeine hier für die Dimension der historischen Zeit geöffnet wird. Daraus lässt sich ein Modell extrapolieren, „das der Geschichtlichkeit seines Gegenstandes (und seiner eigenen Geschichtlichkeit)" innewird, „des ‚Einbruchs der Zeit', der diese (die Zeit) „zur ‚Kategorie der inneren Struktur von Staat und Recht' werden läßt."[61]

In diesem Modell geht es um die innere Struktur des staatlichen Rechts als eines sich temporalisierenden Rechts und nicht lediglich um die Öffnung des staatlichen Rechts für die Beobachtung einer sich wandelnden Wirklichkeit. Damit kommt Hesse einem Paradigma nahe, für das Karl-Heinz Ladeur den Begriff der „Prozeduralisierung zweiter Ordnung" vorgeschlagen hat:[62] Danach besteht die Leistung des westlichen Rechts gerade in der „Bereitschaft und der Fähigkeit, die in die *azentrische heterarchische Ordnung* eingetragen ist, die Öffnung für das Neue, das Unbekannte, zu ermöglichen, ohne den Zerfall der gesellschaftlichen Ordnung insgesamt zu riskieren."[63] Es würde dann auf der einen Seite darum gehen, die Produktivität intelligenter Computernetzwerke als eine Entwicklung zu akzeptieren, die sich ohne vorab aufgestellte Regeln in einem offenen Möglichkeitsraum der „schöpferischen Zerstörung" (Schumpeter) vollzieht, der durch Freiheitsrechte und andere subjektive Rechte geschützt ist und auch weiterhin geschützt werden muss, soweit dabei niemand unmittelbar oder mittelbar geschädigt wird. Das staatliche Recht, auch die politische Gesetzgebung, verlieren dadurch aber nicht an Bedeutung, sie werden nicht einfach durch die künstliche Intelligenz von lernfähigen Algorithmen oder anderen Formen rein gesellschaftlicher Selbstregulierung abgelöst. Die Medienverfassung der Öffentlichkeit der digitalen Medien kann aber nicht mehr auf eine politische Einheitserwar-

60 *Hesse* (Fn. 1), Rn. 152.
61 *Hesse* (Fn. 1), Rn. 9.
62 Vgl. *Ladeur*, Die Textualität des Rechts. Zur poststrukturalistischen Kritik des Rechts, 2016, S. 309; *ders*. (Fn. 8), 34, 132, 178.
63 *Ladeur*, Manuskript, 2018.

tung angelegt sein. Ihr muss eine „heterarchische Rechtskonzeption“[64] zugrunde liegen, die auf eine mitlaufende oder nachträgliche gesellschaftliche Ordnungsbildung zielt, insbesondere durch Anknüpfung an Prozesse der Instituierung von Normativität in den neuen technologischen Infrastrukturen. Das Ziel einer daran anknüpfenden Regulierungsstrategie würde darin bestehen, die Ergebnisse der experimentellen Entwicklung der elektronischen Netzwerke im Nachhinein teilweise zu ordnen,[65] nicht aber wie früher vorab durch eine positive Ordnung zu steuern.

In einer Medienverfassung, die auf die neuartige, von Computernetzwerken geprägten informationstechnologischen Umwelt des Menschen eingestellt wäre, würde auch die Form der Rechtssubjektivität in einer neuen Weise zur Geltung kommen. Dabei käme es darauf an, Personen – wie ursprünglich schon im anglo-amerikanischen Typus einer heterarchisch-dezentralen Gesellschaftsbildung – nicht als souveräne Subjekte zu denken, die der Welt ihren Willen aufprägen. Subjektivität wäre vielmehr wie eine Schnittstelle von ihr vorausliegenden multiplen, heterogenen und sich überlappenden Kraftfeldern (agencies),[66] als environmentale Subjektivität,[67] zu konstruieren. Das Subjekt agiert in einem immer schon bestehenden System von Bezogenheiten, das nicht erst nachträglich die vermeintliche Unabhängigkeit von den anderen, den Dingen und Technologien beschneidet. Dieses System von Bezogenheiten wird in der neuen informationstechnologischen Kultur nicht mehr von großen Gruppen und Organisationen bestimmt, sondern mehr und mehr von der Informationstechnologie selbst, die erst in ihren Anfängen steckt. Je weiter sich diese Technologie als künstliche Intelligenz entwickeln wird, umso weniger wird sie den Subjekten äußerlich bleiben. Schon jetzt kann man sehen, wie die digitalen Medien gerade für Jugendliche und Heranwachsende die Chance bieten, das eigene Selbstverständnis gestalten und die Suche nach der eigenen Identität mit dem Gefühl des Gesehen-Werdens verbinden zu können.[68] Das ließe sich auf einem höheren Abstraktionsniveau als „emergence of the relational self“ beschreiben, als eine Bewegung „from self to relationship“, die sich der reichen kommunikativen (auch bildhaften) Mittel der neuen sozialen Medien bedient und darin die Chance eines

64 *Augsberg*, Schmitt-Lektüren, 2020, 37.
65 *Ladeur* (Fn. 8), 132; vgl. allg. auch *Vesting* (Fn. 42), S. 157 ff.
66 *Hansen* (Fn. 36), S. 36 f.
67 *Hansen*, ebd., 5; vgl. *Ladeur* (Fn. 8), 19, 23, 87.
68 Vgl. den Bericht der Schülerin einer High-School in Utah *Taylor Fang*, Reimagine the Self(ie), MIT Technology Review 123 (2020), No. 1, S. 36.

geteilten „consciousness of relational selves“ in der westlichen Kultur eröffnet.[69]

Das relationale Subjekt könnte sich insbesondere dann vielversprechend weiterentwickeln, wenn es lernt, das eigene Selbst mit den Augen der anderen zu sehen und an die Stelle der Selbststilisierung der Singularität ein Machen in der im zweiten Abschnitt angesprochenen, seit der italienischen Renaissance existierenden Tradition des „poetic making“ zu setzen.[70] Es käme also darauf an, die Prozesse der spontanen gesellschaftlichen Selbstorganisation an einen „powerful impetus to construct a world of our own making“ zu binden.[71] Dieser Impetus müsste darauf angelegt sein, die Möglichkeiten der neuen Informationstechnologien als gemeinsames Projekt zu begreifen und in kreative Innovationen umzusetzen. Die Medienverfassung wäre dann in erster Linie darauf zuzuschneiden, die Spontaneität des „exzessiven Moments“ der Rechtssubjektivität und damit einen Prozess ohne Ende zu schützen.

69 *Kenneth J. Gergen*, The Saturated Self. Dilemmas of Identity in Contemporary Life (1991), New York 2000, 156 f.
70 *Kahn* (Fn. 22), 2.
71 *Kahn* (Fn. 22), 45.

Das Netzwerkdurchsetzungsgesetz: Entwicklung, Auswirkungen, Zukunft

Alexander Peukert[*]

I. Entstehungsgeschichtlicher Kontext und Zweck des NetzDG 2017

Das „Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken" vom 1. September 2017 (Netzwerkdurchsetzungsgesetz – NetzDG 2017)[1] war zum Zeitpunkt seines Erlasses eine regulatorische Innovation, die weltweit wahrgenommen wurde und mehrere Länder zu ähnlichen Kodifikationen inspirierte.[2] Der historische Kontext des NetzDG 2017 war ebenfalls kein spezifisch deutscher, sondern ein europäischer, ja globaler.

Zum einen fällt die Entstehung des NetzDG zeitlich zusammen mit dem Höhepunkt der europäischen „Flüchtlingskrise" im Herbst/Winter 2015. In Anbetracht einer „zunehmende[n] Verrohung der öffentlichen Debatte hin zu fremdenfeindlichen und rassistischen Hassbotschaften" (Stichwort „Hasskriminalität") vereinbarte der damalige Bundesjustizminister Heiko Maas im September 2015 mit Facebook die Bildung einer Task Force von Internetanbietern und zivilgesellschaftlichen Organisationen, deren Auftrag es war, „Vorschläge für den nachhaltigen und effektiven Umgang mit Hassbotschaften im Internet und den Ausbau bestehender Kooperationen zu erarbeiten".[3] Das im Dezember 2015 vorgelegte Ergebnispapier der Task Force-Mitglieder (darunter auch Google/YouTube

---

* Prof. Dr. iur., Fachbereich Rechtswissenschaft, Goethe-Universität Frankfurt am Main.

1 BGBl. I 2017, 3352.

2 *Eifert*, Evaluation des NetzDG im Auftrag des BMJV, 2020, 13 („Vorreiter der weiteren Entwicklung auf unionaler Ebene"); Frankreich: Proposition de loi n° 1785 visant à lutter contre la haine sur internet v. 20.3.2019 und Bericht *Laetitia Avia*, 26; Österreich und Türkei: Wissenschaftliche Dienste des Deutschen Bundestags, Meinungsfreiheit in sozialen Medien, WD 10 - 3000 - 021/21, Mai 2021, 12 f., 16 f.; Japan: https://www.bundesjustizamt.de/DE/Presse/Archiv/2019/20190325.html?nn=3451904.

3 BMJV, Gemeinsam gegen Hassbotschaften, 15.12.2015, https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/12152015_TaskForceErgebnispapier.html, 1.

und Twitter) enthielt bereits zentrale Elemente des späteren NetzDG.[4] Insbesondere verpflichteten sich die beteiligten Unternehmen, anwenderfreundliche Meldemechanismen einzurichten und die Mehrzahl rechtswidriger Inhalte innerhalb von 24 Stunden zu prüfen und zu löschen.[5]

Zum anderen verwies der Gesetzentwurf der aus CDU/CSU und SPD gebildeten Bundesregierung v. 16.5.2017 auf „Erfahrungen im US-Wahlkampf", aufgrund derer „auch in der Bundesrepublik Deutschland die Bekämpfung von strafbaren Falschnachrichten (‚Fake News') in sozialen Netzwerken hohe Priorität gewonnen" habe.[6] Bezug genommen wurde hiermit auf die damals weltweite Debatte im Anschluss an das Brexit-Referendum und die Wahl Donald Trumps zum US-Präsidenten über die Frage, welche Bedeutung manipulativen Falschmeldungen für die demokratische Willensbildung im digitalen Zeitalter zukommt.[7]

Die beiden Anlässe für das NetzDG – Hasskriminalität 2015/2016 und Fake News 2016/2017 – weisen mehrere Gemeinsamkeiten auf. Den politischen Kontext bildet die sog. populistische Revolte in Europa und Nordamerika.[8] Kommunikationswissenschaftliche Untersuchungen haben ferner für beide Diskurslagen bestimmte Spaltungen der öffentlichen Debatte festgestellt. Demnach herrschte in den Leitmedien – in Deutschland also dem öffentlich-rechtlichen Rundfunk und bundesweit erscheinenden Tageszeitungen wie der Frankfurter Allgemeinen Zeitung, der Süddeutschen Zeitung oder der Welt – zu beiden Themenkomplexen (Flüchtlinge, Trump) ein hohes Maß an Gleichklang. Das Flüchtlingsthema wurde bis zum Jahreswechsel 2015/2016 weitgehend in Übereinstimmung mit der politischen Linie der Bundesregierung vermittelt.[9] Über Trump wurde nach seinem Regierungsantritt in den US-amerikanischen und internatio-

4 Bericht der Bundesregierung zur Evaluierung des Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, 2020, 5 (NetzDG löste die freiwillig eingegangen Verpflichtungen ab).

5 Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), BT-Drucks. 18/12356, 1.

6 RegE NetzDG (Fn. 5), BT-Drucks. 18/12356, 1.

7 Vgl. https://www.nytimes.com/2017/01/10/us/politics/obama-farewell-address-speech.html; https://www.independent.co.uk/news/uk/home-news/fake-news-word-of-the-year-2017-collins-dictionary-donald-trump-kellyanne-conway-antifa-corbynmania-a8032751.html.

8 Vgl. *Goodhart*, The Road to Somewhere: The Populist Revolt and the Future of Politics, 2017.

9 *Haller*, Die „Flüchtlingskrise" in den Medien, 2017, 138; *Maurer u.a.*, Publizistik 64 (2019), 15, 32 (Medienberichterstattung überwiegend nicht ausgewogen); skeptisch zu diesen Befunden *Horz*, Global Media Journal – German Edition 2017/7.

nalen Leitmedien weit überwiegend negativ berichtet; den Rekord negativer Berichterstattung hält mit 98 % just die ARD.[10] Folge dieser medialen Konstellation war allerdings nicht etwa ein Gesinnungswandel unter Migrationskritikern bzw. Trump-Anhängern. Vielmehr wichen diese Personenkreise auf Online-Quellen und soziale Netzwerke aus, wo sich Frustration und Wut umso heftiger und eben auch strafrechtlich relevant die Bahn brachen.[11]

Auf diesen „Bruch im gesellschaftlichen Diskurs"[12] reagierte das NetzDG 2017 mit Repression. In der Entwurfsbegründung heißt es unter Bezugnahme auf ein Monitoring der Löschpraxis, die Selbstverpflichtungen der großen sozialen Netzwerke im Kampf gegen Hasskriminalität und andere strafbare Inhalte hätten zwar zu Verbesserungen geführt; Löschquoten von 90 % (YouTube), 39 % (Facebook) und 1 % (Twitter) reichten aber nicht aus.[13] Die Debattenkultur im Netz sei oft aggressiv, verletzend und nicht selten hasserfüllt. Hiergegen nicht vorzugehen berge eine große Gefahr für das friedliche Zusammenleben einer freien, offenen und demokratischen Gesellschaft. Zur Erreichung dieses übergeordneten Ziels bedürfe es einer Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, um strafbare Inhalte wie etwa Volksverhetzungen und Beleidigungen unverzüglich zu entfernen.[14]

II. Inhalt des NetzDG 2017

Zu diesem Zweck wurden Anbietern großer sozialer Netzwerke bußgeldbewehrte Compliance-Pflichten zum Umgang mit Beschwerden über bestimmte strafbare Inhalte auferlegt. Das NetzDG veränderte die materiellrechtliche Grenze zwischen legalen und illegalen Äußerungen also nicht. Vielmehr setzte es auf einer Meta-Ebene an und nahm Anbieter sozialer

10 *Patterson*, Harvard Kennedy School Working Paper No. RWP17-040, 2017, https://ssrn.com/abstract=3040911, 10.

11 *Haller* (Fn. 9), 144 f.; zum „hostile media effect" *Merten/Dohle*, SCM Studies in Communication and Media 8(2) (2019), 272 ff.

12 *Haller* (Fn. 9), 145.

13 RegE NetzDG (Fn. 5), BT-Drucks. 18/12356, 1 f.

14 RegE NetzDG (Fn. 5), BT-Drucks. 18/12356, 1; BReg, Bericht NetzDG (Fn. 4), 6 („Schutz des demokratischen Diskurses in der Gesellschaft vor den destruktiven Auswirkungen strafbarer Hassrede und entsprechender Einschüchterungen").

Netzwerke unter dem Gesichtspunkt der Rechtstreue (Compliance) prozedural in die Pflicht.[15] Daher auch sein Name: Netzwerk*durchsetzungs*gesetz.

Im Anwendungsbereich des Gesetzes kommen Anlass und gesellschaftspolitisches Ziel des NetzDG deutlich zum Ausdruck. Erfasst sind nämlich nur „soziale Netzwerke", die dazu bestimmt sind, dass Nutzer *beliebige* Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen.[16] Zu diesen themenoffenen Netzwerken zählen neben Facebook, YouTube und Twitter beispielsweise auch Instagram, Reddit, TikTok, Soundcloud und Change.org.[17] Selbst verantwortete journalistisch-redaktionelle Angebote (News-Portale), Dienste zur Individualkommunikation (E-Mail und grdstzl. auch Messenger) sowie Plattformen zur Verbreitung spezifischer Inhalte (z.B. Online-Marktplätze) unterfallen dem NetzDG hingegen nicht, da und soweit sie keine erhebliche Gefahrenquelle für die öffentliche, insbesondere politische Debattenkultur darstellen.[18] Selbiges gilt für soziale Netzwerke, die im Inland weniger als zwei Millionen registrierte Nutzer haben. Dienste von solch geringer kommunikativer Bedeutung müssen lediglich einen inländischen Bevollmächtigten benennen, an den rechtsförmige Zustellungen bewirkt werden können; von den das NetzDG kennzeichnenden Beschwerdemanagement- und Berichtspflichten sind sie befreit.[19]

Im Einklang mit seinem spezifischen Regulierungszweck setzt das NetzDG auch nicht jedes strafrechtliche Verbot der Informationsverbreitung in sozialen Netzwerken durch. Vielmehr sind nach § 1 Abs. 3 NetzDG nur solche Inhalte „rechtswidrig" i.S.d. NetzDG und damit nach Maßgabe der NetzDG-Verfahren zu moderieren, die den Tatbestand von 22 enumerativ aufgezählten Straftatbeständen erfüllen und nicht gerechtfertigt sind. 14 dieser Straftatbestände dienen dem Schutz kollektiver Rechtsgüter, insbesondere des demokratischen Rechtsstaats (§§ 86 ff. StGB) und der öffentlichen Ordnung (§§ 126 ff. StGB); acht Tatbestände betreffen individuelle Rechtsgüter wie die sexuelle Selbstbestimmung (§ 184b StGB), die Ehre (§§ 185 ff. StGB), den persönlichen Lebens- und Geheimbereich (§ 201a

15 Soweit der Inhalt des NetzDG im Folgenden im Präsens dargestellt wird, sind die betreffenden Regelungen im Zuge der Reformen des Jahres 2021 unverändert geblieben.

16 § 1 Abs. 1 S. 1 NetzDG (Hervorh. v. Verf.).

17 *Eifert* (Fn. 2), 3 f.

18 § 1 Abs. 1 S. 2 und 3 NetzDG sowie Bundesamt für Justiz (BfJ), NetzDG-Bußgeldleitlinien, 2018, 3 f.; siehe aber https://netzpolitik.org/2021/bussgeldverfahren-telegram-soll-sich-an-das-netzdg-halten/.

19 Vgl. § 1 Abs. 2 NetzDG sowie BReg, Bericht NetzDG (Fn. 4), 41.

StGB) und die persönliche Freiheit (§ 241 StGB). Insgesamt lässt die Aufzählung des § 1 Abs. 3 NetzDG allerdings keine klare Linie erkennen. So umfasst die Liste nicht die Vorschriften zum Schutz des Ansehens der Bundesrepublik Deutschland und seiner Repräsentanten (Verunglimpfung gem. §§ 90-90b StGB), wohl aber eine Norm zur Gewährleistung der Sicherheit und Zuverlässigkeit des Beweisverkehrs (Fälschung beweiserheblicher Daten, § 269 StGB).[20]

Obwohl die Bedeutung der plattformeigenen Gemeinschaftsstandards und sonstigen privaten Nutzungsbedingungen für den Kampf gegen Hass und Fake News von Anfang an klar zutage lag,[21] traf das NetzDG 2017 hierzu keine Regeln. Seine Compliance-Normen statuierten lediglich einen Mindeststandard zum Umgang mit bestimmten strafbaren Äußerungen. Ob die Anbieter weitergehend auch nicht strafbare oder sonst gesetzwidrige Äußerungen auf vertraglicher Grundlage rechtswirksam beschränken konnten, blieb offen.[22] An dieser Zurückhaltung zeigt sich, dass das NetzDG 2017 noch nicht den Schritt vom Gedanken der Durchsetzung des (analogen) Rechts im Internet hin zur umfassenden Plattformregulierung vollzogen hatte.

Kernstück des NetzDG 2017 bildete vielmehr die in § 3 statuierte Pflicht der Betreiber großer sozialer Netzwerke, ein wirksames und transparentes Verfahren für den Umgang mit Beschwerden über rechtswidrige Inhalte vorzuhalten. Die entsprechenden Meldeprozeduren müssen für die Nutzer leicht erkennbar und bedienbar sowie ständig verfügbar sein. Offensichtlich rechtswidrige Inhalte müssen innerhalb von 24 Stunden nach einer Meldung gelöscht werden, sonstige rechtswidrige Inhalte in der Regel innerhalb von sieben Tagen. Über diese Verfahren mussten Netzwerkanbieter seit 2018 halbjährlich einen deutschsprachigen Bericht mit Angaben u.a. über die Anzahl und die Gründe von Beschwerden, über Verfahrensdauern und Löschquoten veröffentlichen (§ 2 NetzDG 2017).

Diese Compliance-Pflichten wurden gem. § 4 NetzDG 2017 mit Bußgeldern bewehrt. Wer seither ein Beschwerdeverfahren oder einen Transparenzbericht schuldhaft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorhält bzw. veröffentlicht, begeht eine Ordnungswidrigkeit, die mit einer Geldbuße bis zu fünf Millionen Euro geahndet werden

---

20 Vgl. Beschlussempfehlung und Bericht Rechtsausschuss zum NetzDG 2017, BT-Drucks. 18/13013, 19.

21 BMJV (Fn. 3), 1 und 3.

22 BReg, Bericht NetzDG (Fn. 4), 22. Zur Frage, ob eine Beschwerde wegen Verstoßes gegen Gemeinschaftsstandards zugleich als „Beschwerde über rechtswidrige Inhalte" gem. NetzDG zu qualifizieren war vgl. *Eifert* (Fn. 2), 23 ff. m.w.N.

kann.[23] Auch in diesem Zusammenhang offenbart sich der prozedural-systemische Ansatz des NetzDG 2017. Denn ein Bußgeld wird nicht bereits fällig, wenn ein einzelner rechtswidriger Inhalt nicht gelöscht oder sonst vereinzelt gegen die Compliance-Pflichten verstoßen wird, sondern erst, wenn der Anbieter bei der Vorhaltung und Durchführung der NetzDG-Verfahren systemisch versagt, also z.B. gar keinen oder einen dysfunktionalen Meldeprozess bereitstellt.[24]

Mit diesem prozeduralen Meta-Ansatz unterscheidet sich das NetzDG 2017 grundlegend vom französischen „Loi Avia" gegen Hass im Netz. Während das NetzDG vereinzelte Fehlentscheidungen der Plattformbetreiber toleriert, statuierte das französische Gesetz unmittelbar bußgeldbewehrte Löschpflichten im Einzelfall.[25] Die Rechtsdurchsetzung im Einzelfall suchte das NetzDG 2017 durch andere Instrumente mittelbar zu fördern. Erstens erhielten die von schwerwiegenden Persönlichkeitsrechtsverletzungen Betroffenen einen Anspruch auf Auskunft zur Feststellung der Identität des Täters.[26] Zweitens wurden sämtliche Anbieter sozialer Netzwerke unabhängig von ihrem Sitz und ihrer Größe wiederum bußgeldbewehrt dazu verpflichtet, Personen zu benennen, an die Zustellungen in Bußgeld- und Zivilgerichtsverfahren sowie Auskunftsersuchen von Strafverfolgungsbehörden bewirkt werden können.[27]

III. Effekte des NetzDG 2017

1. Unmittelbare

Fragt man nach den Auswirkungen dieser Regelungen, so fällt zunächst auf, dass zum NetzDG 2017 und insbesondere zu den Compliance-Pflichten und Bußgeldvorschriften keine substantiell relevanten Gerichtsent-

23 § 4 NetzDG; BfJ (Fn. 18), 11 ff.

24 Gegenäußerung der Bundesregierung, BT-Drucks. 18/12727, 27; RechtsA NetzDG (Fn. 20), BT-Drucks. 18/13013, 22 (beharrliche Verstöße gegen Compliance-Pflichten); BfJ (Fn. 18), 7.

25 Für grundrechts- und verfassungswidrig erklärt von Conseil Constitutionnel, Décision n° 2020-801 DC du 18 juin 2020; dazu *Heldt*, JuWissBlog Nr. 96/2020 v. 23.6.2020, https://www.juwiss.de/96-2020/.

26 § 14 Abs. 3-5 TMG; RechtsA NetzDG (Fn. 20), BT-Drucks. 18/13013, 23 f.; BGH v. 24.9.2019, VI ZB 39/18, juris Rn. 46 ff. (Geltung für Facebook-Messenger); OLG Frankfurt v. 6.9.2018, 16 W 27/18, juris Rn. 38; OLG Nürnberg v. 17.7.2019, 3 W 1470/19, juris Rn. 44 ff.; KG Berlin v. 11.3.2020, 10 W 13/20, juris.

27 § 5 i.V.m. § 4 Nr. 7 und 8 NetzDG 2017.

scheidungen dokumentiert sind. So ist es bis heute zu keiner endgültigen Klärung der in der Literatur intensiv debattierten Frage gekommen, ob das NetzDG mit dem Grundgesetz und dem Unionsrecht, namentlich der E-Commerce-Richtlinie, in Einklang steht.[28] Die Netzwerkbetreiber leugneten zwar zum Teil die Rechtsverbindlichkeit des Gesetzes und befolgten es nur „freiwillig", haben aber erst im Jahr 2021 ein verwaltungsgerichtliches Verfahren zur Überprüfung seiner Gültigkeit lanciert.[29] Für eine abstrakte Normenkontrolle fand sich weder eine Landesregierung noch ein Viertel der Mitglieder des Bundestages bereit.[30] Zwei Versuche einzelner Netzwerknutzer, das NetzDG über eine verwaltungsgerichtliche Feststellungsklage bzw. Verfassungsbeschwerde zu Fall zu bringen, scheiterten bereits an der fehlenden unmittelbaren Betroffenheit der Kläger, die darauf verwiesen wurden, Löschungen ihrer Beiträge abzuwarten und hiergegen vorzugehen.[31]

Ebenso mager ist der Befund im Hinblick auf die Bußgeldbewehrung des NetzDG 2017.[32] Das Bundesamt für Justiz (BfJ) leitete bis zum 30. Juni 2020 zwar 1.462 Bußgeldverfahren ein, die weitaus meisten hiervon (1.353) aufgrund unmittelbar an das BfJ gerichteter Nutzerbeschwerden über nicht erfolgte Löschungen.[33] Ca. die Hälfte dieser Verfahren war zum genannten Stichtag bereits folgenlos eingestellt, weil der dem BfJ gemeldete Inhalt entweder nicht rechtswidrig i.S.d. NetzDG war oder jedenfalls kein systemisches Versagen des betreffenden Netzwerkbetreibers festgestellt werden konnte. Lediglich ein einziges Verfahren wurde im Juli 2019 mit einem Bußgeldbescheid gegen Facebook in Höhe von zwei Millionen Euro abgeschlossen. Doch auch in diesem, im Oktober 2021 noch anhängigen Bußgeldverfahren geht es nicht um den Vorwurf systemischen Versagens beim Löschen. Gerügt wird vielmehr, dass Facebook sein spezielles

28 Dazu m.w.N. *Eifert* (Fn. 2), 9, 13 ff.; weiterhin verfassungsrechtliche Bedenken bei *Liesching u.a.*, Das NetzDG in der praktischen Anwendung. Eine Teilevaluation des Netzwerkdurchsetzungsgesetzes, 2021, 374 f.; zur Unionsrechtskonformität der §§ 3a, 3b und 4a NetzDG siehe nunmehr VG Köln v. 1.3.2022, 6 L 1277/21, juris (Eilentscheidung).

29 *Liesching u.a.* (Fn. 28), 361 (zu YouTube); siehe nunmehr aber VG Köln v. 1.3.2022, 6 L 1277/21, juris.

30 Art. 93 Abs. 1 Nr. 2 und 2a GG und §§ 76 ff. BVerfGG.

31 VG Köln v. 14.2.2019, 6 K 4318/18, juris; BVerfG v. 23.04.2019, 1 BvR 2314/18, juris.

32 Siehe zum Folgenden BReg, Bericht NetzDG (Fn. 4), 39 f.; *Liesching u.a.* (Fn. 28), 360 (marginale praktische Bedeutung der Bußgeldahndungen des NetzDG).

33 https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/NetzDG/Service/Formulare/Meldung/Formular_node.html.

NetzDG-Meldeformular so versteckte, dass nur wenige Meldungen hierüber erfolgten und entsprechend im Transparenzbericht aufgeführt wurden, während die viel zahlreicheren Moderationsentscheidungen auf der Basis der Gemeinschaftsstandards nicht offengelegt wurden.[34]

Die klassische Strafverfolgung von Hasskriminalität und strafbaren „Fake News" profitierte vom NetzDG ebenfalls nur begrenzt. Zwar stieg die Zahl der Auskunftsersuchen von Strafverfolgungsbehörden auch dank des „Briefkastens", den sämtliche Betreiber sozialer Netzwerke im Inland vorhalten müssen.[35] Unverändert aber liegt die Auskunftsquote gegenüber deutschen Behörden mit ca. 50 % deutlich unter der weltweiten Auskunftsquote und noch viel deutlicher unter den Auskunftsquoten gegenüber US-amerikanischen und britischen Behörden.[36] Hintergrund ist, dass das NetzDG bis heute zwar eine allgemeine Pflicht zur „Reaktion" auf behördliche Anfragen statuiert, nicht aber eine Auskunftspflicht in der Sache.[37] Häufig sind daher förmliche Rechtshilfeersuchen erforderlich, die allerdings sehr schwerfällig und bei Straftatbeständen wie dem öffentlichen Verwenden von NS-Symbolen oder der Volksverhetzung (§§ 86a, 130 StGB) von vornherein aussichtslos sind, wenn das ersuchte Unternehmen seinen Sitz in den USA hat.[38]

2. *Mittelbare*

Diese Beobachtungen rechtfertigen jedoch zunächst nicht den Schluss, dass die Betreiber sozialer Netzwerke der Verbreitung von Hasskriminalität und anderen strafbaren Inhalten tatenlos zusehen. Vielmehr belegen die eigenen und die gem. § 2 NetzDG 2017 erstellten Transparenzberichte von Facebook, YouTube und Twitter, dass zumindest diese drei, für die öffentliche Debatte in Deutschland besonders wichtigen sozialen Netzwerke

34 Vgl. BReg, Bericht NetzDG (Fn. 4), 11 f. (in den vier Halbjahren 2018-2019 lediglich 1.704, 1.048, 1.050 und 4.274 NetzDG-Beschwerden); https://www.bundesjustizamt.de/DE/Presse/Archiv/2019/20190702.html?nn=3449818; *Eifert* (Fn. 2), 50.

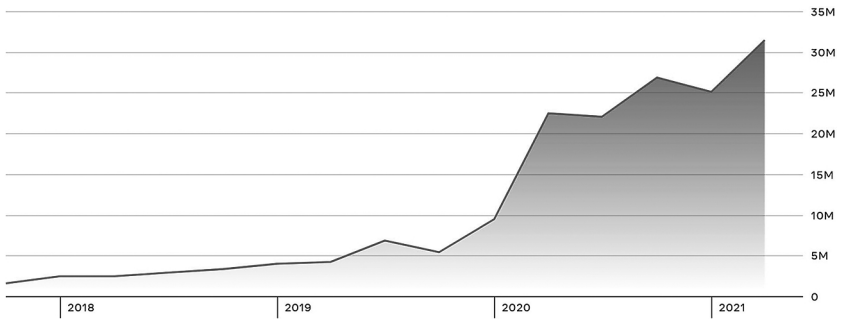
35 § 5 Abs. 2 NetzDG 2017 und RegE NetzDG (Fn. 5), BT-Drucks. 18/12356, 27 („freiwillige[n] unmittelbare[n] Kooperation"); *Eifert* (Fn. 2), 116, 119.

36 *Eifert* (Fn. 2), 117 f.

37 Vgl. § 4 Nr. 8 NetzDG 2021 sowie *Eifert* (Fn. 2), 120.

38 *Eifert* (Fn. 2), 120.

engagiert moderieren.[39] Facebook geht weltweit millionenfach gegen Inhalte vor, die gegen die Gemeinschaftsstandards zu Hassrede verstoßen:[40]



Nach Angaben des Unternehmens sank die Quote von Hassrede-Inhalten von Mitte 2020 bis Mitte 2021 um etwa die Hälfte auf 0,05 %.[41] YouTube und Twitter bearbeiteten allein in Deutschland halbjährlich hunderttausende NetzDG-Beschwerden, und zwar in mehr als 80 % der Fälle innerhalb von 24 Stunden, im Übrigen innerhalb der Regelfrist von sieben Tagen.[42] Zwar zog nur eine relativ geringe Quote von, im Mittel, 28 % der NetzDG-Meldungen eine Löschung nach sich.[43] Hierin wird allerdings kein systemisches Versagen der Netzwerkanbieter gesehen. Vielmehr wird für plausibel erachtet, dass Nutzer viele Inhalte melden, die nicht rechtswidrig i.S.d. NetzDG sind.[44]

Im Hinblick auf die Bedeutung des NetzDG für dieses Verhalten der Netzwerkanbieter ist zu differenzieren. Facebook operiert praktisch ausschließlich auf der Grundlage seiner eigenen Gemeinschaftsstandards; bereits die Meldewege sind hierauf zugeschnitten.[45] YouTube und Twitter halten zwar ein intensiv genutztes NetzDG-Meldetool vor. Prüfung und Entscheidung über diese Meldungen beruhen aber ebenfalls auf den priva-

39 Zur Aussagekraft der Transparenzberichte *Eifert* (Fn. 2), 90 ff.

40 https://transparency.fb.com/data/community-standards-enforcement/hate-speech/facebook/#content-actioned.

41 Ebd.

42 BReg, Bericht NetzDG (Fn. 4), 11 f., 15 (vier Halbjahre 2018-2019, Twitter: 264.818, 256.462, 503.464, 843.527 NetzDG-Beschwerden; YouTube: 214.827, 250.957, 304.425, 277.478).

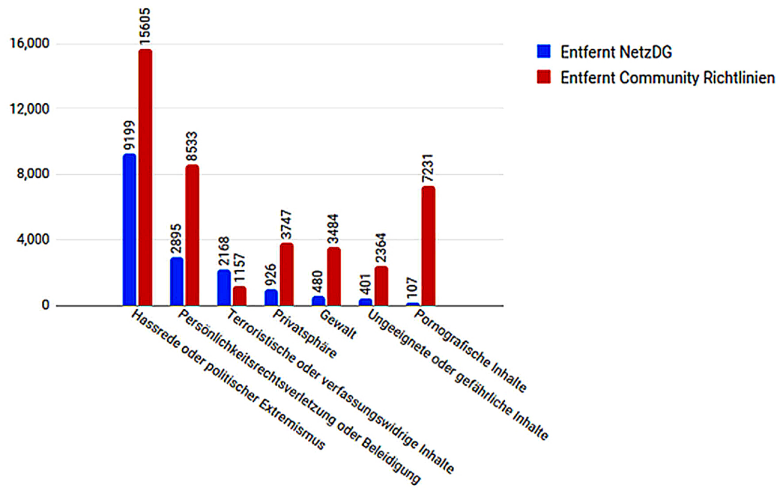
43 BReg, Bericht NetzDG (Fn. 4), 15; Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, BT-Drucks. 19/17741, 15.

44 *Eifert* (Fn. 2), 51.

45 Oben Fn. 34.

ten Nutzungsbedingungen, die stets zuerst geprüft werden.[46] Auf das NetzDG kommt es bei diesem Vorgehen nur noch an, wenn der Inhalt nicht bereits gegen die Netzwerkstandards verstößt. Das ist, wie ein Vergleich der Löschpraxis von YouTube im ersten Halbjahr 2018 mit dem ersten Halbjahr 2021 zeigt, nur noch in einem verschwindend geringen Maße der Fall:

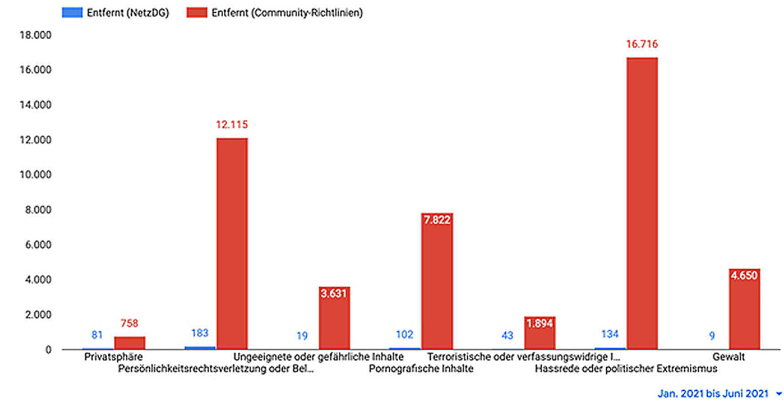
Entfernung wegen eines Community Richtlinien Verstoßes vs. Entfernung wegen NetzDG [47]



46 *Löber/Roßnagel*, MMR 2019, 71 ff.; *Eifert* (Fn. 2), 27; *Liesching u.a.* (Fn. 28), 362.

47 YouTube San Bruno, Entfernungen von Inhalten nach dem Netzwerkdurchsetzungsgesetz, 31.7.2018, Bundesanzeiger.

Entfernung wegen eines Verstoßes gegen die Community-Richtlinien vs. NetzDG 48



Ebenfalls jenseits des NetzDG 2017 liegt der meldeunabhängige, proaktive Einsatz von Technologien zur automatischen Inhaltserkennung und -entfernung. Derartigen Werkzeugen kommt eine immer größere Rolle zu. Bei Facebook und YouTube erfolgen mehr als 90 % aller Moderationsmaßnahmen automatisch.[49]

Der scheinbare Widerspruch zwischen der praktischen Bedeutungslosigkeit der NetzDG-Verfahren und dem hohen Engagement der Netzwerkbetreiber löst sich auf, wenn man davon ausgeht, dass das NetzDG eine Flucht in die AGB befördert hat. „[J]e höher die Anforderungen nach dem NetzDG sind, desto größer ist der Anreiz für die Netzwerkanbieter, die Beschwerden in das weniger stark regulierte System der Beschwerden nach Gemeinschaftsstandards zu lenken".[50] Für diese These spricht aus ökonomischer Sicht, dass die Plattformen auf diesem Wege ihre weltweit einheitlichen Kommunikationsstandards aufrechterhalten und kostenintensive, länderspezifische Versionen vermeiden können. Auch aus juristischer Sicht gibt es Indizien für ein Ausweichen in die AGB. So haben die Netzwerke seit 2017 ihre Hassrede-Regeln deutlich erweitert und – was allerdings näherer Prüfung bedürfte – dabei wohl auch in der Sache ver-

48 Google Ireland, Entfernungen von Inhalten aus Youtube nach dem Netzwerkdurchsetzungsgesetz, 30.7.2021, Bundesanzeiger.

49 *Liesching u.a.* (Fn. 28), 359 f.; Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss), Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes, BT-Drucks. 19/29392, 18.

50 *Eifert* (Fn. 2), 29, 50; *Liesching u.a.* (Fn. 28), 368 (NetzDG-Regeln laufen ins Leere).

schärft.[51] Ferner berufen sich die Diensteanbieter zur Verteidigung gegen Nutzerklagen auf Wiederherstellung von Inhalten, die wegen Verstoßes gegen AGB entfernt wurden, auf das NetzDG, um ihre privaten Regeln vor näherer Überprüfung und ggf. Unwirksamkeitserklärung zu schützen. Einerseits bringen sie vor, das NetzDG etabliere lediglich einen Mindeststandard, und die Gefahr einer NetzDG-Haftung wegen unzureichenden Beschwerdemanagements rechtfertige auch die Löschung nicht strafbarer und sonst äußerungsrechtlich zulässiger Meinungsäußerungen.[52] Andererseits argumentieren sie, dass sich bei gem. § 1 Abs. 3 NetzDG rechtswidrigen Inhalten eine nähere Überprüfung der AGB erübrige, weil der Inhalt auf jeden Fall zu löschen sei.[53] Das NetzDG fungiert mit anderen Worten als Schutzschild für die privaten Netzwerkregeln.

Dass sich NetzDG-Pflichten und AGB auf diese Weise ergänzen, hat einen tieferen, jüngst vom Bundesgerichtshof herausgearbeiteten Grund. Die großen Netzwerkbetreiber und der deutsche (und europäische, s.u.) Gesetzgeber verfolgen nämlich dasselbe Nahziel: Einer Verrohung der Debattenkultur in sozialen Netzwerken soll entgegengewirkt werden.[54] Der Gesetzgeber möchte letztlich das friedliche Zusammenleben in einer freien, offenen und demokratischen Gesellschaft gewährleisten;[55] Facebook und Co. haben ein vitales geschäftliches Interesse, „sowohl für ihre Nutzer als auch für ihre Werbekunden ein attraktives Kommunikations- und Werbeumfeld zu schaffen", in dem möglichst wenige negative oder gar hasserfüllte Äußerungen zirkulieren.[56] Diese Zielkomplementarität macht die Bereitschaft verständlich, mit der sich Big Tech zum Teil sogar vorauseilend an der Entwicklung immer neuer Maßnahmen zur Förderung

51 Zur Neufassung der Facebook-AGB 2018 BGH v. 29.07.2021, III ZR 179/20, juris Rn. 38 – Facebook AGB (keine Abweichung zum Nachteil der Nutzer). Im Juni 2020 strich Facebook den Zusatz "We allow humor and social commentary related to these topics." aus den Hassrede-Regeln; vgl. https://de-de.facebook.com/communitystandards/recentupdates/hate_speech/.

52 OLG Dresden v. 8.8.2018, 4 W 577/18, juris Rn. 21; OLG München v. 17.9.2018, 18 W 1383/18, juris Rn. 37; OLG Stuttgart v. 6.9.2018, 4 W 63/18, juris Rn. 73 ff.; LG Frankenthal v. 8.9.2020, 6 O 238/19, juris Rn. 59 f. (wirtschaftlich nachvollziehbares Interesse); differenzierter BGH v. 29.07.2021, III ZR 179/20, juris Rn. 76-79, 98 – Facebook AGB.

53 OLG Braunschweig v. 5.2.2021, 1 U 9/20, juris Rn. 142; OLG Rostock v. 18.3.2021, 2 U 19/20, juris Rn. 6 ff.

54 BGH v. 29.07.2021, III ZR 179/20, juris Rn. 92 – Facebook AGB unter Verweis auf den RegE NetzDG (Fn. 5), BT-Drs. 18/12356, 13.

55 Oben Fn. 14.

56 BGH v. 29.07.2021, III ZR 179/20, juris Rn. 92 – Facebook AGB.

zuverlässiger und Vermeidung irreführender/gefährlicher Informationen beteiligt.[57] Und sie erklärt, weshalb die „Sicherheit" der Online-Kommunikation ein zentraler Topos sowohl der Facebook-Gemeinschaftsstandards als auch des Vorschlags für einen Digital Services Act (DSA) ist.[58]

Die Zusammenhänge zwischen dem NetzDG und dem Moderationsverhalten der Plattformbetreiber sind auch für die Beurteilung des sog. Overblocking-Problems relevant. Die Behauptung, das NetzDG werde die Diensteanbieter zur Entfernung auch legaler Äußerungen treiben, bildete seit jeher das Hauptargument der Kritiker des Gesetzes. Ob diese Befürchtung berechtigt ist und sich bewahrheitet hat, ist umstritten. Dagegen spricht, dass das NetzDG nur systemisches Versagen sanktioniert, die Löschquote bei NetzDG-Meldungen relativ gering ist und schwierige Grenzfälle seit Januar 2020 von einer Einrichtung regulierter Selbstregulierung entschieden werden.[59] Die Gegenmeinung verweist auf die dargestellte „Flucht" in verschärfte AGB, den hohen Anteil von 24-Stunden-Entfernungen und erfolgreiche Put-back-Klagen vor Zivilgerichten.[60] Insgesamt krankt die Diskussion allerdings an der Unklarheit des Begriffs „Overblocking". Liegt ein solches Verhalten bereits vor, wenn Äußerungen gelöscht werden, die weder gegen Gesetze noch gegen absolute (Persönlichkeits-)Rechte Dritter verstoßen, oder erst dann, wenn eine Moderati-

---

57 Zu Hassrede vgl. BMJV (Fn. 3), 1 („Die in der Task Force Mitwirkenden werden gemeinsam von der Überzeugung geleitet, dass Hassbotschaften in sozialen Medien keinen Platz haben."). Zu „Fake News" vgl. https://www.facebook.com/notes/facebook-security/making-facebook-safe-and-secure-for-authentic-communication/10154362152760766/; Schmid/Braam/Mischke, MMR 2020, 19, 23 m.w.N. Zur Bereitstellung zuverlässiger Informationen im Zuge der COVID-19-Pandemie vgl. https://www.washingtonpost.com/politics/2021/06/03/alleged-fauci-smoking-gun-emails/ (E-Mail von Marc Zuckerberg an Anthony Fauci v. 15.3.2020).

58 Vgl. Präambel Facebook-Gemeinschaftsstandards, https://transparency.fb.com/de-de/policies/community-standards/?from=https%3A%2F%2Fde-de.facebook.com%2Fcommunitystandards%2F („Das Facebook-Unternehmen weiß, wie wichtig es ist, dass Facebook ein Ort ist und bleibt, an dem die Menschen sicher und unbesorgt miteinander kommunizieren können.") mit Art. 1 Abs. 2 Buchst. b Vorschlag für eine Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG, COM/2020/825 („Festlegung einheitlicher Regeln für ein sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld, in dem die in der Charta verankerten Grundrechte wirksam geschützt sind.").

59 Siehe https://www.fsm.de/de/netzdg; BReg, Bericht NetzDG (Fn. 4), 21; *Eifert* (Fn. 2), 53 f.

60 *Liesching u.a.* (Fn. 28), 89 ff., 363 ff. m.w.N.; Wissenschaftliche Dienste des Deutschen Bundestags (Fn. 2), 6; VG Köln v. 1.3.2022, 6 L 1277/21, juris Rn. 269-277.

onsmaßnahme auch nicht von weitergehenden, aber immer noch wirksamen Nutzungsbedingungen gedeckt ist? Und selbst wenn man den Begriff des Overblockings richtigerweise auf Maßnahmen gegen sowohl gesetz- als auch vertragskonforme Inhalte beschränkt, ist auch nach der jüngsten BGH-Entscheidung zu den Facebook-AGB offen, wo genau der privatautonome Gestaltungsspielraum großer Netzwerkbetreiber endet und der Bereich willkürlicher und daher unzulässiger Löschungen beginnt.[61]

IV. NetzDG 2021: Von der Durchsetzung des Strafrechts zur Plattformregulierung

In seinem Urteil deutlich herausgearbeitet hat der BGH hingegen, in welch unangenehme Zwickmühle die Anbieter sozialer Netzwerke seit 2017 geraten sind. Einerseits müssen sie ihre NetzDG-Pflichten erfüllen und aus geschäftlichen Gründen für ein positives Kommunikationsklima sorgen, andererseits waren sie zahlreichen Klagen auf Wiederherstellung gelöschter Posts und Rückgängigmachung von Accountsperrungen ausgesetzt, von denen nicht wenige erfolgreich waren.[62]

In diesem Spannungsfeld entspann sich auch die politische Debatte um die Aufhebung oder Reform des NetzDG 2017, die unmittelbar nach seinem Inkrafttreten am 1.10.2017 mit dem Zusammentritt des 19. Bundestages einsetzte. Während die einen in den „sogenannten" sozialen Medien eine weiter „zunehmende Verrohung der Kommunikation" beobachteten, die den politischen Diskurs in der demokratischen und pluralistischen Gesellschaftsordnung in Frage stelle, riefen die anderen „Zensur"![63] Aus dieser hitzigen Debatte gingen zum Ende der Legislaturperiode zwei Gesetze hervor, nämlich das Gesetz zur Bekämpfung des Rechtsextremismus

61 Vgl. BVerfG v. 22. Mai 2019, 1 BvQ 42/19, juris Rn. 16 – Der III. Weg; BGH v. 29.07.2021, III ZR 179/20, juris Rn. 81, 97 – Facebook AGB; RechtsA NetzDGÄG (Fn. 49), BT-Drucks. 19/29392, 12 f.

62 BGH v. 29.07.2021, III ZR 179/20, juris Rn. 27 ff., 77 – Facebook AGB („Dilemma").

63 Siehe einerseits RegE HasskriminalitätsG (Fn. 43), BT-Drucks. 19/17741, 1 f., 15; andererseits Entwurf eines Gesetzes zur Aufhebung des Netzwerkdurchsetzungsgesetzes v. 20.11.2017, BT-Drucks. 19/81 (AfD); Entwurf eines Gesetzes zur Stärkung der Bürgerrechte v. 8.12.2017, BT-Drucks. 19/204 (FDP); Entwurf eines Gesetzes zur Teilaufhebung des Netzwerkdurchsetzungsgesetzes v. 11.12.2017, BT-Drucks. 19/218 (DIE LINKE); ferner den Antrag v. 22.11.2018, Netzwerkdurchsetzungsgesetz weiterentwickeln, BT-Drucks. 19/5959 (BÜNDNIS 90/DIE GRÜNEN).

und der Hasskriminalität v. 30.3.2021[64] und das Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes v. 3.6.2021.[65] Die hiermit herbeigeführten Änderungen des NetzDG 2017 kommen beiden Bedenken entgegen.

Einerseits werden die großen sozialen Netzwerke noch stärker als bisher in den Kampf gegen Hass- und sonstige Kommunikationskriminalität eingebunden. Der Katalog der NetzDG-Straftaten wurde um das Delikt der Verunglimpfung des Andenkens Verstorbener erweitert.[66] Durch eine Legaldefinition der „Beschwerde über einen rechtswidrigen Inhalt" soll klargestellt werden, dass im Zweifel jede Nutzermeldung unabhängig vom konkreten Meldeweg als NetzDG-Beschwerde zu betrachten und abzuwickeln ist.[67] Zum diesbezüglichen Beschwerdemanagement tritt eine wiederum bußgeldbewehrte Meldepflicht für Inhalte von besonderem Gefährdungspotential für das demokratische System und die öffentliche Ordnung. Wird einem Netzwerkbetreiber z.B. ein volksverhetzender Inhalt gemeldet, ist dieser nebst weiteren, zur Identifikation des Täters geeigneten Informationen unverzüglich dem Bundeskriminalamt zu übermitteln, damit von dort aus die Strafverfolgung veranlasst werden kann.[68] Welch hohe Erwartungen der Gesetzgeber an dieses Meldeverfahren knüpft, wird daran ersichtlich, dass extra eine Rechtsgrundlage zur Ermöglichung eines „allgemeinen Austauschs" zwischen Netzwerkbetreibern und Staatsanwaltschaften geschaffen wurde.[69]

Andererseits finden nunmehr auch die Bedenken gegen ein unberechtigtes Overblocking Niederschlag im NetzDG. Das NetzDG 2017 hatte das Interesse an der Gewährleistung rechtsgleicher Meinungs- und Informationsfreiheit in sozialen Netzwerken noch völlig ausgeblendet.[70] Die

---

64 BGBl. I 2021, 441 (Hasskriminalitätsgesetz).

65 BGBl. I 2021, 1436 (NetzDGÄG); zum gestaffelten Inkrafttreten der Änderungen *Cornils*, NJW 2021, 2465, 2471.

66 § 189 StGB und RegE HasskriminalitätsG (Fn. 43), BT-Drucks. 19/17741, 18 unter Hinweis auf die Ermordung des Kasseler Regierungspräsidenten Lübcke 2019.

67 § 1 Abs. 4 NetzDG 2021 und dazu RegE HasskriminalitätsG (Fn. 43), BT-Drucks. 19/17741, 42; *Cornils*, NJW 2021, 2465, 2466 f.

68 §§ 3a, 4 Abs. 1 Nr. 6a NetzDG 2021; RegE HasskriminalitätsG (Fn. 43), BT-Drucks. 19/17741, 1, 45; RechtsA NetzDGÄG (Fn. 49), BT-Drucks. 19/29392, 14. Nach Auffassung des VG Köln ist § 3a NetzDG wegen Verstoßes gegen die E-Commerce-Richtlinie unanwendbar; VG Köln v. 1.3.2022, 6 L 1277/21, juris Rn. 148 ff.

69 § 3a Abs. 8 NetzDG 2021 und RechtsA NetzDGÄG (Fn. 49), BT-Drucks. 19/29392, 15.

70 *Peukert*, MMR 2018, 572 f.; ferner OLG Köln v. 11.1.2019, 15 W 59/18, juris Rn. 18 ff.; KG Berlin v. 6.3.2019, 10 W 192/18, juris (§ 5 Abs. 1 NetzDG 2017 auf die Zustellung von Put-back-Klagen nicht entsprechend anwendbar).

Zivilgerichte und das Bundesverfassungsgericht gingen hingegen seit dem Frühjahr 2018 einhellig davon aus, dass Nutzer einen Anspruch gegen große soziale Netzwerke auf Unterlassung einer nicht gerechtfertigten Löschung eines Posts oder einer Accountsperre haben können.[71] Strukturierte Online-Verfahren standen für diese Put-back-Ansprüche aber nicht zur Verfügung. Vielmehr mussten die Betroffenen den traditionellen Rechtsweg zu den Gerichten beschreiten, was aufgrund des hiermit verbundenen Zeit- und Kostenaufwands nur vereinzelt geschah. Folge war ein erhebliches prozedurales Ungleichgewicht: Während das NetzDG 2017 Löschungsverfahren digitalisierte und auf 24 Stunden verkürzte, blieben die Gegenrechte in der Trägheit analogen Gerichtshandelns gefangen.[72]

Diese systematische prozedurale Benachteiligung der Meinungs- und Informationsfreiheit wird durch das Gegenvorstellungsverfahren des § 3b NetzDG 2021 behoben. Die Vorschrift verpflichtet die Netzwerkbetreiber zur Vorhaltung eines wirksamen und transparenten Verfahrens, in dem Nutzer eine „unverzügliche" Überprüfung von Löschungsentscheidungen herbeiführen können.[73] Dies gilt nicht nur bei Maßnahmen aufgrund von NetzDG-Beschwerden, sondern auch für Entfernungen oder Sperrungen auf der Grundlage von Nutzungsbedingungen und sogar für automatisiert erfolgende, proaktive Moderationsentscheidungen.[74]

Damit wandelt sich der Charakter des NetzDG grundlegend. Aus einem Regelwerk mit engem Fokus auf die Durchsetzung des Strafrechts in Online-Netzwerken wurde ein Plattformregulierungsgesetz, das sowohl Löschgebote (Strafrecht) als auch Löschverbote (Meinungsfreiheit) prozeduralisiert. Die Compliance- und Transparenzpflichten des NetzDG 2021 gelten sowohl für Beschwerden über strafrechtswidrige Inhalte als auch

71 Zuerst LG Frankfurt am Main v. 14.05.2018, 2-03 O 182/18, juris; ferner BVerfG v. 22. Mai 2019, 1 BvQ 42/19, juris Rn. 16 – Der III. Weg; zuletzt BGH v. 29.07.2021, III ZR 179/20, juris Rn. 27 ff. m.w.N. – Facebook AGB.

72 Vgl. *Peukert*, MMR 2018, 572 ff. sowie die „Initiative für Meinungsfreiheit im Netz", https://meinungsfreiheit.steinhoefel.de/ueber/.

73 *Cornils*, NJW 2021, 2465, 2468 (prozeduraler Befassungs- und Bescheidungsanspruch); vgl. auch VG Köln v. 1.3.2022, 6 L 1277/21, juris Rn. 238 ff. (§ 3b NetzDG mit E-Commerce-Richtlinie und Art. 16 GRCharta vereinbar). Im Ergebnis ebenso auf Grundlage einer grundrechtskonformen Anwendung des allgemeinen Vertragsrechts und unter Verweis auf § 3b NetzDG BGH v. 29.07.2021, III ZR 179/20, juris Rn. 83 ff. – Facebook AGB („Grundrechtsschutz durch Verfahren"); ferner § 14 UrhDaG (internes Beschwerdeverfahren bei urheberrechtlichen Blockierungen).

74 § 3b Abs. 3 S. 1 NetzDG 2021 sowie RechtsA NetzDGÄG (Fn. 49), BT-Drucks. 19/29392, 16; *Cornils*, NJW 2021, 2465, 2468.

für gegenläufige Beschwerden über ungerechtfertigte Entfernungen.[75] Sowohl systematisches Underblocking als auch systematisches Overblocking lösen die verwaltungs- und ordnungswidrigkeitsrechtlichen Sanktionen des Gesetzes aus.[76] An den inländischen Bevollmächtigten der US-amerikanischen und chinesischen Netzwerkbetreiber können nicht nur Zustellungen wegen der Verbreitung rechtswidriger Inhalte bewirkt werden, sondern auch „wegen der unbegründeten Annahme der Verbreitung rechtswidriger Inhalte, insbesondere in Fällen, in denen die Wiederherstellung entfernter oder gesperrter Inhalte begehrt wird".[77] Schließlich hat auch der neue Anspruch von Forschern auf Auskunft über Inhalteerkennungstechnologien sowie über gemeldete und gelöschte Inhalte den umfassenden Zweck, „Art, Umfang, Ursachen und Wirkungsweisen öffentlicher Kommunikation in sozialen Netzwerken und den Umgang der Anbieter hiermit" zu erhellen.[78]

V. Ausblick: Vom NetzDG zum Digital Services Act

Damit ist das NetzDG seinem Ruf als „Pionierleistung der Regulierung der großen sozialen Netzwerke mit internationalem Vorbildcharakter" erneut gerecht geworden.[79] Das ursprüngliche NetzDG 2017 war innovativ in seiner Umsetzung analoger Strafrechtsnormen in die Welt sozialer Netzwerke. Die Verpflichtung der Netzwerkanbieter zur Etablierung wirksamer Verfahren zur Meldung und ggf. Löschung strafrechtlich relevanter Äußerungen konkretisierte die mittelbare Haftung der Betreiber („Compliance") und löste das klassische Quantitätsproblem der Online-Inhalteregulierung:[80] Keine Staatsanwaltschaft kann hunderttausende Anzeigen erledigen, schon gar nicht binnen 24 Stunden. Die Innovationsleistung des NetzDG 2021 bestand darin, auch die Gegenrechte auf rechtsgleiche Meinungs- und Informationsfreiheit in taugliche Online-Prozeduren übersetzt zu haben. Konzeptionell wurde damit der Schritt von der Durchsetzung

75 Vgl. §§ 3b Abs. 1 S. 1 Hs. 1 (sowohl der Beschwerdeführer als auch der Nutzer, für den der beanstandete Inhalt gespeichert wurde, können ein Gegenvorstellungsverfahren in Gang setzen), § 2 Abs. 2 Nr. 11 und 12 NetzDG 2021.

76 Vgl. § 4 Abs. 1 Nr. 2 und 3 i.V.m. § 3b NetzDG 2021.

77 § 5 Abs. 1 S. 2 NetzDG 2021.

78 § 5a Abs. 3 NetzDG 2021; RechtsA NetzDGÄG (Fn. 49), BT-Drucks. 19/29392, 18 ff.

79 Oben Fn. 2 sowie *Cornils*, NJW 2021, 2465, 2471.

80 Dazu *Post*, 17 Berkeley Tech. L.J. 1365, 1385 (2002).

des (analogen) Rechts im Internet hin zur genuin digitalen Plattform- und Kommunikationsregulierung vollzogen. Soziale Netzwerke werden nicht mehr von außen und einseitig als Problem bzw. Gefahr wahrgenommen, sondern auch in ihrer ermöglichenden Funktion für die individuelle und gesamtgesellschaftliche Meinungsbildung.[81] Erst hiermit wurde ein Netzwerk~~durchsetzungs~~gesetz geschaffen, das die erforderliche Balance zwischen Meinungsfreiheit und allgemeinen Gesetzen wahrt.[82]

Die Halbwertszeit des reformierten NetzDG könnte jedoch kurz sein. Denn mit dem DSA hat die Europäische Kommission am 15.12.2020 einen Rechtsakt vorgeschlagen, der das NetzDG 2021 vollständig verdrängen könnte. Wie das NetzDG soll auch der DSA für ein „sicheres, vorhersehbares und vertrauenswürdiges Online-Umfeld" sorgen, „in dem die in der Charta verankerten Grundrechte wirksam geschützt sind".[83] Um die Verbreitung „illegaler Inhalte" einschließlich „illegaler Hassrede" zu minimieren, werden soziale Netzwerke („Online-Plattformen") zahlreichen Sorgfaltspflichten unterworfen, u.a. zur Einrichtung von Melde- und Abhilfeverfahren sowie zur Veröffentlichung von Transparenzberichten.[84] Zugleich müssen sie ein internes Beschwerdemanagementsystem vorhalten, das ggf. zur Rückgängigmachung nicht gerechtfertigter Moderationsmaßnahmen führt.[85] Zwar enthält der Kommissionsvorschlag keine ausdrückliche Regelung zum Verhältnis zwischen dem DSA und dem Recht der Mitgliedstaaten.[86] Es ist aber das „Hauptziel" des Vorschlags, einen Beitrag zum reibungslosen Funktionieren des Binnenmarkts für Online-Vermittlungsdienste zu leisten.[87] Und zu den mitgliedstaatlichen Gesetzen, die zur Fragmentierung des Binnenmarkts für Onlinedienste beitragen, zählt die Kommission zuvorderst das NetzDG.[88]

Würde der DSA an die Stelle des NetzDG treten, hätte der deutsche Gesetzgeber zum dritten Mal einen wichtigen Beitrag zur Rechtsentwicklung geleistet, diesmal in Gestalt eines Impulses zur Europäisierung der

81 Hierzu EGMR v. 18.12.2012, Nr. 3111/10, Ahmet Yıldırım gegen Türkei, §§ 48-54; EGMR v. 13.6.2020, Nr. 12468/15 u.a., OOO Flavus u.a. gegen Russland, § 37.

82 Vgl. hierzu im Kontext der Urheberrechtsdurchsetzung auf Sharing-Plattformen Schlussanträge GA Saugmandsgaard Øe v. 15.7.2021, Rs. C-401/19, Republik Polen gegen Europäisches Parlament, Rat der Europäischen Union, Rn. 70 ff.

83 Art. 1 Abs. 2 Buchst. b DSA (Fn. 58).

84 Siehe ErwGrd. 12 sowie Art. 2 Buchst. g und h, 14 DSA (Fn. 58).

85 Vgl. Art. 17 Abs. 3 DSA (Fn. 58) (Wiederherstellungspflicht).

86 Anders Art. 1 Abs. 5 Vorschlag für ein Gesetz über digitale Märkte (Digital Markets Act, DMA), COM/2020/842.

87 COM/2020/825 (Fn. 58), 6; Art. 1 Abs. 2 Buchst. a DSA (Fn. 58).

88 DSA Impact Assessment Report, SWD(2020) 348 final PART 2/2, 117 ff., 124 f.

Plattformregulierung. Mit der Verlagerung auf die Ebene des Unionsrechts hätte das NetzDG seine Vorbildfunktion erfüllt und sich damit selbst überflüssig gemacht.

Der Kommissionsentwurf eines Digital Services Act – Regelungsinhalte, Regelungsansatz, Leerstellen und Konfliktpotential

Johannes Buchheim

I. Einführung: Europäische Antwort auf systemische Risiken digitaler Vermittlungsdienste

Die in diesem Sammelband erörterten Herausforderungen, vor die digitale Technologien und Dienste, insbesondere digitale Äußerungsplattformen, demokratische Öffentlichkeiten stellen, sind nicht ohne regulatorische Antwort geblieben. Dabei scheint sich in den letzten Jahren ein Konsens gebildet zu haben, dass der eher deregulative Ansatz der frühen Digital-Ära[1] bestimmte Gefahren digitaler Vermittlungsdienste strukturell nicht erfassen kann.[2] So sind etwa die jedermann verfügbare Möglichkeit, mit gänzlich ungefilterten und unedierten Äußerungen ein Millionenpublikum zu erreichen,[3] oder die Tendenzen zu einer fortwährenden Individualisierung und Spezifizierung von Medienerlebnissen und Informationsangeboten[4] Phänomene, die gerade durch digitale Plattformen und deren Geschäftsmodell begründet werden. Diese spezifischen Gefahren liegen nicht in einzelnen Äußerungen und Inhalten begründet, sondern ergeben

1 S. etwa Art. 12 bis 15 Richtlinie 2000/31/EG (e-Commerce-Richtlinie) oder U.S. Code, Titel 47, Section 230 (eingeführt durch den Communications Decency Act 1996); zur deregulativen Tendenz der „Gründerjahre" Eifert, NJW 2017, S. 1450 (1450); für einen Überblick Wagner, GRUR 2020, S. 329.

2 Ebenso Wagner, GRUR 2020, S. 329 (333): „Die Schlüsselstellung der Plattformen hat indessen dazu geführt, dass sie zunehmend Objekte staatlicher Regulierungsanstrengungen wurden."; s. näher Spindler, Funktion und Verantwortung von Plattformen als Informationsintermediären, in diesem Band, S. 67 (68 ff.); Schiff, Informationsintermediäre, 2021.

3 Zu diesem Problem Bimber/Zuniga, new media & society 22 (2020), S. 700.

4 S. etwa Ritzi, Politische Öffentlichkeit zwischen Vielfalt und Fragmentierung, in: Hofmann u.a. (Hrsg.), Politik in der digitalen Gesellschaft, 2019, S. 61 (73 m.w.N.); differenziert Thiel, Der digitale Strukturwandel von Öffentlichkeit, in diesem Band, S. 33 (44 f.); Kelber/Leopold, Personalisierung durch Profiling, Scoring, Microtargeting und mögliche Folgen für die Demokratie, in diesem Band, S. 141 (155 ff.).

sich aus deren aggregierten Wirkungen und der Art der Inhaltsverbreitung durch Plattformdienste. Dementsprechend braucht es regulatorische Antworten, die nicht nur individuell bei einzelnen Inhalten, sondern systemisch bei den Diensteanbietern ansetzen, die eben diese neuen Möglichkeiten schaffen.[5] Nach ersten mitgliedstaatlichen Versuchen in diese Richtung, etwa in Gestalt des deutschen Netzwerkdurchsetzungsgesetzes (NetzDG), hat nun die europäische Kommission in Umsetzung ihrer Digitalstrategie[6] durch die Entwürfe eines Digital Services Act[7] (DSA-E) und eines Digital Markets Act[8] wieder das Regulierungs-Zepter übernommen. Während der im Weiteren nicht beleuchtete DMA-E die wettbewerbsrechtliche Frage betrifft, wie größere Plattformen ihre erhebliche *wirtschaftliche Marktmacht* einsetzen dürfen, widmet sich der hier gegenständliche DSA-E dem *Schutz eher ideeller Interessen* demokratischer Öffentlichkeiten, die durch die Tätigkeit digitaler Vermittlungsdienste berührt sein können.[9]

II. Grobüberblick

Vor diesem Hintergrund regelt zunächst Kapitel II des Entwurfs (Art. 3 bis 9) die Haftung der Anbieter digitaler Vermittlungsdienste für rechtswidrige Inhalte, die Nutzerinnen mithilfe dieser Dienste generieren, übermitteln oder speichern. Das Haftungsmodell der e-Commerce-Richtlinie wird hier weitgehend unverändert fortgeführt.[10]

---

5 So etwa der Regierungsfraktionsentwurf des NetzDG, BTDrucks 18/12356, S. 2: „Verantwortung, der sie gerecht werden müssen"; ähnlich Eifert, NJW 2017, S. 1450 (1451); s. auch Djeffal, Soziale Medien und Kuratierung von Inhalten, in diesem Band, S. 169 (178 ff.).

6 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Eine europäische Datenstrategie, 19.2.2020, COM/2020/66 final.

7 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, 15.12.2020, COM(2020) 825 final.

8 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte), 15.12.2020, COM(2020) 842 final.

9 S. etwa EG 53 („ordnungspolitische Bedenken"); Belange in EG 56 f.; Vorschlag (Fn. 8), S. 2 f., 14; einen Fokus des DSA-E auf nicht-wirtschaftlichen Interessen sehen auch Busch/Mak, EuCML 2021, S. 109 (109).

10 So auch die Bewertung bei Härting/Adamek, CR 2021, S. 165 (165); Berberich/Seip, GRUR-Prax 2021, S. 4 (4 f.); ausführlicher Spindler, GRUR 2021, S. 545 (548 ff.).

Kapitel III des Entwurfs (Art. 10 bis 37) normiert demgegenüber neue allgemeine Pflichten digitaler Vermittlungsdienste, insbesondere von ihnen einzurichtende Verfahren und Transparenzpflichten. Dabei differenziert der Entwurf zwischen verschiedenen Dienstearten. Abschnitt 1 (Art. 10 bis 13) schafft neue Pflichten für alle Anbieter von Vermittlungsdiensten, insbesondere zur AGB-mäßigen Regelung der Inhaltsmoderation (Art. 12), zu jährlichen Berichten über die Moderationspraxis (Art. 13) und zur Benennung von Kontaktstellen bzw. Vertretern innerhalb der EU.

Abschnitt 2 (Art. 14 f.) normiert besondere Pflichten von Hosting-Anbietern. Kernstück dieser Vorgaben ist die verpflichtende Schaffung eines der Allgemeinheit offenstehenden, nutzerfreundlichen Meldesystems für Nutzerinhalte, an denen Anstoß genommen wird. Die auf eine Meldung hin getroffenen Entscheidungen der Anbieter sind zu begründen und der Öffentlichkeit anonymisiert zugänglich zu machen (Art. 15).

Abschnitt 3 (Art. 16 bis 24) regelt zusätzliche, darauf aufbauende Verpflichtungen mittlerer und großer Online*plattformen*, also solcher Hosting-Anbieter, die die bei ihnen gespeicherte Inhalte *öffentlich sichtbar* machen. Hervorzuheben ist insoweit die Pflicht zur Schaffung benutzerfreundlicher Beschwerdesysteme, die eine leicht verfügbare Einspruchsmöglichkeit gegen von Plattformen vorgenommene Sperrungen oder Löschungen individueller Nutzerinhalte schaffen (Art. 17).

Abschnitt 4 (Art. 25 bis 33) widmet sich den darüber noch hinausgehenden Pflichten „sehr großer Online-Plattformen" (*very large online platforms*; VLOP) mit mehr als 45 Millionen regelmäßigen Nutzerinnen in der EU. Diese sollen fortan mit Blick auf ihren systemischen Einfluss auf Öffentlichkeit, Informationsangebot und politische Systeme in den Mitgliedstaaten die von ihnen ausgehenden Systemrisiken regelmäßig evaluieren (Art. 26), geeignete Gegenmaßnahmen beschließen (Art. 27) und darüber Rechenschaft abgeben (Art. 33). Abschnitt 5 des Kapitels (Art. 34 bis 37) betrifft schließlich neue Instrumente der Selbstregulierung wie Verhaltenskodizes.

Kapitel IV des DSA-E (Art. 38 bis 70) widmet sich dem auf diese Vorgaben bezogenen behördlichen Aufsichts- und Durchsetzungsregime. Abschnitt 1 (Art. 38 bis 46) sieht die Schaffung mit Unabhängigkeit ausgestatteter Digitale-Dienste-Koordinatoren (Art. 39) in den einzelnen Mitgliedstaaten vor. Diese sollen mittels umfassender Befugnisse (Art. 41) die Befolgung der Vorgaben des DSA überwachen und sich untereinander abstimmen (Art. 45). Abschnitt 2 (Art. 47 bis 49) schafft nach dem Vorbild der DS-GVO ein Europäisches Gremium für Digitale Dienste zur formalisierten Koordination der DSA-bezogenen behördlichen Aufsichtstätigkeit. Abschnitt 3 (Art. 50 bis 66) regelt besondere Befugnisse und Strukturen im

Bereich der Aufsicht über VLOP, wobei hier der Kommission eigene Untersuchungs- und Entscheidungsbefugnisse (Art. 51 ff.) zugewiesen werden. Abschnitte 4 und 5 (Art. 67 bis 70) betreffen schließlich die Einrichtung eines wirksamen Informationssystems zwischen den Aufsichtsbehörden durch die Kommission und ermächtigt diese zu bestimmten nach dem DSA-E zu erlassenden delegierten Rechtsakten (u.a. zur Methode der Ermittlung der regelmäßigen Nutzerzahl bestimmter Dienste).

III. Kernpunkte und Regulierungsansatz des Entwurfs

1. Fortschreibung bestehender Haftungsprivilegierungen

Kapitel I des DSA-E übernimmt die geltenden Haftungsprivilegierungen digitaler Intermediäre aus Art. 13 bis 15 e-Commerce-Richtlinie und hebt sie in den Rang unmittelbar anwendbaren europäischen Rechts (Art. 288 II AEUV). Die mitgliedstaatlichen Regelungen in Umsetzung dieser Privilegierungen, wie sie aktuell unter Geltung der e-Commerce-Richtlinie bestehen, sollen so vereinheitlicht werden.[11] Allerdings handelt es sich trotz der Rechtsform der Verordnung nicht um eine echte Harmonisierung des Haftungsrechts für digitale Dienste. Denn der DSA-E enthält weiterhin nur Privilegierungstatbestände, setzt also eine Haftung positiv begründende mitgliedstaatliche Normen voraus. Soweit diese fehlen, unterschiedlich zugeschnitten sind, oder bewusst Lücken lassen und eigene Steuerungsziele verfolgen, ändert der DSA-E daher nichts an der unionsweiten Vielgestaltigkeit. Haftungstatbestände und Haftungsfolgen für digitale Inhalte bleiben damit Sache mitgliedstaatlicher Gestaltung. Diese zurückhaltende Harmonisierung ist unter theoretischem Aspekt zu begrüßen. Sie beachtet, dass Maßstäbe und Grenzen für Online-Inhalte und Äußerungen – und damit auch das Haftungsrecht –[12] wegen ihrer besonderen Nähe zum politischen Prozess und ihrer Prägungskraft für die demokratische Öffentlichkeit durch die Mitgliedstaaten bestimmt werden sollten.[13] Denn dort finden demokratische Öffentlichkeit und politische Prozesse nach wie vor

11 Zur Harmonisierungsabsicht s. EG 2, 4, 6; näher Grünwald/Nüßing, MMR 2021, 283, 286 f.

12 Ausführlich zu Rechtsgestaltung und Steuerung durch Haftungsrecht Wagner, AcP 206 (2006), S. 352 (451 ff.).

13 Zu den Problemen einer Entkopplung der Inhaltsmoderation von den politischen Prozessen und Öffentlichkeiten s. Abiri, Brigham Young Univ. L. Rev. 47 (2022), S. 757 (insb. 797 ff.).

hauptsächlich statt. Die Vollharmonisierung weiter Teile des Datenschutzrechts durch die DS-GVO[14] ist gerade auch deshalb kritisch zu sehen. Sie zieht umfassende und unionsweit einheitliche materielle Grenzen für das Handeln in der Informationsgesellschaft und bestimmt damit maßgeblich unser Kommunikationshandeln. Diese Uniformität des datenschutzrechtlichen Persönlichkeitsschutzes passt nicht zur Vielgestaltigkeit der politischen und äußerungsverfassungsrechtlichen Kulturen der Mitgliedstaaten.

Die Zurückhaltung bei der Harmonisierung des Haftungsregimes für einzelne Online-Inhalte passt auch zum eingangs skizzierten Ziel des DSA-E. Dieser soll die spezifischen Gefahren für demokratische Öffentlichkeiten angehen, die von digitalen Vermittlungsdiensten ausgehen können. Diese besonderen Herausforderungen spielen nicht auf Ebene einzelner Inhalte, sondern ergeben sich aus deren Aggregierung und den neuen Vervielfältigungs- und (Missbrauchs-)Möglichkeiten, die Vermittlungsdienste eröffnen. Es ist daher konsequent, dass der DSA-E bei den Pflichten, die an die spezifische Tätigkeit der Vermittlungsdienste und deren besondere Gefahren anknüpfen, durchaus zum Mittel der Vollharmonisierung greift und neue Verfahren, Instrumente und Durchsetzungsmittel unmittelbar unionsrechtlich festlegt.[15]

Auch die Konturen der im DSA-E vorgesehenen Haftungsprivilegierungen gleichen denen der e-Commerce-Richtlinie weitestgehend. Art. 3 bis 5 stellen Anbieter von Durchleitungsdiensten, „Caching"-Diensten und Hosting-Dienste – letztere bis zum Zeitpunkt der Kenntnis der Rechtswidrigkeit – von einer Haftung frei. Art. 7 schließt in Fortschreibung des Art. 15 e-Commerce-Richtlinie allgemeine Überwachungspflichten und Verpflichtungen zu aktiven Nachforschungsbemühungen aus. Gleichzeitig stellt der Entwurf klar, dass diese Privilegierungen hoheitlichen Anordnungen, bestimmte Zuwiderhandlungen abzustellen, nicht entgegenstehen (Art. 3 III, 4 II, 5 V). Die bestehenden Unsicherheiten, wie weit Löschungs- und Nachforschungspflichten im Gefolge hoheitlicher Einzelfallanordnungen

14 Zu den vielen nicht vollharmonisierten Bereichen s. etwa Kühling/Martini, EuZW 2016, S. 448 (449 f.): „Handlungsformenhybrid" zwischen Richtlinie und Verordnung.

15 Zur diesbezüglichen Harmonisierungsabsicht des DSA-E s. EG 34; eine weitgehende Sperrwirkung für mitgliedstaatliche Plattformregulierungen sehen etwa Grünwald/Nüßing, MMR 2021, S. 283 (287); so auch die Befürchtung des Bundesrats mit Blick auf das NetzDG, s. BRDrucks 96/1/21, S. 9 f.

reichen dürfen,[16] überlässt der Entwurf der Klärung durch Dogmatik und Praxis.

Neu sind allerdings die Anforderungen des DSA-E bei hoheitlichen Einzelfallanordnungen (Art. 8 f.).[17] Dies betrifft Anordnungen, gegen bestimmte Inhalte vorzugehen, und die oftmals vorgelagerten Anordnungen, Auskunft über bestimmte Dienstenutzerinnen und deren Nutzungsverhalten zu geben. Der Entwurf setzt – wie auch im Übrigen –[18] auf formelle und verfahrensmäßige Vorgaben, um Konflikte um die Auskunft über Nutzerdaten und die Sperrung von Nutzerinhalten zu strukturieren und lösbar zu machen. Anbieter verpflichtet er, der anordnenden Stelle unverzüglich über die Maßnahmen zur Umsetzung der Anordnung zu berichten. Dadurch dürfte die Vorschrift die Aufsicht über die Umsetzung von Anordnungen erheblich erleichtern. Sowohl unzureichenden Maßnahmen zur Entfernung illegaler Inhalte als auch überschießenden Schritten – zu Unrecht für verpflichtend gehaltenen generellen Überwachungsanstrengungen – kann so besser begegnet werden.[19] Die anordnenden Stellen unterliegen ihrerseits einer umfassenden Informationspflicht über den Grund der Löschungsanordnung bzw. die Notwendigkeit einer Auskunft, ebenso wie über Beschwerdeverfahren und Rechtsbehelfe, die dem Diensteanbieter und betroffenen Nutzerinnen gegen die Anordnung zustehen.

2. Verfahrensmäßige Abbildung mehrpoliger Konflikte um Nutzerinhalte

Mit der Einbeziehung der betroffenen Nutzerinnen beweist der Entwurf Gespür für die Mehrpoligkeit dieser Konfliktlagen. Er greift die notwendige Mitbetroffenheit der Nutzerinnen, um deren Inhalte oder persönliche Daten es geht, verfahrensmäßig auf und macht sie sichtbar. Der Konflikt zwischen Online-Vermittlungsdiensten und Personen, die durch Online-Inhalte in ihren Rechten beeinträchtigt werden, betrifft immer auch die Interessen der Sprecherinnen, deren Inhalte geteilt werden. Eben diese Einbeziehung der jeweiligen Sprecherin hatte in der Google Spain-Ent-

16 S. dazu die Diskussion um EuGH v. 3.10.2019, C-18/18, Glawischnig-Piesczek v. Facebook Ireland; ausführlich L. Danwitz, Michigan Technology L. Rev. 27 (2020), S. 167.

17 Diese hervorhebend etwa auch Spindler, GRUR 2021, S. 545 (550).

18 S. unten III.2.-4.

19 Zu dieser in beide Richtungen gehenden Absicht s. EG 29.

scheidung des EuGH[20] und in der ursprünglichen Version des NetzDG[21] noch gefehlt. Die Versuche des BVerfG, hier in den Entscheidungen zum Recht auf Vergessen gegenzusteuern,[22] scheinen also auf europäischer Ebene Gehör gefunden zu haben.

Die verfahrensmäßige Einbeziehung aller von einer Entscheidung über Löschung, Sperrung oder Auskunft betroffenen Interessenträger zeigt sich nicht nur hier, sondern zieht sich durch den gesamten Entwurf. Nach Art. 14 V sind Personen, die Inhalte melden, unverzüglich in begründeter Form über die Entscheidung des Diensteanbieters zu informieren. Spiegelbildlich sind nach Art. 15 die betroffenen Nutzerinnen über jede Entfernung von ihnen bereitgestellter Inhalte formalisiert und in begründeter Form zu unterrichten. Daran anknüpfend trifft größere Online-Plattformen die weitere Pflicht, den von einer Löschung betroffenen Nutzerinnen ein Beschwerdeverfahren zu eröffnen (Art. 17). Führt dieses Verfahren zu dem Ergebnis, dass die vorgenommene Sperrung unberechtigt war, ist sie rückgängig zu machen (Art. 17 III). In jedem Fall sind die betroffenen Nutzerinnen über die Beschwerdeentscheidung und deren Gründe zu informieren (Art. 17 IV).[23] Hierbei sind sie auf die Bedingungen und Möglichkeiten hinzuweisen, um gegen die Entscheidung eine neutrale Streitschlichtungsstelle (Art. 18) oder staatliche Stellen anzurufen.

Hier zeigt sich der Ansatz des DSA-E, den mehrpoligen Konflikt um einzelne Nutzerinhalte verfahrensmäßig abzubilden, zu formalisieren und in einem gestuften Verfahren unter Beteiligung der interessierten Öffentlichkeit und der Betroffenen aufzulösen. Aus der Unzahl gepostete On-

---

20 EuGH v. 13.5.2014, C-131/12, Rn. 96 ff.; kritisch zur Nichtberücksichtigung der Interessen der Sprecherinnen Masing, Verfassungsblog v. 14.8.2014, https://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/, These 3; diese Auslassung des EuGH durch die fehlende Grundrechtsberechtigung des Sprechers im Fall Google Spain (behördliche Versteigerungsanzeige) erklärend BVerfGE 152, 216 – Recht auf Vergessen II, Rn. 141.

21 Zu dieser Kritik s. etwa Schiff, MMR 2018, S. 366 (368).

22 BVerfGE 152, 216, Rn. 121, 135; hieran anschließend, aber nicht ganz so weitgehend (keine vorherige Anhörung bei Löschung einzelner Beiträge) nunmehr auch BGH v. 29.7.2021, III ZR 179/20, Rn. 85 ff.; zu den Verfahrensanforderungen s. auch BVerfGE 148, 267 – Stadionverbot, Rn. 46 f.; kritisch zu verfahrensmäßigen Ableitungen aus Art. 3 Abs. 1 GG Buchheim, Rechtfertigungszentrierte Grundrechtslehren, in: Müller/Dittrich (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, Band VI, 2022, S. 3 (35 ff.).

23 Nicht genannt ist eine Pflicht, die meldende Person über die Wiederherstellung zu unterrichten. Auch hier zeigt sich, dass der DSA-E seinen Fokus nicht auf die Interessen der Meldenden, sondern der Allgemeinheit und der Sprecherinnen legt, s. näher unten IV.2.c.

line-Inhalte werden zunächst durch Hinweisgeber (Art. 14) und „vertrauenswürdige Hinweisgeber“ (Art. 19) – also durch Teile der Öffentlichkeit – diejenigen Inhalte identifiziert, die einer Prüfung durch den Diensteanbieter zuzuführen sind. Die Anforderungen an entsprechende Hinweise werden formalisiert,[24] um eine sinnvolle und qualifizierte Prüfung zu ermöglichen (Art. 14 II). Die dadurch verpflichtend ausgelöste Prüfung durch die Diensteanbieter (Art. 14 VI) darf vollautomatisiert – und dementsprechend standardisiert – ablaufen. Bereits dieser Umstand zeigt, dass es dem Meldemechanismus um eine erste Filterung zu tun ist. Diese lenkt die Moderationstätigkeit der Diensteanbieter in gewisse Bahnen und beschafft die für eine mindestrationale Moderationspraxis benötigten Informationen. Das Meldesystem muss aber nicht schon im ersten Schritt Ergebnisrichtigkeit in allen Einzelfällen herstellen. Das zeigt sich auch daran, dass die Hinweisgeberinnen zwar zu bescheiden sind, eine Pflicht zur Entfernung für rechtswidrig erkannter Inhalte aber – anders als die spiegelbildliche Pflicht zur Wiederherstellung rechts- und vertragsmäßiger Inhalte – nicht normiert ist.[25] Es geht hier also nicht um individuelle Rechtsdurchsetzung und Einzelfallgerechtigkeit, sondern um die Möglichkeit der interessierten Öffentlichkeit, auf die politisch relevante und prägende Moderationspraxis digitaler Dienste durch Meldungen formalisiert Einfluss zu nehmen.[26]

Die formalisierte Benachrichtigung über Entscheidungen der Hosting-Anbieter versetzt die von einer Sperrung Betroffenen wiederum in die Lage, ein Überprüfungsverfahren anzustrengen. Dieses zielt entschiedener auf Richtigkeit und Sicherung der Kommunikationsfreiheiten im Einzelfall. Es sieht Ergebnispflichten vor (Wiederherstellung recht- und vertragsmäßiger Nutzerinhalte) und erfordert eine auch-händische Bearbeitung (Art. 17 V). Diese mündet wiederum in eine Entscheidung mit formalisierter und differenzierter Begründung, die auf weitere Angriffsmöglichkeiten – vor Schlichtungsstellen und Gerichten – verweisen muss. In diesen Verfahrensschritten ist dann rechtlich geschultes Personal mit einer Klärung der aufgeworfenen Fragen befasst, um die noch verbliebenen Streitfragen zu klären. Im Extremfall löst ein anstößiger Online-Inhalt damit vier hintereinander geschaltete formalisierte, teils private, teils staatliche Überprüfungsverfahren aus (Verfahren auf Hinweis, Beschwerdeverfahren, Schlichtungsverfahren, gerichtlicher Rechtschutz). Mit diesen Verfahren korrespondieren jeweils Vorprüfungen der Verfahrensbeteiligten, ob sie ihre je-

24 Ebenso Spindler, GRUR 2021, S. 545 (552); s. dazu auch EG 41 f.
25 Ebenso BRDrucks 96/1/21, S. 9 f.; Grünwald/Nüßing, MMR 2021, S. 283 (285).
26 s. dazu näher unten IV.2.c.

weiligen Initiativbefugnisse wahrnehmen wollen. Ein solcher Aufwand lässt sich selbstverständlich nicht in jedem Einzelfall treiben, sondern baut darauf, dass die meisten Fälle schon auf einer der vorangehenden Verfahrensstufen erledigt werden. Die Vorschriften zur Sperrungsmöglichkeit bei einem Missbrauch, also bei einer exzessiven erfolglosen Inanspruchnahme der Initiativbefugnisse im Melde- oder Beschwerdesystem (Art. 21), zeigen die Erwartung des Entwurfs, die Probleme schrittweise abzuschichten.

3. Gestaltung des digitalen Raums qua Verfahren

Der Entwurf ist damit ein Paradefall einer typischen rechtlichen Strategie: Eine schwierige normative Frage – wer in welcher Weise und nach welchen Maßstäben über die Entfernung der zahllosen Inhalte auf Online-Plattformen und damit auch über Inhalt, Gestalt und Ton der öffentlichen Debatte entscheiden soll – wird in einer Vielzahl gestufter Verfahren einer Klärung zugeführt, ohne die inhaltlichen Maßstäbe der Konfliktlösung wirklich vorzugegeben. Dieser Ansatz einer bewusst verfahrensmäßigen Gestaltung[27] ist der auf das materielle Recht fixierten deutschen Rechtskultur – wie sie etwa auch im Verwaltungsrecht[28] oder im Anspruchssystem des BGB[29] zu beobachten ist – [30] eher fremd. Das Unionsrecht bleibt hier seiner verfahrensrechtlichen Tendenz[31] treu. Das zeigt sich nicht zuletzt am Kontrast zum Pflichtenprogramm des NetzDG. Anders als das NetzDG schreibt der Entwurf für rechtswidrige Inhalte keine materiellen Löschungspflichten fest, die innerhalb fester Fristen zu erfüllen sind. Andererseits ist der Entwurf verfahrensrechtlich anspruchsvoller als das NetzDG, das in seiner ersten Fassung den Schutz der Sprecherinnen vernachlässigte[32] und trotz entsprechender Forderungen[33] bis heute keine Veröffentlichung von Einzelentscheidungen (vgl. Art. 15 V DSA-E) vorsieht. Der verfahrensrechtliche Ansatz des Entwurfs zieht sich bis in das Aufsichtsver-

27 Diesen betont mit Blick auf das NetzDG auch Eifert, NJW 2017, S. 1450 (1452).
28 S. etwa § 46 VwVfG, § 214 ff. BauGB; zur ausufernden Literatur um den Verfahrensgedanken im Verwaltungsrecht statt aller Ziekow, NuR 2014, S. 229 (230 m.w.N.).
29 Windscheid, Die Actio des römischen Zivilrechts vom Standpunkt des heutigen Rechts, 1856, S. 1 ff.
30 Zur Kritik mit Blick auf das Prozessrecht siehe Buchheim, Actio, Anspruch, subjektives Recht, 2017.
31 Ziekow, NuR 2014, S. 229 (230 m.w.N.).
32 Zur Kritik Schiff, MMR 2018, S. 366 (368).
33 Zu dieser Forderung Eifert, NJW 2017, S. 1450 (1452 f.).

fahren, das Einzelnen nur das Recht auf Beschwerde bei den Aufsichtsbehörden, nicht aber ein Recht auf Bescheidung oder gar rechtmäßige Bescheidung vermittelt (Art. 43).[34]

Der DSA-E garantiert also hauptsächlich Verfahren und Formen, nicht Ergebnisse. Der Entwurf setzt darauf, dass Öffentlichkeit, Durchlaufen und Ausgestaltung der Verfahren, Begründungspflichten und Beteiligungsmöglichkeiten global betrachtet dazu führen werden, dass das Inhalteangebot auf Online-Plattformen einem regulatorisch angestrebten Zustand entspricht und sich bestimmte Risiken – wie die exponentielle Verbreitung rechtswidriger Inhalte – nicht im Übermaß verwirklichen. Damit ist der DSA-E zum einen konsequent systemisch ausgerichtet und zum andern erfrischend agnostisch hinsichtlich des gewünschten Gesamtbilds der Kommunikation auf Online-Plattformen. Er gibt inhaltlich kaum etwas vor, sondern schafft neue Formen und Verfahren für den komplexen, viele Akteure und Interessen einschließenden Aushandlungsprozess darüber, wie öffentliche Kommunikation aussehen soll, was gehen soll, was nicht, was wir uns voneinander gefallen lassen wollen und was nicht, und warum. Dieser kollektive Aushandlungsprozess wird durch den DSA-E eingerahmt und konturiert. Die faktisch wirksam werdenden Maßstäbe für Online-Inhalte werden so weiterhin in großem Umfang durch private Intermediäre, die „New Governors" des digitalen Raums,[35] gestaltet. Der vorausliegende Prozess läuft dann jedoch nicht mehr nach den intransparenten und kaum angreifbaren internen Vorgaben der Diensteanbieter, sondern entlang einer rechtlich vorgesehenen Struktur, mit verbrieften Initiativ- und Einflussmöglichkeiten der Öffentlichkeit und der Betroffenen, gerichtlichen Letztkonkretisierungsmöglichkeiten und umfassender Transparenz (u.a. Art. 10 bis 13, 15 V, 23, 24, 33, 34). Die Inhaltsmoderationspraxis der Diensteanbieter wird in einer Weise sichtbar, nachvollziehbar und kritisierbar, die sowohl individuelle Einflussnahme der Interessierten und Betroffenen als auch politisches Gegensteuern und Eingreifen ermöglicht. Das verschafft dem daraus resultierenden Gesamtbild der Online-Inhalte ein Maß an demokratischer Legitimation und Rückkoppelung, das eine inhaltsfixierte absolute Bestimmung rechtlicher Grenzen durch materielle Vorgaben an die Moderationspraxis nicht erreichen könnte.[36] Äußerungs-

34 S. dazu unten III.5.

35 Klonick, Harvard L. Rev. 131 (2018), S. 1598; zur Unaufhebbarkeit der Entscheidungsmacht privater Intermediäre Eifert, NJW 2017, S. 1450 (1451).

36 Ausführlich zu einem ähnlichen, nicht auf das Ergebnis, sondern auf das Verfahren der Mitwirkung an kollektiven Entscheidungen blickenden Argument Post, Michigan L. Rev. 95 (1996), S. 1517 (1522 ff.).

rechtliche Grenzen und das Gesamtbild öffentlicher Kommunikation müssen in konkreten Verfahren immer neu bestimmt und ausgestaltet werden. Sie sind nicht einfach da, werden „gefunden" und festgestellt.[37]

4. Selbstregulierung sehr großer Plattformen unter dem Auge der Öffentlichkeit

Ähnlich agnostisch ist der DSA-E hinsichtlich der systemischen Risiken, die von VLOP ausgehen, und der gebotenen Instrumente, um sie einzudämmen. Art. 26 ff. deuten nur vage an, dass die VLOP und ihr mächtiger Einfluss auf die digitale Öffentlichkeit gewisse systemische Risiken bergen. Das sind namentlich die Risiken der ungezügelten Verbreitung illegaler Inhalte (Art. 26 I a), einer Beeinträchtigung der Grundrechtswahrnehmung (Art. 26 I b) und „vorsätzlicher Manipulationen" mit nachteiligen Folgen für die öffentliche Gesundheit, Minderjährige, die öffentliche Debatte und die öffentliche Sicherheit (Art. 26 I c). Dieser breite Strauß der in der aktuellen Diskussion mit VLOP in Verbindung gebrachten Systemrisiken wird in den Erwägungsgründen (56 f.) nicht wesentlich konkretisiert. Genau welche Funktionen der VLOP auf genau welche Weise diese Risiken verursachen, wird der Phantasie und Assoziation der Leserinnen und Anwenderinnen überlassen. Nicht anders verhält es sich mit den „sorgfältig" auf die ermittelten Risiken abzustimmenden Risikominderungsmaßnahmen (Art. 27). Dass zu solchen Maßnahmen eine „Anpassung der Funktionsweise der Moderation von Inhalten" oder eine Umgestaltung algorithmischer Empfehlungssysteme gehören kann (Art. 27 I a), ist ebenso wenig überraschend wie weiterführend. Das klärt in etwa so viel wie das Gebot „höflich zu sein", ohne die Gebote der Höflichkeit zu erläutern. Noch am spezifischsten sind hier die Vorgaben zur nachvollziehbaren und von Nutzerinnen beeinflussbaren Gestaltung von Empfehlungssystemen (Art. 29) und zur umfassenden Transparenz von Online Werbung (Art. 30). Allerdings bleibt auch hier das Meiste den VLOP überlassen und ist zudem unklar, wie genau diese Fragen mit den systemischen Risiken des Art. 26 DSA-E in Verbindung stehen.

Der Regelungsfokus liegt daher auch in diesem Abschnitt nicht auf den inhaltlichen Andeutungen des Entwurfs, sondern in den vorgesehenen Formen und Verfahren. Die Pflicht zu regelmäßigen Risikobewertungen

37 Daher auch das Gebot zur kontextspezifischen Abwägung im Äußerungsverfassungsrecht, s. zuletzt die Kompilation in BVerfG (K) v. 19.5.2020, 1 BvR 1094/19, Rn. 15-28.

und entsprechenden Berichten zielt darauf, das nötige Wissen um Risiken und deren Remedien zu generieren und Öffentlichkeit und politischem Prozess aussagekräftige Erfahrungen aus der Praxis der Plattformregulierung verfügbar zu machen. Ebenso verhält es sich mit der Pflicht, in „sorgfältiger" Weise auf die Ergebnisse der eigenen Risikobewertung zu reagieren. Auch hier scheint es darum zu gehen, über verpflichtende Selbstregulierungsexperimente der Anbieter einen Wissens- und Erfahrungsschatz für eine möglicherweise später einmal stattfindende harte inhaltliche Regulierung der Tätigkeit der VLOP zu schaffen. Die Vorschriften zu den VLOP begründen insoweit im Wesentlichen neue Formate, um das Gespräch und die Debatte um die Risiken großer Plattformen überhaupt sinnvoll führen zu können. Indem hier ein kontinuierlicher Output an Berichten über Risiken und Reaktionsmaßnahmen angestoßen wird, dieser Prozess vor den Augen der Öffentlichkeit stattfindet und einem Nachvollzug durch unabhängige Stellen ausgesetzt ist (Auditpflicht, Art. 28; wissenschaftliche Datenzugriffsrechte, Art. 31 II, IV), sollen die VLOP in Richtung einer bewussteren und vorsichtigeren Gestaltung der Möglichkeiten und Funktionen ihrer Dienste gelenkt werden.[38] Der DSA-E setzt darauf, dass bereits die gestärkte öffentliche Rechenschaft und Sichtbarkeit der Plattformpraxis als solche – etwa mit Blick auf Empfehlungssysteme und Werbeanzeigen, Art. 29 f. – ein Gegengewicht innerhalb der bei der Fortentwicklung der Dienste wirkenden primär wirtschaftlichen Logiken bilden können.[39] Auch hier zeigt sich also ein verfahrensrechtlicher Grundansatz, der hauptsächlich auf Transparenz und Kritisierbarkeit baut. Ob dieser Zugriff auf längere Sicht ausreichend ist, um den gesellschaftlichen Herausforderungen aufgrund der VLOP Herr zu werden, lässt sich noch nicht absehen. Möglicherweise wird man nicht umhinkommen, irgendwann auch inhaltlich Farbe zu bekennen, genau welchen Risiken des Geschäftsmodells durch genau welche Maßnahmen begegnet werden sollte. Der Moment für solche inhaltlichen – notwendig politisch umstrittenen und heiklen – Regulierungen dürfte aber noch nicht gekommen sein. Das Phänomen der Plattformen ist eher jung und das Wissen über Risiken und Nebenwirkungen noch zu andeutungshaft und vage.

38 S. EG 56.
39 Zu dieser Hoffnung mit Blick auf das NetzDG Eifert, NJW 2017, S. 1450 (1452).

5. Durchsetzungsregime – nicht bereit für subjektive Rechte

Eine gewisse Vorsicht und Zurückhaltung des Entwurfs ist auch auf Ebene des Durchsetzungsregimes zu erkennen. Dieses ist – anders als das *private* und *public enforcement* verbindende Mischmodell der DS-GVO – stark behördlich und objektivrechtlich geprägt.[40] Die Einrichtung der Verfahren und die jeweils gebotenen Mitteilungen, Transparenzmaßnahmen und Begründungen sind als öffentlich-rechtliche, behördlich durchzusetzende Pflichten, nicht als private Rechte formuliert. Ein eigener Abschnitt mit unmittelbar privatrechtswirksamen, zivilgerichtlich durchsetzbaren (Art. 79 DS-GVO) Betroffenenrechten wie in den Art. 12 ff. DS-GVO fehlt. Das rechtliche Verhältnis zwischen Plattform und Nutzerinnen wird damit weiterhin primär vertraglich gestaltet. Auch das Deliktsrechtsverhältnis zu Dritten wird nur negativ durch unmittelbar wirkende Haftungsprivilegierungen bestimmt.[41] Die Pflicht zu einer transparenten Gestaltung der Moderationspraxis durch allgemeine Geschäftsbedingungen (Art. 12) dürfte allerdings dazu führen, dass die neuen öffentlichrechtlichen Pflichten im Rahmen der Inhaltsmoderation als gesetzliche Leitbilder auf die private Gestaltung und gerichtliche Kontrolle der Community Standards einwirken.[42] Das Vertragsrecht dürfte damit – trotz des primär öffentlichrechtlichen Regelungszugriffs – mittelbar zu einem Hauptfaktor der Implementierung des DSA werden. Anderes gilt für die VLOP-spezifischen Pflichten zur systemischen Risikovorsorge, für die eine mittelbare vertragsrechtliche Durchsetzung eher fernliegend erscheint. In Hinblick auf diese und die meisten übrigen Pflichten des DSA-E bleibt damit die behördliche Rechtsdurchsetzung nach Kapitel IV der Regelfall. Diese ist – erneut anders als in der DS-GVO (Art. 77 f. DS-GVO) – allerdings nicht (zumindest ausschnittsweise)[43] subjektivrechtlich zugeordnet. Einzelne haben zwar die Möglichkeit, ein behördliches Tätigwerden durch Beschwerden anzustoßen (Art. 43). Eine gerichtliche Kontrolle behördlicher Entscheidungen über solche Beschwerden oder eine Untätigkeitsklage sind jedoch nicht vorgesehen. Das spricht dafür, dass die Pflichten des DSA und die darauf bezogenen Aufsichtsbefugnisse nach der Konzeption des Entwurfs nicht

40 Mit ähnlichem Ergebnis Spindler, GRUR 2021, S. 653 (u.a. 654, 657, 659, 661); ebenso die Kritik des Bundesrats BRDrucks 96/1/21, S. 16.

41 S. dazu oben III.1.

42 Ebenso Spindler, GRUR 2021, S. 545 (553).

43 Zur wenig beachteten Frage der Reichweite der subjektiv-öffentlichen Rechte aus der DS-GVO s. Will, ZD 2020, S. 97; VG Ansbach v. 8.8.2019, AN 14 K 19.00272; OVG Rheinland-Pfalz v. 26.10.2020, 10 A 10613/20, Rn. 41-47.

drittschützend sind, also keine subjektiven Rechte von Bürgerinnen begründen, die ein behördliches Einschreiten begehren. Es erscheint allerdings nicht ausgeschlossen, dass die deutsche Praxis in Anwendung der Schutznormlehre hier teils zu anderen Ergebnissen gelangen wird.[44] Eine solche Subjektivierung wäre allerdings nicht unionsrechtlich vorgezeichnet. Diese Zurückhaltung gegenüber einer Subjektivierung des neuen Regulierungs- und Aufsichtsregimes passt zum vorsichtigen Gesamtansatz des DSA-E. Wer noch nicht genau weiß, wohin die Reise geht und wie eine Plattformregulierung bestmöglich zu bewerkstelligen ist, sollte mit einer subjektivrechtlichen Zuordnung vorsichtig sein. Diese brächte notwendig die Beharrungskräfte und Interessen unzähliger Berechtigter ins Spiel bringt. Denn jede Subjektivierung normativer Vorgaben entzieht deren konkretisierende Anwendung ein Stückweit dem steuernden Einfluss der mit der Umsetzung befassten Behörden und überantwortet sie der dezentralen, unkoordinierten und kaum vorhersehbaren gerichtlichen Ausdeutung und Fortentwicklung.[45]

IV. Leerstellen und Konfliktpotential

Versteht man den DSA-E in der hier geschilderten Weise als zurückhaltenden, ersten Rahmungsversuch, erschließt sich, dass der Entwurf für die meisten Fragen der Plattformregulierung gar keine inhaltlichen Antworten und Orientierungen bereitzuhalten beansprucht. Dementsprechend lassen sich in fast allen Hinsichten Leerstellen ausmachen: Wie genau stellt sich der Entwurf das Vorgehen der Netzwerke gegen Hate Speech, Social Bots oder lose koordinierte Nutzeraktionen vor? Wie verhalten sich die umfassenden Offenlegungs- und Meldepflichten (u.a. an Sicherheitsbehörden, Art. 21) zu den Vorgaben und Grenzen des europäischen Datenschutzrechts?[46] All dies sind Fragen, für die der Entwurf fast nur verfah-

44 Zur Möglichkeit eines Auseinanderfallens unionsrechtlich gebotener und mitgliedstaatlicher Subjektivierung des Aufsichtsregimes s. Will, ZD 2020, S. 97 (98 ff.).

45 Zu diesem Zusammenhang Buchheim, Actio (Fn. 30), S. 97 f.; ders./Möllers, § 46: Gerichtliche Verwaltungskontrolle als Steuerungsinstrument, in: Voßkuhle u.a. (Hrsg.), GVerwR, 3. Aufl. 2022, Rn. 144 f.; 156 f., 159.

46 Härting/Adamek, CR 2021, S. 165 (170 f.); zu den Auswirkungen datenschutzrechtlicher Vorgaben auf die Regulierung von Äußerungsplattformen s. Buchheim, JZ 76 (2021), S. 539.

rensrechtliche Rahmungen vorgibt. Einige besonders drängende Leerstellen und Fragen sollen hier dennoch beleuchtet werden:

1. Unterentwickelte Ansätze der Eindämmung von Fake News

Auffällig ist zunächst, dass der DSA-E die verbreitete Sprach- und Konzeptlosigkeit bezüglich des Problems einer exponentiellen Verbreitung von Fake News über Online-Plattformen weitgehend fortführt. Schon das NetzDG ist insoweit nur eine Scheinantwort, weil es die Verbreitung von Desinformation als ein Hauptproblem der sozialen Netzwerke benennt,[47] regulatorisch aber nur das kleine Feld bestimmter strafrechtlich relevanter, zumeist auf bestimmte Personen bezogener Falschbehauptungen erfasst.[48] Desinformation über kollektivrelevante Sachverhalte – z.B. über angeblichen Wahlbetrug in großem Umfang – kann man so nicht in den Griff bekommen. Denn sie lässt sich in der Regel nicht als individualbezogene Unwahrheit rekonstruieren, sodass nur wenige Konstellationen überhaupt in den Bereich des Strafrechts und damit des NetzDG gelangen. Der DSA-E ist hier zwar weiter gefasst, indem er jede Form der Inhaltsmoderation durch Diensteanbieter erfasst und Desinformation bzw. „Manipulation" als eines der von den VLOP anzugehenden Systemrisiken benennt. Hinsichtlich der Kernfragen, was als „Manipulation" zu gelten hat und wie die Macht der Plattformen zur Definition des in Tatsachenfragen „Richtigen" und „Vertrauenswürdigen" eingehegt werden soll, schweigt sich der Entwurf aber aus. Diese Leerstelle ist problematischer als die sonstige inhaltliche Abstinenz des Entwurfs, weil es in Tatsachenfragen keine Rückbindung an mitgliedstaatliche Rechtmäßigkeitsmaßstäbe oder vertragliche Regelungen in den Community Standards gibt. Es gibt in einer liberalen Ordnung keinen Bestand gesicherten, autoritativ markierten Tatsachenwissens, auf den man zurückgreifen könnte.[49] Interne Verfahren der Diensteanbieter, Schlichtungsverfahren und staatlicher Rechtschutz gegen Löschungen haben damit keine gesicherte Referenz, um über die Löschung oder Nichtlöschung gemeldeter Inhalte mit Blick auf deren Wahrheitsgehalt zu entscheiden. Die Definition dessen, was anhand welcher Quellen in welchen Verfahren als „Manipulation" zu gelten hat, bleibt damit gänz-

47 BTDrucks 18/12356, S. 1.

48 Zu diesem Problem näher Buchheim, Der Staat 59 (2020), S. 159 (161 f.; 166 f.).

49 Hierzu und zu den dennoch bestehenden Möglichkeiten eines bereichsspezifischen Schutzes der Tatsachenrichtigkeit Buchheim, Der Staat 59 (2020), S. 159 (167-170).

lich in der Hand der Diensteanbieter – mit der damit verbundenen immensen Macht. Diese Macht einfach so hinzunehmen steht quer zu dem ansonsten konsequenten Ansatz des Entwurfs, den prägenden Einfluss der Plattformen auf die digitale Öffentlichkeit durch geeignete Verfahren und Transparenzanforderungen demokratisch und politisch rückzubinden.[50]

2. *Verhältnis zu mitgliedstaatlicher Plattformregulierung*

a) Kompetenzgerechte Beschränkung auf Verfahrensgestaltung

Auch wenn man den zurückhaltenden Ansatz des DSA-E in Hinblick auf die Einhegung von Fake News oder auch allgemein für unzureichend halten mag, ist insgesamt zu begrüßen, dass sich der Kommissionsentwurf einer harten inhaltlichen Steuerung des Content Management der Online-Plattformen enthält. Es gilt insoweit, was oben zum Haftungsrecht ausgeführt wurde.[51] Die Tätigkeit der Plattformen, insbesondere der VLOP, weist zwar einen starken Binnenmarktbezug auf und berührt die politischen und sozialen Gegebenheiten in der gesamten Union. Fragen der Plattformregulierung sind jedoch zu stark bezogen auf die höchst verschiedenen politischen Prozesse, Kulturen und Öffentlichkeiten der Mitgliedstaaten, um sie zum jetzigen Zeitpunkt inhaltlich zu harmonisieren. Demgegenüber erscheint es schlüssig, unter Wahrung der mitgliedstaatlichen Rechtsordnungen den allgemeinen verfahrensmäßigen Rahmen der Plattformregulierung – insbesondere die von den Anbietern bereitzustellenden internen Verfahren – unionsweit einheitlich zu gestalten. Denn es sind gerade die Unübersichtlichkeit vielfältiger mitgliedstaatlicher Verfahrensvorgaben und die Unterschiede in den seitens der Dienste dafür aufzuwendenden Ressourcen, die die Binnenmarktrelevanz solcher Regelungen – und damit auch die Kompetenz der Union – begründen.[52] Gleichzeitig beeinträchtigt ein gemeinsamer verfahrensrechtlicher Rahmen für die Moderation und Selbstregulierung der Plattforminhalte nicht die Fähigkeit der Mitgliedstaaten, inhaltliche Regeln ihres öffentlichen Kommunikationsraums und Grenzen zulässiger Inhalte weithin selbst zu verhandeln und zu gestalten. Die regulatorische Zurückhaltung des DSA-E hat also auch einen kompetenzrechtlichen Hintergrund.

---

50 Zu diesem – vom NetzDG verschiedenen – Fokus des DSA-E unten IV.2.c.
51 Oben III.1.
52 S. EG 2, 4 und 6.

b) Einheitlicher europäischer Verfahrensrahmen der Plattformregulierung

Die hiermit betretene Kompetenzebene führt zur Frage, wie sich der DSA-E zu den bereits vorhandenen mitgliedstaatlichen Versuchen im Bereich der Plattformregulierung verhält.[53] Das betrifft besonders das in vielen Punkten vorbildgebende NetzDG. Die Frage wird im DSA-E und in den begleitenden Materialien nur mittelbar angesprochen.[54] Es ist damit zu rechnen, dass jedenfalls auf deutscher Seite ein erhebliches Interesse bestehen wird, zumindest in Teilen am NetzDG als international sichtbarem und innovativem Stück Digitalregulierung festzuhalten.[55]

Auf Seiten der regulierten Dienste ist davon auszugehen, dass sie großes Interesse an einem einheitlichen unionsweiten Verfahrensrahmen für die Inhaltsmoderation haben. Ein Nebeneinander der nach dem NetzDG vorgesehenen Verfahren (Beschwerde, § 3 NetzDG, und Gegenvorstellung, § 3a NetzDG, Schlichtung, § 3b NetzDG) und des gleichfalls differenzierten Regimes des DSA-E dürfte von den Plattformen schon allein wegen des damit verbundenen mehrfachen Verwaltungs- und Vorhalteaufwands kritisch gesehen werden. Ein solches Nebeneinander dürfte aber auch der Intention des DSA-E zuwiderlaufen. Denn der Kommissionsentwurf setzt erkennbar auf Einheitlichkeit. Er erklärt sein Regime für jede Löschung oder Sperrung für anwendbar und differenziert nicht nach Art der Verfahrensinitiierung (auf Meldung oder ohne Meldung) oder Löschungsgründen (Rechtswidrigkeit/Vertragswidrigkeit). Diese Tendenz zu einheitlichen Verfahren der Inhaltsmoderation ist nicht nur eine Frage des Ressourcenaufwands, sondern erschließt sich auch mit Blick auf die bisherigen Erfahrungen bei der Plattformregulierung. Diese deuten darauf, dass staatliche Interventionen wie das NetzDG nicht nur unmittelbar dadurch wirken, dass sie für eine Verletzung staatlicher Rechtsnormen effektive Verfahren und Abhilfemöglichkeiten schaffen. Sogar vornehmlich wirken sie dadurch, dass sie eine Umgestaltung und verschärfte Durchsetzung der

53 Zu dieser Frage s. auch Grünwald/Nüßing, MMR 2021, S. 283 (286 f.), BRDrucks. 96/1/21, S. 4 f., 9 f., 11: „Anspruch der Vollharmonisierung (, die) keinen nationalen Spielraum zulässt".

54 Ebenso Grünwald/Nüßing, MMR 2021, S. 283 (286); der Kommissionsvorschlag nennt allerdings die verschiedenen mitgliedstaatlichen Regulierungen als Grund für die Heranziehung der Binnenmarktkompetenz, s. Vorschlag (Fn. 8), S. 6 f. sowie EG 2, 4, 6.

55 So etwa die Stellungnahme des Bundesrats BRDrucks 96/1/21, S. 9 f., 11; näher zu Entwicklung und Hintergründen des NetzDG Peukert, Das Netzwerkdurchsetzungsgesetz, in diesem Band, S. 221 (221 ff.).

eigenen Community Standards der Plattformen anstoßen.[56] Das macht es sinnvoll, auch die Rahmenbedingungen vertragsrechtlicher Durchsetzungsmaßnahmen schärfer zu zeichnen, wie es zuletzt der BGH getan hat.[57] Ohne solche Vorgaben auch für die privatautonom gestaltete und motivierte Inhaltsmoderation wäre eine Löschung oder Sperrung unter Verweis auf das Vertragsrecht ein einfacher Ausweg aus dem regulatorischen Rahmen und damit die Moderationspraxis der Netzwerke wieder ihnen allein überlassen. Im Ergebnis zeigt sich hier also eine Tendenz zur Verfahrenskonvergenz. Früher oder später dürfte sich eine in der Masse praktikable und in den meisten Fällen beschrittene Verfahrensweise der Inhaltsmoderation herausschälen. Die regulatorische Aufgabe besteht darin, die Gestaltung dieser Verfahren so zu beeinflussen, dass sie die durch Plattforminhalte involvierten Interessen und Herausforderungen in der großen Masse der Fälle adäquat aufgreifen und verarbeiten. Ein Nebeneinander von vielen hoheitlich geforderten, zweck- und maßstabsähnlichen, aber im Einzelnen distinkten Verfahren würde dem entgegenlaufen. Keines der Verfahren könnte in der Praxis mit echter Selbstverständlichkeit und Routine implementiert werden.[58] Es spricht also viel dafür, dass nicht nur der Harmonisierungswille, sondern auch die praktische Wirksamkeit des DSA-E eine Verdrängung des Verfahrensregimes des NetzDG fordert.

56 Tworek/Leerssen, An Analysis of Germany's NetzDG Law, Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2019, https://pure.uva.nl/ws/files/40293503/NetzDG_Tworek_Leerssen_April_2019.pdf, S. 6: „In this light, it may be that NetzDG's most important effect was to ensure swifter and more consistent removal of content within Germany under the companies' community guidelines."; s. insoweit gleichbleibend für den jüngsten Berichtszeitraum Google (Youtube) NetzDG-Transparenzbericht (Januar bis Juni 2021), https://storage.googleapis.com/transparencyreport/legal/netzdg/YT-NetzDG-TR-Bundesanzeiger-latest.pdf, S. 14; zur vertragsrechtlichen Zulässigkeit einer über die Gesetzeslage hinausgehenden Löschungspraxis jüngst BGH v. 29.7.2021, III ZR 179/20, Rn. 78.

57 BGH v. 29.7.2021, III ZR 179/20, Rn. 78 ff.

58 Die Bedeutung der implementierenden Verfahren zeigt sich auch an der äußerst geringen von Facebook registrierten Zahl von NetzDG-Beschwerden. Diese geht maßgeblich darauf zurückgeht, dass für Beschwerden nach dem NetzDG ein eigenes Meldeformular vorgesehen ist und dieses nicht in den allgemeinen Meldemechanismus der Plattform integriert ist, s. Tworek/Leerssen (Fn. 57), S. 5.

c) Akzentverschiebungen: Einhegung der Plattformmacht statt effektiver Rechtsdurchsetzung

Eine solche Verdrängung hätte – trotz der in Vielem ähnlichen Ziele und Instrumente von NetzDG und DSA-E – einige entscheidende Änderungen zufolge. Denn das Grundanliegen der Verfahrensvorgaben des DSA-E ist ein anderes als beim NetzDG. Letzteres zielt klar auf die Schaffung effektiver interner Verfahren zur Durchsetzung der Rechte und Interessen der durch Online-Inhalte negativ Betroffenen.[59] Das Gegenvorstellungsverfahren und andere Schutzvorkehrungen zugunsten der kommunikativen Freiheit der Plattformnutzerinnen wurden erst später nachgereicht. Demgegenüber ist es dem Meldesystem der DSA-E nicht primär um die Durchsetzung von Betroffeneninteressen zu tun, sondern um die Einrichtung eines die gesamte europäische Öffentlichkeit einbeziehenden Informationssystems. Dieses ermöglicht der Allgemeinheit, auf die Moderationspraxis der Plattformen formalisiert Einfluss zu nehmen. Diese allgemeinheitsbezogene Stoßrichtung zeigt sich sowohl am Kreis der Initiativberechtigten (alle, nicht nur Plattformnutzer) als auch terminologisch (*Melde*system statt *Beschwerde*). Sie erschließt sich aber vor allem beim Blick auf die Rechtsfolgen: Meldende sind nur qualifiziert über den Ausgang von ihnen angestoßener Verfahren zu informieren, eine Pflicht zur Löschung rechtswidriger Inhalte besteht nicht und die erfolglos Meldenden – anders als die durch Löschungen betroffenen Sprecherinnen – sind im Beschwerdesystem der Art. 17 ff. DSA-E nicht antragsberechtigt. Die eigentliche individuelle *Betroffenheit*, auf die mit der Schaffung eines internen *Beschwerde*systems reagiert wird, verortet der DSA-E bei den Sprecherinnen, deren Inhalte – aus welchem Grund auch immer – seitens der Plattformen gelöscht werden. Dies zeigt sich an den zur Initiative berechtigenden Tatbeständen (jede Löschung von Nutzerinhalten) wie auch daran, dass der Entwurf nur hier eine Ergebnispflicht (Wiederherstellung zu Unrecht gelöschter Beiträge) vorsieht. Das Beschwerdesystem des DSA-E sichert also das grundrechtlich unterfütterte Interesse der Sprecherinnen an einer Sichtbarkeit ihrer Beiträge verfahrensrechtlich ab. Überspitzt gesagt adressieren die Verfahren des DSA-E damit in erster Linie das Problem der demokratischen Rückbindung der „New Governors", nicht – wie das NetzDG – das Rechtsdurchsetzungsdefizit und drohende Rechtsverletzungen im digitalen Raum.

59 BTDrucks 18/12356, S. 1 f.; näher zum NetzDG Peukert (Fn. 55).

d) Fortbestehen inhaltlicher Vorgaben der Mitgliedstaaten

Eine andere Lösung als eine Verdrängung mitgliedstaatlicher Vorgaben erscheint allerdings für die nach dem NetzDG vorgesehenen Löschungsergebnispflichten vorstellbar.[60] Bei solchen Löschungspflichten innerhalb vorgegebener Zeiträume (§ 3 II NetzDG) handelt es sich um Regelungen, die die Verfahrensebene offenkundig übersteigen und auf ein überschaubares Rechtsregime (§ 1 III NetzDG) verweisen. Vergleichbare Pflichten sieht der DSA-E, der den Konflikt wie gesehen verfahrensmäßig zu moderieren sucht, nicht vor. Ihre Fortgeltung beeinträchtigte auch nicht die praktische Wirksamkeit des durch den DSA-E vorgegebenen Verfahrensrahmens, sondern ergänzte ihn um ein abgrenzbares Pflichtenprogramm mit Blick auf wenige und definierte Straftatbestände. Solche zusätzlichen materiellen Pflichten der Plattformanbieter könnten umstandslos mitgliedstaatsspezifisch im Rahmen des jeweils geltenden Kollisionsrechts umgesetzt werden. Auch hier sollte sich auswirken, dass der DSA-E keine Harmonisierung des Verhaltens- und Haftungsnormen hinsichtlich einzelner Inhalte anstrebt und auch nicht anstreben sollte.[61] Mit einer solchen Kompetenzabgrenzung bliebe den Mitgliedstaaten Raum für eigene Gestaltungen und könnte zugleich eine zu einem späteren Zeitpunkt versuchte Inhaltsregulierung bestimmter Digitale-Dienste-Risiken durch regulatorische „Testballons" auf mitgliedstaatlicher Ebene vorbereitet werden. Zugleich bliebe das Interesse der Diensteanbieter und der Nutzerinnen an einem einheitlichen, in allen Melde- und Löschungskonstellationen wirksam werdenden Verfahrenskorsett gewahrt. Demgegenüber erscheint nach aktuellem Stand des Entwurfs eine vermittelnde Lösung für Pflichten, die wie etwa Berichtspflichten das Verfahren der Inhaltsmoderation nicht unmittelbar betreffen, angesichts des Ziels der Rechtsharmonisierung kaum gangbar. Vorstellbar wären hier allerdings Zugeständnisse im Laufe des Gesetzgebungsverfahrens, weil ein Nebeneinander solcher Berichtspflichten die Effektivität des unionsrechtlich vorgegebenen Pflichtenprogramms nicht berühren dürfte.

60 Insoweit a.A. Grünwald/Nüßing, MMR 2021, S. 283 (287); gegen eine Verdrängung der nach dem NetzDG vorgesehenen Löschpflichten hinsichtlich rechtswidriger Inhalte BRDrucks 96/1/21, S. 10.

61 S. oben III.1.

3. Konfliktträchtiges Aufsichtsregime

Eine weitere Frage, die im Gesetzgebungsverfahren Auseinandersetzungen erwarten lässt, betrifft die Rechtsetzungs- und Aufsichtsbefugnisse der Kommission sowie den Status der neu zu schaffenden nationalen Aufsichtsbehörden („Digitale-Dienste-Koordinatoren").

Im Fall der DS-GVO ist es der Kommission nicht gelungen, weitreichende eigene Befugnisse – u.a. im Rahmen der Öffnungsklauseln – durch das Gesetzgebungsverfahren zu boxen.[62] Auch im Fall der Plattformregulierung ist nicht damit zu rechnen, dass die Mitgliedstaaten ihre Möglichkeiten zur Gestaltung ihrer Kommunikationsräume übermäßig werden beschneiden wollen. Die Fortführung des Haftungsregimes der e-Commerce-Richtlinie und die inhaltliche Abstinenz des gesamten Entwurfs deuten vielmehr darauf, dass man sich der Relevanz der Plattformregulierung für die politischen Prozesse der Mitgliedstaaten bewusst ist. Insofern ist unwahrscheinlich, dass sich die Mitgliedstaaten hier das Heft des Handelns zugunsten der Kommission aus der Hand werden nehmen lassen.

Ähnliches gilt für den Status der Digitale-Dienste-Koordinatoren.[63] Die Frage, ob Aufsichtsbehörden mit politischer Unabhängigkeit ausgestattet werden, ist jedenfalls nach deutschem Verfassungsverständnis eine demokratische Kernfrage.[64] Zuletzt hat das BVerfG insoweit auch auf Ebene des Unionsrechts Parallelen zum deutschen Modell demokratischer Verantwortlichkeit behauptet[65] und unabhängige Regulierungsbehörden als demokratisch „prekär"[66] bezeichnet. Ob diese Position unionsweit mehrheitsfähig ist und auch Geltung beanspruchen kann, wenn das Unionsprimärrecht – wie im Fall der EZB, Art. 282 III AEUV – die Unabhängigkeit einer Institution garantiert, lässt sich gut diskutieren. Im Fall des neu zu schaffenden Digitale Dienste-Koordinators ist die politische Unabhängigkeit jedoch nicht in den Verträgen vorgezeichnet. Sie ist auch nicht – wie

62 Härting/Adamek, CR 2021, S. 165 (168).

63 Für ersten Widerstand s. BRDrucks 96/1/21, S. 5 (kein Eingriff in nationale Behördenstrukturen).

64 Zusammenfassend BVerfGE 151, 202 – Europäische Bankenunion, Rn. 129 ff. m.w.N.; grundlegend Böckenförde, § 24 – Demokratie als Verfassungsprinzip, in: Isensee/Kirchhof (Hrsg.), HdStR, Band II, 3. Aufl. 2004, S. 289; zur Relativierung Lassahn, Rechtsprechung und Parlamentsgesetz, 2017, S. 113 ff.

65 BVerfGE 151, 202, Rn. 135-139; bezugnehmend insbesondere auf EuGH v. 13.6.1958, C-9/56, *Meroni*.

66 BVerfGE 151, 202, Rn. 138.

beim Datenschutzbeauftragten –[67] durch eine Tradition solcher Behörden in Teilen der Union unterfüttert. Vielmehr spricht alles dagegen, die Regulierungsbehörde im Bereich der digitalen Dienste mit einem unabhängigen Status auszustatten.

Der DSA-E wäre zu allererst in sich inkonsequent, weil er die mitgliedstaatlichen Aufsichtsbehörden in die politische Unabhängigkeit entließe, während auf europäischer Ebene der Kommission – also einer politisch eingebetteten und kontrollierten Behörde – umfassende Aufsichtsbefugnisse (Art. 51 ff.) eingeräumt werden sollen. Hier will die Kommission offenbar die politischen Zügel gegenüber den VLOP in der Hand behalten, ohne zugleich die Diensteregulierung auch auf mitgliedstaatlicher Ebene als eminent politische Frage anzuerkennen. Die Kommission predigt hier Wasser und trinkt selbst Wein.

Auch ungeachtet derlei doppelten Maßes wäre ein verpflichtender unabhängiger Status der Digitale-Dienste-Koordinatoren in den Mitgliedstaaten ein – zumindest nach deutschem Verfassungsrecht problematischer – Fehler. Ein sachlicher Grund für eine Unabhängigkeit ist nicht ersichtlich. Anders als der Datenschutzbeauftragte hat der Digitale-Dienste-Koordinator keinen – zumindest in den Kernbereichen – klaren und durch eine längere Tradition umrissenen Regulierungsauftrag.[68] Die Gefahren, die er zu bekämpfen antreten soll, sind bestenfalls vage vorgestellt und wesentlich vielgestaltiger als das Datenschutz-Anliegen. Anders als im Fall der Datenschutzrichtlinie und nunmehr der DS-GVO gibt es kein unionsrechtlich einheitliches, gesetzlich definiertes inhaltliches Regulierungsprogramm. Die Koordinatoren wären damit unabhängige Regulierungsbehörden ohne gesetzliches Aufsichtsprogramm. Das würde dazu einladen, dieses Programm selbst erst in der Praxis zu formulieren und konturieren – ohne dass dabei ein politischer Zugriff gegeben wäre. Zudem und vor allem gibt es im Bereich der Aufsicht über die Tätigkeit und Gefahren digitaler Vermittlungsdienste keinen Zielkonflikt, der wie im Fall des Datenschutzbeauftragten den unabhängigen Status der Aufsichtsbehörde rechtfertigen könnte. Das Regulierungsprogramm der Datenschutzbehörden betraf ursprünglich zum wesentlichen Teil staatliche Datenverarbeitungen. Es ging also darum, einen Teil der staatlichen Institutionen als Kontrollbehörde und Sachwalter individueller Datenschutzinteressen gegen die – politisch

67 Zum Konflikt um die Unabhängigkeit des Datenschutzbeauftragten s. EuGH v. 9.3.2010, C-518/07, Rn. 41 ff.

68 Zur Relevanz eines gesetzlich hinreichend klar umrissenen Auftrags BVerfGE 151, 202, Rn. 137 (mit Verweis auf EuGH v. 13.6.1958, C-9/56, *Meroni*, Slg. 1958, I-16).

beaufsichtigte und determinierte – staatliche Zweckverfolgung zu wenden.[69] Um dies zu gewährleisten, braucht es jedenfalls plausibler Weise politische Unabhängigkeit. Ein entsprechender Zielkonflikt und ähnliches Reibungspotential mit den Zwecksetzungen und Logiken einer politisch verantwortlichen Behörde ist im Fall der Digitale-Dienste-Koordinatoren nicht erkennbar. Durch den DSA-E wird schlicht ein bestimmter Dienstleistungszweig wegen bestimmter Risiken für gesellschaftliche und politische Prozesse einer besonderen staatlichen Regulierung unterworfen. Warum das nur mit unabhängigem Status funktionieren sollte, erschließt sich nicht. Im Gegenteil könnte eine *regulatory capture* bei unabhängigen Behörden, die nicht an den allgemeinen politischen Raum und damit an andere Einflüsse jenseits des regulierten Sachbereichs zurückgebunden sind, unter Umständen sogar wahrscheinlicher sein.[70] Eine Rückbindung der Diensteregulierung an die politische Ebene ist schließlich auch deshalb unerlässlich, weil der DSA-E die besonderen Gefährdungen des politischen, alle Bürgerinnen einer Demokratie angehenden Prozesses durch Geschäftsmodell und Tätigkeit digitaler Vermittlungsdienste einhegen soll. Der DSA-E ist – wie das NetzDG – eine Form politischer Selbstbehauptung demokratischer Öffentlichkeiten gegenüber einer spezifischen Marktlogik und neuen technischen Möglichkeiten. Was für diese Selbstbehauptung nötig ist, kann nicht neutral und unabhängig durch einen vermeintlich allwissenden Regulator bestimmt, sondern muss politisch ausgehandelt und umkämpft werden. Eben das wäre – jenseits auf Unionsebene äußerst schwerfälliger legislativer Steuerung – bei einem unabhängigen Status der neu zu schaffenden Regulierungsbehörde ausgeschlossen. Ebenso wenig wie sich demokratische Zustände und Institutionen herbeiregulieren lassen,[71] können grundlegende Gefährdungen demokratischer Öffentlichkeit apolitisch und allein technokratisch bewältigt werden. Es wäre schade und trübte das positive Gesamtbild, wenn dem Entwurf seine Sensibilität für Machtfragen, politischen Aushandlungsbedarf und den stets unfertigen und spannungsreichen Charakter öffentlicher Kommunikationsregulierung an dieser Stelle abhandenkäme.

---

69 Für diesen Hintergrund der gerichtlichen Unabhängigkeit s. Buchheim/Möllers (Fn. 45), Rn. 46.

70 In diese Richtung (ohne empirische Belege) auch Wren-Lewis, Regulatory Capture: Risks and Solutions, in: Estache (Hrsg.), Emerging Issues in Competition, Collusion, and Regulation of Networked Industries, 2011, Kap. 7, S. 12 f.

71 Möllers/Schneider, Demokratiesicherung in der Europäischen Union, 2018, S. 26 f. (in Hinblick auf neue Autoritarismen in einigen Mitgliedstaaten).

Die Datenschutz-Grundverordnung als demokratisches Level Playing Field?

Stefan Brink, Kira Vogt

Entwicklung des Datenschutzrechts in Europa

Das Sammeln ist ein Urbedürfnis der Menschen. Ebenso ist es ein Urbedürfnis, einmal gesammelte Dinge auch behalten zu wollen, wenn sie nicht getauscht oder verkauft werden. Zu erkennen, dass etwas nicht mehr gebraucht wird und sich davon zu trennen, fällt dagegen schwer. Daher verwundert es nicht, dass auch bei personenbezogenen Daten bislang häufig eine „Hamster-Mentalität" anzutreffen war - und es bis heute ist. Getreu dem Motto „Das könnte noch einmal nützlich werden, behalten wir mal vorsorglich die Daten." legten Einzelpersonen, aber auch Unternehmen und Staaten, eine regelrechte Datensammelwut an den Tag – was sich bitter rächte. Denn vom ungesteuerten Datensammeln bis zur Zweckentfremdung von Daten, die ja ohnehin schon mal da sind, ist es nur ein sehr kurzer Schritt. Der Blick auf dunkle Seiten von Europas Vergangenheit zeigt, wie leicht es ist, Daten für missbräuchliche Zwecke zu verwenden, wenn es keine Gesetze gibt, die dies verhindern. In den Niederlanden war etwa es zu Beginn des letzten Jahrhunderts üblich, ein Register aller Einwohner*innen zu erstellen, in dem unter anderem auch die Religionszugehörigkeit verzeichnet wurde. Als die Nationalsozialisten im zweiten Weltkrieg die Macht übernahmen, fiel es ihnen daher noch leichter als anderswo, Menschen jüdischen Glaubens zu identifizieren, in Konzentrationslager zu stecken und zu ermorden.[1] Vor der Wiederholung der Geschichte bewahrt uns – hoffentlich – auch das Menschenrecht Datenschutz.

Für die Einordnung der EU-Datenschutz-Grundverordnung als demokratisches Level playing field bedarf es zunächst der Betrachtung des Datenschutzes als Menschenrecht. Menschenrechte und Demokratie sind, jedenfalls in der europäischen Geschichte und Rechtstradition untrennbar miteinander verbunden. Nach dem Zweiten Weltkrieg war es zunächst

1 S. *Ehmann*, ZD 2021, 509, Fn. 31 m. w. N.

der Europarat, der in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) das Recht jeder Person auf Achtung des Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz statuierte. Vor der Einführung unionsrechtlicher Datenschutzbestimmungen war es ebenfalls der Europarat, der Anfang der 1980er Jahre mit der Konvention 108 das erste internationale, rechtliche bindende Übereinkommen im Bereich des Datenschutzes erzielte.[2] Daher ist es nicht verwunderlich, dass die ersten europäischen Urteile zum Datenschutz ebenfalls aus Straßburg stammen. Schon 1987 stellte der Europäische Gerichtshof für Menschenrechte fest, dass die Speicherung von Informationen über das Privatleben einer Person durch eine öffentliche Behörde einen Eingriff in das Recht aus Artikel 8 darstellt.[3] Dies gelte, wie er im Jahr 2000 klarstellte, unabhängig davon, ob die gespeicherten Daten später verwendet werden oder nicht.[4]

Während der EGMR den Schutz von Informationen in das Recht auf Privatleben hineinlas und dies bis heute tut, stellte das Bundesverfassungsgericht bereits 1983 neben das Allgemeine Persönlichkeitsrecht, das selbst keine einfachgesetzliche Ausprägung erfahren hatte, ein aus der Allgemeinen Handlungsfreiheit nach Artikel 2 Abs. 1 in Verbindung mit dem Recht auf Menschenwürde aus Artikel 1 Abs. 1 GG abgeleitetes „Recht auf informationelle Selbstbestimmung". Unter den Bedingungen der modernen Datenverarbeitung, so das Bundesverfassungsgericht im *Volkszählungsurteil*, wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten auf verfassungsgesetzlicher Ebene geleistet. Das Grundrecht gewährleiste insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[5]

In der Europäischen Union wurde neben dem Recht auf Privatleben in Artikel 7 der Charta der Grundrechte der Europäischen Union (GRCh) ganz ausdrücklich auch ein Recht auf Datenschutz aufgenommen. Gemäß Artikel 8 GRCh hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Dass der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht ist, betont auch Erwägungsgrund 1 der EU-Datenschutz-Grundverordnung (EU) 2016/679 (DS-GVO), seit dem 25. Mai 2018 geltende Nachfolgerin der Richtli-

2 Übereinkommen Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981.
3 EGMR, *Leander gegen Schweden*, Urteil vom 26. März 1987, Az. 9248/81 Rn. 48.
4 EGMR, *Amann gegen Schweiz*, Urteil vom 16. Februar 2000 (Große Kammer), Az. 27798/95, Rn. 69.
5 BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83, Rn. 147.

nie 95/46/EG. Dabei verfolgt die DS-GVO umfassend das Ziel der Wahrung von Demokratie und Rechtsstaatlichkeit in einer freiheitlichen Informationsgesellschaft.[6] Gemäß Erwägungsgrund 2 der DS-GVO sollten die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Die Datenschutz-Grundverordnung soll so zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen. Damit schafft die DS-GVO das Fundament für einen viel umfangreicheren digitalen Grundrechtsschutz in Europa, bei dem der Datenschutz mit weiteren Rechtsgebieten verzahnt werden muss.[7] Schon in Artikel 1 Abs. 1 der DS-GVO wird dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten der freie Verkehr solcher Daten an die Seite gestellt. Auch Erwägungsgrund 4 Satz 2 betont, dass das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht ist; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.

Betroffenenrechte

Der demokratische Ansatz der DS-GVO zeigt sich zuerst in der Ausgestaltung der Betroffenenrechte. Im Vergleich zur Vorgängerin, der Datenschutzrichtlinie, setzt die DS-GVO hier auf noch größere Partizipation der Betroffenen. Die Verfügungsgewalt über die eigenen Daten soll so weit wie möglich bei der betroffenen Person liegen bzw. dieser so schnell wie möglich wieder zurückgegeben werden.

Bester Beleg dafür ist Artikel 15 DS-GVO: Dieser normiert nicht nur, wie der Titel suggeriert, ein Recht auf Auskunft über die verarbeiteten Daten, sondern auch ein Recht auf Kopie. Gemäß Artikel 15 Abs. 1 DS-GVO können betroffene Personen zunächst eine Bestätigung des Verantwortlichen anfordern, ob dieser sie betreffende personenbezogene Daten verar-

6 *Weichert*, vorgänge Nr. 231/232, 147, 152.
7 *Weichert*, vorgänge Nr. 231/232, 147, 156.

beitet. Ist dies der Fall, haben sie ein Recht auf Auskunft über diese Daten und auf weitere Informationen wie die Zwecke, zu denen die Daten verarbeitet werden, und die Empfänger, gegenüber denen die Daten offengelegt worden sind oder zukünftig offengelegt werden. Während die Informationspflichten nach Artikel 13 und 14 DS-GVO Verantwortliche verpflichten, gewisse (abstrakte) Angaben im Zeitpunkt der Datenerhebung zur Verfügung zu stellen, erhalten Betroffene mit Artikel 15 DS-GVO die Möglichkeit, den Weg ihrer personenbezogenen Daten möglichst konkret nachzuvollziehen. Artikel 15 Abs. 3 DS-GVO gewährt zudem ein Recht auf Kopie der verarbeiteten Daten, die häufig auch in elektronischer Form, zum Beispiel zum (geschützten) Download, bereitgestellt werden kann. Mit diesem Anspruch haben Betroffene also das Recht, ihre Daten im Kontext der Verarbeitung zu sehen. Artikel 15 DS-GVO gibt Betroffenen damit den Schlüssel zur Schatztruhe der weiteren Betroffenenrechte in die Hand. Wenngleich alle Betroffenenrechte auch unabhängig voneinander geltend gemacht werden können und Betroffene nicht mit dem Auskunftsrecht starten müssen, ist dies in der Regel der sinnvollste Ausgangspunkt. Mithilfe des Auskunfts- und Kopierechts erhalten Betroffene den notwendigen Überblick zur besseren Einschätzung, ob ihre personenbezogenen Daten richtig sowie zweck- und rechtmäßig verarbeitet werden und ob eine Geltendmachung weiterer Betroffenenrechte sinnvoll erscheint.

Der oben angesprochene Aspekt der informationellen Selbstbestimmung spiegelt sich auch im Recht auf Löschung und Vergessenwerden des Artikels 17 DS-GVO wider. Wo das digital abrufbare Bild einer Person zum Teil wichtiger wird als das reale und wo dieses Bild nicht allein und im Laufe der Zeit sogar immer weniger von der betroffenen Person selbst bestimmt wird, soll Betroffenen damit das Bestimmungsrecht so weit wie möglich zurückgegeben werden.[8] In der Informationstechnologie herrschte lange die Auffassung vor, ein bestmöglicher Schutz vor Angriffen könne nur erreicht werden, wenn Daten weitestmöglich vor Zugriffen und Zerstörung geschützt würden. Dies führte dazu, dass etliche IT-Systeme gar nicht darauf ausgelegt waren, einzelne Datenfelder, aber auch ganze Datengruppen eines bestimmten Alters wieder zu löschen. Erst neuerdings setzt sich die Erkenntnis durch, dass Daten dann am besten vor Angriffen geschützt sind, wenn sie nicht mehr vorhanden sind. Bei Verzahnung der Grundsätze der Zweckbindung, Datenminimierung und Speicherbegrenzung (Artikel 5 Abs. 1 lit. b, c und d DS-GVO) ergibt sich genau dieses

8 S. BeckOK Datenschutzrecht, Wolff/Brink-*Worms*, 37. Edition vom 01.08.2021, Art. 17 Rn. 2.

Bild: Personenbezogene Daten dürfen nur, soweit für festgelegte Zwecke erforderlich, verarbeitet werden und grundsätzlich auch nur für diese Zeit in einer Form gespeichert werden, welche die Identifizierbarkeit der Betroffenen ermöglicht. Das Recht auf Löschung ergänzt diese Prinzipien, indem Betroffene die Löschung zusätzlich aktiv einfordern können. Erwägungsgrund 65 berücksichtigt dabei die hohe Schutzbedürftigkeit von Kindern und betont in Satz 3 das Recht auf Löschung insbesondere in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten – insbesondere die im Internet gespeicherten – später löschen möchte. Daher sollten Betroffene nach Satz 4 das Recht auch noch ausüben können, wenn sie keine Kinder mehr sind.

Neben dieser Rücksichtnahme auf besonders vulnerable Personen einerseits erkennt die DS-GVO andererseits auch, dass das Individuum nicht in jedem Fall im Vordergrund stehen sollte. Für den Erhalt einer Demokratie ist es unerlässlich, relevantes Wissen für die nachkommenden Generationen zu bewahren. Daher enthält die DS-GVO an mehreren Stellen Ausnahmen für (ausschließlich) im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke. Das Prinzip der Speicherbegrenzung nach Artikel 5 Abs. 1 lit. e DS-GVO gestattet für diese Fälle ein längeres Vorhalten personenbezogener Daten, sodass gemäß Artikel 17 Abs. 3 lit. d DS-GVO von der unverzüglichen Löschpflicht abgewichen werden. Selbstverständlich unterliegt die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person, wie Artikel 89 DS-GVO klarstellt. Eine solche Weiterverarbeitung personenbezogener Daten erfolgt nach Erwägungsgrund 156 Satz 3 erst dann, wenn der Verantwortliche geprüft hat, ob es möglich ist, diese Zwecke durch die Verarbeitung von personenbezogenen Daten, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, zu erfüllen, sofern geeignete Garantien bestehen. Als Öffnungsklausel gestattet Artikel 89 DS-GVO den Mitgliedstaaten die genauere Ausgestaltung. Von der Möglichkeit, die Betroffenenrechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung und Widerspruch zu beschränken, hat der deutsche Gesetzgeber für Forschungs- oder Statistikzwecke in § 27 Abs. 2 Bundesdatenschutzgesetz (BDSG) Gebrauch gemacht, jedoch nur unter der Bedingung, dass diese Rechte voraussichtlich die Verwirklichung Zwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Zweckerfüllung notwendig ist. Eine

entsprechende Regelung für die Beschränkung der Rechte auf Einschränkung der Verarbeitung und Widerspruch im Falle im öffentlichen Interesse liegender Archivzwecke findet sich in § 28 Abs. 4 BDSG. Die datenschutzrechtlichen Normen schaffen so eine Balance zwischen Individualrechtsschutz und dem Schutz von Kollektivgütern.

Artikel 20 DSGVO normiert darüber hinaus das Recht auf Datenübertragbarkeit. Danach hat die betroffene Person das Recht, sie betreffende personenbezogene Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format (zurück) zu erhalten, um diese Daten einem anderen Verantwortlichen ohne Behinderung durch den ersten Verantwortlichen zu übermitteln. Allerdings gilt dies nur bei automatisierten Verarbeitungen, deren Rechtsgrundlage eine Einwilligung oder ein Vertrag bildet. Wie Erwägungsgrund 68 erläutert, sollen Betroffene bei Verarbeitungen mit automatischen Mitteln so eine bessere Kontrolle über ihre Daten erhalten.

Absatz 2 sieht noch eine weitere Erleichterung vor. Danach kann die betroffene Person erwirken, dass die personenbezogenen Daten direkt von einem an den anderen Verantwortlichen übermittelt werden. Die großzügige Einschränkung „soweit dies technisch machbar ist", trägt jedoch leider dazu bei, dass Datenübertragbarkeit in der Praxis noch nicht weit verbreitet ist – schließlich sollen Verantwortliche nach Erwägungsgrund 68 Satz 2 lediglich dazu „aufgefordert werden", interoperable Formate zur Ermöglichung der Datenübertragbarkeit zu entwickeln. Hier wäre es hilfreich, schon die Hersteller in die Pflicht zu nehmen, um schnellere Fortschritte bei der Datenübertragbarkeit zu erreichen.

Durch dergestalt differenzierte und effektive Datenschutzrechte lässt die DS-GVO das angestrebte demokratische level playing field entstehen.

Verantwortlicher

Ein demokratisches level playing field setzt aber nicht nur differenzierte Betroffenenrechte voraus. Es kann nur effektiv werden, wenn es auf der Gegenseite auch die Verantwortlichen für die Datenverarbeitung in die Pflicht nimmt.

Genau das tut die DS-GVO in überzeugender Weise: Nach Artikel 5 Abs. 2 der EU-Datenschutz-Grundverordnung unterliegen verantwortliche Stellen, die personenbezogene Daten verarbeiten, einer Rechenschaftspflicht. Das bedeutet, dass sie jederzeit nachweisen können müssen, die Verordnung einzuhalten. Verantwortliche müssen sich also rechtfertigen können: Sie dürfen die Daten nur verarbeiten, wenn sie dafür eine Rechts-

grundlage haben (Grundsatz der Rechtmäßigkeit). Außerdem dürfen sie personenbezogene Daten grundsätzlich nur für den vorgesehenen Zweck verwenden (Grundsatz der Zweckbindung). Nach Artikel 4 Nr. 7 DS-GVO ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Begriff des Verantwortlichen ist dabei weit zu verstehen – auch dieses Verständnis ist wesentliche Grundlage für die Effektivität des Schutzes der Betroffenen. Laut Europäischem Gerichtshof ist zum Beispiel auch ein Petitionsausschuss insoweit als Verantwortlicher im Sinne der DS-GVO einzustufen, als er allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet.[9] Ein Betroffener hatte eine Petition beim Petitionsausschuss des Hessischen Landtags eingereicht und anschließend ein Auskunftsersuchen nach Artikel 15 DSGVO gestellt. Der Landtagspräsident lehnte den Auskunftsantrag mit der Begründung ab, dass das Petitionsverfahren eine parlamentarische Aufgabe sei und das betreffende Parlament nicht in den Anwendungsbereich der Verordnung 2016/679 falle.[10] Dabei ließ der EuGH offen, ob der Petitionsausschuss als „Behörde" oder „andere Stelle" im Sinne der Definition des Begriffs „Verantwortlicher" in Artikel 4 Nr. 7 DS-GVO anzusehen ist[11] – der Rechenschaftspflicht über die Einhaltung des Datenschutzes unterliegt der Petitionsausschuss in jedem Fall.

Grundsätzlich zielt die DS-GVO auf eine Gleichbehandlung aller verantwortlichen Stellen ab. Nur zum Teil sieht sie Erleichterungen für bestimmte Verantwortliche wie kleinere Unternehmen vor. Diese wirken sich in der Praxis jedoch nur zum kleinen Teil wirklich erleichternd aus. Nach Artikel 30 Abs. 5 DSGVO müssen die Verzeichnisse der Verarbeitungstätigkeiten nicht von Unternehmen oder Einrichtungen geführt werden, die weniger als 250 Personen beschäftigen – es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Abs. 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10. Vor allem die Rückausnahme der „nicht nur gelegentlich[en]" Verarbeitung

9 EuGH, Urteil vom 9. Juli 2020, Rs. C-272/19, Rn. 74.
10 EuGH, Urteil vom 9. Juli 2020, Rs. C-272/19, Rn. 19.
11 S. EuGH, Urteil vom 9. Juli 2020, Rs. C-272/19, Rn. 65, 73.

führt dazu, dass kleinere Unternehmen einen dem der großen nicht unähnlichen Aufwand betreiben müssen.

Ein demokratisches level playing field wird so geschaffen – ob dies immer auf verhältnismäßige Weise gelingt, sei dahingestellt.

Fehlende Herstellerhaftung

Um ein echtes „level playing field" darstellen zu können, fehlt es der Datenschutz-Grundverordnung derzeit daher noch an einer entscheidenden Voraussetzung: der Haftung nicht nur für die personenbezogene Daten verarbeitenden Verantwortlichen und Auftragsverarbeitern, sondern auch für diejenigen, die Datenverarbeitungsprogramme herstellen. Die in der DS-GVO aufgestellten Grundsätze *Data protection by design and default* sind derzeit nur dann ausreichend erfüllbar, wenn Unternehmen zum Beispiel bei der Erstellung eines Online-Formulars selbst entscheiden können, welche personenbezogenen Daten sie wirklich benötigen und eben auch nur diese abfragen bzw. abfragen lassen – oder jedenfalls eine Differenzierung zwischen Pflicht- und freiwilligen Datenfeldern nutzen. Möchte das verantwortliche Unternehmen dagegen Daten mithilfe eines altbekannten Programms oder auch einer neuen App erfassen, sind seine Möglichkeiten der Implementierung dieser Grundsätze wesentlich begrenzter. In Deutschland wird zwar zum Teil eine datenschutzrechtliche Herstellerbindung über den Umweg der deliktischen Produzentenhaftung § 823 Abs. 1 BGB erwogen: Wenngleich danach keine unmittelbare Pflicht bestehe, ein Produkt bereits in der Planungsphase datenschutzkonform auszugestalten, ließe sich eine den Grenzen der Zumutbarkeit unterliegende Herstellerpflicht begründen, nur solche Produkte in den Verkehr zu bringen, die datenschutzkonform nutzbar sind.[12] Solange aber nicht die DS-GVO den Datenschutz-Aufsichtsbehörden die Möglichkeit gibt, mithilfe (der Androhung) abschreckender Bußgelder und anderer Maßnahmen Herstellende in die Pflicht zu nehmen, wird sich dies weiterhin negativ auf die Schlagkraft des Datenschutzes auswirken.

12 *Specht-Riemenschneider*, MMR 2020, 73, 77.

Modell DS-GVO

In nicht wenigen Ländern dieser Erde ist das zu Beginn erwähnte umfassende Datensammeln bis heute anzutreffen – allen voran in China mit seinem Sozialkreditsystem. Dort führt unerwünschtes bis straffälliges Verhalten zu Punktabzug, während erwünschtes Verhalten den Punktestand erhöht. Dazu werden jedwede Daten verwendet, auf welche die Regierung durch Videoüberwachung mit Gesichtserkennung oder Analyse von Internetnutzungsverhalten dank Übermittlung der Daten durch chinesische Internetriesen zugreifen kann.[13]

Der Blick über die Grenzen Europas hinaus zeigt aber auch, dass demokratische Ansätze nicht nur datenschutzrechtlichen Parlamentsgesetzen inhärent sein können. So findet der California Consumer Privacy Act (CCPA) seinen Ursprung sogar in einer basisdemokratischen Volksabstimmung.[14]

Die Vorteile einer Stärkung des Datenschutzes haben auch andere Länder erkannt. Darauf reagiert auch die DS-GVO, indem sie vergleichbares Datenschutzniveau weltweit anerkennt. Nach Angemessenheitsbeschlüssen für Argentinien, Japan, Kanada und weitere Staaten[15] hat die EU-Kommission im Sommer 2021 das Verfahren zur Annahme des Angemessenheitsbeschlusses für die Republik Korea eingeleitet.[16] Mit den Angemessenheitsbeschlüssen soll nach Artikel 45 der DS-GVO in den jeweiligen Staaten ein mit dem der EU vergleichbares Schutzniveau für personenbezogene Daten aus der Europäischen Union bescheinigt werden. Die endgültige Überprüfung solcher Beschlüsse obliegt dem Europäischen Gerichtshof. Mit den Urteilen gegen das Safe-Harbor-Abkommen[17] und das EU/US-Privacy-Shield[18] hat dieser bereits zwei Angemessenheits-beschlüsse für die USA gekippt. Dennoch stellen Angemessenheitsbeschlüsse aus Sicht der Datenexporteure und -importeure die einfachste Möglichkeit der Datenübermittlung dar. In derartigen Fällen dürfen personenbezogene Da-

13 *Wagner*, ZD 2020, 140, 141.
14 *Botta*, DSRITB 2019, 657, 660.
15 Die Liste der Drittländer mit Angemessenheitsbeschlüssen veröffentlicht die EU-Kommission unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.
16 S. Pressemitteilung der Europäischen Kommission vom 16. Juni 2021, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/ip_21_2964.
17 EuGH, Urteil vom 6. Oktober 2015, Rs. C-362/14 (*Schrems I*).
18 EuGH, Urteil vom 16. Juli 2020, Rs. C-311/18 (*Schrems II*).

ten nämlich, wie Erwägungsgrund 103 Satz 2 erläutert, ohne weitere Genehmigung aus Europa an dieses Land übermittelt werden.

Nicht zuletzt aufgrund des Erlasses neuer Datenschutzgesetze, die zu großen Teilen als Abbild der DS-GVO modelliert sind, sowie der Einrichtung neuer Datenschutz-Aufsichtsbehörden zählen dadurch immer mehr Staaten zu den sogenannten „sicheren Drittländern" – und erweitern das menschenrechtliche level playing field.

Fazit

Die DS-GVO erschafft ein demokratisches level playing field, indem sie alle betroffenen Bürgerinnen und Bürger mit differenzierten Rechten hinsichtlich ihrer personenbezogenen Daten ausstattet, gleichzeitig die Verantwortlichen (mit Ausnahme der Hersteller) effektiv in die Pflicht nimmt und ihre Wirkung auch im außereuropäischen Bereich entfaltet. Auch wenn die DS-GVO dabei durchaus als Modell dienen kann, wird sie in den kommenden Jahren der Weiterentwicklung bedürfen, um mit dem digitalen Fortschritt mithalten zu können.

Polarization Presidentialism.
How social media reshaped Brazilian politics: a case study on the 2018 elections

Marco Ruediger[1], Amaro Grassi[2]

1. Introduction[3, 4]

The Brazilian 2018 Elections were, in several ways, a landmark in the political history of the country, reshaping many relatively consensual beliefs on how the campaigns and open public discussions traditionally unfold – at least within the current democratic regime, dating back to the democratic transition in 1985 and the 1988 Constitution. The election that brought to power the self-described outsider and far-right president, Jair Bolsonaro, as well as unexpected names to govern some of the most important states such as Minas Gerais and Rio de Janeiro, was also – we could say – the first "digital election" in the country. In it, social media not only played a significant role, but also became perhaps the most important resource to

---

1 PhD in Sociology, Director of the Department of Public Policy Analysis (FGV DAPP) and of the Communications, Media and Information School of Fundação Getulio Vargas (FGV ECMI).

2 PhD Candidate in Political Science, Research and Project Coordinator at FGV DAPP.

3 This article uses extensive social media data collected during the experience of the Digital Democracy Room - #observa2018, a 100 days monitoring of 2018 election in Brazil, that can be accessed at observa2018.dapp.fgv.br/en. The authors thank all the researchers that took part of it, bringing together an incredibly diverse team of scholars from different fields, which made possible to address the extremely challenging and innovative objectives it was created for: Ana Celia Guarnieri, Ana Freitas, Ana Guedes, Andressa Contarato, Bárbara Silva, Beatriz Franco, Beatriz Meirelles, Dalby Dienstbach, Danielle Sanches, Danilo Silva, Felipe Cruz, Flávio Costa, Gabriela Lapadula, Janderson Pereira, Júlia Faber, Kimberly Anastacio, Letícia Lopes, Lucas Calil, Lucas Roberto da Silva, Luis Gomes, Mônica Braga, Rachel Bastos, Polyana Barboza, Tatiana Ruediger, Thais Lobo, Thamyres Dias, Wagner Oliveira, Yasmin Curzi.

4 The opinions expressed represent exclusively the opinions of the authors and not necessarily the institutional position of FGV.

the political dispute, outpacing the TV and regional alliances as the main force in the race. Therefore, it is not an overstatement to imply that social media reshaped Brazilian politics, both in the (growingly digital) public sphere and in the political system.

In 2014, Ruediger, Souza, Luz and Grassi (2014) showed how the 2013 June Journeys had generated a "conflict perspective" to the public discussion, in opposition to a widely consensus-based agenda that had organized Brazilian politics during more than two decades after the constitutional process. This was largely due to the transformations the digital revolution had generated, bringing several new actors to the scene, with new resources for social mobilization and collective action. It was the inauguration of a completely new chapter in our recent history, starting a wave of mass protests that would arise again in 2015 and 2016, culminating with the impeachment of then President Dilma Rousseff. It took no more than a few years after that for the aftershock of those profound transformations to hit the institutional structure that allowed Brazil to reach its most recent years of prosperity. Then, the democratization of social media became a game changer, an extremely powerful toolbox that political actors were still trying to find out how to explore in its full capacity.

The storm that was forming on the horizon could be anticipated, in part, by the astonishing impact of social media in two political events of global dimensions in 2016: the Brexit referendum in the UK and the election of President Donald Trump in the US. Both events shed light, in a radical way, on how the misuse of digital resources could potentially disrupt democratic regimes and hurt the informational environment in our societies. Disinformation and fake news rapidly became popular terms, repeatedly used on political discourses – even by those who perpetrated them the most efficiently in the digital environment. Of course, things would not be different in Brazil, especially after the events that had developed in the past few years and the disruption they were causing in the political system – even though several political analysts and experienced politicians still doubted it could change the way elections were conducted in the country.

In 2018, we at the Department of Public Policy Analysis in Fundação Getulio Vargas (FGV DAPP) designed the Digital Democracy Room, an effort to monitor the general elections based on the assumption that we were about to see the most disruptive political process in Brazilian history, with the huge impact of social media and the culmination of social processes we had been watching since the 2013 June Journeys. The events that developed throughout that year could not have had a bigger impact: the arrival of the fake news era in Brazil, the downfall of traditional TV-based

(and hugely expensive) campaigns and the rise of social media, and an intense public debate on the most relevant topics for Brazilians. Together, these factors made that year a once-in-an-era political earthquake. The election of President Jair Bolsonaro retired several of the most prominent politicians from the last 30 years, based on a novel structure of digital campaign with massive use of Facebook, Youtube and, for the first time in a large scale, Whatsapp. This brought to power not only a new political group which had been marginalized for the past quarter of century, but also a new way of governing.

Since the end of 1980s, when Abranches (1988) suggested that the Brazilian political system could be better described as a Coalition Presidentialism (a presidential system with a coalition-like governing with the National Congress), it became the most used concept by researchers, journalists and political analysts to make sense of the relationship between the Executive and Legislative branches. The pursuit of a stable coalition in the Congress was the lighthouse that oriented the elected presidents, organizing how the government was run and defining the next electoral cycle. However, the 2018 election subverted that logic, giving room to a model most resembling a "Polarization Presidentialism" – a system where the most important asset for a candidate (and for a President) is the capacity to polarize the public opinion, particularly through the extensive use of digital strategies, exploring the most divisive issues in society and fostering anti-establishment sentiments.

We will see that the 2018 election developed into a competition for more engagement inside a massive echo chamber, reinforcing the algorithmic logic of delivering the content people really engaged with. The huge reach of Facebook and an unknown number (certainly hundreds of thousands, perhaps millions) of WhatsApp groups were the perfect space to disseminate videos, campaigning ads and lots of anonymous, fake content, using bots. In other words, these spaces were used to foster political narratives different from the traditional means of political discussion, relying on a digital environments almost completely unregulated by electoral authorities and with the non-interference approach employed by most of the time-oriented social media platforms. Polarization became the rule for politicians, defining a logic of political confrontation that would go beyond the election itself and define the parameter for governing after that – the never-ending promotion of division, confrontation and extremism, pursuing engagement first, as a sign of strength that would enable a better position to negotiate the agenda with other political actors in Congress and with state governors.

In this article, we present a selection of data and analyses on how the 2018 election unfolded in social media, based on the Digital Democracy Room, enabling a better understanding of the general environment that reshaped Brazilian politics – first in the electoral campaign, but also after that, with a governing strategy of polarization and extensive use of digital resources to defeat traditional communication channels. "Polarization Presidentialism" turned into the main target of political extremism in what would become the main characteristic of the relationship between the Executive, Legislative, and increasingly the Judiciary branch. In the end, we point out a few general trends observed in subsequent years that may help prepare for the main challenges, but also opportunities, for the Brazilian digital democracy.

2. *Heading to election, the impact of "fake news"*

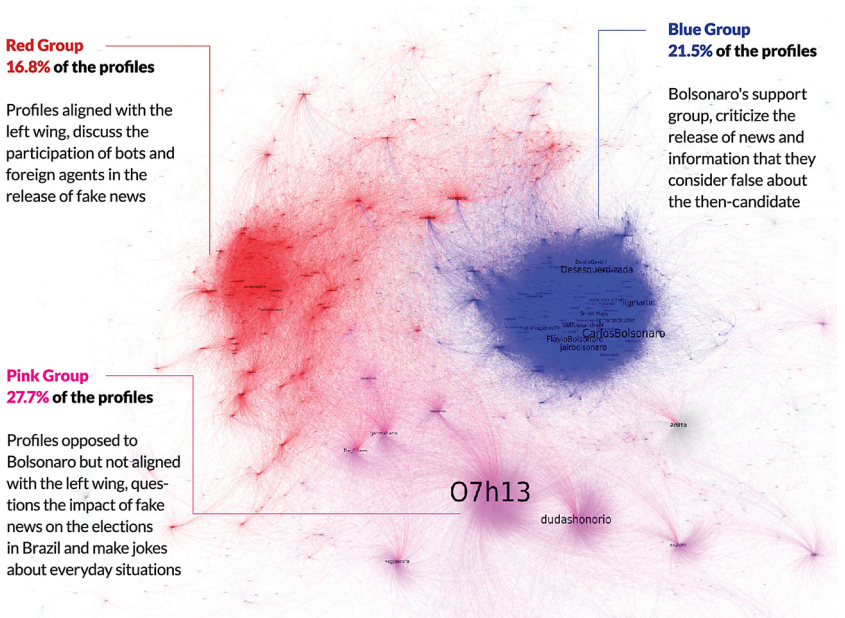
In Brazil's 2018 electoral cycle, the dissemination of fake news in different public and private social networks, as well as the public debate on the web about the emergence of the fake news phenomenon as a political marketing and disinformation tool, played an unprecedented role in the country. With the different sides of the Brazilian political scenario questioning or reiterating information, news articles, memes and publications as false or true (from their respective points of view), with no consensus or widely accepted sources, any potential dialogue between adversaries became very fragile from the beggining, and so did the ability of the traditional press to operate as an interlocutor between adversaries.

Towards the end of the electoral calendar, with the ramifications of the campaigns and the release of news articles about the use of social networks to produce content with no legitimacy – especially WhatsApp –, the protagonism of disinformation in politics became more evident for the Brazilian civil society. However, even before the official start of the campaigns, fake news were already present in the public debate as topics of discussion, following the impact and repercussion they obtained in other recent electoral races, such as in France, Germany, the UK and especially the US – where the use of the term by Donald Trump expanded the concept of "fake news" internationally in the threads of online conversation and as a topic of public interest.

Between August 1st and 15th – the last 15 days before the official electoral campaign –, we analyzed 387.9 thousand publications on Twitter about the dissemination of fake news; among those, there were 206.6 thousand retweets, which compose the following map of interactions. At

this moment in the debate, the main groups of the general political debate in the country remained as protagonists: the red group, with profiles supporting candidates from center-left (PT) and left-wing (PCdoB) parties; the pink group, with critical or comic discussions usually opposing the right-wing candidacy of the PSL, but with no alignment to any party; and the blue group, which supported the PSL and proved to be very cohesive, active and articulated through the voices of specific and established influencers of the network environment.

Fig. 1 - Map of interactions in the debate about fake news before the electoral period
206.574 retweets | Analysis date: August 1st to August 15th



Source: Twitter | Elaborated by: FGV DAPP

Although it garnered the highest number of profiles in this graph (27.7% of the total), the pink group, the only major group in the political map of the networks which moved away from the left/right polarization, mobilized the least interactions about fake news, which accounted for only 17% of their retweets. The group was organized around tweets that approached the topic of disinformation in a non-polarized way, often jokingly. A common meme used by the group, for example, is the phrase "the biggest

fake news this year was...", which was completed by users with different themes, such as relationships, job interviews and diets, among other non-political topics; an appropriation of the debate for the ironic discussion of everyday life topics.

The group supporting the PSL candidate was the second with the highest number of profiles, garnering 21.5% of the total number of users present in the map of interactions and mobilizing the most interactions (47.4%). Then-candidate Jair Bolsonaro, his sons Flávio and Carlos, and comedian Danilo Gentili were the main influencers in the group, whose main narrative line was the idea that the candidate was a victim of a fake news "factory", which supposedly involved traditional media outlets.

The suspension of pages and profiles appeared in the blue group in complaint posts and was seen as a sabotage of the PSL campaign. However, some of the users stated that the candidate would be able to fight this "persecution", while other profiles pointed out a "narrative" construed by the left wing to disqualify a potential victory of a right-wing candidate. According to them, the adversaries would attribute the victory to a "false" dissemination of fake news by the congressman.

The red group was as polarized as the blue group, but much less cohesive due to the presence of some profiles; it accounted for 16.8% of the profiles and 19.9% of the interactions registered in the map. The main influencers in this group were Dilma Rousseff and Lula. The discussion about the use of automated accounts associated with the spread of fake news was the biggest highlight in this group, which often reinforced the idea of a supposed interference of bots from foreign countries in the political debate.

The group frequently shared fact checking initiatives done by agencies or by the traditional media. However, the media in general was frequently criticized; similarly to what happened in the blue group, it was accused of producing fake news, although the red group defends that these news were intended to demoralize political actors from the left wing and the center-left. Other pre-candidates could also be found in this group, especially due to their publications associating the right wing with fake news.

3. The election, campaigning in digital environments

Social networks became the axis of political discussion in the 2018 presidential campaign, with the impact of disinformation as a central theme. Analyses indicated a massive use of these strategies in all political fields.

They used different procedures of virtual campaigning, and automated accounts and fake news were identified on Twitter, Facebook and YouTube.

3.1. *The reach of fake news*

In the final weeks of the electoral race, we analyzed references to the main pieces of fake news on open social networks – Twitter, Facebook and YouTube – between September 22nd and October 21st, in order to measure the reach they obtained in each platform and what was the network's response to the content – that is, whether they were subjected to fact-checking and the refuted facts shared, or the false information continued to have an impact after appearing on the web.

Among the pieces of fake news, the supposed fraud in the electronic voting machines was mentioned the most on Twitter: there were 1.1 million tweets about the alleged lack of security of the devices, with posts requesting a return of printed voting and reporting "errors" that were supposedly seen by electors in the first round. The so-called "gay kit" also mobilized around 1 million references on the network. The posts spread the fake news that Fernando Haddad, during his administration of the Ministry of Education, supposedly authorized the creation of the material. The third piece of fake news with the most mentions on Twitter – with a much less significant volume of references – was related to lies about one of the books published by the PT candidate: "In defense of socialism". There were 48.7 thousand references.

False publications associated with the right wing had a more limited reach. Speculation about the candidate having "simulated" an attack against himself in order to disguise a cancer surgery was the most mobilized rumor in the period, with 34.6 thousand references. The change of Brazil's patron saint, falsely spread as if proposed by the candidate, was mentioned 16.7 thousand times. An article stating that a right-wing candidate was the most honest politician in the world had 6.5 thousand mentions.

3.2. *Fact-checking*

Analyses by FGV DAPP in partnership with the fact-checking agency Lupa demonstrated that at least three pieces of fake news figured among the links with the most engagement on social networks in few months. In

the repercussion of the first presidential debate, a news piece stating that Twitter supposedly removed hashtags in support of one of the candidates had almost 13 thousand interactions on Facebook, figuring among the ten major links. On Twitter, there were 32 thousand references to the supposed "takedown"[5].

News pieces stating that the traditional Veja magazine supposedly received R$ 600 million to defame the PSL campaign also had large repercussion on the networks. Since September 24, when the rumor started, 16 links about the case were identified, mobilizing 117.6 thousand interactions on Facebook and Twitter, and none of those links came from traditional media outlets.

An analysis of the news pieces with the most engagement on the social networks and the demonstrations by the two movements organized to oppose and support the right wing, which took to the streets in Brazil and in dozens of cities around the world on September 29 and 30, also indicated a significant presence of disinformation. The most frequently shared link on Facebook and Twitter in the period between September 28 and October 1st, with 182.6 thousand interactions, was a news article published by the newspaper O Estado de S. Paulo in February, 2017, about the occupation of the public square Largo da Batata by carnival goers. As reported by the newspaper itself, the false affirmations circulating on WhatsApp and other social networks stating that images used in news articles about the act organized by the left at Largo do Batata, in São Paulo, on Saturday were "actually carnival images".

3.3. Suspicions and discussions about the electoral process

The elections were also the target of disputes and different narratives, one of which was the suspicion of fraud in the vote results – anticipating a narrative that would develop continuously in following years. Some episodes were crucial in the mobilization of that debate, such as the suspension of the implementation of a printed voting system by the Supreme Federal Court on June 6 and the denial of former President Lula's candidacy.

5 Together, FGV DAPP and Agência Lupa checked whether the supposed removal of mentions to the presidential candidate Jair Bolsonaro was true or false. Available at: https://piaui.folha.uol.com.br/lupa/2018/08/10/verificamos-twitter-nao-removeu-mencoes-bolsonaro-durante-debate-na-band/. Accessed on: January 15, 2019.

In one month, from August 19 to September 18, suspicions about the integrity of the elections mobilized 841,800 mentions on Twitter. The debates were polarized between at least two lines: one questioned an electoral process with the absence of a candidate from a leftist party; the other questioned the reliability of the electronic voting machines and of the whole process surrounding the race. The peak of debate happened on August 29, with around 205 thousand tweets about the topic after a GloboNews interview with one of the candidates, in which the presidential candidate stated that he did not believe in electoral polls.

The mentions associating Lula's denied candidacy with a potential fraud in the elections were more intense in August, especially in repercussion to the note issued by the UN Human Rights Committee recommending that Brazil allowed the former president's candidacy. The hashtag #eleiçãosemlulaéfraude ("elections without Lula are a fraud") garnered majority of the mentions.

In turn, other comments referenced the allegations of adulterated electronic voting machines in previous elections and a statement in which he attributed his potential loss in October to fraud in the voting system. A video released by a candidate in his Facebook page, in which he spoke about the possibility of fraud in the elections, prompted more than 470 thousand comments.

3.4. Bots and disinformation

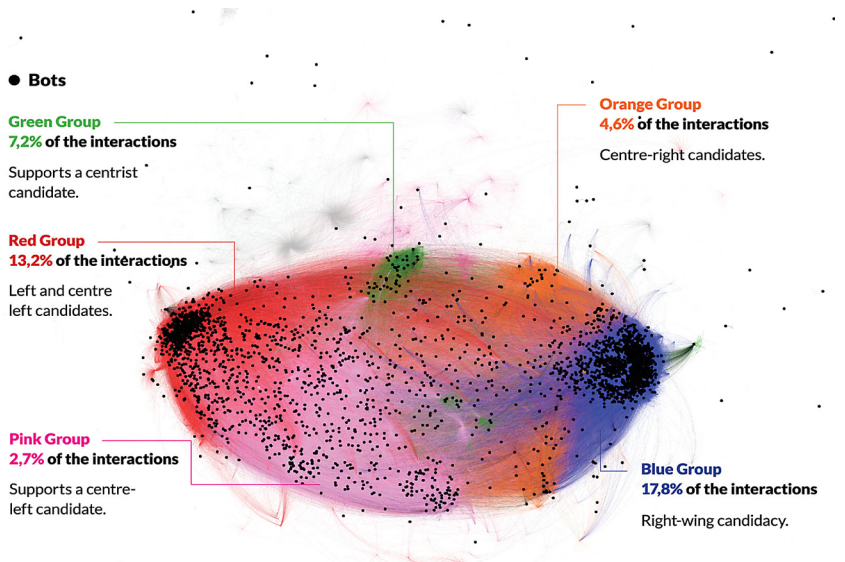
FGV DAPP carried out daily analyses on the presence of automated accounts in the electoral debate. Beginning on September 6, we observed an increase in the percentage of interactions (retweets) prompted by bots in the discussions about the presidential candidates, which remained above 10% every week in September. The absolute volume also increased, reaching 3,258 accounts on September 27, despite the efforts made by the platform.

The expansion of the interference of automated profiles with the political debate coincided with the approximation of the first round and with the revival of the "useful vote" concept as an argument of persuasion and recruitment of followers and influence on the social networks.

The interferences caused by bots often happened in an articulated and synchronized way through botnets. In the pre-campaign period, at least three botnets were responsible for publishing 1,589 tweets in one week. In general, those messages sought to propel and/or demobilize candidacies, especially inside the most polarized groups: PSL-PT.

We must clarify that the presence of bots in any discussion group (or in positive or negative interactions about political parties and political actors) does not necessarily signify an intentional action by the campaigns or these actors in conducting disinformation strategies. The research developed by FGV DAPP does not aim to attribute the coordination of digital actions of content automation on social networks to citizens, governments or business entities.

Fig. 2 - Map of interactions with bots about the presidential candidates 5,285,575 retweets | Analysis date: September 12th to September 18th



Source: Twitter | Elaborated by: FGV DAPP

The pro-right and pro-left support groups also presented most of the bot interference in the campaign period. For example, we collected 7,465,611 tweets and 5,285,575 retweets regarding the candidates from September 12 to 18. Inside this database, FGV DAPP's bot detection methodology found 3,198 automated accounts, which prompted 681,980 interactions – 12.9% of the total amount of retweets in the figure below.

Pictured on the right side of the figure, automated accounts were responsible for 17.8% of the retweets in the group; on the other side, the

interactions aligned with left and center-left candidacies accounted for 13.2% of the retweets.

However, in moments of more organic debate, such as the mobilization of the hashtag #elenão ("not him") – which originated in a women's movement on social media and later expanded online, with references by supporters and artists –, the opposite happened. Between September 12 and 24, while more than 73 thousand users retweeted about the theme, only 164 automated accounts did so as well, representing 0.22% of the debate.

In the period analyzed, we did not identify any automated mass distribution of fake news. Disinformation was present throughout the electoral race, but bots were not the biggest responsible for its dissemination. In the week of the knife attack[6] against Bolsonaro, for example, the biggest interaction group in the debate (64.4% of the total number of profiles), which was also the most organic one (with only 0.9% automated interactions coming from bots), concentrated the largest part of profiles who were suspicious about the veracity of the episode.

3.5 The role of Youtube

The campaign in the second round of the presidential elections has consolidated YouTube as a place for political clashes. In one week, from October 8 to 15, we identified 991 videos about the candidates in the race, Fernando Haddad and Jair Bolsonaro. That volume is higher than that registered in all the three previous months together (from July 4 to October 7), when 939 videos were shared. The publications, which had a variety of contents, formats and target audiences, generated 118 million views and were centered on Jair Bolsonaro; he was present in 63% of the views.

There were 498 videos with references to Bolsonaro, most of them (48%) with positive comments about his performance in interviews and/or debates, as well as support for his candidacy in the second round. The negative videos (15%) criticize Bolsonaro's behavior and the agendas he defends.

6 Then candidate Jair Bolsonaro was stabbed in the stomach during a campaign activity in the city of Juiz de Fora, state of Minas Gerais, an episode considered by many analysts a central chapter of his rising in the polls during the last month of the election.

Regarding Fernando Haddad, there were 488 videos mentioning his name directly, often with a critical tone (50%). The negative videos dismantled the proposals and personality of Haddad and his vice president, Manuela D'Ávila, also talking about PT, communism and anti-Christianism as negative aspects. The positive mentions (18%) defended him against supposed fake news, demonstrated support for the maintenance of democracy and showed fragments of the party's TV program and the campaign jingles.

3.6 Whatsapp, the "blind spot"

At the final stage of the second round campaign, WhatsApp became the main topic of debate about the presidential candidates, with notable impact on the discussion on other social networks – which signal the most relevant trends and agendas in the country's political discussion via web. The app is always present in the discussions on Twitter and its repercussion as an electoral topic has been growing; from October 1 to October 21, there were 2.57 million references to WhatsApp on the network, 1.57 million of which happened since the 15th.

The debate about the app started to increase on Twitter in the beginning of October, just before the first round. Until then, the topics of discussion were the impact of message chains and private groups on the dissemination of fake news and data, with a strong ironic tone directed to users who believed blindly in the content that they received and made voting decisions based on unverified information.

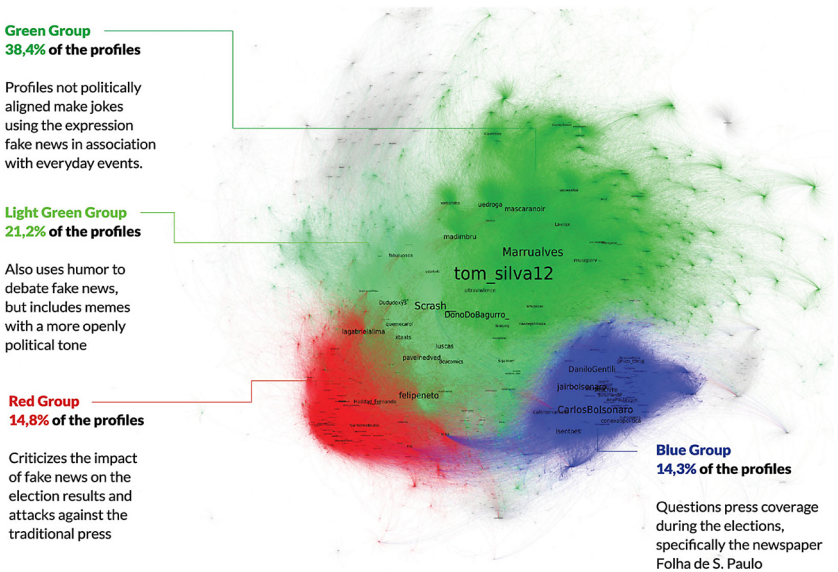
4. The after election

After the result of the elections, from October 29 to November 12, the debate about fake news gained a new contour and increased in volume significantly, with 1,444,369 tweets identified, of which 1,026,306 were retweets – five times more than in the two weeks before the start of the electoral campaign. The group with the biggest number of profiles on the network in this period was the green one, with 38.4%, and accounting for the second highest number of interactions (25.9%).

This group maintained discursive and thematic similarities with the pink group (which was predominant in the pre-campaign period) and contained publications using the term fake news jokingly on the network.

The appropriation of the expression "fake news" as slang, incorporated to everyday vocabulary, was a phenomenon already observed before the electoral race; after the elections, the green group resumed the satire "the biggest fake news this year", which had been used in situations of personal frustration since the beginning of August. In general, what differs the green groups from the pink one is the more explicitly comic contour of their internal debates, with less subgroups that use the expression "fake news" in a "literal" and critical sense.

Fig. 3 - Map of interactions in the debate about fake news after the elections 1,026,306 retweets | Analysis date: October 29th to November 13th



Source: Twitter | Elaborated by: FGV DAPP

The blue group garnered the highest number of total interactions (29%, with 14.3% of the profiles). The red group was the third in total interactions (20.5%, with 14.8% of the profiles) and concentrated its publications on opposing the president-elect and supporting press outlets, integrating politicians and actors aligned with left-wing parties, as well as influencers from other areas of the political spectrum who were opposed to right-wing candidates.

The blue group produced attacks against the press and to the left wing, criticizing the newspaper Folha de S. Paulo and stating that the media has published false information about him. Comedian Danilo Gentili stated that the Folha de S. Paulo lied when saying that it was denied access at a press conference during the electoral campaign. Due to the acts of these influencers, who are very strong in the blue group, the attacks against the newspaper were highly significant in this part of the debate about fake news, which materialized in the dissemination of several hashtags, such as #folhafakenews and #folhafalhamasnaoemplaca (roughly translated as "the Folha fails and does not make an impression").

In turn, the red group criticized the manipulation of information and stated it was a decisive factor for the elections. The "gay kit" topic became a highlight as an example of a paradigm of the effect of disinformation on the outcome of the electoral race. In addition, profiles in the group called attention to the use of WhatsApp to spread of fake news, which they argue was done strategically by candidates. Lastly, they also criticized the low effectiveness of the Superior Electoral Court in combating disinformation on the network. The clashes with the press – especially with the Folha de S. Paulo – are a reason for concern in this group.

Differently from the map of interactions in the period before the official campaign, a fourth highlighted group was established, with smaller expression in the total interactions (16.7%), but with the second highest number of profiles (21.2%), in light green. This group also had a comic tone regarding the use of expressions associated with fake news, and the main topic in this group was the spread of more critical memes (with more open political association) than the ones present in the green group.

5. What to expect

In retrospect, the timeline described in the sections above portrays an election that clearly represented a breakthrough regarding the electoral process in the previous 30 years in Brazil. It culminated a process initiated back in 2013, with the mass demonstrations all over the country, which were organized mostly through social media and surfaced an entirely new agenda of social demands from recently arrived groups in the public scene. During the following years, Brazilians experienced a spiral of political instability that relied heavily on street demonstrations and massive demonstrations of dissatisfaction through the social media, absorbing a broad sentiment of frustration with the economic crisis, corruption scandals and deep distrust

in political institutions and the old school politicians that had led the country during almost three decades.

It should not be a surprise that this process culminated in the next election – but it still was, at least for several politicians, journalists and political analysts. The electoral process that brought to power President Jair Bolsonaro, a self-proclaimed outsider and far-right politician, showed that social media had become not only a tool for political communication, but also the primary space where people informed themselves to decide on who to vote. It is for that reason that the candidate that consistently led the digital campaign – even when he was still behind in the polls – was the winner, bringing with him several other candidates for the Congress and in the states.

The observation of the digital public debate also clearly demonstrated the main issues that were driving the winning message, especially corruption, unemployment and public security (a growing concern for Brazilians not only in big cities, but also in the smaller towns). On the other hand, voters became totally exposed to the widespread disinformation strategies that were used by political campaigns, turning into easy targets in an almost completely unregulated digital information space. Social media became the game changer of Brazilian politics.

Nevertheless, this was not the final stop of the general process of reshaping Brazilian politics. Since then, the governing activity has increasingly turned into a constant dispute of narratives in digital environments, the unstopping creation of events to be posted, live streamed and disseminated through all the possible channels, mobilizing a mass of supporters in a 24/7 basis in order to keep the pressure on public opinion, the press, the Congress and the legal system. The following year of 2019 showed a glimpse of what would become a true narrative war on the digital space and the main strategy during the Covid-19 pandemic just a few months later. Polarization Presidentialism, a constant pursuit of division to foster engagement in an algorithmic-like logic, became the key element to understand the actions of the government, having social media as the absolute central piece in its political strategy.

The unfolding of this process is still not totally clear for the following years and the 2022 general election in Brazil, but it is certain that the role of social media in Brazilian politics (just as practically all over the world) is at a point of no return. Of course, Polarization Presidentialism will face the challenge of having stressed its relationship with the institutions too much, with damaging consequences for the economy and public administration, which could probably lead a future government to take a step

back in the confrontation and in the permanent pursuit of likes, views and shares in all social media platforms.

An evolving public discussion (as well as the growing pressure from governments towards social media) is also changing the general environment of the digital space, prompting more action from the companies or stronger regulations otherwise, as is the case in Brazil with the tightening grip of the legal system on the engineering of disinformation and the Fake News Law currently under discussion in the Congress. The challenges posed by social media to democracies, such as the spread of hate speech or a growing inequality in access to digital services, also come with several opportunities for a "digital democracy building", a development process in which the principles of democracy can be enhanced by governments and society, instead of threatened by it.

References

ABRANCHES, S. Presidencialismo de Coalizão: O Dilema Institucional Brasileiro. Dados Revista Ciências Sociais, Rio de Janeiro. vol 31, 1988.

RUEDIGER, M.A. (Coord.). Bots, social networks and politics in Brazil: A study on illegitimate interferences with the public debate on the web, risks to the democracy and the 2018 elections. Rio de Janeiro: FGV, DAPP, 2017 a.

RUEDIGER, M.A. (Coord.). Not so simple: the challenge of monitoring public policies on social networks. Reference Textbook on Methodology 1. 2nd edition. Rio de Janeiro: FGV DAPP, 2017 b.

RUEDIGER, M.; SOUZA, R.M..; LUZ, M.; GRASSI, A. Ação Coletiva e Polarização na Sociedade em Rede: Para uma Teoria do Conflito no Brasil Contemporâneo. Revista Brasileira de Sociologia, v. 02, p. 205-234, 2015.

Die Transformation der Haftung der Intermediäre in Brasilien: zwischen Öffentlichkeit und Privatheit

Ricardo Campos

1. Einführung

Niklas Luhmann beginnt sein Buch über die Realität der Massenmedien mit einem Satz, der genau illustriert, wie die soziale Kommunikation im Körper der Gesellschaft abläuft: „Was wir über unsere Gesellschaft, ja über die Welt, in der wir leben, wissen, wissen wir durch die Massenmedien."[1] Fast dreißig Jahre später können wir ohne Gegenargumente feststellen, dass die Repräsentation der öffentlichen Sphäre in den digitalen Diensten heute zentraler ist als in den traditionellen Massenmedien, und zwar auch durch die Konvergenz der alten Medien mit dem digitalen Medium. In diesem Sinne könnten wir die Luhmannsche Formulierung wie folgt umschreiben: „Was wir über unsere Gesellschaft, ja über die Welt, in der wir leben, wissen, wissen wir durch die digitalen Medien."

Dies sollte der Ausgangspunkt für jeden Ansatz sein, der sich mit der Moderation von Inhalten auf digitalen Plattformen und ihren positiven und negativen Auswirkungen befasst. Vor allem sollte das der Ausgangspunkt sein für die zentrale Frage, welches die beste rechtliche Regelung für die Haftung von Internetvermittlern ist. Hierbei ist zu bedenken, dass die Moderation von Inhalten erst dann zu einem neuen Thema wird, wenn es zu einer Entkopplung der Inhaltsproduktion und Moderation durch Organisationen mit redaktioneller Arbeit von den alten Massenmedien kommt. Während früher professionelle journalistische Standards, die an den Organisationsplan der Fernseh-, Radio- und Zeitungsmedien gebunden waren, den Rahmen vorgaben für die Produktion der Inhalte, die in der Gesellschaft zirkulierten, stellt sich jetzt, mit dem neuen Medium Internet und der Konvergenz der alten Medien mit dem digitalen Medium, die Frage, wie die im öffentlichen Raum zirkulierenden Inhalte von privaten digitalen Diensten kuratiert werden.[2]

---

1 *Niklas Luhmann*, Die Realität der Massenmedien, 1996, S. 9.

2 *Tarleton Gillespie*, Custodians of the Internet. Platforms, content moderation, and the hidden decisions that shape social media, New Haven 2018, S. 197 ff.

An dieser Stelle lohnt sich ein Blick auf die Infrastruktur bei der Verbreitung sozialer Informationen. Der Unterschied zwischen dem Informationsmoment der Massenmedien und dem Informationsmoment der digitalen Dienste besteht darin, dass die neuen privaten digitalen Dienste nicht – wie eine Zeitung – die Inhalte selbst produzieren, sondern ihre kommerzielle Tätigkeit auf die Organisation der von anderen produzierten Inhalte konzentrieren. In diesem Sinne könnte man festlegen, dass die Moderation von Inhalten das funktionale Äquivalent der Netzgesellschaft zum Content Management durch Redaktionen der Gesellschaft der Organisationen ist. Denn in dem neuen Kontext unterscheiden sich die eigentlichen Waren, die die digitalen Unternehmen ihren Nutzern/Kunden anbieten, während sich die Art und Weise, wie diese Wirtschaft durch Werbung finanziert wird, nicht wesentlich von der Art und Weise unterscheidet, in der die traditionellen Massenmedien ebenfalls durch Werbung finanziert wurden. Die Art und Weise, wie die Verbreitung sozialer Informationen strukturiert ist, hat sich jedoch tiefgreifend gewandelt, und das Recht muss sich an diese Veränderungen anpassen.

Der vorliegende Beitrag versucht, die wichtigsten Entwicklungen der Haftung von Internetvermittlern in Brasilien unter dem Gesichtspunkt des Wandels der Öffentlichkeit durch digitale Medien zu beleuchten. Dafür wird zunächst auf den rechtlichen Rahmen vor der bekannten Marco Civil da Internet von 2014 (Internet Bill of Rights) eingegangen. In einem zweiten Schritt wird erläutert, wie das genannte Gesetz die brasilianische Diskussion zur Haftung von Internetvermittlern verändert hat. Abschließend werden die beiden jüngsten brasilianischen Entwicklungen zur Änderung des Rechtsrahmens im Zusammenhang mit der Verantwortung von Internetanbietern behandelt, nämlich das Präsidialdekret (Medida Provisória) von 2021 und der Gesetzentwurf 2630 von 2020, der derzeit im brasilianischen Kongress diskutiert wird und sich in der Endphase der Verabschiedung befindet.

2. Die rechtliche Grundlage der Haftung der Intermediäre in Brasilien vor 2014

Vor dem Marco Civil da Internet (Internet Bill of Rights, Gesetz Nr. 12.965 von 2014) wurden die Beziehungen zwischen den Nutzern und

den Anbietern[3] von Internetanwendungen durch die Bestimmungen des Gesetzes Nr. 8.078 von 1990 (Verbraucherschutzgesetz[4]) und des Gesetzes Nr. 10.406 von 2002, dem brasilianischen Zivilgesetzbuch, geregelt. Im Rahmen dieses rechtlichen Regulierungsrahmens forderten einerseits die Opfer verleumderischer oder falscher Inhalte Schadensersatz, während die Plattformen und Websites sich darauf beriefen, dass es ihnen nicht möglich sei, die eingestellten Informationen oder Inhalte, die Gegenstand der Beschwerden waren, zu kontrollieren oder zu überprüfen. Die Moderation und eventuelle Entfernung von Inhalten, die von Dritten im Internet erstellt wurden, hat zu intensiven Debatten vor brasilianischen Gerichten geführt, und die Diskussionen über die zivilrechtliche Haftung in diesem Zusammenhang haben in den letzten Jahren unterschiedliche Richtungen eingeschlagen.

Kurzum: Vor Inkrafttreten des Marco Civil da Internet waren Doktrin und Rechtsprechung in Bezug auf die zivilrechtliche Haftung von Anbietern von Internet-Anwendungen in drei verschiedene Richtungen unterteilt. Erstens wurde davon ausgegangen, dass der Anbieter nicht für das Verhalten seiner Nutzer hafte, da der Server oder Anbieter nur ein Vermittler zwischen den Nutzern sei. Zweitens wurde davon ausgegangen, dass eine objektive zivilrechtliche Haftung des Anbieters auf der Grundlage des Begriffs des Tätigkeitsrisikos (auf der Grundlage des brasilianischen Zivilgesetzbuchs) oder auf der Grundlage von Mängeln bei der Erbringung von Dienstleistungen (auf der Grundlage des Verbraucherschutzgesetzes) bestehe. Schließlich begründet eine dritte Strömung, die sich in zwei Richtungen teilt, eine subjektive zivilrechtliche Haftung einmal mit der Untertätigkeit nach dem Bekanntwerden des illegalen Inhalts (in einer etwas ungeregelten Art von *Notice and Take Down*) bzw. verteidigt die Haftung nur im Falle der Nichteinhaltung einer spezifischen gerichtlichen Anordnung (ein Verständnis, das vom Marco Civil übernommen wurde, wie wir weiter unten sehen werden).

---

3 Nach dem Gesetz Nr. 12.965/2014 ist ein Anbieter von Internetanwendungen ein Anbieter, der „eine Reihe von Funktionalitäten bereitstellt, auf die über ein mit dem Internet verbundenes Endgerät zugegriffen werden kann" (Artikel 5, VIII).

4 Das Gesetz Nr. 8.078/1990 ist auf den Fall anwendbar. „Die Tatsache, dass die vom Internetdienstanbieter erbrachte Dienstleistung kostenlos ist, stellt keine Verzerrung des Verbrauchsverhältnisses dar, da der Begriff ‚gegen Entgelt' in Art. 3 § 2 Verbraucherschutzgesetzbuch weit auszulegen ist, um den indirekten Gewinn des Anbieters zu erfassen." (Sonderberufung 1316921, Berichterstatterin Richterin Nancy Andrighi, Dritte Kammer, Urteil vom 26.06.2012).

Für die Verfechter der ersten Strömung sind die Internet-Diensteanbieter lediglich Vermittler zwischen dem Verursacher des Schadens (dem Nutzer der Internet-Anwendung) und dem Opfer (auch Nutzer der Internet-Anwendung). In den Fällen, in denen dieses Verständnis zugrundegelegt wurde, waren die Anwendungsanbieter von der passiven Seite der Klagen ausgeschlossen. Das geht zum Beispiel aus der folgenden Entscheidung des Gerichtshofs von dem Bundesland Rio Grande do Sul hervor:

> Berufung in Zivilsachen. Zivilrechtliche Haftung. Kompensationsmaßnahmen. *Die passive Illegitimität von Facebook*.
> Die zivilrechtliche Haftung des Anbieters von Internet-Inhalten ist nur dann gegeben, wenn er, nachdem er ordnungsgemäß benachrichtigt wurde, den beleidigenden oder rechtswidrigen Beitrag nicht entfernt. *Anbieter von Internetinhalten sind für Veröffentlichungen auf ihren Websites nur dann zivilrechtlich haftbar, wenn sie es versäumen, die beleidigenden Beiträge nach ordnungsgemäßer Benachrichtigung der Betroffenen zu entfernen.* [...]. Der Nutzer des sozialen Netzwerks muss den Schaden ersetzen, der der außerbetrieblichen Vermögenssphäre des Inhabers des verletzten höchstpersönlichen Rechts entsteht. [...] DIE BERUFUNG DER BEKLAGTEN WIRD ZURÜCKGEWIESEN. DER BERUFUNG DES KLÄGERS WIRD TEILWEISE STATTGEGEBEN. [5]

Es wurde daher davon ausgegangen, dass Anbieter nicht für Handlungen Dritter haften, sondern nur für Schäden, die ausschließlich auf ihre eigene Tätigkeit bzw. ihr pflichtwidriges Unterlassen zurückzuführen sind – was sowohl für Anbieter von Internetanwendungen als auch für Hosting-Anbieter gilt. Die Pflicht zur Entschädigung würde den Internetnutzer treffen, der für den vom Opfer erlittenen Sach- oder Nichtvermögensschaden verantwortlich ist. Diese Position wurde durch Entscheidungen gestützt, die den Anbieter als bloßen Vermittler zwischen dem Nutzer, der den unrechtmäßigen Schaden verursacht hat, und dem Geschädigten bezeichnen, wie z.B. in der oben zitierten Entscheidung. Sobald klar wurde, dass es kein Verhalten des Anbieters gibt, das in einem kausalen Zusammenhang mit dem Schaden steht, stellt sich die Frage der Haftung für das Verhalten anderer nicht mehr und der Anbieter sollte lediglich mit dem Opfer zusammenarbeiten, um den Verursacher des Schadens zu ermitteln.[6]

---

5 TJRS, Zivilberufung Nr. 70061451191, 9. C.C., Rel. Des. Miguel Ângelo da Silva, Urteil vom 29.10.2014.

6 *Carlos Affonso Pereira de Souza*, Responsabilidade civil dos provedores de acesso e de aplicações de internet: evolução jurisprudencial e os impactos da Lei

Im zweiten Fall ist die Haftung des Diensteanbieters eine objektive Haftung, die sich auf zwei Hauptgründe stützt: das mit der Tätigkeit des Diensteanbieters verbundene Risiko und die zwischen dem Nutzer und dem Diensteanbieter bestehende Verbraucherbeziehung. Es gäbe nämlich eine objektive Haftung des Anbieters, ohne dass es eines Verschuldens bedürfe, die sich auf den Begriff des Risikos der ausgeübten Tätigkeit (Artikel 927, einziger Absatz des Zivilgesetzbuches[7]) oder auf den Mangel bei der Erbringung der Dienstleistung in einer Verbraucherbeziehung (Artikel 14 des Verbraucherschutzgesetzes[8]) stützen könne. Vor Inkrafttreten des Marco Civil wurde die Theorie des mit der Tätigkeit verbundenen Risikos von den Gerichten eine Zeit lang als Grundlage für die Bestimmung der Haftung des Dienstleistungserbringers herangezogen und war sogar ursprünglich das vorherrschende Verständnis in der Rechtsprechung des Obersten Bundesgerichtshofs (Superior Tribunal de Justiça).

Im Laufe der Zeit hat die Rechtsprechung des Obersten Bundesgerichtshof (Superior Tribunal de Justiça) das Verständnis jedoch in die entgegengesetzte Richtung gefestigt. Der Gerichtshof stellte fest, dass der einzige Absatz von Artikel 927 nicht auf die Definition der zivilrechtlichen Haf-

---

12.695/2014 (Marco Civil da Internet), in: George Salomão Leite/Ronaldo Lemos (Hrsg.), *Marco Civil da Internet*, São Paulo 2014, S. 809.

7 Art. 927: Wer durch eine unerlaubte Handlung (Art. 186 und 187) einem anderen einen Schaden zufügt, ist verpflichtet, diesen zu ersetzen.
Einziger Absatz. *Es besteht die Verpflichtung, den Schaden unabhängig von der Schuld in den gesetzlich festgelegten Fällen zu beheben, oder wenn die Tätigkeit, die normalerweise vom Urheber des Schadens ausgeübt wird, aufgrund ihrer Art eine Gefahr für die Rechte anderer darstellt*. [Hervorhebung R.C.].

8 Art. 14: Der Dienstleistungserbringer haftet verschuldensunabhängig für die Behebung von Schäden, die dem Verbraucher durch Mängel bei der Erbringung von Dienstleistungen sowie durch unzureichende oder unangemessene Informationen über deren Nutzung und Risiken entstehen.
§ 1 Die Dienstleistung ist mangelhaft, wenn sie nicht die Sicherheit bietet, die der Verbraucher unter Berücksichtigung der relevanten Umstände erwarten kann, einschließlich
I – die Art der Zustellung;
II – das Ergebnis und die vernünftigerweise zu erwartenden Risiken;
III – der Zeitpunkt, zu dem sie bereitgestellt wurde.
§ 2 Die Leistung wird nicht als mangelhaft angesehen, weil neue Techniken eingeführt wurden.
§ 3 Der Dienstleister haftet nur dann nicht, wenn er beweist:
I – dass nach Erbringung der Leistung der Mangel nicht besteht;
II – das ausschließliche Verschulden des Verbrauchers oder eines Dritten.
§ 4 Die persönliche Haftung von Selbstständigen wird durch die Feststellung des Verschuldens ermittelt.

tung von Anbietern von Internetinhalten anwendbar ist, wie aus der folgenden Entscheidung hervorgeht:

> ZIVILRECHTLICHE HAFTUNG. BEZIEHUNGSSEITE. BELEIDIGENDE NACHRICHTEN.
> Die objektive Verantwortung, die in Artikel 927, einziger Absatz, des CC vorgesehen ist, gilt nicht für das Host-Unternehmen einer Social-Networking-Website im Falle von Nachrichten mit beleidigendem Inhalt, die von Nutzern eingefügt wurden. Das Gremium geht davon aus, dass die aus diesen Nachrichten resultierenden Schäden kein inhärentes Risiko für die Tätigkeit der Inhaltsanbieter darstellen. Die vorherige Kontrolle des Inhalts der vom Nutzer geposteten Informationen ist keine Tätigkeit des Administrators des sozialen Netzwerks, so dass seine Pflicht darin besteht, den Text oder das Bild mit rechtswidrigem Inhalt zu entfernen, sobald er übermittelt wird, wobei er nur in der Lage ist, auf seine Unterlassung[9] zu reagieren.

Generell kann festgestellt werden, dass sowohl die Gerichte als auch der Oberste Bundesgerichtshof die Auffassung vertraten, dass Internet-Diensteanbieter für Inhalte Dritter haftbar gemacht werden sollten. Entweder weil sie als inhärenten Aspekt ihrer Tätigkeit einen Raum für die Verbreitung von Nachrichten ihrer Nutzer bieten oder weil sie aus der direkten oder indirekten Nutzung dieses kommunikativen Raums wirtschaftliche Gewinne erzielen.[10] Nach Ansicht des Obersten Bundesgerichtshofes (Superior Tribunal de Justiça) unterliegt „die kommerzielle Nutzung des Internets und die sich daraus ergebenden Verbraucherbeziehungen dem Gesetz 8078/90“[11], d.h. den Bestimmungen des Verbraucherschutzgesetzes. Bei mehr als einer Gelegenheit hat sich der Gerichtshof in diesem Sinne geäußert:

> „Wer es technisch möglich macht, wer wirtschaftlich profitiert und die Schaffung von Gemeinschaften und Beziehungsseiten im Internet

9 STJ, Bulletin Nr. 0460. Zitierte Präzedenzfälle: REsp 1.186.616-MG, DJe 31.8.2011; REsp 1.175.675-RS, DJe 20.9.2011; REsp 1.306.066-MT, Urteil vom 17.4.2012.

10 *Anderson Schreiber*, Marco Civil da Internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro, in: Newton de Lucca/ Adalberto Simão Filho/ Cíntia Rosa Pereira de Lima (Hrsg.), Direito & Internet. Tomo II: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo 2015.

11 REsp. 1316921, Berichterstatterin Richterin Nancy Andrighi, Dritte Kammer des Obersten Bundesgerichtshofes (Superior Tribunal de Justiça), entschieden am 26.6.2012.

> aktiv fördert, ist für die Kontrolle möglicher Missbräuche und für die Gewährleistung der Persönlichkeitsrechte von Internetnutzern und Dritten ebenso verantwortlich wie die Internetnutzer selbst, die Informationen erzeugen und verbreiten, die gegen die elementarsten Werte des Gemeinschaftslebens verstoßen, sei es real oder virtuell."

Obwohl das Bürgerliche Gesetzbuch und das Verbraucherschutzgesetz die objektive Haftung des Anbieters in der Regel festlegen, milderte die Rechtsprechung des Obersten Bundesgerichtshofs die Strenge des Gesetzgebers[12] ab, indem sie „eine Art bedingte[r] Verantwortung festlegte, die erst ab dem Zeitpunkt eingeschaltet wurde, zu dem der Anbieter, nachdem er von der Existenz illegaler Inhalte Kenntnis erlangt hatte, keine Maßnahmen ergriff, um dieses Material von seiner Website zu entfernen"[13]. Darüber hinaus hat sich die Rechtsprechung des Obersten Bundesgerichtshofes (Superior Tribunal de Justiça) dahingehend gefestigt, dass der Anbieter, sobald er von der Existenz illegaler Inhalte erfährt, diese unverzüglich entfernen muss, da er sonst dafür haftbar gemacht werden kann.[14]

Daraus folgt, dass die einfache außergerichtliche Benachrichtigung über unangemessene Inhalte, auf die ein Nutzer hingewiesen hat, in jedem Fall für die Haftung des Anbieters ausreichen würde, wenn dieser die Inhalte nicht sofort entfernt.[15] Außerdem sollte der Anbieter aufgrund dieser Verantwortung über die Möglichkeit verfügen, die Nutzer zu identifizieren – etwa über die Protokollnummer (IP) des Computers –, um Anonymität

---

12 „Der materielle Schaden, der sich aus den vom Nutzer in die Website eingefügten Nachrichten mit beleidigendem Inhalt ergibt, stellt kein inhärentes Risiko für die Tätigkeit der Inhaltsanbieter dar, so dass die verschuldensunabhängige Haftung gemäß Art. 927, einziger Absatz CC/02, nicht auf sie anwendbar ist." (Sonderberufung 1186616/MG, Berichterstatterin Richterin Nancy Andrighi, Dritte Kammer des Obersten Bundesgerichtshofes (Superior Tribunal de Justiça), Urteil vom 23.08.2011).

13 *Schreiber* (Fn. 10), op. cit.

14 „Wenn der Anbieter darüber informiert wird, dass ein bestimmter Text oder ein bestimmtes Bild einen rechtswidrigen Inhalt hat, muss er energisch handeln und das Material *unverzüglich* von der Website entfernen, unter Androhung einer gesamtschuldnerischen Haftung mit dem direkten Urheber des Schadens, der durch die Unterlassung entstanden ist." (Sonderberufung 1186616/MG, Berichterstatterin Richterin Nancy Andrighi, Dritte Kammer, Urteil vom 23.8.2011 – Hervorhebung R.C.).

15 *Cíntia Rosa Pereira de Lima*, A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do Marco Civil da Internet (Lei n. 12.965/14), Revista da Faculdade de Direito da Universidade de São Paulo, v. 110, p. 157, jan./dez. 2015.

zu verhindern, da er sonst subjektiv für das *culpa in omittendo* haftbar gemacht werden könnte:

> 6. Wenn er einen Dienst anbietet, über den die Nutzer ihre Meinung frei äußern können, muss der Anbieter darauf achten, dass er Mittel zur Verfügung stellt, um jeden dieser Nutzer zu identifizieren, die Anonymität zu wahren und jeder Äußerung eine bestimmte Urheberschaft zuzuordnen. Im Rahmen der vom Anbieter zu erwartenden durchschnittlichen Sorgfalt muss er unter Androhung der subjektiven Verschuldenshaftung *bei Unterlassung* die Maßnahmen ergreifen, die ihm nach den konkreten Umständen des Einzelfalls zur Individualisierung der Nutzer der Website möglich sind.
> 7. Auch wenn er keine personenbezogenen Daten von seinen Nutzern verlangt, verfügt der Inhaltsanbieter, der die Internetprotokollnummer (IP) der für die Registrierung der einzelnen Konten verwendeten Computer registriert, über ein einigermaßen effizientes Mittel zur Verfolgung seiner Nutzer, eine Sicherheitsmaßnahme, die der durchschnittlichen Sorgfalt entspricht, die von dieser Art von Internetdienstanbietern erwartet wird.[16]

Die Konsolidierung der Rechtsprechung des Obersten Bundesgerichtshofs (Superior Tribunal de Justiça) ist daher zu einem „transversalen Weg" geworden, durch den „die so genannte *Notice-and-Takedown-Theorie* in die brasilianische Realität Einzug gehalten hat"[17]. Das aus dem *Digital Millennium Copyright Act* (DMCA) in den Vereinigten Staaten von Amerika stammende Konzept der „*Notice and Take Down*" (Benachrichtigung und Entfernung) ist im Urheberrecht als eine Art Ausnahme von der Haftung für Urheberrechtsverletzungen im Internet zu sehen, mit der sichergestellt wird, dass Anbieter nicht haften, wenn sie, nachdem sie über das Vorhandensein von unangemessenem (urheberrechtlich geschütztem) Material auf ihren Plattformen benachrichtigt wurden, unverzüglich auf die Aufforderung der beleidigten Partei reagieren und das betreffende Material entfernen.

Es ist festzustellen, dass die Anwendung des „*Notice and Take Down*"-Mechanismus im Zusammenhang mit der zivilrechtlichen Haftung für Schäden, die durch von Dritten erstellte Inhalte entstehen, in gewisser Weise „eine Spaltung des brasilianischen Systems der zivilrechtlichen

16 REsp. 1186616/MG, Berichterstatterin Richterin Nancy Andrighi, Dritte Klage, Urteil vom 23.8.2011.
17 *Schreiber* (Fn. 10), op. cit.

Haftung“[18] darstellt. Dies liegt daran, dass es sich um einen im Wesentlichen verfahrensrechtlichen Mechanismus handelt, der zwar in der brasilianischen Rechtsprechung Bedeutung erlangt hat, aber weder über ein geregeltes Verfahren noch über die Garantien verfügte, die ihn in den Diskussionen über das *Urheberrecht* in den Vereinigten Staaten ursprünglich begleitet haben.[19] Es wurde erwartet, dass die Schaffung eines Gesetzes zur Regulierung der Internetnutzung in Brasilien diese Lücke schließen und eine größere Rechtssicherheit bei der Anwendung der Theorie in Brasilien schaffen würde. Die Erwartungen wurden jedoch enttäuscht, da Artikel 19 des Marco Civil da Internet – auf den weiter unten eingegangen wird – eine Bestimmung enthielt, die ausdrücklich im Widerspruch zur Rechtsprechung im Lande und damit zum Mechanismus der *Benachrichtigung und Entfernung* stand.

Kurzum, die im Marco Civil da Internet festgelegte Regelung macht den Anbieter einer Anwendung nur dann für Schäden haftbar, die durch von Dritten generierte Inhalte entstehen, wenn er einer bestimmten gerichtlichen Anordnung nicht nachkommt, und dies auch nur im Rahmen der technischen Möglichkeiten seines Dienstes. Diese Antinomie wurde sogar von Richter Luis Felipe Salomão in einer Entscheidung hervorgehoben, in der er die Diskrepanz zwischen der vorherrschenden Rechtsprechung des STJ und den neuen, durch den Marco Civil eingeführten Regeln erörtert. Wörtlich heißt es:

> „Nach dem neuen Gesetz besteht die zivilrechtliche Haftung des Internetdienstanbieters in der Haftung für Schäden, die sich aus der Nichteinhaltung einer gerichtlichen Anordnung ergeben, eine Bestimmung, die sich stark von der derzeitigen Rechtsprechung des STJ unterscheidet, die sich, um das rechtswidrige Verhalten des Anbieters herauszufiltern, mit der Untätigkeit nach der außergerichtlichen Zustellung begnügt.“[20]

3. *Die Veränderung der rechtlichen Grundlage der Haftung der Intermediäre in Brasilien durch das Marco Civil da Internet (2014)*

Im Jahr 2014 trat eines der wichtigsten brasilianischen Gesetze zur Regulierung des Internets und der neuen digitalen Beziehungen insgesamt in

18 Id, ibid.
19 Siehe U.S. Code, Title 17, Chapter 5, Section 512, und Section 512 (g) (2) und (3).
20 STJ, REsp. 1.512.647-MG, Berichterstatter Richter Luis Felipe Salomão.

Kraft.[21] Das Gesetz Nr. 12.965, bekannt als Marco Civil da Internet (MCI), hat die Aufgabe, Grundsätze, Garantien, Rechte und Pflichten für die Nutzung des Internets im Land festzulegen,[22] wobei die Meinungsfreiheit die wichtigste Grundlage darstellt.[23] Um die Regelung zur Entfernung von Inhalten im Marco Civil da Internet richtig zu verstehen, ist es jedoch nützlich und notwendig, ihre Entstehung, wenn auch nur kurz, zu analysieren, da der Entstehungsprozess des MCI dazu beiträgt, bestimmte auf legislativer Ebene getroffene Entscheidungen zu verstehen, und der Entstehungsprozess gleichzeitig seine Bedeutung für das brasilianische Rechtssystem hervorhebt, da an seinem Entwurfsprozess eine bis dahin unbekannte Beteiligung der Zivilgesellschaft stattfand.[24]

Der Rahmen für die Bürgerrechte im Internet entstand in Opposition zu dem Gesetzentwurf mit dem Spitznamen „Azeredo"-Gesetz (Gesetzentwurf Nr. 84/1999, verfasst vom Kongressabgeordneten Eduardo Azeredo), dessen Hauptziel darin bestand, verschiedene im Internet praktizierte Verhaltensweisen strafrechtlich zu typisieren. Nach einer umfassenden Konsultation der Bevölkerung wurde das MCI als Alternative zu den bestehenden Gesetzesentwürfen zur Kriminalisierung von Handlungen im Netz erlassen. Schon der Titel „Marco Civil", der sich auf den Begriff „Bill of *Rights*" bezieht, verdeutlicht die Zielsetzung, die im Gegensatz zu dem Gesetzentwurf steht, der damals im Kongress behandelt wurde, indem er den

21 Neben den hier analysierten Bestimmungen zur Inhaltsmoderation enthält das Gesetz auch in anderen Bereichen Neuerungen. Einer der wichtigsten Punkte ist vielleicht die Bestimmung zur Netzneutralität. Zu diesem Thema siehe unter anderem *Daniel César/ Irineu F. Barreto Junior*, Marco Civil da Internet e neutralidade da rede: Aspectos jurídicos e tecnológicos, Revista Eletrônica do Curso de Direito da UFSM 12 (1):65 v. 19. April 2017.

22 Art. 2: Die Disziplin der Internetnutzung in Brasilien beruht auf der Achtung der Meinungsfreiheit sowie auf der Anerkennung
I – der globalen Dimension des Netzes;
II – der Menschenrechte, der Entwicklung der Persönlichkeit und der Ausübung der Staatsbürgerschaft in den digitalen Medien;
III – der Pluralität und Vielfalt;
IV – der Offenheit und Zusammenarbeit;
V – freier Initiative, freiem Wettbewerb und Verbraucherschutz; und
VI – dem sozialen Zweck des Netzes.

23 *Marcelo Thompson*, Marco Civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na Internet do Brasil, RDA – Revista de Direito Administrativo 261 (2012), S. 203 (208).

24 *Ronaldo Lemos*, Uma breve história da Criação do Marco Civil, in: Newton da Lucca/ Alberto Simão Filho/ Cíntia Rosa Pereira de Lima (Hrsg.), Direito & Internet III: Marco Civil da Internet. Tomo I. São Paulo 2015, S. 82.

Umfang der Festlegung der Bürgerrechte der Internetnutzer vor Straftaten aufzeigt.[25]

Auch wenn in diesem Beitrag nicht die detaillierte Geschichte der öffentlichen Konsultationen, aus denen der Marco Civil da Internet hervorging, erzählt werden kann, ist es doch wichtig, darauf hinzuweisen, dass die erste Phase der Konsultationen mit einem Grundlagentext begann, der sich auf zwei wichtige Dokumente bezog: die Verfassung der Föderativen Republik Brasilien von 1988, aus der die Bedeutung der freien Meinungsäußerung und der damit verbundenen Rechte hervorgeht, und die Grundsätze für die Verwaltung und Nutzung des Internets in Brasilien.[26] In dieser ersten Phase betonte der Entwurf des neuen Gesetzes den prinzipiellen Charakter und die axiologische Grundlage der Norm sowie ihr Ziel, als Referenz für die Lösung von Konflikten auf der Grundlage einer Harmonisierung dieser Werte zu dienen, anstatt durch ausdrückliche und starre Normen.[27]

In einer zweiten Phase, die von einer intensiven Beteiligung der Bevölkerung geprägt war, fanden Debatten über den Rechtstext statt, an dem erhebliche Änderungen vorgenommen wurden. Die Hauptdiskussion drehte sich um die zivilrechtliche Haftung von Internetanbietern: Der ursprüngliche Vorschlag der Konsultation hatte sich für das vom Obersten Gerichtshof anerkannte System entschieden, d.h. *für* das System der *Meldung und Löschung* in brasilianischem Portugiesisch. Da an den öffentlichen Anhörungen und Debatten jedoch Personen aus verschiedenen Sektoren teilnahmen, die wiederum unterschiedliche Interessen innerhalb der Zivilgesellschaft selbst vertraten, wurde der Text soweit geändert, bis der derzeitige Wortlaut entstand.

In Artikel 19 des Marco Civil da Internet wurde die bis dahin geltende Rechtsauffassung dahingehend geändert, dass die Haftung der Anbieter von Internetdiensten erst dann eintritt, wenn einer gerichtlichen Anordnung zur Entfernung oder Nichtverfügbarkeit der als schädlich angesehenen Inhalte nicht Folge geleistet wird. *In verbis:*

---

25 *João Quinelato de Queiroz*, Aplicabilidade do Marco Civil da Internet na responsabilidade civil por uso indevido de conteúdo protegido por direitos autorais na internet, Civilistica.com. Rio de Janeiro, a. 5, n. 2, 2016. Verfügbar unter: <http://civilistica.com/aplicabilidade-do-marco-civil-da-internet/> – letzter Aufruf: 14 Feb. 2022.

26 Id, ibid.

27 *Guilherme Alberto Almeida*,. Marco Civil da Internet – Antecedentes, formulação colaborativa e resultados alcançados, in: Gustavo Artese (Hrsg.), Marco Civil da Internet: análise jurídica sob uma perspectiva empresarial, São Paulo 2015, S. 40.

> Art. 19. Um die Meinungsfreiheit zu gewährleisten und Zensur zu verhindern, kann der Anbieter von Internetanwendungen nur dann zivilrechtlich für Schäden haftbar gemacht werden, die durch von Dritten erstellte Inhalte entstehen, wenn er es nach einer ausdrücklichen gerichtlichen Anordnung unterlässt, innerhalb des Umfangs und der technischen Grenzen seines Dienstes und innerhalb der festgesetzten Frist Maßnahmen zu ergreifen, um die als rechtsverletzend bezeichneten Inhalte unzugänglich zu machen, vorbehaltlich anders lautender gesetzlicher Bestimmungen.

Seit dem Inkrafttreten des Marco Civil da Internet reicht daher eine bloße außergerichtliche Meldung nicht mehr aus, um den Anbieter zu verpflichten, den Inhalt unter Androhung von Strafe zu entfernen. Unter dem Argument des Schutzes der freien Meinungsäußerung und der Verhinderung von Zensur ist eine gerichtliche Anordnung erforderlich geworden, damit der Anbieter für die Entfernung von Inhalten verantwortlich gemacht werden kann. Das bedeutet, dass nach der MCI Inhalte erst nach einer Bewertung durch einen Richter[28] als schädlich angesehen werden, selbst wenn dies im Wege einer einstweiligen Verfügung geschieht.

In der Praxis ist die Einreichung einer Klage nicht mehr nur ein Instrument zum Schutz der Rechte des Opfers und zur Erlangung von Schadenersatz, sondern sie wird zu einer *unabdingbaren Voraussetzung* für die zivilrechtliche Haftung des Anbieters im Rahmen des Marco Civil Systems. Wörtlich:

> Das Opfer, das bisher als letztes Mittel den Rechtsweg beschritten hat, um den Beklagten zur Rechenschaft zu ziehen, *muss* nun den Rechtsweg beschreiten und den Erlass eines bestimmten Gerichtsbeschlusses beantragen, so dass der Betreiber der Website oder des sozialen Netzwerks nur dann und nur im Falle der Nichteinhaltung des Gerichtsbeschlusses haftbar gemacht werden kann.[29]

Die Lektüre der Bestimmung lässt auch den Schluss zu, dass die zivilrechtliche Haftung nur dann besteht, wenn die spezifische gerichtliche Anordnung zur Entfernung illegaler Inhalte nicht befolgt wird, die unter Androhung der Nichtigkeit die klare und spezifische Identifizierung der als

---

28 *Ricardo Alberto Kanayama*, A liberdade de expressão do Marco Civil da Internet e o procedimento de notificação e retirada para as "infrações" aos direitos autorais, Civilistica.com. Rio de Janeiro, a. 10, n. 1, 2021. Verfügbar unter: <http://civilistica.com/a-liberdade-de-expressao-do-marco-civil/> – letzter Aufruf: 14. Feb. 2022.

29 *Schreiber* (Fn. 10), op. cit.

rechtsverletzend bezeichneten Inhalte enthalten muss, was die eindeutige Lokalisierung des Materials *ermöglicht*, wie in Artikel 19 §§ 1, 2 vorgesehen ist: „*[a] court order referred to the caput must contain, under penalty of nullity, the clear and specific identification of the content pointed as infringing, which allows the unequivocal location of the material*". Ohne den rechtlich festgestellten Verstoß gegen eine solche Anordnung besteht also keine Verpflichtung zur Entschädigung.

Aber auch ohne Gerichtsbeschluss kann der Hosting-Anbieter nach einer außergerichtlichen Benachrichtigung die illegalen Inhalte von seinen Plattformen entfernen.[30]

Die im Gesetz Nr. 12.*965*/14 vorgeschlagene Lösung sieht nicht vor, dass der Betroffene unbedingt eine Klage auf Entfernung des Inhalts einreichen muss,[31] da dies von den Nutzungsbedingungen der Websites, dem veröffentlichten Inhalt und der Verurteilung der von der Partei eingereichten Mitteilung abhängt. Mit anderen Worten, der Inhalt kann ohne gerichtliche Anordnung entfernt werden, wenn er gegen die Nutzungsbedingungen eines Dienstes verstößt oder wenn es ein spezielles Gesetz gibt, das die Entfernung von bestimmten Inhalten regelt. Ein Anwendungsdienst kann nach eigenem Ermessen entscheiden, welche Inhalte er auf seiner Plattform akzeptiert; vorausgesetzt, diese Regeln werden von der Plattform vorgelegt und von den Nutzern akzeptiert, bevor sie die angebotenen Dienste in Anspruch nehmen.[32]

Um den in Artikel 19[33] *genannten* „eklatanten Rückschritt" abzumildern, sieht der Gesetzgeber in den Absätzen desselben Artikels die Möglichkeit vor, dass die Schäden, die sich aus der Verfügbarkeit von Inhalten im Internet ergeben, die sich auf die Ehre, den Ruf oder die Persönlich-

30 Artikel 19 des MCI „knüpft die zivilrechtliche Haftung der Antragsteller an die Nichteinhaltung einer bestimmten gerichtlichen Anordnung. Diese Aussage hindert die Anbieter in keiner Weise daran, bei der Organisation ihrer Aktivitäten Regeln aufzustellen, die festlegen, was auf ihrer Plattform angezeigt werden kann und was nicht", *Carlos Affonso Souza/ Chiara Spadaccini de Teffé*, Responsabilidade dos provedores por conteúdos de terceiros na internet, CONJUR. Verfügbar unter: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet – letzter Aufruf: 14. Feb. 2021.

31 *Carlos Affonso Souza/ Ronaldo Lemos*, Marco civil da internet: construção e aplicação. Juiz de Fora 2016.

32 *Renato Opice Blum/ Paulo Sá Elias/ Renato Leite Monteiro*, Marco regulatório da internet brasileira: "Marco Civil". Verfügbar unter: <https://www.migalhas.com.br/depeso/157848/marco-regulatorio-da-internet-brasileira---marco-civil> – letzter Aufruf: 10. März 2022.

33 *Schreiber* (Fn. 10), op. cit.

keitsrechte beziehen, auf schnellere und weniger belastende Weise für das Opfer vor den Sondergerichten verhandelt werden können. Gemäß den Bestimmungen von Artikel 19 § 3 können Fälle, die sich mit dem Ersatz von Schäden befassen, die durch im Internet verfügbare Inhalte in Bezug auf Ehre, Ruf oder Persönlichkeitsrechte entstehen, sowie mit der Nichtverfügbarkeit solcher Inhalte durch Anbieter von Internetanwendungen, vor den Sondergerichten eingereicht werden.

Art. 19 § 4 wiederum sieht die Möglichkeit vor, im Falle der Entfernung von Inhalten, die die Ehre, den Ruf oder die Persönlichkeitsrechte des Opfers betreffen, einen einstweiligen Rechtsschutz zu gewähren, sofern ein eindeutiger Beweis für diese Tatsache vorliegt:

> § 4 Der Richter kann, auch im Rahmen des in § 3 vorgesehenen Verfahrens, bei Vorliegen eindeutiger Beweise und unter Berücksichtigung des Interesses der Allgemeinheit an der Verfügbarkeit der Inhalte im Internet die Wirkungen der im ursprünglichen Antrag beabsichtigten Unterlassungsverfügung ganz oder teilweise vorwegnehmen, sofern die Voraussetzungen der Wahrhaftigkeit der Behauptung des Klägers und der begründeten Befürchtung eines nicht wiedergutzumachenden oder schwer wiedergutzumachenden Schadens vorliegen.

Der Marco Civil da Internet legt mit den oben genannten Anforderungen die endgültige Verpflichtung fest, „die als verletzend angegebenen Inhalte nicht verfügbar zu machen" (Artikel 19, *in fine*). Die Entfernung des Inhalts ist sicherlich die einschneidendste Maßnahme, um die Ausbreitung des Schadens zu verhindern und ein Mittel zu schaffen, das sich für die häufigeren Fälle der Übertragung schädlicher Inhalte (Hassreden, Desinformation, unerlaubte Veröffentlichung sexueller Inhalte anderer etc.) als angemessen erweist. In bestimmten Fällen kann die Entfernung jedoch einen Eingriff in das Recht auf freie Meinungsäußerung darstellen, so dass der Marco Civil in Artikel 20 verlangt, dass die Entfernung mit einer umfassenden Unterrichtung des Dritten einhergeht, der den mutmaßlich schädlichen Inhalt verbreitet hat:

> Art. 20: Wenn der Anbieter von Internetanwendungen über die Kontaktdaten des Nutzers verfügt, der unmittelbar für die in Artikel 19 genannten Inhalte verantwortlich ist, obliegt es ihm, dem Nutzer die Gründe und Informationen bezüglich der Nichtverfügbarkeit der Inhalte mitzuteilen, wobei die Informationen eine widersprüchliche und umfassende Verteidigung vor Gericht ermöglichen, es sei denn, es gibt eine ausdrückliche gesetzliche Bestimmung oder eine ausdrückliche begründete gerichtliche Feststellung, die dem entgegensteht.

Dem Dritten, dessen Inhalte entfernt wurden, wird außerdem das Recht zugesichert, dass er vom Anbieter verlangen kann, „die nicht [mehr] verfügbaren Inhalte durch die Begründung oder den Gerichtsbeschluss, der die Nichtverfügbarkeit begründet hat“[34], zu ersetzen.

Um die Analyse der Regelung zur Entfernung von Inhalten und der zivilrechtlichen Haftung des Internetanbieters nach dem Marco Civil abzuschließen, müssen die beiden im Gesetz vorgesehenen Ausnahmen untersucht werden: die Entfernung von urheberrechtlich geschützten Inhalten und der Fall der Verfügbarkeit von „Rache-Pornografie“.

In Bezug auf die Urheberrechte enthält der Marco Civil da Internet einen Vorbehalt zu der in Artikel 19 festgelegten Regel, so dass das zuvor eingeführte System der *Bekanntmachung und der Entfernung von Daten* beibehalten werden kann. Auf diese Weise kann der Anbieter der Anwendung (Hosting und Inhalt) ab dem Zeitpunkt haftbar gemacht werden, an dem er aufgefordert wurde, Inhalte zu entfernen, die gegen das Urheberrechtsgesetz (Gesetz Nr. 9610 von 1998) verstoßen, und dies nicht tut. Wie Artikel 19 § 2,[35] und Artikel 31[36] MCI klarstellen, ist diese Möglichkeit der gerichtlichen Anordnung nicht auf Fälle anwendbar, in denen es um Inhalte geht, die Urheberrechte verletzen, die – wie der STJ bereits in Urteilen sowohl vor als auch nach der Einführung der MCI bestätigt hat[37] – dem bisherigen Verständnis des Gerichts unterliegen, d.h. dem Melde- und Beseitigungsverfahren für die Nichtverfügbarkeit von Inhalten Dritter.[38]

---

34 Art. 20, einziger Absatz. Auf Verlangen des Nutzers, der den nicht verfügbaren Inhalt zur Verfügung gestellt hat, ersetzt der Anbieter der Internetanwendung, der diese Tätigkeit in organisierter Weise, professionell und zu wirtschaftlichen Zwecken ausübt, den nicht verfügbaren Inhalt mit der Begründung oder dem Gerichtsbeschluss, der die Nichtverfügbarkeit begründet hat.

35 § 2 Die Anwendung der Bestimmungen dieses Artikels bei Verletzungen des Urheberrechts oder verwandter Schutzrechte richtet sich nach einer besonderen Rechtsvorschrift, die die Meinungsfreiheit und die anderen in Art. 5 der Bundesverfassung vorgesehenen Garantien respektieren muss.

36 Art. 31 – Bis zum Inkrafttreten des in § 2 von Art. 19 vorgesehenen Sondergesetzes richtet sich die Haftung des Anbieters von Internetanwendungen für Schäden, die durch von Dritten erstellte Inhalte entstehen, wenn es sich um eine Verletzung des Urheberrechts oder verwandter Schutzrechte handelt, weiterhin nach dem zum Zeitpunkt des Inkrafttretens dieses Gesetzes geltenden Urheberrecht.

37 BRAZIL, STJ, REsp 1.512.647/MG. Berichterstatter: Minister Luís Felipe Salomão. Brasília. Urteil vom 13.5.2015.

38 *Carlos Affonso Pereira de Souza/Ronaldo Lemos*, Marco Civil da Internet: construção e aplicação, 2017. Verfügbar unter: <https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf> – letzter Aufruf: 29. März 2017, S. 106.

Der Marco Civil da Internet sieht auch eine Sonderregelung für Fälle von Inhalten vor, die gemeinhin als „Rachepornografie" bezeichnet werden.[39] Die Verordnung weicht von der Regel der Überschrift von Artikel 19 ab und sieht in Anlehnung an den Wortlaut von Artikel 21 vor:

> Artikel 21. Der Anbieter von Internetdiensten, der von Dritten generierte Inhalte zur Verfügung stellt, haftet subsidiär für die Verletzung der Intimsphäre, die sich aus der Veröffentlichung von Bildern, Videos oder sonstigem Material ergibt, das Nacktszenen oder sexuelle Handlungen privater Natur enthält, ohne dass der Teilnehmer oder sein gesetzlicher Vertreter dies genehmigt hat, wenn er es nach Erhalt der Mitteilung durch den Teilnehmer oder seinen gesetzlichen Vertreter unterlässt, im Rahmen des Umfangs und der technischen Grenzen seines Dienstes sorgfältig für die Nichtverfügbarkeit dieser Inhalte zu sorgen.
>
> Einziger Absatz. Die im *Caput* vorgesehene Benachrichtigung muss unter Androhung der Nichtigkeit Angaben enthalten, die es ermöglichen, das Material, das als die Privatsphäre des Teilnehmers verletzend bezeichnet wird, genau zu identifizieren und die Legitimität des Antrags zu überprüfen.

In einem solchen Fall sieht Artikel 21 abweichend von der allgemeinen Regel eine subsidiäre Verantwortung des Anwendungsanbieters vor, wenn er über den rechtswidrigen Inhalt informiert wird und es unterlässt, die Entfernung des Materials aus dem Netz zu fördern. Wie man sieht, gibt es jedoch eine Reihe von Voraussetzungen für das Bestehen einer solchen Haftung, darunter die Tatsache, dass der Anbieter, nachdem er benachrichtigt wurde, es unterlässt, „im Rahmen des Umfangs und der technischen Grenzen seines Dienstes die Nichtverfügbarkeit dieser Inhalte sorgfältig zu fördern". Darüber hinaus muss die Meldung „unter Androhung der Nichtigkeit Elemente enthalten, die die genaue Identifizierung des Materials ermöglichen, das als Verletzung der Intimsphäre bezeichnet wird", sowie die Überprüfung der Legitimität des Antragstellers. Trotz der Bedingungen bleibt in Artikel 21 das wesentliche Element der *Notice and Takedown* erhalten: der außergerichtliche Charakter der Mitteilung.

---

39 Mit den Worten von *Schreiber* (Fn. 10): „[D]ie Kennzeichnung ist streng genommen unzulässig, da die Wörtlichkeit der Norm auf Nacktheitsszenen und Sex anspielt, unabhängig von der Motivation, die zu ihrer Offenlegung geführt hat. Nordamerikanismus ist verzeihlich, solange er nicht zu einer restriktiven Auslegung der Norm führt."

All diese Rahmen der rechtlichen Regulierung digitaler Dienstleistungen wurden in den letzten Jahren in Brasilien in Frage gestellt und diskutiert. Diskutiert wurden vor allem zwei neue Initiativen: ein Präsidialdekret aus dem Jahr 2021 und das aktuelle Gesetz 2630 aus dem Jahr 2000, das die Grundlagen der Haftung der Internetanbieter neu formulieren will.

4. Dekret 1.068/21 und Gesetzentwurf 2630 von 2020: die Debatte über die Änderung der Haftung von Internetvermittlern in Brasilien

Auf globaler Ebene haben sich wichtige Akteure distanziert und versucht, die wichtigsten rechtlichen Grundlagen, die in den 90er und 2000er[40] Jahren die Grundlage für die rechtliche Einbindung des Internets bildeten, neu zu formulieren. Derzeit wird im US-Kongress über die Reform von § 230 CDA debattiert, mit dem eine Haftungsimmunität für Anbieter[41] geschaffen wurde. In Europa wird die E-Commerce-Richtlinie aus dem Jahr 2000 mit der Debatte um den „Digital Services Act" und den „Digital Markts Act" reformiert. Und Deutschland hat mit dem Netzwerkdurchsetzungsgesetz von 2017 und auch mit der Einbeziehung digitaler Dienste in den neuen Rechtsrahmen für Massenmedien (*Medienstaatsvertrag)* konkrete Schritte im Kampf gegen digitale Straftaten unternommen, die die gesamte europäische Debatte beeinflussen. Bei all diesen Entwürfen stellt sich jedoch die Frage nach der Vereinbarkeit der neuen Regelungen mit den in den Verfassungen der betreffenden Länder verankerten Freiheiten.[42]

---

40 *Rebecca Tushnet*, Power without Responsibility: Intermediaries and the First Amendment, George Washington Law Review 76 (2008), S. 1001 ff., 1009: „Die Kehrseite dieser gesetzgeberischen Gnade ist, dass die Befugnisse und Freiheiten der Körperschaft von Gesetzen herrühren, die ihr besondere Vorteile verschaffen sollen, die aber nicht die Fähigkeit einschließen müssen, sowohl den Status eines Sprechers gegenüber der Regierung als auch die Immunität gegenüber der Behandlung als Sprecher gegenüber privaten Klägern zu beanspruchen."

41 „Die Möglichkeit privater Plattformen, Inhalte zu moderieren, ergibt sich aus § 230 des Communications Decency Act (CDA), der Online-Vermittlern weitgehende Immunität von der Haftung für nutzergenerierte Inhalte auf ihren Websites gewährt." *Kate Klonick*, The New Governors: The People, Rules, and Processes Governing Online Speech. 131 Harv. L. Rev. 2018, S. 1602.

42 *Thomas Vesting*, Die Rundfunkfreiheit und die neue Logik der »Content-Curation« in elektronischen Netzwerken, Juristenzeitung 75 (2020), S. 975.

Brasilien steht nicht außerhalb dieses globalen Kontextes der Neuformulierung der Verantwortung bzw. Haftung von Internet-Vermittlern. Der Gesetzentwurf 2630 von 2020, der derzeit im Repräsentantenhaus diskutiert wird, ist Brasiliens Chance, über das neue digitale Umfeld, in dem wir leben und seine Risiken und Chancen nachzudenken. Anders als in anderen Ländern stößt diese Überlegung jedoch auf eine diskursive Blockade, die durch eine fast sakrale Bedeutung des Marco Civil da Internet von 2014 hervorgerufen wird. Das Schreiben von Gesetzen für das Internet wie in Stein gemeißelt anzusehen, widerspricht der digitalen Dynamik selbst, in der der Schutz der Grundrechte von Einzelpersonen und Kollektiven eine ständige Verpflichtung zur (Neu-)bewertung, Korrektur und Verbesserung sowohl durch den Gesetzgeber als auch durch höhere Gerichte erfordert. Das präsidentielle Dekret 1.068 von 2021 ist hingegen der Gegenpol zu dieser anachronistischen Heiligkeit, da es einerseits darauf abzielt, die Exekutive als Hüter des Kommunikationsflusses der Gesellschaft zu etablieren und andererseits die private inhaltliche Moderation von Themen im Zusammenhang mit Straftaten und Desinformation zu verhindern.

In diesem Kontext muss man sich fragen, was eine globale Welle der Neuformulierung der Internet-Gesetzgebung legitimiert. Der Schlüssel zu dieser Antwort liegt in zwei grundlegenden Punkten: Der erste hängt mit den faktischen Veränderungen des digitalen Umfelds in den letzten zwei Jahrzehnten zusammen und der zweite grundlegende Punkt ergibt sich aus der verfassungsrechtlichen Semantik moderner demokratischer Staaten selbst. Die derzeitige Situation im Internet unterscheidet sich von der ersten Situation, in der die ersten Rechtsvorschriften nur erlassen wurden, um die Innovation in einem neuen und unsicheren Bereich zu fördern. Das derzeitige digitale Umfeld ist viel stärker durch die starke Konzentration auf einige wenige Anwendungen gekennzeichnet, eine Bewegung, die als „Plattformisierung des Internets“ bezeichnet wird. Sogar der Erfinder des World Wide Web, Tim Berners-Lee, hat zu Initiativen aufgerufen, die nach seinen eigenen Worten „die Werte der individuellen und gruppenbezogenen Selbstbestimmung wiederherstellen sollen, die das Internet einst hatte und nun verloren zu haben scheint“.

Genau dieser faktische Wandel hat den Gegenstand der ersten Internet-Gesetzgebung vernebelt und erfordert eine Aktualisierung, um einen besseren Schutz der Institutionen und der Rechte des Einzelnen zu gewährleisten. Und hier kommt der zweite grundlegende Punkt ins Spiel, der die globale Welle der Reformulierung legitimiert. Was zum Beispiel die spezifische Frage der Inhaltsmoderation betrifft, so wurden in demokratischen Staaten die verschiedenen Formen der Kommunikation rechtlich immer

unterschiedlich gehandhabt: Für die private Kommunikation galt schon immer ein höherer Schutz der Geheimhaltung und der Privatsphäre, während für die öffentliche oder kollektive Kommunikation aufgrund ihrer Auswirkungen auf die öffentliche Meinungsbildung und die Demokratie immer eine differenzierte Regelung galt.

Hier sehen wir den Zusammenhang zwischen den jüngsten faktischen Veränderungen und dem Recht. Da nur wenige Internetanwendungen eine echte Infrastruktur für die tägliche Kommunikation der Bevölkerung darstellen, muss das Recht in diesem neuen Szenario nicht nur als uneingeschränkter Förderer der Privatautonomie, sondern auch als Beschützer der individuellen und kollektiven Rechte fungieren. An dieser Stelle ist es notwendig, zwischen der Meinungsfreiheit des Einzelnen und einer strukturellen Ebene zu unterscheiden, die die große Meinungsfreiheit dieser Personen verwaltet, monetarisiert und steuert. Hier stellt sich die Frage, welche Verpflichtungen und Aufgaben für diesen Strukturplan, der die Meinungsfreiheit der Bevölkerung verwaltet, angesichts seiner zentralen Stellung als Kommunikationsinfrastruktur mit direktem Einfluss auf die Einschränkung der individuellen Rechte und Garantien und der Demokratie geschaffen werden sollten.

4.1 Die neue Debatte um die Intermediäre Haftung in Brasilien: das brasilianische Gesetz für Freiheit, Verantwortung und Transparenz im Internet

Der unter dem Spitznamen „PL das Fake News" bekannte Gesetzentwurf (PL) 2630/2020 zielt darauf ab, ein „brasilianisches Gesetz für Freiheit, Verantwortung und Transparenz im Internet" zu schaffen. Ziel des Gesetzentwurfs ist es, Maßnahmen zur Bekämpfung der Verbreitung von Fehlinformationen sowohl in sozialen Netzwerken als auch in privaten Nachrichtendiensten und Suchmaschinen zu schaffen, indem Regeln, Leitlinien und Transparenzmechanismen für diese Einrichtungen festgelegt werden, wobei Dienste für die Nutzung durch Unternehmen und die elektronische Post[43] vom Anwendungsbereich ausgenommen sind. Der Text wurde 2020 von Senator Alessandro Vieira vorgelegt und im Senat

43 Aus Artikel 1 des PL 2630/2020 geht Folgendes hervor: Art. 1 Das brasilianische Gesetz über Freiheit, Verantwortung und Transparenz im Internet wird geschaffen, um Standards, Leitlinien und Transparenzmechanismen für Anbieter von sozialen Netzwerken, Suchmaschinen und Instant-Messaging-Diensten im Internet sowie Leitlinien für deren Nutzung festzulegen.

abgestimmt und 2021 an das untere Repräsentantenhaus (Camara dos Deputados) weitergeleitet, wo er vom Abgeordneten Orlando Silva als Berichterstatter betreut wird. Es wird erwartet, dass die Abstimmung über den Gesetzesentwurf bald stattfinden wird. Das Thema wird besonders relevant, wenn man bedenkt, dass im Jahr 2022 die Präsidentschaftswahlen sowie die Wahlen der Regierungschefs der Bundesstaaten und des Kongresses stattfinden werden, was den Kampf gegen Fehlinformationen zu einem der wichtigsten und dringendsten Themen in diesem Jahr macht.[44]

An dieser Stelle sei darauf hingewiesen, dass dem Gesetzentwurf 2630 mehr als 70 weitere Gesetzentwürfe beigefügt sind, von denen sich die Hälfte – 35 Gesetzentwürfe – mit Regeln und Kriterien für die Entfernung oder Moderation von Online-Inhalten[45] befassen. Obwohl die Gesetzesvorlage 2630/2020 noch nicht angenommen wurde, verdienen einige Punkte besondere Aufmerksamkeit, vor allem soweit sie sich auf die Moderation von Inhalten beziehen. Eines der Hauptanliegen von PL 2630 ist, wie der Titel des Gesetzes schon sagt, die Festlegung von Transparenzkriterien. So heißt es in Artikel 8 des Textes:

> Die Anbieter stellen auf zugängliche Weise in portugiesischer Sprache klare, öffentliche und objektive Informationen über alle Regeln zur Verfügung, die für die Äußerung Dritter gelten, wie z.B. Politiken, Verfahren, Maßnahmen und Instrumente, die zu den in Art. 15 dieses Gesetzes vorgesehenen Zwecken eingesetzt werden, einschließlich der Kriterien für die Entfernung von Inhalten, mit Ausnahme von Geschäfts- und Betriebsgeheimnissen.

Die Regeln in Bezug auf die Transparenzpflichten können vom Gesetzgeber im Gesetz und in anderen normativen Rechtsakten festgelegt werden oder von den Plattformen selbst, die ihre eigenen Regeln ausarbeiten können, solange die von der nationalen Gesetzgebung auferlegten Grenzen sowie das Recht auf Zugang zu Informationen und das Recht auf freie

---

44 *Roberto Beijato Júnior*, Combate à desinformação é o grande desafio de 2022, verfügbar unter: https://www.conjur.com.br/2022-jan-05/beijato-junior-combate-desinformacao-desafio-2022 – letzter Aufruf: 10. März 2022.

45 Gesetzentwürfe Nr. 3063/2020, 283/2020, 2854/2020, 2883/2020, 649/2021, 3119/2020, 2393/2021, 3385/2020, 291/2021, 449/2021, 3573/2021, 213/2021, 495/2021, 2401/2021, 127/2021, 246/2021, 1362/2021, 865/2021, 2390/2021, 10860/2018, 5776/2019, 475/2020, 4418/2020, 4925/2019, 5260/2019, 437/2020, 2284/2020, 6531/2019, 7604/2017, 9647/2018, 2601/2019, 2602/2019, 1941/2020, 2196/2020 und 1897/2021 sind diejenigen, die Regeln und Kriterien für die Entfernung oder Einschränkung von Inhalten festlegen.

Meinungsäußerung[46] respektiert werden. Es handelt sich also um einen Anreiz des Gesetzgebers zur regulierten Selbstregulierung der Plattformen. Außerdem wird die Verpflichtung zur Erstellung von Transparenzberichten eingeführt, die sowohl von Anbietern sozialer Netzwerke und Instant-Messaging-Dienste (Artikel 9) als auch von Suchmaschinenanbietern (Artikel 10) zu erstellen sind. Zu den obligatorischen Bestandteilen der Berichte gehört ihre Häufigkeit (sie müssen in beiden Fällen halbjährlich erstellt werden) und die Angabe der Anzahl der Nutzer der Dienste oder Plattformen sowie der Anzahl der Löschungen von Inhalten.

Auch einige andere, mehr oder weniger polemische Punkte des PL sind erwähnenswert. In Artikel 11 ist vorgesehen, dass akademische Forschungseinrichtungen Zugang zu aufgeschlüsselten Daten erhalten, sofern das Recht auf den Schutz personenbezogener Daten und gegebenenfalls des geistigen Eigentums[47] gewahrt bleibt. Das Gesetz legt auch die Begrenzung der massenhaften Verbreitung von Inhalten und Medien fest – eine Pflicht, die von den Anbietern von Instant-Messaging-Diensten zu beachten ist[48] – sowie die Notwendigkeit, die angepriesenen Inhalte und die Werbung zu identifizieren, sowohl von den Anbietern sozialer Netzwerke

---

46 Art. 7: Um die Einhaltung der in diesem Gesetz festgelegten Ziele zu gewährleisten, stellen die Anbieter ihre eigenen Regeln auf, die die nationale Gesetzgebung respektieren, und wenden sie in gerechter und kohärenter Weise an, wobei sie das Recht auf Zugang zu Informationen und das Recht auf freie Meinungsäußerung respektieren.

47 Art. 11: Vorbehaltlich der Wahrung des Schutzes personenbezogener Daten und des geistigen Eigentums erleichtern die Anbieter akademischen Forschungseinrichtungen den Zugang zu aufgeschlüsselten Daten zum Zweck der akademischen Forschung, vorbehaltlich des Gesetzes Nr. 13.709 vom 14. August 2018.

48 Art. 12: Anbieter von Instant-Messaging-Diensten sollten ihre Plattformen so gestalten, dass der zwischenmenschliche Charakter des Dienstes erhalten bleibt und die massenhafte Verbreitung von Inhalten und Medien begrenzt wird:
I – verbietet die Weiterleitung von Nachrichten oder Medien, die von einem anderen Benutzer empfangen wurden, an mehrere Empfänger;
II – legt fest, dass Übermittlungslisten in jedem Fall nur von Personen weitergeleitet und empfangen werden dürfen, die gleichzeitig in den Kontaktlisten von Absendern und Empfängern aufgeführt sind;
III – führt einen Mechanismus zur Überprüfung der vorherigen Zustimmung des Benutzers zur Aufnahme in Gruppen von Nachrichten, Übermittlungslisten oder gleichwertige Mechanismen zur Gruppierung von Benutzern ein;
IV – deaktiviert standardmäßig die Genehmigung zur Aufnahme in Gruppen und in Übermittlungslisten oder gleichwertige Mechanismen zur Weiterleitung von Nachrichten an mehrere Empfänger.
§ 1 Der Verkauf von Software, Plug-ins und anderen Technologien, die eine Massenverbreitung in Instant-Messaging-Diensten ermöglichen, ist verboten.

als auch von Instant-Messaging-Diensten[49] – Informationen, die für die Nutzer[50] leicht zugänglich sein müssen. Für das Boosten von Inhalten, die Wahlpropaganda enthalten oder einen Kandidaten, eine Koalition oder eine politische Partei[51] erwähnen, werden besondere Regeln festgelegt.

Was schließlich die Transparenzpflichten von sozialen Netzwerken und Instant-Messaging-Diensten betrifft, so enthält Artikel 15 des PL 2630 Bestimmungen über ordnungsgemäße Verfahren, die festlegen,

> „bei der Anwendung ihrer eigenen Regeln, die den Ausschluss, die Nichtverfügbarkeit, Reduzierung des Umfangs und Kennzeichnung von Inhalten, die von Dritten und ihren Konten generiert wurden oder andere Maßnahmen zur Einschränkung der Meinungsäußerung müssen die Anbieter den Nutzer über die Art und die Gründe der angewandten Maßnahme, die Fristen und die Verfahren zur Beantragung einer Überprüfung der Entscheidung informieren, einen geeigneten Kanal zur Einsichtnahme in die bereitgestellten Informationen zur Verfügung stellen und in begründeter Weise auf Anträge auf Überprüfung von Entscheidungen reagieren."

§ 2 Instant-Messaging-Anbieter sollten Lösungen entwickeln, um externe Mechanismen der Massenverbreitung zu erkennen und zu verhindern.
§ 3 Der Verhaltenskodex sollte Instant-Messaging-Anbieter dazu verpflichten, andere Präventivmaßnahmen zu ergreifen, um die massenhafte Verbreitung von Inhalten über ihre Dienste einzudämmen.

49 Art. 16: Anbieter von sozialen Netzwerken und Instant Messaging müssen gepushte und werbliche Inhalte so kennzeichnen, dass
I – das für den Boost verantwortliche Konto oder der Inserent identifiziert ist; und
II – der Nutzer sich an den für das Boosten verantwortlichen Account oder an den Inserenten wenden kann.
Einzelner Absatz: Suchmaschinenanbieter müssen Werbeinhalte so kennzeichnen, dass ein Name und eine Kontaktmöglichkeit des Werbenden für die Nutzer zugänglich sind.

50 Art. 17: Die Anbieter müssen den Nutzern durch einen einfachen Zugang die Visualisierung aller Inhalte von geboosteter Wahlpropaganda zur Verfügung stellen.

51 Siehe Artikel 18 des Gesetzentwurfs.

4.2. Das Dekret („Medida Provisória")

Im September 2021 erließ Präsident Jair Bolsonaro ein Dekret (Medida Provisória)[52], das darauf abzielt, durch Änderung von Teilen des Marco Civil da Internet den Handlungsspielraum sozialer Netzwerke bei der Moderation von Inhalten einzuschränken. Mit der Begründung, dass die Änderung den Grundlagen des Marco Civil entspräche, insbesondere im Hinblick auf die Gewährleistung der Meinungsfreiheit, zielt die Maßnahme laut dem Sekretariat für Regierungskommunikation (Secom) darauf ab, „die willkürliche und unmotivierte Entfernung von Konten, Profilen und Inhalten durch die Anbieter zu bekämpfen".[53] Laut Secom soll die Maßnahme die „Strategien, Verfahren, Maßnahmen und Instrumente" klären, die von Anbietern sozialer Medien zur Löschung oder Sperrung von Inhalten und Konten[54] verwendet werden und eine Reihe von Rechten und Garantien für Nutzer sozialer[55] Medien festlegen.

---

52 Im brasilianischen System, kann der Chef der Exekutive auf einige eigene normative Instrumente zurückgreifen, wie die vorläufige Maßnahme („Medida Provisória") und das Exekutivdekret. Die provisorische Maßnahme ist ein Instrument mit Gesetzeskraft, das vom Präsidenten der Republik in Fällen von Bedeutung und Dringlichkeit für das Land erlassen wird. Es handelt sich um eine Norm, die unmittelbare Wirkungen entfaltet, d.h. sie ist bereits gültig, während sie vom Kongress geprüft wird, obwohl sie von der Zustimmung der Abgeordnetenkammer und des Senats abhängt, um endgültig in ein Gesetz umgewandelt zu werden. Das Dekret hingegen schafft kein Gesetz, kein neues Recht und keine neue Verpflichtung, sondern regelt lediglich ein bestehendes Gesetz, das jedoch sehr weit gefasst oder vage ist und durch die Vorschrift näher ausführt wird. Wie das Medida Provisória kann auch das Dekret nur vom Präsidenten der Republik erlassen werden.

53 Vgl. https://twitter.com/secomvc/status/1434952385324068864?s=19.

54 Vgl. https://twitter.com/secomvc/status/1434952387085619202.

55 Siehe Artikel 8-A der vorläufigen Maßnahme:
Art. 8-A: Den Nutzern werden in den Beziehungen zu den Anbietern sozialer Netzwerke unbeschadet der Bestimmungen von Abschnitt I dieses Kapitels die folgenden Rechte gewährt:
I – Zugang zu klaren, öffentlichen und objektiven Informationen über alle Strategien, Verfahren, Maßnahmen und Instrumente, die zum Zweck einer möglichen Mäßigung oder Begrenzung des Umfangs der Veröffentlichung von nutzergenerierten Inhalten eingesetzt werden, einschließlich der Kriterien und Verfahren, die für menschliche oder automatisierte Entscheidungen verwendet werden, mit Ausnahme von Geschäfts- und Betriebsgeheimnissen;
II – Gegnerschaft, vollständige Verteidigung und Berufung, die im Falle der Moderation von Inhalten zwingend zu beachten sind, und der Anbieter des sozialen

Zu den von der Exekutive vorgeschlagenen Änderungen gehören das Recht auf „Zugang zu klaren, öffentlichen und objektiven Informationen über alle Politiken, Verfahren, Maßnahmen und Instrumente, die zum Zweck einer eventuellen Mäßigung oder Einschränkung des Umfangs der Verbreitung von nutzergenerierten Inhalten eingesetzt werden", die Einhaltung des kontradiktorischen Verfahrens, ausreichende Verteidigungsmöglichkeiten und Rechtsmittel bei der Entfernung von Inhalten sowie das Recht auf Rückgabe der entfernten Inhalte und Wiederherstellung des Nutzerkontos in bestimmten Fällen. Darüber hinaus sollte die Plattform in Fällen der Löschung oder Aussetzung von Konto- oder Profilfunktionen[56] einen triftigen Grund und eine Begründung liefern. Als „triftigem Grund" umfasst der Text der Maßnahme Inhalte, die Gewalt oder diskriminierende Handlungen, Anstiftung zum Terrorismus, Drogenkonsum,

---

Netzwerks muss mindestens einen elektronischen Kommunikationskanal für die Ausübung dieser Rechte anbieten;
III – Rückgabe der vom Nutzer zur Verfügung gestellten Inhalte, insbesondere personenbezogene Daten, Texte, Bilder, u.a., auf Anfrage;
IV – Wiederherstellung des Kontos, des Profils oder der Inhalte in den Zustand, in dem sie sich im Falle einer unzulässigen Moderation durch den Anbieter des sozialen Netzwerks befanden;
V – kein vollständiger oder teilweiser Ausschluss, keine Stornierung oder Aussetzung von Diensten und Funktionen des Kontos oder des Profils, es sei denn, es liegt ein triftiger Grund vor, gemäß den Bestimmungen von Art. 8-B;
VI – kein Ausschluss, keine Aussetzung oder Sperrung der Veröffentlichung von nutzergenerierten Inhalten, außer bei Vorliegen eines berechtigten Grundes, unter Beachtung der Bestimmungen von Art. 8-C; und
VII – Zugang zu einer Zusammenfassung der Nutzungsbedingungen des sozialen Netzwerks, in der die für den Nutzer wichtigsten Regeln hervorgehoben werden.
Einziger Absatz. Den Anbietern von sozialen Netzwerken ist es untersagt, gemäß den Bestimmungen von Art. 8-B und Art. 8-C Kriterien zur Mäßigung oder Einschränkung des Umfangs der Veröffentlichung von Inhalten anzuwenden, die eine politische, weltanschauliche, wissenschaftliche, künstlerische oder religiöse Zensur beinhalten. (NR).

56 Art. 8b: Unter Wahrung der Freiheit der Meinungsäußerung, der Kommunikation und der Gedankenäußerung darf der vollständige oder teilweise Ausschluss, die Löschung oder die Aussetzung der Dienste und Funktionalitäten des Kontos oder des Profils eines Nutzers eines sozialen Netzwerks nur bei Vorliegen eines berechtigten Grundes und einer Begründung erfolgen.
§ 1 Der berechtigende Grund wird durch die folgende Hypothese charakterisiert:
I – Vorgabe durch den Benutzer;
II – Konten, die mit dem Ziel erstellt werden, die Identität Dritter anzunehmen oder zu simulieren, um die Öffentlichkeit zu täuschen, mit Ausnahme des Rechts, einen sozialen Namen und ein Pseudonym zu verwenden, und der ausdrücklich humoristischen oder parodistischen Absicht;

Urheberrechtsverletzungen und die Förderung von Handlungen gegen die öffentliche Sicherheit, die Landesverteidigung und die Staatssicherheit enthalten. Die Förderung von Desinformation, die Verbreitung von Falschnachrichten über die Covid-19-Pandemie oder Hassreden beispielsweise werden jedoch nicht als berechtigender Grund genannt.

Eine Woche nach der Vorlage wurde die MP jedoch durch eine Entscheidung des Bundesgerichts (STF) ausgesetzt. Das Bundesgericht entschied, dass eine provisorische Maßnahme keine Bestimmungen zu den Grundrechten enthalten kann.[57] Vor diesem Hintergrund hat der Chef der Exekutive dem Nationalkongress einen Gesetzentwurf vorgelegt, der dasselbe Ziel verfolgt wie die ausgesetzte provisorische Maßnahme.[58]

5. Fazit

In diesem Zusammenhang stellt der Gesetzentwurf 2630 aus dem Jahr 2020 genau zwei Herausforderungen an die inhaltliche Moderation: eine auf der strukturellen Ebene und eine auf der individuellen Ebene. Auf struktureller Ebene muss sie eine legale und angemessene Antwort auf das Problem der Schaffung einer Ökonomie der Desinformation und der institutionellen Angriffe gegen das brasilianische Verfassungsgericht und Parlament bieten, mit dem sich das brasilianische Verfassungsgericht in den Fake-News-Ermittlungsverfahren[59] konfrontiert sah. Hier müssen wir

---

III – Konten, die überwiegend von einem Computerprogramm oder einer Technologie verwaltet werden, die menschliche Tätigkeiten bei der Verbreitung von Inhalten bei Anbietern simulieren oder ersetzen;
IV – Wiederholte Ausübung der in Art. 8-C vorgesehenen Handlungen;
V – Konten, die Produkte oder Dienstleistungen anbieten, die Patent-, Marken-, Urheberrechte oder andere Rechte an geistigem Eigentum verletzen; oder
VI – Befolgung eines Gerichtsbeschlusses.

57 Vgl. *Sergio Rodas,* Rosa Weber suspende MP que limita remoção de conteúdo em redes sociais. Verfügbar unter: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet – letzter Aufruf: 14. Feb. 2021.

58 Obwohl der Text des Gesetzentwurfs noch nicht verfügbar ist, lässt sich dies aus der Veröffentlichung auf der offiziellen Website der Regierung ableiten. Siehe: Der Präsident der Republik schlägt einen Gesetzesentwurf vor, um die Rechte der Nutzer sozialer Netzwerke zu garantieren, Verfügbar unter: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2021/09/presidente-da-republica-propoe-projeto-de-lei-para-garantir-direitos-dos-usuarios-de-redes-sociais – letzter Aufruf: 16. Feb. 2022.

59 Im März 2019 eröffnete der damalige Präsident des Obersten Gerichtshofs, Dias Tofolli, eine Untersuchung, um Angriffe durch Fake News, Verleumdungen und

auf die strukturelle Ebene abzielen (und nicht nur auf die individuelle), sonst laufen wir Gefahr, ähnlich wie in der griechischen Mythologie der lernäischen Hydra, für jeden abgeschlagenen Kopf mehrere andere an seiner Stelle erscheinen zu lassen. Eine einfache, wirksame und strukturelle Lösung bestünde darin, alle Formen der Monetarisierung (die durch Werbung erfolgen) dem nationalen Werberecht zu unterstellen, das in diesem Sektor bereits seit Jahrzehnten durch eine Art regulierter Selbstregulierung einen wirksamen Rahmen geschaffen hat, um so Erfahrungen für künftige Bewertungen, Korrekturen und Regelungen zu sammeln.[60]

Auf individueller Ebene liegt die große Herausforderung in der Frage des Zugangs zum Recht und der Umsetzung von Verfahrenspflichten. Zum Schutz des Einzelnen sollte die erste Verteidigung des Nutzers auf vereinfachte und kostenlose Weise auf der Plattform selbst erfolgen, die den Nutzern vor der Entfernung von Inhalten ein ordnungsgemäßes Informationsverfahren mit ständiger Berichterstattung an die öffentliche Gewalt bieten sollte. In diesem Zusammenhang würde die Justiz als Beobachter zweiter Ordnung fungieren, der prüft, ob die befolgten Normen mit den öffentlichen Vorgaben übereinstimmen, aber auch jederzeit die Möglichkeit hat, zu entscheiden.

Eine Möglichkeit, die Verantwortung neuer Intermediäre jenseits der auf dem politischen Prozess (des Nationalstaates) basierenden Meinungsfreiheit zu modellieren, liegt in einer Art Prozeduralisierung der kommunikativen und medialen Grundrechte, die den Schutz eines unpersönlichen Meinungsbildungsprozesses stark betont. Eine Prozeduralisierung des Rechtsschutzes in der Plattformgesellschaft sollte die Dynamik aktuel-

---

Drohungen zu untersuchen, die den Gerichtshof, seine Minister und deren Familien betreffen. Der Richter Alexandre de Moraes wurde zum Berichterstatter der Untersuchung ernannt, der unter anderem mehrere Anhänger und Verbündete von Präsident Jair Bolsonaro sowie der Präsident selbst angehören.

60 Der Exekutivrat für Standardnormen – CENP – ist das Gremium, das für die Regulierung der internen Organisation und die Arbeitsweise von Werbeagenturen zuständig ist und die Bescheinigung ausstellt, die die Agentur zu ihrer Tätigkeit berechtigt. Der Erhalt eines solchen Dokuments hängt davon ab, dass die Agentur die Anforderungen der Agenturnormen erfüllt. Für die inhaltliche Kontrolle der von einer Agentur tatsächlich ausgeführten Arbeiten, wie z.B. Anzeigen und Plakate, ist der Rat für die Selbstregulierung der Werbung – CONAR – zuständig. Die Agentur wurde während der Militärdiktatur von Mitgliedern mehrerer brasilianischer Werbeklassen gegründet, um zu verhindern, dass die Zensur der Presse auch die Werbung erreicht. Das wichtigste Instrument, auf das der Rat seine Entscheidungen stützt, ist der brasilianische Selbstregulierungskodex für Werbung.

ler Computernetzwerke und Geschäftsmodelle berücksichtigen, um den Rechtsschutz im Medium selbst mit einer ständigen Beobachtungspflicht durch staatliche[61] Gerichte zu gewährleisten.

Referenzen

ALMEIDA, Guilherme Alberto Almeida de. Marco Civil da Internet – Antecedentes, formulação colaborativa e resultados alcançados. In: ARTESE, Gustavo (Coord.). *Marco Civil da Internet*: análise jurídica sob uma perspectiva empresarial. São Paulo: Quartier Latin, 2015.

Gillespie, Tarleton. *Custodians of the Internet*. Platforms, content moderation, and the hidden decisions that shape social media, New Haven 2018.

KANAYAMA, Ricardo Alberto. A liberdade de expressão do Marco Civil da Internet e o procedimento de notificação e retirada para as "infrações" aos direitos autorais. *Civilistica.com*. Rio de Janeiro, a. 10, n. 1, 2021. Disponível em: <http://civilistica.com/a-liberdade-de-expressao-do-marco-civil/>. Acesso em: 14 fev. 2022.

Klonick, Kate. The New Governors: The People, Rules, and Processes Governing Online Speech. 131 *Harv. L. Rev*. 2018, S. 1602–1670.

Ladeur, Karl-Heinz. Helmut Ridders Konzeption der Meinungsfreiheit als Prozessgrundrecht, *KJ* 53/2 (2020), S. 172–182.

LEMOS, Ronaldo. Uma breve história da Criação do Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: Marco Civil da Internet. Tomo I. São Paulo: Quartier Latin, 2015, S. 82.

LIMA, Cíntia Rosa Pereira de. A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do Marco Civil da Internet (Lei n. 12.965/14). *Revista da Faculdade de Direito da Universidade de São Paulo* 110 (jan./dez. 2015), S. 157.

Luhmann, Niklas. *Die Realität der Massenmedien*. Opladen: Westdt. Verlag, 1996.

Rodas, Sergio. Rosa Weber suspende MP que limita remoção de conteúdo em redes sociais. Verfügbar unter: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet – letzter Aufruf: 14. Feb. 2021.

61 *Karl-Heinz Ladeur*, Helmut Ridders Konzeption der Meinungsfreiheit als Prozessgrundrecht, KJ 53/2 (2020), S. 172 (178); *Gunther Teubner*, Zum transsubjektiven Potential subjektiver Rechte. Gegenrechte in ihrer kommunikativen, kollektiven und institutionellen Dimension, in: Hanna Franzki/ Johann Horst/ Andreas Fischer-Lescano (Hrsg.), Gegenrechte: Recht jenseits des Subjekts, Tübingen 2018, S. 357.

SCHREIBER, Anderson. Marco Civil da Internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: LUCCA, Newton de; SIMÃO FILHO; Adalberto; LIMA, Cíntia Rosa Pereira de (Coords). *Direito & Internet*. Tomo II: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015.

SOUZA, Carlos Affonso Pereira de. Responsabilidade civil dos provedores de acesso e de aplicações de internet: evolução jurisprudencial e os impactos da Lei 12.695/2014 (Marco Civil da Internet). In: SALOMÃO LEITE, George; LEMOS, Ronaldo (Coord.). *Marco Civil da Internet***.** São Paulo: Atlas, 2014.

SOUZA, Carlos Affonso Pereira de; LEMOS, Ronaldo. *Marco Civil da Internet*: construção e aplicação. [*s.l.*], 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf>. Acesso em: 14 fev. 2022.

SOUZA, Carlos Affonso e TEFFÉ, Chiara Spadaccini de. Responsabilidade dos provedores por conteúdos de terceiros na internet. *CONJUR*. Disponível em: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet. Acesso em: 14 fev. 2021

QUEIROZ, João Quinelato de. Aplicabilidade do Marco Civil da Internet na responsabilidade civil por uso indevido de conteúdo protegido por direitos autorais na internet. *Civilistica.com*. Rio de Janeiro, a. 5, n. 2, 2016. Disponível em: <http://civilistica.com/aplicabilidade-do-marco-civil-da-internet/>. Acesso em: 14 fev. 2022.

Souza, Carlos Affonso; Lemos, Ronaldo. *Marco civil da internet: construção e aplicação*. Juiz de Fora: Editora Associada Ltda, 2016.

Blum, Renato Opice; Sá Elias, Paulo; Monteiro, Renato Leite. Marco regulatório da internet brasileira: "Marco Civil". Disponível em: <https://www.migalhas.com.br/depeso/157848/marco-regulatorio-da-internet-brasileira---marco-civil>. Acesso em: 10 mar. 2022.

CÉSAR, David; BARRETO JUNIOR, Irineu F. Marco Civil da Internet e Neutralidade da Rede: Aspectos Jurídicos e Tecnológicos. *Revista Eletrônica do Curso de Direito da UFSM*, v. 12, n. 1, S. 65, 19 abr. 2017.

Beijato Júnior, Roberto. Combate à desinformação é o grande desafio de 2022. Disponível em: <https://www.conjur.com.br/2022-jan-05/beijato-junior-combate-desinformacao-desafio-2022>. Acesso em: 10 mar. 2022.

Teubner, Gunther. Zum transsubjektiven Potential subjektiver Rechte. Gegenrechte in ihrer kommunikativen, kollektiven und institutionellen Dimension, in: Franzki, Hanna; Horst, Johann; Fischer-Lescano, Andreas (Hrsg.), *Gegenrechte*: Recht jenseits des Subjekts, Tübingen: Mohr Siebeck 2018, S. 357–375.

Thompson, Marco. Civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na Internet do Brasil, RDA – *Revista de Direito Administrativo* 261 (2012), S. 203–251.

Tushnet, Rebecca. Power without Responsibility: Intermediaries and the First Amendment, *George Washington Law Review* 76 (2008).

Vesting, Thomas. Die Rundfunkfreiheit und die neue Logik der »Content-Curation« in elektronischen Netzwerken, *JZ* 75 (2020), S. 975–982.

Opportunities and Limits of European Social Network Regulation

Marco Almada, Andrea Loreggia, Juliano Maranhão, Giovanni Sartor

1 Introduction

Social networks are a distinctive feature of modern society. As of 2022, people in almost every country of the world rely on one network or another for a multitude of tasks: to get information about local and global affairs, to interact with acquaintances old and new, to find—and even carry out—work, among other relevant aspects of social life. By creating spaces that lend themselves to such diverse uses, the companies running the largest social networks have managed to position themselves among the largest businesses in the world.[1] Yet, the sheer diversity of the interactions ongoing in social networks means some of such interactions are relevant to the law in one form or another, either for the prevention and repression of potentially harmful activities, or for the promotion of beneficial services and interactions. Therefore, the regulation of social networks is a problem that legislators and courts worldwide have to face, and the European Union (EU) is no exception.

Regulating social networks is a complex issue for a variety of factors. Some of the complexity stems from the global reach of platforms, which have users in various countries and are, accordingly, subject to various jurisdictions.[2] Moreover, regulation has to take into account the business model adopted by social networks: users normally can join and use networks for free,[3] but companies use the content they generate to attract new

1 See, e.g., 'Facebook Reports Third Quarter 2021 Results', Meta Investor Relations, 25 October 2021, https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Third-Quarter-2021-Results/default.aspx.

2 On the challenges of global governance, see, e.g., Robert Fay, 'A Model for Global Governance of Platforms', ed. Martin Moore and Damian Tambini (Oxford: Oxford University Press, 2021), 255–79, https://doi.org/10.1093/oso/9780197616093.003.0016.

3 Some networks, however, have experimented with tiered subscription models, in which users pay for having access to features not available to a general audience: Sara Beykpour and Smita Gupta, 'Introducing Twitter Blue - Twitter's First-Ever

consumers and render these users legible to various forms of marketing, notably targeted advertising.[4] As such, strategies used to regulate other kinds of business might not be as effective when directed towards social networks. A final challenge inheres in the technological complexity of social networks. These networks rely on sophisticated technical infrastructures that enable user communication and render users legible by storing the data they provide and drawing inferences from such data,[5] a practice that is compounded by the ongoing development of artificial intelligence (AI) technologies. On the one hand, legibility allows the use of AI systems directed at influencing user behaviour in ways that are not necessarily in their best interest, ranging from selling products[6] to shaping political behaviour through targeted propaganda[7] and forgeries that are indistinguishable from real content.[8] On the other hand, AI systems may be used to protect users' rights online, for example, by contributing to the detection and elimination of these kinds of influence.[9] Consequently, the debates on social networks are increasingly tangled with the present and future of AI.

Regulating social networks is a task that involves multiple levels. Competition law sets up rules meant to prevent social networks from abusing

---

Subscription Offering', Company Blog, *Twitter* (blog), 3 June 2021, https://blog.twitter.com/en_us/topics/company/2021/introducing-twitter-blue.

4 On this point, see Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford, New York: Oxford University Press, 2019), chap. 2.

5 On the role of inferences as a source of data, see Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI', *Columbia Business Law Review* 2019, no. 2 (2019): 494–620.

6 See, e.g., Federico Galli, 'Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD', in *Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges*, ed. Martin Ebers and Marta Cantero Gamito, Data Science, Machine Intelligence, and Law (Cham: Springer International Publishing, 2021), 109–35, https://doi.org/10.1007/978-3-030-50559-2_6.

7 See, e.g., Ronan Ó Fathaigh et al., 'Microtargeted Propaganda by Foreign Actors: An Interdisciplinary Exploration', *Maastricht Journal of European and Comparative Law* 28, no. 6 (1 December 2021): 856–77, https://doi.org/10.1177/1023263X211042471.

8 Bobby Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', *California Law Review* 107, no. 6 (2019): 1753–1820.

9 Giovanni Sartor and Andrea Loreggia, 'The Impact of Algorithms for Online Content Filtering or Moderation. Upload Filters', Study for the committee on Citizens' Rights and Constitutional Affairs (Brussels: European Parliament, 2020).

dominant positions.[10] Other norms govern user-generated content as a source of data, notably data protection law.[11] Finally, some norms can be said to establish social network regulation in a narrow sense, as they establish what networks can or cannot do in their everyday operation. This latter set is the object of the present chapter.

This chapter argues that social networks are currently undergoing a turn towards adopting procedural safeguards and duties of care regarding the substantive rights of users. Section 2 presents the backdrop for this argument. The current EU regulatory framework, centred on the eCommerce Directive,[12] was thought for a different online environment. Therefore, it is strained by social networks in ways legislators and courts are currently trying to address. Some of these strains are produced by the institutional design of the regulatory framework, but these institutional factors only become a problem in light of the harms that social networks introduce or amplify, which are the subject of Section 3. Despite the fact that harmful user behaviour may sometimes be advantageous to social networks (e.g., by attracting certain groups of users), social networks may be induced to adopt content moderation approaches not only in the interest of the users that could be harmed or repelled by such behaviour, but also to avoid losing the liability exemption they enjoy as intermediary carriers of user-generated content. As Section 4 shows, content moderation may itself introduce risks to users' rights, and EU courts and legislators have sought to constrain the range of discretion available to moderators. In this context, we argue the regulation of social networks should be perceived as a socio-technical problem, in which neither technical approaches nor general law alone are conducive to socially desirable outcomes. Instead, regulation needs to be aware of the social impacts of platforms, and the role technology can play in amplifying or mitigating them.

---

10 In the European Union, see Nicolas Petit, 'The Proposed Digital Markets Act (DMA): A Legal and Policy Review', *Journal of European Competition Law & Practice* 12, no. 7 (1 September 2021): 529–41, https://doi.org/10.1093/jeclap/lpab062.

11 See, e.g., Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence', *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (28 November 2018), https://doi.org/10.1098/rsta.2018.0089.

12 European Union, 'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce')' (2000), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031.

2 The European regulatory landscape

The eCommerce Directive,[13] adopted in 2000, provides the general framework for the regulation of the online environment in the European Union. This Directive harmonises the rules applicable to information society services, that is, to "service[s] normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[14] As outlined in the introduction, a social network meets all elements of this definition: it provides services to users who voluntarily join the network through electronic means. Since these services are usually provided through a by-profit model, social networks fall into the scope of the existing regulatory framework for information society services.

Social networks are part of a well-defined regulatory environment, which contains not only a broad set of applicable norms but also enforcement structures at the national and EU levels.[15] But, as the short name of the Directive suggests, this regulatory framework was originally designed to deal with a different set of concerns than the ones raised by social network's current role in European society.[16] While eCommerce services profit from enabling the acquisition of goods through a virtual environment, and platforms such as newspapers act themselves as sources of content, social networks are doubly dependent on the information produced by the users in different ways: user-generated content makes the platform relevant to content-consuming users, while information about users allows for the monetisation strategies described above and for individualised strategies aimed at keeping users engaged with the platform. As a result, the frame-

13 European Union.

14 Article 1(1)(b) of European Union, 'Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services (Text with EEA Relevance)' (2015), http://data.europa.eu/eli/dir/2015/1535/oj/eng. This directive repealed and replaced Directive 98/34/EC, to which Article 2(a) of the eCommerce Directive referred when defining "information society services".

15 Alexandre de Streel and Martin Husovec, 'The E-Commerce Directive as the Cornerstone of the Internal Market. Assessment and Options for Reform', Study for the committee on Internal Market and Consumer Protection (Luxembourg: European Parliament, 2020), sec. 2.3.4.

16 For a historical overview of the evolution of platform regulation in the European Union, see Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union', *International Journal of Constitutional Law* 19, no. 1 (2021): 41–70, https://doi.org/10.1093/icon/moab001.

work established by the eCommerce Directive shows some signs of strain as it attempts to fit social networks into rules conceived for a different moment of the Internet.

The first issue demanding attention is that of regulatory fragmentation. By their very digital nature, social networks can reunite under the same virtual environment users physically located in different countries. From a legal perspective, geographical dispersion brings at least two challenges to the regulatory system. The first one is that two or more legal systems may have a claim to apply their laws to a given event, for example, in the case of a dispute between users based in two different countries. Such situations are in principle covered by existing rules on conflicts of law and court jurisdiction.[17] However, these rules are complicated subjects in their own right,[18] so their application to the context of online platforms may pose practical problems to lawyers and courts. Moreover, a single harmful act may have effects that are relevant to multiple jurisdictions.

Thus, users of the same network may be covered by different norms regarding the same conduct. Social networks are thus required to consider a user's location in the physical world to identify which laws apply to them, and possibly also other locations in which harmful effects were produced. Within the European Union, the eCommerce Directive reduces regulatory complexity, as it provides various requirements that the EU Member States must observe when designing their own laws for information society services. But the harmonisation provided by a Directive is only partial, as each Member State can choose the form and methods it will use to comply with the requirements imposed by EU legislation.[19] This partial harmonisation allows Member States to adopt regulation beyond the minimum guidelines set at the Union level. Indeed, Germany has done so in its own approach to network regulation.[20] As a result, EU nationals using the

17 In fact, the eCommerce Directive explicitly rejects the creation of new rules on these matters: see Article 1(4) and the accompanying Recital 23.

18 See, e.g., Pedro de Miguel Asensio, *Conflict of Laws and the Internet* (Edward Elgar Publishing, 2020), chap. 2; Ilaria Pretelli, 'Protecting Digital Platform Users by Means of Private International Law', *Cuadernos de Derecho Transnacional* 13, no. 1 (2021): 574–85.

19 On EU directives and their legal effects, see, e.g., Robert Schütze, 'Direct Effect', in *An Introduction to European Law*, 3rd ed. (Oxford: Oxford University Press, 2020), 109–32, https://doi.org/10.1093/he/9780198858942.003.0005.

20 See, in addition to the relevant chapters in this book, Robert Gorwa, 'Elections, Institutions, and the Regulatory Politics of Platform Governance: The Case of the German NetzDG', *Telecommunications Policy*, Norm entrepreneurship in Internet Governance, 45, no. 6 (1 July 2021): 102145, https://doi.org/10.1016/j.telpol.20

same network—and potentially interacting with the same content—might be subject to substantively different norms.

Fragmentation in European network regulation is not produced just by the Member States. Within the European Union legal order itself, various *lex specialis* instruments govern specific practices at the core of how social networks operate. This chapter engages directly with two such instruments— the Copyright Directive[21] and the Terrorist Content Regulation.[22] This fragmentation is not necessarily harmful to regulation, especially if it supplies an effective response to harms that would be ill-addressed by changes to general legislation. Yet, by definition, the adoption of specialised norms[23] may increase compliance costs for social networks and make users less certain about the rules that apply to their circumstances.

However, we should not overestimate the level of fragmentation seen in EU social network regulation. After all, the eCommerce Directive establishes various requirements for Member State legislation. Some of these are directed at ensuring harmonised conditions for the information society services themselves, such as the functioning of the internal market for such services,[24] their establishment,[25] or the possibility of relying on out-of-court dispute settlement.[26] Other provisions provide guarantees for the users of such services, such as the minimum standards for information to

---

21.102145; Patrick Zurth, 'The German NetzDG as Role Model or Cautionary Tale? – Implications for the Debate on Social Media Liability', *Fordham Intellectual Property, Media & Entertainment Law Journal* 31, no. 4 (2021): 1084–1153, https://doi.org/10.2139/ssrn.3668804.

21 'Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC (Text with EEA Relevance.)' (n.d.).

22 'Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online (Text with EEA Relevance)' (2021).

23 On generality as a legal value, see, e.g., Gregor Kirchhof, 'The Generality of the Law: The Law as a Necessary Guarantor of Freedom, Equality and Democracy and the Differentiated Role of the Federal Constitutional Court as a Watchdog', in *Rational Lawmaking under Review: Legisprudence According to the German Federal Constitutional Court*, ed. Klaus Meßerschmidt and A. Daniel Oliver-Lalana, Legisprudence Library (Cham: Springer International Publishing, 2016), 89–127, https://doi.org/10.1007/978-3-319-33217-8_5.

24 Article 3 eCommerce Directive.

25 Article 4 eCommerce Directive excludes any need for prior authorisation before offering an information society service.

26 Article 17 eCommerce Directive.

be provided by the service[27] or the specific rules for commercial communications,[28] contracts concluded through electronic means,[29] and the liability of intermediary service providers for the content they provide.[30] Regardless of how the Member States exercise their legislative power with regard to platforms, they are still required to *at least* comply with the Directive and—more than that—cooperate actively in rendering it effective.[31] The eCommerce Directive thus provides users and platforms with a regulatory baseline, setting expectations for how social networks function.

Yet, this baseline is somewhat thin. While adequate transposition of the eCommerce Directive leads to various requirements being imposed upon social networks, these still have considerable leeway to determine the conditions for providing their service. Indeed, large social networks are notorious for adopting extensive terms of service,[32] which empower them with vast discretion regarding content removal, monetisation of user data, and various other aspects.[33] This discretion is somewhat reduced by the *sp*ecialised norms mentioned above, as their strict rules on content removal are accompanied by requirements that mandate procedural safeguards that users can invoke in case of removed content.[34] But the Directive itself has little to say about how platforms should set up their Terms of Service, leaving them considerable room for manoeuvre within the general constraints of the legal system to private autonomy. Given the centrality of social networks in modern social life, these decisions may have a considerable impact upon a person's social life or even their livelihood, thus prompting users to resort to judicial or administrative authorities to assert their rights liberties, and interests.

A final source of tension between social networks and regulation based on older models of information society services is data governance. Tradi-

27 Article 5 eCommerce Directive.
28 Articles 6–8 eCommerce Directive.
29 Articles 9–11 eCommerce Directive.
30 Articles 12–15 eCommerce Directive, which Section 4 below examines in further detail.
31 Article 19 eCommerce Directive.
32 These terms are often opaque, in the sense they are difficult reading even for a trained lawyer: Marco Lippi et al., 'CLAUDETTE: An Automated Detector of Potentially Unfair Clauses in Online Terms of Service', *Artificial Intelligence and Law* 27, no. 2 (1 June 2019): 117–18, https://doi.org/10.1007/s10506-019-09243-2.
33 See, *inter alia*, Dan Wielsch, 'Private Law Regulation of Digital Intermediaries', *European Review of Private Law* 27, no. 2 (1 April 2019), http://kluwerlawonline.com/journalarticle/European+Review+of+Private+Law/27.2/ERPL2019013.
34 See Section 4 below.

tional information society services produced—and made use of—substantial volumes of data about users and their transactions. As a result, data protection law was already a key factor in their governance.[35] For social networks, however, users' data is not just an instrument for controlling their operation but also a central element in their business models. Acknowledging this new reality, the EU has substantially revamped its data governance framework, most notably by adopting a General Data Protection Regulation.[36] Those norms are directly applicable to the operations of social networks and provide safeguards to the rights of platform users and third parties that might be affected by content shared on the networks or by inferences made from it.[37] Yet, data protection law, by construction, focuses on individuals rights, thus failing to account for the systemic effects that data may have within social networks.[38]

35 Accordingly, the CJEU has produced a considerable volume of case law on information society services. For an overview, see Giovanni De Gregorio, 'From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society', *European Journal of Legal Studies* 11 (2019): sec. III.1.

36 At the same time the GDPR supplies a stricter framework for the governance of personal data, other pieces of EU legislation—such as the proposed Data Governance Act—seek to create favourable conditions for the circulation of non-personal data. For an overview of data governance in the European Union, see Thomas Streinz, 'The Evolution of European Data Law', in *The Evolution of EU Law*, ed. Paul Craig and Gráinne de Búrca, 3rd ed. (Oxford: Oxford University Press, 2021), 902–36, https://doi.org/10.1093/oso/9780192846556.003.0029. It is important to keep in mind, however, that the distinction between personal data and non-personal data is not always clearcut: Marco Almada, Juliano Maranhão, and Giovanni Sartor, 'Article 4 Para. 5. Pseudonymisation', in *General Data Protection Regulation. Article-by-Article Commentary*, ed. Indra Spiecker gen. Döhmann et al. (Munich; Baden-Baden; Oxford: Beck; Nomos; Hart Publishing, 2022).

37 Pedro A. de Miguel Asensio, 'Data Protection in the Internet: A European Union Perspective', in *Data Protection in the Internet*, ed. Dário Moura Vicente and Sofia de Vasconcelos Casimiro, Ius Comparatum - Global Studies in Comparative Law (Cham: Springer International Publishing, 2020), 457–77, https://doi.org/10.1007/978-3-030-28049-9_18.

38 For general analyses of the limits of this individualistic framework, see Przemysław Pałka, 'Data Management Law for the 2020s: The Lost Origins and the New Needs', *Buffalo Law Review* 68, no. 2 (1 April 2020): 559–640; Cohen, *Between Truth and Power*, chap. 2. For an example, consider how data protection law offer little remedy against the production of filter bubbles through algorithmic recommender systems: Marco Almada, Juliano Maranhão, and Giovanni Sartor, 'Article 6 Para. 1. Content Personalisation', in *General Data Protection Regulation. Article-by-Article Commentary*, ed. Indra Spiecker gen. Döhmann et al. (Munich; Baden-Baden; Oxford: Beck; Nomos; Hart Publishing, 2022).

Considering these challenges posed by social networks to the governance of the information society, the EU legislator is currently seeking to update this overall framework. The key idea beyond the changes to social network regulation is *digital constitutionalism*,[39] that is, the extension to the digital environment of the constitutionalist ideals of separation of powers and protection of fundamental rights.[40] In the context of social networks, these ideals are translated into a double movement: introducing substantive requirements for the protection of rights online[41] and adopting due process considerations regarding network decisions on whether to remove online content.[42]

This movement towards digital constitutionalism has been reflected in the specialised instruments mentioned above, but it is particularly salient in the Digital Services Act package proposed by the European Commission.[43] At the core of this package lie two pieces of legislation. The first one is the eponymous legal instrument, which amends the framework of the eCommerce Directive to extend its principles to a context marked by different technologies and the substantial power of very large online platforms.[44] This proposal is complemented by Digital Markets Act, which includes a broad range of measures to restrict the power of so-called gatekeeper services, such as advertising services and the social networks themselves.[45] While these legal instruments focus on different legal challenges posed by platforms such as social networks, they nevertheless share the two elements of digital constitutionalism presented above, as they impose limits to what platforms can do and forces them to adopt formal

39 De Gregorio, 'The Rise of Digital Constitutionalism in the European Union'.

40 Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation', *International Review of Law, Computers & Technology* 33, no. 1 (2 January 2019): 76–99, https://doi.org/10.1080/13600869.2019.1562604.

41 See, e.g., De Gregorio, 'From Constitutional Freedoms to the Power of the Platforms', V.II.

42 See, e.g., De Gregorio, V.I.

43 https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

44 See European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' (Brussels: European Commission, 15 December 2020).

45 For an introduction to the DMA as it stands as of December 2021, see Filomena Chirico, 'Digital Markets Act: A Regulatory Perspective', *Journal of European Competition Law & Practice*, no. lpab058 (2021), https://doi.org/10.1093/jeclap/lpab058; Petit, 'The Proposed Digital Markets Act (DMA)'; Natalia Moreno Belloso, 'The Proposal for a Digital Markets Act (DMA): A Summary', 3 January 2022, https://papers.ssrn.com/abstract=3999966.

procedures for handling complaints. Still, they retain the core element of the governance regime described above: treating social network liability as the exception and not the rule.

3 User-generated content and online harms

Social networks, as seen in the Introduction, are not in the business of producing content. Instead, they provide their users with a digital environment to interact with other users.[46] This interaction, in turn, produces *user-generated content* of various forms, such as private messages to other users, texts aimed at a general audience, memes, or live streams of audiovisual content. User-generated content may benefit users: they may learn new things from online sources, find joy in meeting new people and reconnecting with old acquaintances, and so on. However, online interactions may also negatively affect users, leading to psychological or even material harm. This section provides a brief overview of the various mechanisms through which users may be harmed within social networks and how these networks respond to harmful content within the current EU regulatory framework.

Online harm may take various forms. In some cases, harm comes from practices much older than social networking. Scammers can use social networks to identify and contact potential victims, bullies can expose their victims to ridicule or worse, and racists and other hate groups can direct their vitriol against vulnerable individuals and groups. While these practices are long-standing social issues, social networks transform how they take place. Through social networks, users with harmful intent can contact a larger number of victims simultaneously, even if these targets are geographically distant from one another. Social networking may also amplify the effect of harms committed in public, such as bullying: given the difficulties of removing content from the Internet,[47] targeted users may be forced to revisit the pain and humiliation of what they have been through. .

46 These users might be natural persons or collective profiles standing for a legal person or other groupings of people.

47 Not just from the technical issues of removal, but also because the very attempt of removing something might call attention to the original content, in the so-called Streisand Effect: Daphne Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling', *GRUR International* 69, no. 6 (1 June 2020): 622, https://doi.org/10.1093/grurint/ikaa047.

User-generated content may also be directed towards forms of harm with no clear offline analogue. One such phenomenon is *doxing*, that is, the disclosure of personal information about a user within a network.[48] This practice is often, though not always, directed towards users that express controversial opinions online[49] as an attempt to highlight to these users that their opinion will have offline consequences. In fact, the information disclosure is often accompanied by pressure towards real-world acquaintances of the targeted user, such as calls for their employer to fire them for their online expression.[50]

The recent developments in artificial intelligence technologies, combined with the vast amounts of data available in social networks,[51] introduce new avenues for harm. Artificial Intelligence (AI) is a field of Computer Science whose aim is studying and developing methodologies to build artefacts that can engage in intelligent behaviour. A formal definition of AI that may satisfy everyone does not exist due to the absence of a definition of intelligence. One of the founding fathers of the discipline, Marvin Minsky, defines "artificial intelligence" as "the science of making machines do things that would require intelligence if done by men".[52] As you can notice, this does not provide a clear definition of the discipline but rather defines what artificial means, that is, something done by a machine.

Recently, the High-Level Expert Group on AI ventured a definition: "AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is

48 Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection', *European Journal of Risk Regulation* 12, no. 4 (2021): 767, https://doi.org/10.1017/err.2021.8.

49 Here, it is important to keep in mind that what counts as "controversial" for a xenophobe might be simply called "respect to human rights" for most of us.

50 A particularly gruesome example was the case of Samuel Paty, a French teacher murdered in 2020 after being the target of a social media campaign that, among other issues, publicised his home address: Bahar Makooi, '"The Violence Shook Me Profoundly": Teachers, Students Remember Samuel Paty's Murder', *France 24*, 15 October 2021, sec. france, https://www.france24.com/en/france/20211015-the-violence-shook-me-profoundly-teachers-students-remember-samuel-paty-s-murder.

51 Francesca Lagioia and Giovanni Sartor, 'Artificial Intelligence in the Big Data Era: Risks and Opportunities', in *Legal Challenges of Big Data*, ed. Joe Cannatacci, Valeria Falce, and Oreste Pollicino (Northampton: Edward Elgar, 2020), 280–307.

52 Marvin Minsky, ed., *Semantic Information Processing* (Cambridge, Mass.: MIT Press, 1968), v.

affected by their previous actions".[53] Thus, AI is a wide area that comprehends a heterogeneous set of methodologies that can be divided into two macro-categories: symbolic AI and sub-symbolic AI. The former focuses on top-down approaches that leverage high-level symbolic representation of problems. Symbolic AI is based on logical representation coupled with reasoning processes. This approach makes the functioning of such systems comprehensible to humans, but it has difficulties in scaling up, given the difficulty of capturing complex real-life scenarios through human-generated formalisations. Instead, sub-symbolic AI is based on bottom-up approaches that learn from data how to reach particular objectives. This reliance on machine learning tasks allows sub-symbolic AI to generalise to extraordinarily complex situations, but it requires a huge amount of data to train the systems.

During the last few years, we witnessed the rise of machine learning techniques. Due to the impressive performance that these technologies can get in many different domains, they were also adopted in moderation to filter unwanted content. A machine learning model learns from data a probabilistic model that generalises to unseen scenarios. Let us consider a standard classification model, for instance, one based on a neural network (many models in machine learning are based on neural networks and their variants). A classification model has as many inputs as the number of features representing the input sample, and it has as many outputs as the number of classes or categories. For each sample, the model computes the probability that the input belongs to each class, returning as the model prediction the class with the highest probability. To do that, the model must be trained. During the training phase, the model is fed with samples and the corresponding real label, thus allowing the system to compare its prediction with the correct one and compute the error. This comparison is used to adjust the internal state to minimise the error. If the data is representative of the domain, this process teaches the model how to generalise its predictions also to input that is not seen during the training phase.

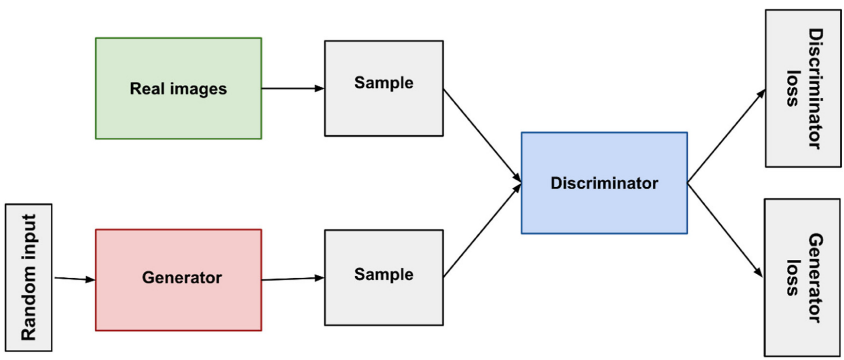
Recently, Generative Adversarial Networks (GAN)[54] have come to the attention of many researchers, practitioners, and to the public audience as an immensely promising tool and very risky threat at the same time. A GAN is a model made by two machine learning modules (usually two

53 AI HLEG, 'Ethics Guidelines for Trustworthy AI', Independent High-Level Expert Group on Artificial Intelligence (Brussels: European Commission, 2019).

54 Ian Goodfellow et al., 'Generative Adversarial Nets', in *Advances in Neural Information Processing Systems*, vol. 27 (NIPS, 2014).

neural networks), one is called the generator, and the other is called the discriminator. The aim of the generator is to produce synthetic data that can be used as an input to the discriminator. The latter aims at identifying whether a given input is fake (i.e., generated by the generator module) or genuine. The generator gets a positive reward when the discriminator is fooled. Similarly, the discriminator gets a positive reward when it correctly classifies an input. During the first part of the training phase, the generator produces low-quality data. Still, if the model is configured correctly and there is enough training data, at the end of the training phase the generator becomes really good at generating data such that it is almost impossible to distinguish fake contents from the real ones. Figure 1 shows a schema of the architecture of a standard GAN.[55]

Figure 1 Overview of a standard GAN schema.



This technology has rapidly spread on the Internet as it generates data for research purposes, data augmentation,[56] or the generation of computational art.[57] Unfortunately, this technology has many nefarious uses. For instance, it is possible to employ the tool to change the tone of a recorded voice to make it resemble somebody else's voice.[58] With some adjustments,

55 https://developers.google.com/machine-learning/gan/gan_structure.

56 Data augmentation refers to the expansion of existing data sets through synthetic data. GANs contribute to this task as they produce "realistic" data, in the sense that the data generated by the network resembles the properties of the original data set.

57 For an example, see the "Dream" application: https://www.wombo.art/.

58 In 2019, this kind of new attack has been used to impersonate the CEO of a company voice and demand a fraudulent transfer: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

this approach can be applied to different media to generate fake videos, images, text, and their combinations.

Generating fake content can be harmful in multiple ways. For example, one can create a false image, or edit an existing one, by generating faces of individuals that do not exist but are nevertheless remarkably similar to real faces.[59] This verisimilitude raises the question of how these contents can be spotted to prevent the spread of fake content,[60] especially considering the potentially harmful uses that can be made of such content. Despite the novelty of these technologies, some examples of harmful uses have already been spotted, such as using real photos of people as source material to generate fake pornographic videos involving those people, which can be used for blackmail or revenge.[61] In these cases, social networks can be both the source of the material used for generating the fakes and the means for potentially spreading the fake content.

Social networks are not—at least in most cases—the producers of this harmful content. They nevertheless play a pivotal role in shaping the various forms through which harm may come to pass in digital environments, both through their decisions regarding which types of content to carry. Accordingly, these networks often rely on content moderation approaches to remove or constrain the reach of potentially harmful content, either to comply with legal requirements or to ensure users are not driven away from their platforms. As they do so, social networks are subject to various legal constraints, which we examine in the following section.

4 Content moderation and the challenges of automation

The term "content moderation" covers a broad range of interventions platforms may adopt towards user-generated content. Some types of intervention are directed at specific content items. For example, a network may take down a post that does not comply with its Terms of Service or add geographical restrictions to content that is lawful in some jurisdictions but not in others. Other interventions target the users that produce unaccept-

59 https://thispersondoesnotexist.com/.

60 Article 52(3) of the AI Act proposal seeks to set up a disclosure requirement: any uses of deep fake must disclose the artificial generation or manipulation of the content.

61 https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/. For a legal analysis of deep fakes, see Chesney and Citron, 'Deep Fakes'.

able content: banning or suspending them from the network altogether, restricting the visibility of their posts, flagging them with some warning regarding the content of their profile, or adding relevant content to the user's feed to correct or highlight possible disinformation, among other approaches.[62] While the details of each intervention may differ, they all require platforms to adopt a proactive approach to identifying potentially harmful content and responding to it.

Why might social networks want to do so? After all, the eCommerce Directive treats social networks as intermediaries rather than content producers,[63] a decision that restricts their liability for user-generated content. In fact, the general rule is that social networks can only be held liable for this kind of content if they fail to act expeditiously after learning that a user is using the network to store illegal information or conduct illegal activities.[64] Since, as a rule, they are not required to actively pursue this knowledge,[65] social networks are exempted from most forms of liability regarding harms produced through them.

Yet, content moderation is a sensible practice even in the absence of an obligation to that effect. From a business perspective, users might be less inclined to remain in a social network in which they are exposed to scams, hate speech, toxic debates, and other forms of harmful content. By fostering a healthy online environment,[66] content moderation allows networks to offer users a more interesting value proposition, thus retaining their engagement and content production. But the implementation of moderation policies requires a more proactive position regarding user content, thus raising questions on whether the social network is a mere host of user-generated content—and thus excluded from liability—or a co-creator that can be held liable by harms ensuing from that content.

---

62 Social networks may also exercise controls toward the content that is provided to each specific user, for example by ensuring a diversity of viewpoints to avoid filter bubbles. Full coverage of this topic would exceed the scope of this chapter, but we point the interested reader towards Almada, Maranhão, and Sartor, 'Content Personalisation'; Lucien Heitz et al., 'Benefits of Diverse News Recommendations for Democracy: A User Study', *Digital Journalism* 0, no. 0 (8 February 2022): 1–21, https://doi.org/10.1080/21670811.2021.2021804.

63 Sartor and Loreggia, 'The Impact of Algorithms for Online Content Filtering', 30–31.

64 Article 14(1) eCommerce Directive. This provision is retained in Article 5(1) DSA.

65 Article 15 of the eCommerce Directive, preserved in Article 7 DSA.

66 Sartor and Loreggia, 'The Impact of Algorithms for Online Content Filtering', sec. 2.1.

Under current CJEU case law, hosting services—such as social networks—only become liable for content if they turn out to play "an active role of such a kind as to give it knowledge of, or control over, the data" they host.[67] It is not *prima facie* implausible to say that moderation gives platforms control over specific items of user-generated content, as they may decide whether any such item remains available or not.[68] But even if one is willing to grant this point, such control would only exist with regard to the small fraction of user-generated content that is effectively moderated, not to their operations as a whole.[69] Furthermore, holding networks liable due to moderation would substantially reduce a network's incentives to address online harms, as a strong legal pull towards inaction would counter the business rationales described above. Instead, the European Commission has adopted a "good Samaritan" approach, which acknowledges that addressing some categories of harm requires proactive measures and considers this activity is not enough, in itself, to remove the liability exemption.[70] To consolidate this possibility, Article 6 of the DSA explicitly states that voluntary own-initiative investigations for complying with legal requirements do not render a network ineligible for the liability exemption. We welcome this provision, as it increases legal certainty regarding proactive content moderation, thus contributing to a safer online environment.

This is not to say there are not several fault lines between content moderation and the framework of the eCommerce Directive. The first challenge for regulation is determining the proper scope of content moderation. Current instruments oblige platforms to remove illegal content, as liability exemptions only apply when platforms expeditiously remove illegal content or activities they are made aware of.[71] However, online harm is not solely produced by unlawful activity: for example, users may

67 *L'Óreal* (Case C-324/09), para. 116.

68 After all, the liability exclusion in Article 14(1) eCommerce Directive does not apply if service providers fail to act against unlawful content they know about.

69 Increasing the share of content that undergoes moderation, in turn, might be problematic, given the prohibition of general monitoring duties under Article 15 eCommerce Directive.

70 Sartor and Loreggia, 'The Impact of Algorithms for Online Content Filtering', 30–31.

71 Article 14(1)(b) eCommerce Directive conditions the protection from liability to the expeditious removal (or disabling) of unlawful content. Article 17(4)(c) of the Copyright Directive and Article 3 of the Terrorist Content Regulation establish similar duties, but with additional obligations a platform must follow after removal to preserve their protection from liability.

engage in toxic debate, even within the reasonable limits of their freedom of expression, as a result of political polarisation[72] or other forms of echo chambers.[73] Users may also be harmed not by a single post, but by the cumulative product of various lawful practices.[74] To the extent platforms currently address such lawful harms, they do so based on their Terms of Service rather than any general empowerment stemming from the law. As a result, there are several questions about the legitimacy of platforms grounding their content moderation decisions—which impact fundamental rights, notably freedom of expression—on private law instruments,[75] especially considering such instruments are notoriously opaque to the end-user.[76] The moderation of lawful content may thus be a source of tension between users, platforms, and the legal system.

Issues also appear when content moderation follows legal requirements. The eCommerce Directive and the Copyright Directive both require social networks to act "expeditiously" when it comes to unlawful content. Still, the definition of what counts as expeditious action is left to each Member State. For example, Germany's *NetzDG* requires the removal of manifestly illegal content within 24 hours of receiving notice.[77] This tendency to

72 See, e.g., Mathias Osmundsen et al., 'Partisan Polarization Is the Primary Psychological Motivation behind Political Fake News Sharing on Twitter', *American Political Science Review* 115, no. 3 (2021): 999–1015, https://doi.org/10.1017/S0003055421000290; Richard Fletcher, Alessio Cornia, and Rasmus Kleis Nielsen, 'How Polarized Are Online and Offline News Audiences? A Comparative Analysis of Twelve Countries', *The International Journal of Press/Politics* 25, no. 2 (1 April 2020): 169–95, https://doi.org/10.1177/1940161219892768.

73 See, e.g., C. Thi Nguyen, 'Echo Chambers and Epistemic Bubbles', *Episteme* 17, no. 2 (June 2020): 141–61, https://doi.org/10.1017/epi.2018.32.

74 For a case study on this kind of harm, see Burkhard Schafer, 'Death by a Thousand Cuts: Cumulative Data Effects and the Corbyn Affair', *Datenschutz und Datensicherheit - DuD* 45, no. 6 (1 June 2021): 385–90, https://doi.org/10.1007/s11623-021-1456-8.

75 For an introduction to such critiques, see Naomi Appelman, João Pedro Quintais, and Ronan Fahy, 'Using Terms and Conditions to apply Fundamental Rights to Content Moderation: Is Article 12 DSA a Paper Tiger?', *Verfassungsblog* (blog), 1 September 2021, https://verfassungsblog.de/power-dsa-dma-06/; Cauffman and Goanta, 'A New Order', 768. On the legitimacy issues stemming from regulation by code, see Laurence Diver, *Digisprudence: Code as Law Rebooted* (Edinburgh: Edinburgh University Press, 2021).

76 Lippi et al., 'CLAUDETTE'.

77 NetzDG, § 3 para. 2, n. 2. Note, however, that this timeframe is not applicable to all content, but only to items in which unlawfulness can be assessed without an in-depth examination: see Zurth, 'The German NetzDG as Role Model or Cautionary Tale?', 1113.

narrow timeframes is also seen in the deadlines set at the EU level, notably in the one-hour deadline for giving effect to a removal order relating to terrorist content.[78] Social networks are thus required to make decisions within a very narrow timeframe, a duty they largely comply with. This compliance, however, introduces risks not only for the workers involved in the moderation process, who may be subject to excessive pressure,[79] but also to the proper assessment of the fundamental rights of the users in particular cases.

Content moderation arrangements must also cope with a broad range of requirements to remove specific types of content. One of the key ideas behind the current regulatory platform is that information society services cannot be subject to any general obligation to moderate the content they carry or actively pursue facts or circumstances relating to illegal activity. In one form or another, this prohibition appears in all EU instruments on social networks.[80] Still, the notion of a "general obligation" is not seen as incompatible with various monitoring duties, some of them constructed very broadly. Within the regulatory sub-system defined by the Copyright Directive, social networks are required to not only remove specific content items deemed to violate copyright protection but also to ensure the unavailability of some works even before there is any complaint[81] and to prevent future uploads of any content deemed to be equivalent to a content item already subject to a removal order.[82] Member State courts have ordered similar measures under the general regime of the eCommerce Directive, mandating the remotion of any content equivalent to specific posts which were deemed unlawful, and the CJEU has found such decisions do not amount to a general obligation to remove content.[83] Furthermore, even the duty to remove "equivalent" content would not amount to a general duty of removal, as platforms are required to remove only content items that can be deemed equivalent to the target of the original order without an in-depth assessment.[84] Social networks can thus be obliged, by

78 Article 3(3) Terrorist Content Regulation.

79 See, e.g., Queenie Wong, 'Facebook Content Moderation Is an Ugly Business. Here's Who Does It', CNET, 19 June 2019, https://www.cnet.com/tech/mobile/facebook-content-moderation-is-an-ugly-business-heres-who-does-it/.

80 See, e.g., Article 15(1) eCommerce Directive, Article 17(8) Copyright Directive, Article 5(8) Terrorism Content Regulation.

81 Article 17(4)(b) Copyright Directive.

82 Article 17(4)(c) Copyright Directive.

83 *Glawischnig-Piesczek* (Case C-18/18), paras. 31–37.

84 *Glawischnig-Piesczek* (Case C-18/18), paras. 38–47. For an in-depth analysis of the decision, see Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's

legislation and courts, to actively pursue specific kinds of content in *all* posts made in a platform, so long as this duty is defined in narrow enough terms to avoid the label of a "general obligation".

Social networks have adopted multiple approaches to the sources of strain described above, which share two major features. When it comes to choosing the means for moderation, platforms are increasingly relying on automated tools, such as systems based on machine learning.[85] This turn is partially driven by other factors, such as the Covid-19 pandemic[86] or the growing capabilities of natural language processing systems. However, it is also a response to legal demands,[87] as using AI technologies may be *de facto* unavoidable to evaluate a large amount of content potentially covered by broad-but-technically-not-general monitoring obligations.[88] Faced with such demands, platforms have embraced the promise of efficiency represented by automated moderation techniques.

Despite its immense potential, automation of content moderation practices may fail to deliver satisfactory results in practice. Sometimes, these failures stem from technical limitations of the existing technologies available for moderation. One of the first applications of automation to moderation relies on the fixed representation of contents of interest—e.g., copyrighted, unlawful, or specific harmful content items—, using these representations to compare new information from digital platforms to find unwanted data. This goal can be achieved through various techniques, such as blacklists, fingerprinting, hash-functions, which aim at creating a fixed and unique representation of input. When two inputs have the same representation, they are deemed to refer to the same content. Unfortunate-

---

Glawischnig-Piesczek Ruling'. Drawing from this rationale, Advocate General Øe has argued that Article 17(4) of the Copyright Directive provides sufficient safeguard to freedom of expression online, thus recommending the dismissal of the action for annulment Poland has proposed with regard to this provision (Case C-401/19). As of February 2022, the CJEU has not ruled on the matter.

85 Robert Gorwa, Reuben Binns, and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance', *Big Data & Society* 7, no. 1 (2020), https://doi.org/10.1177/2053951719897945.

86 Tarleton Gillespie, 'Content Moderation, AI, and the Question of Scale', *Big Data & Society* 7, no. 2 (2020): 2, https://doi.org/10.1177/2053951720943234.

87 This is the case even though none of the applicable directives and regulations mandate the use of automated moderation techniques. In fact, Article 5(8) Terrorist Content Regulation explicitly states compliance with the specific measures required under the remainder of this article does not require the adoption of automated tools.

88 Gillespie, 'Content Moderation, AI, and the Question of Scale', 2.

ly, it is quite easy to fool these approaches, as simple and minor changes in the input lead to different representations.[89]

As the moderation problems become more complex, AI technologies face additional challenges. For example, posts on social networks often involve parodies, jokes, memes, and other humoristic content, but humour is a very contextual form of human communication that current linguistic models do not capture well.[90] As such, automated filters may produce erroneous results in dealing with uses of humour within posts, and those errors may, in turn, impinge upon the rights of platform users.[91] There is also the risk that automatic filters produce discriminatory decisions[92] or produce other forms of harm.[93] To address such risks, EU legislation

89 For assessments of technologies used for content filtering, see Felipe Romero Moreno, '"Upload Filters" and Human Rights: Implementing Article 17 of the Directive on Copyright in the Digital Single Market', *International Review of Law, Computers & Technology* 34, no. 2 (3 May 2020): 153–82, https://doi.org/10.1080/13600869.2020.1733760; Sartor and Loreggia, 'The Impact of Algorithms for Online Content Filtering'. For a case study, see Hal Abelson et al., 'Bugs in Our Pockets: The Risks of Client-Side Scanning', *ArXiv:2110.07450 [Cs]*, 14 October 2021, http://arxiv.org/abs/2110.07450.

90 For a primer on the difficulties in automating humour, see also Julia Taylor Rayz and Victor Raskin, 'Fuzziness and Humor: Aspects of Interaction and Computation', in *Fuzzy Techniques: Theory and Applications*, ed. Ralph Baker Kearfott et al., Advances in Intelligent Systems and Computing (Cham: Springer International Publishing, 2019), 655–66, https://doi.org/10.1007/978-3-030-21920-8_58; Tony Veale, *Your Wit Is My Command Building AIs with a Sense of Humor* (The MIT Press, 2021).

91 On online humour as a legal problem, see Joao Paulo Capelotti, 'The Dangers of Controlling Memes through Copyright Law', *The European Journal of Humour Research* 8, no. 3 (12 October 2020): 115–36, https://doi.org/10.7592/EJHR2020.8.3.Capelotti; Renata Vaz Shimbo and Marco Almada, 'A Robot and a Moderator Walk into a Bar: The Use of AI in Online Moderation of Humoristic Content' (Artificial Intelligence: The New Frontier of Business and Human Rights, The Hague: T.M.C. Asser, 2021).

92 On algorithmic discrimination, see, *inter alia*, Alexander Tischbirek, 'Artificial Intelligence and Discrimination: Discriminating Against Discriminatory Systems', in *Regulating Artificial Intelligence*, ed. Thomas Wischmeyer and Timo Rademacher (Cham: Springer International Publishing, 2020), 103–21, https://doi.org/10.1007/978-3-030-32361-5_5; Sandra Wachter, Brent Mittelstadt, and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI', *Computer Law & Security Review* 41 (July 2021), https://doi.org/10.1016/j.clsr.2021.105567.

93 For an assessment of the shortcomings of large language models, see Emily M. Bender et al., 'On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?', in *Proceedings of the 2021 ACM Conference on Fairness, Accountability,*

has increasingly added safeguards regarding the use of automation in social network contexts, such as requiring platforms to disclose the use of content moderation algorithms[94] and removing certain kinds of decisions from the reach of automation.[95] Consequently, even advanced AI techniques are not a sure-fire response to content moderation challenges.

Regardless of the extent to which they automate content moderation procedures, social networks face a strategic challenge: how much content should they remove? As examined above, failure to remove unlawful content in a timely fashion may expose platforms to liability for user-generated content. But, in some contexts, determining the lawfulness of a content item might not be a straightforward task. For example, moderators might find themselves needing to evaluate whether a post by a user is an anti-immigration discourse or, in fact, a satire against this kind of discourse.[96] Since the decision on whether a content item should or not stay up must be taken in a short window of time, moderators often tend to engage in *over-removal*, that is, in the removal of any content items that have anything beyond a minimal probability of being unlawful.[97] In doing so, they

---

and Transparency, FAccT '21 (New York, NY, USA: Association for Computing Machinery, 2021), 610–23, https://doi.org/10.1145/3442188.3445922.

94 At the EU level, Article 7(1) and 7(3) of the Terrorist Content Regulation require that platforms be transparent about their use of automated tools for moderation, a duty Article 23(1)(c) of the DSA would extend to platforms in general. In addition, Article 15(2)(c) DSA establishes a duty to explain the role automated means played in a specific decision. The Parliament position at first reading broadens this requirement by replacing "decision" with "action", thus encompassing all uses of AI as a guide for moderation practices.

95 Article 17(5) DSA proposal precludes the automation of decisions about complaints submitted by users to the platform.

96 In New Year's Day, 2018, the German comedian Sophie Passmann made a post mocking the national tradition of airing "Dinner for One" on TV, which was taken down after it was construed as a joke targeted at immigrants: Kristen Chick and Sara Miller Llana, 'Is Germany's Bold New Law a Way to Clean up the Internet or Is It Stifling Free Expression?', *Christian Science Monitor*, 8 April 2018, https://www.csmonitor.com/World/Europe/2018/0408/Is-Germany-s-bold-new-law-a-way-to-clean-up-the-internet-or-is-it-stifling-free-expression.

97 As an example, YouTube's first transparency report found that more than 60% of the disputed claims on copyright it adjudicated in the first half of 2021 were resolved in favour of the claimant, meaning that the original decision to remove the content item was unwarranted: 'YouTube Copyright Transparency Report H1 2021' (YouTube, December 2021), https://blog.youtube/news-and-events/access-all-balanced-ecosystem-and-powerful-tools/. However, general evidence on over-removal is hard to come by, given the various challenges in collecting and assessing metrics on content moderation: Daphne Keller and Paddy Leerssen, 'Facts and

reduce the risk of non-compliance with legal requirements while acting within the margin of the discretion afforded by the network's Terms of Service.

Over-removal is a risk-mitigating strategy for social networks, but it may affect users by impinging on their freedom of expression. If moderators are likely to remove content at the slightest whiff of a problem, users might be prompted to self-censorship, as users try to avoid posts that might cause problems with moderators.[98] This is particularly true in cases where platforms do not offer clear mechanisms for questioning or obtaining information about removals; in these cases, a user can either accept the removal decision or seek to strike it down through judicial means, in a procedure that takes much more time than the original decision-making by the network.[99] Without clear guidance on acceptable content or channels to contest removal decisions,[100] users thus find themselves at the mercy of opaque decision-making by platforms.

As it reforms the social network regulatory framework, the EU addresses the concerns mentioned above through the digital constitutionalist turn mentioned in Section 2. Separation of powers is translated to the context of content moderation by the creation of procedural requirements for moderation decisions, such as the need to provide internal channels for receiving complaints about takedown decisions[101] and the information

---

Where to Find Them: Empirical Research on Internet Platforms and Content Moderation', in *Social Media and Democracy: The State of the Field, Prospects for Reform*, ed. Joshua A. Tucker and Nathaniel Persily, SSRC Anxieties of Democracy (Cambridge: Cambridge University Press, 2020), 220–51.

98 Yenn Lee and Alison Scott-Baumann, 'Digital Ecology of Free Speech: Authenticity, Identity, and Self-Censorship', ed. Simeon Yates and Ronald E. Rice (Oxford University Press, 2020).

99 As of 2021, German courts took about 680 days to reach a decision in cases relating to takedown decisions: Jacob Mchangama, Natalie Alkiviadou, and Raghav Mendiratta, 'Rushing to Judgment: Are Short Mandatory Takedown Limits for Online Hate Speech Compatible with The Freedom of Expression?' (Copenhagen: Justitia, 2021).

100 There is, however, some non-binding guidance in the form of private standards and the EU Code of Conduct on countering illegal hate speech online, which counts with the participation of several of the largest platforms currently in operation: Didier Reynders, 'Countering Illegal Hate Speech Online. 6th Evaluation of the Code of Conduct', Factsheet (Brussels: European Commission, 7 October 2021).

101 Article 10 Terrorist Content Regulation and Article 17(9) of the Copyright Directive. Article 17 of the DSA extends this obligation beyond the scope of these legal instruments.

that a user needs to appeal against a decision,[102] such as the role automated systems played in it.[103] These procedural guarantees are accompanied by substantive limits to what platforms can do, as case law[104] and *lex specialis*[105] require platforms to protect the fundamental rights of their users. This duty of care is consolidated in the DSA, which renders it applicable to all forms of content moderation and commands platforms to interpret their Terms of Service in light of the protection of fundamental rights.[106] In the case of very large platforms, the DSA introduces a risk-based approach, under which platforms mitigate risks to these rights that may stem during their operation.[107] Finally, the Parliament position at first reading includes a new paragraph into Article 6 DSA, which requires voluntary own-initiative moderation to be "effective and specific", including a broad set of safeguards to "demonstrate that those investigations and measures are accurate, non-discriminatory, proportionate, transparent and do not lead to over-removal of content". Therefore, barring a radical change of course by legislators and courts, the future of content moderation in the EU moves towards the protection of fundamental rights in the online environment through substantive and procedural mechanisms.

5 Concluding remarks

The regulation of social networks is not a novel challenge for the European Union's legal order. While the framework established around the eCommerce Directive underwent various changes through case law and specialised legislation, its main tenets remain stable. Platforms are largely

102 Article 17 DSA.

103 Article 15(2)(c) DSA. Article 7(1) and 7(3) of the Terrorist Content Regulation provide a more abstract duty of transparency regarding the use of AI, which is not present in the Copyright Directive but also finds an analogue in.

104 For an overview of the applicable CJEU decisions, see De Gregorio, 'The Rise of Digital Constitutionalism in the European Union', sec. 3.

105 In the Copyright Directive, the opening to fundamental rights appears mostly in recitals (especially Recital 84, which states "this Directive should be interpreted and applied in accordance with those rights and principles"). The Terrorist Content Regulation explicitly refers to fundamental rights in Article 5(3), which sets conditions for the design of specific measures to address terrorist content.

106 Article 12 DSA explicitly states the need to observe fundamental rights in the application of the terms of service.

107 Articles 26 and 27 DSA require very large online platforms to assess and mitigate risks to fundamental rights.

protected from liability stemming from user-generated content, encouraged—but compelled only in a narrow set of cases—to adopt a proactive approach for maintaining a healthy online environment, and enjoy considerable discretion in addressing lawful but undesirable content. In this sense, the DSA promotes continuity within the regulatory regime rather than a radical rupture with the eCommerce Directive.

Nevertheless, the DSA—at least as of February 2022—brings substantial changes to this regulatory regime. Platforms only retain their protections against liability and their normative discretion to the extent they protect users' fundamental rights and ensure transparent and fair procedures for exercises of power such as banning users or removing content items. As a result of these changes, the safeguards introduced by case law and specialised legislation are extended to all aspects of a social network's operation, effectively establishing a duty of care towards users that modulates the exercise of private autonomy by platforms.

This procedural turn in social network regulation is a global phenomenon,[108] partly driven by the increased complexity of the online environment in which these networks operate. Since AI technologies are an important part of this environment, for good and for bad, the Copyright Directive, the Terrorist Content Regulation, and the DSA dedicate some attention to them. On the one hand, these systems are seen as sources of risk, which require tailored techno-social safeguards which cannot be directly provided by binding law, but rather require the active engagement of social networks themselves. On the other hand, the need to process large volumes of data, often in a narrow time frame, turns automation into a *de facto* requirement for legal compliance. There is a risk that legislation and platforms become overly confident on the efficacy of AI tools to monitor harmful content in social networks, as the tools available still face several technical challenges and may also incorporate biases, and consequently may affect human rights. It remains to be seen how this tension will be managed in practice.

Since many of the provisions examined above are directed at the internal procedures of social networks, their effectiveness in protecting users

108 Within the EU itself, see the aforementioned example of NetzDG. Outside the EU, debates around the reform of Section 230 of the Communications Decency Act in the US and the Internet Transparency and Responsibility Bill proposed in Brazil also reflect this trend: Juliano Maranhão et al., 'Nota Técnica sobre Procedimentos de Moderação de Conteúdo' (São Paulo: Instituto Legal Grounds, 10 September 2020), https://institutolgpd.com/blog/nota-tecnica-sobre-procedimentos-de-moderacao-de-conteudo/.

will depend on their implementation through such internal procedures. The examination of specific enforcement structures, many of them defined at the national and sub-national levels, exceeds the scope of this chapter. Nevertheless, we believe these structures would do well only if they are based on a socio-technical approach that understands technologies in terms of the social change they enable. If such an approach is effectively implemented in the internal processes of social networks, we believe that the EU approach which focuses in promoting and directing moderation may succeed in limiting harm to user and encouraging beneficial online interactions.

Acknowledgements

The authors would like to thank Renata Shimbo for her comments on the overarching legal framework and by pointing out the challenges involved in humour moderation.

Marco Almada is a doctoral researcher at the European University Institute, funded by a Fundación Carolina grant.

Andrea Loreggia is an assistant professor at the Department of Information Engineering of the University of Brescia, Italy.

Juliano Maranhão is associate Professor at the University of São Paulo Law School and associate researcher at the University of São Paulo's Center For Artificial Intelligence (C4AI).

Giovanni Sartor is professor in Legal theory and legal informatics at the University of Bologna and the European University Institute of Florence.

CompuLaw, that stands for 'Computable Law', is an ERC Advanced Grant proposal coordinated by Prof. Giovanni Sartor. The project was selected for funding by the European Research Council in the 2019 (G.A. 833647). Motivation for CompuLaw lies in the need for the law to govern intelligent computational entities, and the human-artificial social ecology in which they participate. These entities are so many, so fast, and so ubiquitous that it is impossible for humans to monitor them and anticipate illegal behaviour. The solution envisaged by CompuLaw is to make law computation-oriented. That is, to integrate, map and partially translate legal and ethical requirements into computable representations of legal knowledge and reasoning. The European University Institute (EUI) and the University of Bologna provide the main expertise for the five-year multi-disciplinary project. All the information of the project as well as news and publications are available at https://site.unibo.it/compulaw

Autoritäre Modelle der Internetregulierung: Chinas Vorstoß in den digitalen Raum und Implikationen für liberale Demokratien

Julia Gurol

Einleitung: Chinas Digitaloffensive

Chinas digitale Offensive im In- sowie im Ausland stelle eine wachsende Herausforderung für westliche, liberale Demokratien dar. Das betrifft nicht mehr nur die repressive Regulierung des Internets innerhalb der Volksrepublik oder den chinesischen Export digitaler Technologien, Überwachungssoftware und Künstlicher Intelligenz, sondern zunehmend auch den Versuch, dem offenen und freien Internet ein autoritäres Gegenmodell entgegenzusetzen und dieses international zu exportieren. Damit ist die Volksrepublik China zwar bei weitem nicht alleine – auch Russland, Iran und andere autoritäre Staaten bemühen sich um eigene Modelle der Internet- und Datenregulierung sowie deren bilateralen und multilateralen Export – doch mit Abstand der aktivste und organisierteste Akteur. Schon längst gilt die chinesische „Great Firewall" als das umfassendste und dadurch auch restriktivste System der Onlinezensur weltweit.[1]

Während diese Prozesse nicht zuletzt seit dem Beginn der Implementierung der digitalen Seidenstraße (Digital Silk Road, 数字丝绸之路 *shuzi sichou zhi lu*) an Fahrt aufgenommen haben, stellte insbesondere die Corona-Pandemie ein weiteres Möglichkeitsfenster für die Volksrepublik dar, mit dem Argument der Nachverfolgung von Infektionsketten sowie der Pandemiebekämpfung, sowohl innerhalb des eigenen Landes im großen Stil Daten zu sammeln, und gleichzeitig eigene Technologien an andere Staaten zu exportieren. Dies wird an späterer Stelle in diesem Kapitel anhand der Verflechtungen zwischen China und den Vereinigten Arabischen Emiraten (VAE) im digitalen Sektor veranschaulicht. Die Gesundheitsseidenstraße (Health Silk Road, 健康丝绸之路 *jiankang sichou zhi lu*), die auf dem Höhepunkt der ersten globalen Infektionswelle im Frühjahr 2020 offiziell verabschiedet wurde, beispielsweise, soll eng mit der digitalen

1 Griffiths, 2019.

Seidenstraße verflochten sein. Dies trug zu einer Verbreitung chinesischer digitaler Technologien bei – die Volksrepublik China entwickelte sich damit zu einer zentralen Lieferantin von Überwachungstechnologien, CCTV Equipment, sowie Künstlicher Intelligenz.[2] Kurz: der chinesische Techno-Autoritarismus stellt eine wachsende Herausforderung für liberale Demokratien dar – nicht nur im Bereich der Technologiediffusion sondern zunehmend auch im Internet. Der folgende Beitrag skizziert den chinesischen Vorstoß in den digitalen Raum im Bereich Technologieexport sowie Internetregulierung und stellt die Herausforderung für liberale Demokratien dar, diesen Tendenzen stärkere, eigene Modelle entgegenzusetzen.

Das folgende Kapitel widmet sich dem Thema der Internetregulierung sowie dem Export eines autoritären Gegenmodells zum freien, offenen und weitgehend unregulierten Internet als Mechanismus zur Wahrung autoritärer Stabilität. Der Fokus der Betrachtung liegt dabei auf der Volksrepublik China als „Pionier" der Internetregulierung. Zunächst erfolgt eine kurze Darstellung, welche Rolle die Regulierung des Internets für innenpolitische Stabilität autoritärer Regime bedeutet. Darauf aufbauend folgt eine Diskussion des Exports autoritärer Regulierungsmodelle, die anhand des Beispiels chinesisch-emiratischer Verflechtungen im digitalen Sektor veranschaulicht werden soll. Abschließend nimmt das Kapitel die daraus entstehenden Herausforderungen für liberale, westliche Demokratien in den Blick und skizziert Herausforderungen und Handlungsmöglichkeiten.

Internetregulierung als Mechanismus zur Wahrung autoritärer Stabilität

Die politikwissenschaftliche Forschung zur Stabilität autoritärer Regime unterscheidet zwischen drei Säulen der innenpolitischen Stabilität: 1) Legitimation, 2) Ko-optation sowie 3) Repression.[3] Bei letzterer wird zudem zwischen „high intensity repression" und „low intensity repression" unterschieden[4]. High intensity repression beinhaltet sichtbare Maßnahmen gegen Oppositionelle oder politische Organisationen, wie beispielsweise die Zerschlagung von Massendemonstrationen oder politische Attentate. Oft kommt es dabei auch zur Anwendung von Gewalt. Low intensity repression dagegen, zielt auf die Einschränkung bürgerlicher Freiheiten ab und ist damit subtiler und weniger sichtbar – allerdings nicht weni-

2 Demmelhuber et al., 2022.
3 Gerschewski, 2013.
4 Levitsky und Way, 2002.

ger weitreichend. Low intensity repression beinhaltet auch die gezielte und von oben gesteuerte Einschränkung der Informations- und Meinungsfreiheit, da ein freier und unkontrollierter Fluss an Informationen als Bedrohung für das Regime wahrgenommen wird. Überwachung und Propaganda waren daher schon immer ein zentraler Bestandteil autokratischer Regime. Und nicht zuletzt seit dem sogenannten Arabischen Frühling ist klar: das Internet schafft Transparenz und bietet Mobilisierungspotential. Gleichzeitig stellen digital Technologien jedoch auch eine Möglichkeit für autokratische Akteure dar, die Möglichkeit, Unterdrückung und Kontrolle viel durchdringender, effizienter und subtiler zu gestalten. Immer mehr autoritäre Regime vertreten daher die Annahme, dass eine Kontrolle des Internets kritisch für ihren Machterhalt ist.[5]

Dies ist auch ein zentraler Bestandteil von Xi Jinpings Vision einer datengestützten Regierungsführung. Der Versuch, das Internet zu überwachen und Inhalte zu zensieren, hat in China somit innenpolitische Wurzeln und dient nicht zuletzt der Machtmanifestation der Kommunistischen Partei unter dem amtierenden Präsidenten Xi Jinping. Ein freier, unzensierter Informationsfluss sowie der uneingeschränkte Zugang der Bevölkerung zur Informationen im Netz werden dabei als zentrale Bedrohung für die Stabilität der Partei angesehen[6]. Daher hat die Kommunistische Partei eine eigene Version fast aller Internetdienste entwickelt. Statt Twitter gibt es den Mikroblogging-Dienst Sino Weibo, statt Google wird die Suchplattform Baidu benutzt und als Alternative zu Facebook oder WhatsApp gilt der Instant-Messenger WeChat. Alle anderen gängigen Netzwerke werden durch die sogenannte Great Firewall blockiert. Dies hat, aus der Perspektive des Regimes, den Vorteil, Inhalte und Nutzungsverhalten kontrollieren und zudem in großem Stil Daten sammeln zu können.[7]

Im 14. Fünfjahresplan (2021-2025) für die Digitalwirtschaft erklärte die Volksrepublik Daten sogar zu „kritischen Produktionsfaktoren" und unterstellt sie daher einer zentralisierten Planung – ein weiterer Schritt der Volksrepublik in Richtung Pionier der Datenregulierung.[8] Desweiteren nennt der Plan Schlüsselbereiche wie High-End-Chips, Betriebssysteme sowie Schlüsselalgorithmen für künstliche Intelligenz und Sensoren als besonders zentral. Eine wichtige Rolle kommt damit auch Unternehmen

5 Gunitsky, 2015.
6 Interview, geführt am 26. Februar 2019, in Shanghai.
7 Stockmann und Gallagher, 2011.
8 Grünberg und Brussee, 2021.

wie Huawei oder Hikvision, über deren Netze und Server in großem Stil Daten gesammelt und gespeichert werden und deren modernste Technologie die Erstellung und Analyse riesiger Datensätze möglich machen.[9] Doch der chinesische Sicherheitsapparat profitiert nicht nur von den engen Beziehungen zu chinesischen Technologieunternehmen, insbesondere Huawei, SenseTime, Hikvision, iFlytek und Megvii, sondern auch von einem Umfeld, in dem es weder Datenschutzgesetze noch Möglichkeiten gibt, sich bei den Behörden zu beschweren, noch Umfragen, bei denen man seinem Ärger Ausdruck verleihen kann. Da die Beziehungen zwischen der chinesischen Regierung und dem Privatsektor immer komplexer werden, könnte Peking auch den privaten chinesischen Technologiesektor dazu zwingen, Technologien zu entwickeln, die speziell dazu dienen, neue Formen gesellschaftlicher Kontrolle auszuüben.[10]

Dies passiert jedoch nicht nur in Form einer Einschränkung der Informations- oder Meinungsfreiheit vonseiten der Kommunistischen Partei, sondern auch durch vermeintlich subtilere aber nicht minder wirksamen Anreizsysteme, wie das bereits viel diskutierte Sozialkreditsystem Chinas – der sogenannte „citizen score" – das ebenfalls zur Datensammlung beiträgt, dieser jedoch ein positives Image verpassen soll. Kaufverhalten, soziales Engagement, Chatverläufe, GPS-Daten – durch das Sozialkreditsystem entsteht eine gläserne Bürgerschaft gewissermaßen qua Zuckerbrot und Peitsche. Wer sich beispielsweise in der Nachbarschaft engagiert, bekommt Pluspunkte, wer dagegen eine rote Ampel übersieht oder eine Rechnung zu spät bezahlt, bekommt Punkte abgezogen. Jede Alltagshandlung der Bürgerinnen und Bürger wird somit erfasst und anhand einer Sozialtauglichkeitsskala erfasst und bewertet. Was öffentlich durch die Kommunistische Partei als eine Art freiwillige Erziehung des chinesischen Volkes propagiert wird, dient letztlich der Datenbegehrlichkeit der politischen Führung sowie Xi Jinpings Vision, eine datengestützte Regierungsführung zu etablieren.[11]

9 Benner und Hohmann, 2018.
10 Lamenesch, 2021.
11 Drinhausen und Brussee, 2022.

Export eines autoritären Gegenmodells zum freien und offenen Internet als Mechanismus der Autokratieförderung

Repression (und damit auch die Einschränkung der Meinungsfreiheit) als zentrale innenpolitische Säule autoritärer Stabilität ist weitgehend erforscht[12] – ihre Ausweitung in den digitalen Raum im Kontext der steigenden Bedeutung des Internets somit wenig überraschend. Neu ist jedoch die internationale Verbreitung autoritärer Modelle der Internetregulierung. Zu dieser internationalen Dimension autoritärer Staaten werden in der politikwissenschaftlichen Forschung vier Mechanismen unterschieden, bei denen jeweils entweder das Senderland, das Empfängerland oder beide aktiv agieren. Daraus ergeben sich die in der folgenden Tabelle dargestellten Konstellationen (siehe Tabelle 1).

		Akteur	
		Senderland	Empfängerland
Direkter Einfluss	Autokratieförderung	✓	
	Kooperation	✓	✓
Indirekter Einfluss	Lernen/Nachahmung		✓
	Diffusion		

Tabelle 1: Internationale Dimensionen von Autoritarismus, dargestellt nach Bank und Josua, 2017.[13]

Bei einer *Autokratieförderung* („autocracy promotion")[14] geht es um eine „direkte, gezielte Unterstützung und Stärkung autoritärer Regime durch einflussreiche Groß- und Regionalmächte" [15], wie beispielsweise durch China. Im Sinne einer Autokratieförderung bzw. eines Autokratieexports geht es also darum, ein bestimmtes Modell der Internetregulierung bilateral oder multilateral zu verbreiten. Alternativ arbeitet China, ebenfalls als aktives Senderland, in *Kooperation* mit anderen Autokratien („autocratic collaboration") gemeinsam an autoritären Gegenentwürfen. Nicht selten treten zudem sogenannte *Diffusionseffekten* („autocratic diffusion")[16] auf, also weitgehend nichtintendierte, unkoordinierte und kaum zentral ge-

12 Keremoğlu und Weidmann, 2020.
13 Bank und Josua, 2017
14 Bader und Kästner, 2013.
15 Bank und Josua, 2017
16 Ambrosio, 2010.

steuerte Prozesse. Ein Beispiel dafür wäre die Verbreitung staatlicher Einschränkungen des Internetaktivismus durch Diffusionsprozesse. Nicht selten kommt es darüber hinaus zu sogenannten Nachahmungseffekten beziehungsweise *Lernprozessen* („autocratic learning/emulation"), bei denen es zu einer Übernahme und Implementierung von politischen Strategien und Taktiken anderer Autokratien kommt. Durch die Entwicklung Chinas zu einem Vorreiter in Sachen Digitalisierung und technologischer Innovation, sind diese Nachahmungseffekte in den vergangenen beiden Jahrzehnten deutlich stärker geworden. Dies wird oft auch als Verbreitung eines „digitalen Autoritarismus" (digital authoritarianism) bezeichnet.[17]Der Aufstieg Chinas zur digitalen Großmacht hat somit verheerende Folgen für das globale Internet. Denn die Volksrepublik hat längst damit begonnen, ihre eigenen Modelle der Informationskontrolle international erfolgreich zu vermarkten – ihre Führungsrolle im Technologiesektor spielt ihnen dabei in die Hände. Im Kontext der digitalen Seidenstraße exportiert China seine Digitaltechnik und Software bereits jetzt in die ganze Welt.

In Chinas White Paper vom März 2015 wurde die digitale Konnektivität zur obersten Priorität erklärt – in diesem Kontext investiert China international in Glasfaserkabel, baut Datenzentren, die von Peking als „grundlegende strategische Ressource"[18] bezeichnet werden und errichtet damit nach und nach ein digitales Ökosystem, in welches die Länder, die Teil der digitalen Seidenstraße sind, involviert werden.[19] So werden international bereits chinesische Algorithmen für die Entwicklung von Apps zur Nachverfolgung von Bewegungsprofilen genutzt und kommen chinesische Technologien bereits in Smart-City Projekten weltweit zum Einsatz – auch mitten in Europa. Der Belgrader Platz in Serbien beispielsweise steht unter dauerhafter Kamerüberwachung durch ein in China hergestelltes und von dem chinesischen Technologiekonzern Huawei installiertes Überwachungskamerasystem. Diese Beispiele zeigen: Was China im eigenen Land verfeinert hat, exportiert es nun auch ins Ausland.

2019 schlugen gar Forschende von Huawei, China Unicom und dem Ministerium für Industrie und Informationstechnik der Volksrepublik China bei der Internationalen Fernmeldeunion (ITU) eine weitreichende Reform des Internet-Protokolls vor.[20] Dies birgt Gefahren für Meinungsfreiheit, Datensicherheit und, ganz generell, für das freie, offene und

17 Shahbaz, 2018.
18 National Development and Reform Commission, 2016.
19 Russell und Berger, 2020; Hart, 2019.
20 Holz, 2022.

interoperable Internet weltweit und erfordert somit eine stärkere multilaterale Standardsetzung durch liberale Demokratien in den Bereichen Datenschutz, Netzwerkregulierung sowie Kuratierungsalgorithmen.

„China goes global": Chinesisch-Emiratische Verflechtungen im Bereich der Überwachungstechnologie[21]

Eines der illustrativsten Beispiele an der Schnittstelle zwischen der Diffusion autoritärer Praktiken im digitalen Raum sowie der aktiven Verbreitung von Technologien stellen die Verflechtungen zwischen der Volksrepublik China und den Vereinigten Arabischen Emiraten dar, dies insbesondere seit dem Ausbruch der Corona-Pandemie an Fahrt aufgenommen haben.[22] Dabei stehen drei chinesisch-emiratische Netzwerke im Fokus, deren verbindendes Element das emiratische Firmenkollektiv Group 42 (kurz: G42) darstellt. G42 ist ein führendes Unternehmen für künstliche Intelligenz und Cloud-Computing, das 2018 in Abu Dhabi gegründet wurde und seitdem mehrere Unterauftragnehmer und Tochtergesellschaften gegründet hat. Im Laufe der Zeit hat sich G42 zu einem der wichtigsten Knotenpunkte für die autoritäre Zusammenarbeit zwischen China und den VAE entwickelt und steht exemplarische für transregionale Elitenetzwerke, die ausgeprägte Machtbeziehungen zwischen der politischen und wirtschaftlichen Elite Chinas mit und innerhalb der Al Nahyan, der Herrscherfamilie in Abu Dhabi, umfassen.[23] Während der Corona-Pandemie kam es zu einer Diffusion autoritärer Praktiken und Technologien innerhalb dieses Netzwerks, mit der chinesischen Firma Beijing YeeCall Interactive Network Technology als „Sender" und zwei Tochterfirmen von G42, namens Breej Holding Ltd. und ToTok Technology, als „Empfängern". Breej Holding Ltd. und ToTok Technology waren aktiv an der Entwicklung und Programmierung der emiratischen Voice over IP (VoIP) und Chat App ToTok beteiligt, die während der Pandemie zur weitreichenden Kontrolle und Überwachung ihrer Nutzer und Nutzerinnen diente. ToTok basiert nicht nur auf demselben Algorithmus wie die chinesische Tracing App YeeCall (一块), dieser wurde von den Entwicklern von ToTok sogar ko-

21 Die im folgenden Kapitel dargestellten Informationen sind Teil eines von der Volkswagen-Stiftung geförderten Forschungsprojekts zu „Global autocratic collaboration in times of COVID-19: Game changer of business as usual in Sino-Gulf relations?" (Förderzeitraum 2021-2022).

22 Gurol et al., 2022.

23 Demmelhuber et al., 2022.

piert und an den emiratischen Kontext angepasst – klare Evidenz für eine Nachahmung chinesischer Modelle der Repression und Kontrolle im digitalen Raum.[24] Beide Apps greifen auf Geo-Daten, Bewegungsprofile, Fotos und Kontaktdaten der Nutzerinnen und Nutzer zu und sammeln damit weit mehr Daten, als für eine Nachverfolgung im Sinne der Pandemiebekämpfung notwendig wäre.

Dass es sich bei G42 nicht einfach um ein reguläres Unternehmen handelt, das auf der Suche nach Profit und innovativen Ideen international Ausschau hält, zeigt die Gründungsgeschichte des Firmenkollektivs. Vor der offiziellen Gründung von G42, operierten ähnliche Strukturen und Akteure unter einem anderen Namen, DarkMatter. Die sogenannte DarkMatter Group wurde 2015 gegründet, von der emiratischen staatlichen Aktiengesellschaft Mubadala mit Hauptsitz in Abu Dhabi finanziert, und erlangte insbesondere durch die digitalen Angriffe auf Dissidentinnen und Dissidenten sowie Kritikerinnen und Kritikern des emiratischen Regimes an internationaler Bekanntheit. Im Jahr 2019 wurde DarkMatter jedoch endgültig durch den emiratischen Staat aufgelöst, bedingt durch die wachsende öffentliche Kritik. Dennoch operieren zentrale Akteure und Strukturen weiter – nun unter dem Namen der Group42, von der sie nahezu eins zu eins übernommen wurden.[25] Dies zeigt, dass Chinas Modelle der Datensammlung, Kontrolle und Unterdrückung – insbesondere im digitalen Raum – international längst Nachahmende gefunden hat. Desweiteren legt es die Bedeutung digitaler Infrastruktur im Bereich der aktiven Verbreitung aber auch der unintendierten, unkontrollierten Diffusion autoritärer Praktiken dar.[26]

Herausforderungen und Handlungsoptionen für liberale Demokratien

Noch im Jahr 2000 beschrieb der damalige Präsident der Vereinigten Staaten, Bill Clinton, den Versuch das Internet zu regulieren, als vergleichbar schwierig wie „einen Pudding an die Wand zu nageln". Dies zeigt nicht nur Kontinuitäten zur amerikanischen Deregulierungspolitik der 1990er Jahre, die heute weitgehend überholt scheint, sondern wird durch die restriktive Regulierung des Internets durch die Kommunistische Partei in China ganz klar widerlegt – hier wurde der Pudding bereits an die

24 Marczak, 2020.
25 Intelligence Online, 2021.
26 Gurol und Schütze, im Erscheinen.

Wand genagelt. Das Erstarken autoritärer Regime wie China und ihr zunehmender Versuch, dem offenen und freien Internet ein autoritäres Modell entgegenzusetzen, stellt somit eine große Herausforderung für liberale Demokratien dar, ihre eigenen Modelle zu revidieren und über die Notwendigkeit demokratischer Regulierung nachzudenken. Die auf dem libertären Modell der 1990er Jahre beruhende Prämisse, der Staat solle sich aus der Regulierung des Internets so weit wie möglich heraushalten, scheint in seiner Ursprungsform nicht mehr zeitgemäß und dem Wettbewerb mit dem autoritären Gegenmodell nicht gewachsen. Kurz: auch in Demokratien benötigt es Regulierungsmodelle, allerdings solche die demokratisch legitimiert sind und unter Beteiligung einer Vielzahl an Akteuren – staatlichen wie privaten – entwickelt werden. Diese sollten sich auf alle vier Ebenen der Internetregulierung beziehen: 1) Die *infrastrukturelle* Ebene, die Hardware, welche die Grundstruktur des globalen Netzes bildet also Glasfaserkabel, Router oder Server, 2) die *logische* Ebene, die technische Normen und Standards beinhaltet, 3) die *Anwendungsebene* mit Software-Anwendungen, Systemen und Website sowie 4) die *inhaltliche* Ebene, also Text, Bild, Ton, und Video sowie virtuelle Realitätswelten.[27]

Problematisch ist dabei, dass die Internetkommunikation in freien Gesellschaften häufig von privaten Technologieunternehmen kontrolliert wird. Regierungen dagegen fehlt es oft an technischem Fachwissen über die sich schnell entwickelnden Technologien. Der digitale Autoritarismus gedeiht unbestreitbar in einem Umfeld schwacher Regierungsführung und schwacher Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor.[28] Es bedarf demnach einer verstärkten intergouvernementalen, also zwischenstaatlichen, sowie Multistakeholder-Koordinierung, um die digitale Kompetenz zu fördern, böswillige Akteure zu identifizieren und ihre Wirkung einzudämmen. Wenn es um den Schutz von Daten geht, müssen Nutzerinnen und Nutzern zudem die Möglichkeit haben, sich gegen unzulässige Eingriffe in ihr persönliches Leben sowohl durch die Regierung als auch durch Unternehmen zu wehren.

Dabei ist es ein delikater Balanceakt Regulierung und den Schutz der Freiheitsrechte und der Meinungsvielfalt gleichermaßen zu berücksichtigen und nicht etwa durch redaktionelle Filter die Möglichkeiten demokratischer Beteiligung im Netz zu beschneiden. In den EU-Vorschriften beispielsweise ist der Grundsatz des offenen Internetzugangs tief verankert: Der Internetverkehr ist ohne Diskriminierung, Blockierung, Drosselung

27 Niesyto und Otto, 2016.
28 Yayboke, 2020.

oder Priorisierung zu behandeln.[29] Diese Regulierung (2015/2120) ist Kernbestandteil der Europäischen Digitalstategie, die europaweit einheitliche Reglungen anstrebt. Als europäisches Gremium, in dem alle nationalen Regulierungsbehörden (NRB) vertreten sind, stützt sich der sogenannte Body of European Regulators for Electronic Communications (BEREC) auf das Wissen, die Erfahrung und den technischen Sachverstand der ihm angehörenden NRB vor Ort. Im europäischen Gesetz zur Gründung des BEREC ist festgelegt, dass es sowohl die europäischen Institutionen als auch die NRB im Bereich der elektronischen Kommunikation beraten soll. Um zur einheitlichen Anwendung der Open-Internet-Verordnung beizutragen, verpflichtet Artikel 5 Absatz 3 der Open-Internet-Verordnung das BEREC ausdrücklich, Leitlinien für die Umsetzung der Verpflichtungen der NRB aus der Verordnung herauszugeben.

Ein Vorstoß in Richtung Verankerung klarerer Regeln und stärkerer Regulierung war ein EU-Parlamentsbeschluss im Januar 2022 und damit die Verabschiedung des sogenannten „Digital Services Act" (DSA). Dieser soll den digitalen Raum transparenter und fairer machen und legt klarere Regeln für Plattformen fest, wie sie gegen Hassnachrichten und „fake news" vorgehen sollen. Die Kommission hat bei der Ausarbeitung dieses Legislativpakets ein breites Spektrum von Interessengruppen konsultiert. Dazu gehörten der Privatsektor, Nutzer digitaler Dienste, Organisationen der Zivilgesellschaft, nationale Behörden, die Wissenschaft, die Fachwelt, internationale Organisationen und die breite Öffentlichkeit. Darüber hinaus wurde eine Reihe ergänzender Konsultationsschritte durchgeführt, um die Ansichten der Beteiligten zu Fragen im Zusammenhang mit digitalen Diensten und Plattformen umfassend zu erfassen.[30]

Fazit und Ausblick

Ziel dieses Kapitels war es, die chinesische Offensive im digitalen Raum zu umreißen und die Herausforderungen darzulegen, die sich durch Entwicklung und Export eines autoritären Gegenmodells zum freien und offenen Internet für liberale Demokratien ergeben. Es wurde deutlich, dass sich autoritäre Staaten, wie China, längst nicht mehr damit begnügen ihre Modelle der Daten- und Internetregulierung innerstaatlich anzuwenden, sondern dass es zunehmend auch zu einem Export von Regulierungsmo-

29 Amtsblatt der Europäischen Union, 2015.
30 Europäische Kommission, 2022.

dellen, Technologien sowie autoritären Praktiken der Überwachung und Datensammlung kommt. Dieser Vorstoß in den digitalen Raum kann gleichermaßen als Strategie der Wahrung innerstaatlicher Stabilität und der Machtmanifestation der Kommunistischen Partei unter Xi Jinping, sowie auch als Mechanismus der Außenpolitik der Volksrepublik China im Sinne einer Autokratieförderung interpretiert werden. Gleichzeitig setzt die Entwicklung Chinas zum digitalen Vorreiter und Ausgangspunkt zahlreicher digitaler Technologien und Standards Mechanismen des autoritären Lernens sowie der Diffusion autoritärer Praktiken der Internetregulierung, Datensammlung und flächendeckenden Überwachung in Kraft, die ebenso wie die aktive Verbreitung autoritärer Modelle zu einer Ausbreitung des digitalen Autoritarismus weltweit beitragen.

Wenngleich die Volksrepublik China nicht der einzige Akteur ist, der dies aktiv betreibt, so stellt insbesondere die Digitale Seidenstraße eine zentrale Herausforderung in dieser Hinsicht dar. Zusammenfassend lässt sich festhalten, dass das chinesische, autoritäre Gegenmodell zum freien und offenen Internet innerstaatlich bereits alle vier Ebenen der Internetregulierung (*infrastrukturelle Ebene*, *logisch Ebene*, *Anwendungsebene*, *inhaltliche Ebene*) abdeckt, außenpolitisch bislang vor allem die infrastrukturelle, sowie die Anwendungsebene und nur in Teilen die logisch und die inhaltliche Ebene exportiert wird. Insbesondere auf diesen Ebenen gibt daher von Seiten liberaler Demokratien Handlungsbedarf. Hier ist es insbesondere notwendig, insbesondere auf europäischer Ebene, Internetregulierung nicht allein als nationale Aufgabe zu verstehen, sondern EU-weite Standards zu entwickeln.

Bibliografie

Bader, Julia, & Kästner, Antje (2013). Externe Autokratieförderung? In: S. Kailitz & P. Köllner (Hrsg.), Autokratien im Vergleich (1. Auflage, S. 564–586). Nomos.

Bank, André, & Josua, Maria (2017). Gemeinsam stabiler: Wie autoritäre Regime zusammenarbeiten. German Institute for Global and Area Studies (GIGA), Focus 2. Online abrufbar unter: https://www.giga-hamburg.de/de/publikationen/giga-focus/gemeinsam-stabiler-wie-autoritaere-regime-zusammenarbeiten (zuletzt besucht: 28.06.2022).

Benner, Thorsten und Hohmann, Mirko (31. August 2018). Wider das autoritäre Modell: Plädoyer für eine neue deutsch-europäische Internet-Außenpolitik. Internationale Politik. Online abrufbar unter: https://internationalepolitik.de/de/wider-das-autoritaere-modell (zuletzt besucht: 18.09.2022).

Demmelhuber, Thomas, Gurol, Julia und Zumbrägel, Tobias (2022). The Corona temptation? Autocratic linkages in times of a global pandemic. In: Jan Völkel, Lena-Marie Möller and Zeina Hobaika (Hrsg.), The MENA Region and COVID-19: Impact, Implications, and Future Prospects (1. Auflage, S. 19-35). Routledge.

Drinhausen, Katja und Brussee, Vincent (9. Mai 2022). Chinas Sozialkreditsystem im Jahr 2021: Von Fragmentierung zu Integration. Mercator Institute for China Studies (MERICS) Online abrufbar unter: https://merics.org/de/studie/chinas-sozialkreditsystem-im-jahr-2021-von-fragmentierung-zu-integration (zuletzt besucht: 18.09.2022).

Europäische Kommission (7. Juni 2022). The Digital Services Act Package. Online abrufbar unter: https://digital-strategy.ec.europa.eu/de/node/27 (zuletzt besucht: 22.06.2022).

Europäisches Parlament (26 November 2015). Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union. Amtsblatt der Europäischen Union. Online abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R2120&from=EN (zuletzt besucht: 25.06.2022).

Gerschewski, Johannes (2013). The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. In: Democratization, 20(1), pp. 13–38. https://doi.org/10.1080/13510347.2013.738860.

Griffiths, James (2019). The Great Firewall of China: How to Build and Control an Alternative Version of the Internet. Zed Books.

Grünberg, Nils und Brussee, Vincent (9. April 2021). China's 14th Five-Year-Plan – strengthening the domestic base to become a superpower. Mercator Institute for China Studies (MERICS). Online abrufbar unter: https://merics.org/de/kurzanalyse/chinas-14th-five-year-plan-strengthening-domestic-base-become-superpower (zuletzt besucht: 18.09.2022).

Gunitsky, Seva (2015). Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. In: Perspectives on Politics, 13(1), pp. 42–54. https://doi.org/10.1017/S1537592714003120.

Gurol, Julia, Zumbrägel, Tobias, & Demmelhuber, Thomas (2022). Elite Networks and the Transregional Dimension of Authoritarianism: Sino-Emirati Relations in Times of a Global Pandemic. In: Journal of Contemporary China, online first. https://doi.org/10.1080/10670564.2022.2052444.

Gurol, Julia und Schuetze, Benjamin (im Erscheinen). Infrastructuring Authoritarian Power: Arab Gulf–Chinese Transregional Collaboration beyond the State. In: International Quarterly for Asian Studies.

Hart, Melanie (28. Februar 2019)). Mapping China's Global Governance Ambitions. Online abrufbar unter: https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/ (zuletzt besucht: 24.06.2022).

Holz, Sebastian (26. April 2022). Welche Normen regieren das Internet? GTAI – German Trade and Invest. Online abrufbar unter: https://www.gtai.de/de/trade/eu/specials/welche-normen-regieren-das-internet--831930 (zuletzt besucht: 18.09.2022).

Intelligence Online (21. Januar 2021). Digital14 picks up Darkmatter's key activities, including vulnerabilities. Intelligence Online. Online abrufbar unter: https://www.intelligenceonline.com/surveillance–interception/2021/01/21/digital14-picks-up-darkmatter-s-key-activities-including-the-vulnerabilities-researcher-xen1th labs,109636378-gra (zuletzt besucht: 19.06.2022).

Keremoğlu, Eda und Weidmann, Nils B. (2020). How Dictators Control the Internet: A Review Essay. In: Comparative Political Studies, 53(10–11), pp. 1690–1703. https://doi.org/10.1177/0010414020912278.

Lamenesch, Marie (9. Juli 2021). Authoritarianism has been reinvented for the digital age. Center for International Governance Innovation. Online abrufbar unter: https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/ (zuletzt besucht: 22.06.2022).

Levitsky, Steven und Way, Lucan A. (2002). Elections without Democracy: The Rise of Competitive Authoritarianism. In: Journal of Democracy 13, pp. 51-65.

Marczak, Bill (2. Januar 2020). A Breej too far: How Abu Dhabi's Spy Sheikh hid his Chat App in Plain Sight. Medium. Online abrufbar unter: https://medium.com/@billmarczak/how-tahnoon-bin-zayed-hid-totok-in-plain-sight-group-42-breej-4e6c06c93ba6 (zuletzt besucht: 19.06.2022).

National Development and Reform Commission (2016). The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China (2016–2020). Online abrufbar unter: https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf (zuletzt besucht: 24.06.2022).

Niesyto, Johanna und Philipp Otto (2016). Wer regiert das Internet? Akteure und Handlungsfelder. Friedrich-Ebert-Stiftung. Online abrufbar unter: https://library.fes.de/pdf-files/akademie/12736.pdf (zuletzt besucht: 24.06.2022).

Russell, Daniel R. und Berger, Blake H. (2020). Weaponizing the Belt and Road Initiative. Asia Policy Society Institute Report. Online abrufbar unter: https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf (zuletzt besucht: 24.06.2022)

Shahbaz, Adrian (2018). Freedom on the Net 2018: The Rise of Digital Authoritarianism. Freedomhouse. Online abrufbar unter: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism (zuletzt besucht: 12.09.2022).

Stockmann, Daniela, & Gallagher, Mary E. (2011). Remote Control: How the Media Sustain Authoritarian Rule in China. In: Comparative Political Studies, 44(4), pp. 436–467. https://doi.org/10.1177/0010414010394773.

Vanderhill, Rachel (2013). Promoting authoritarianism abroad. Lynne Rienner Publishers.

von Soest, Christian (2015). Democracy prevention: The international collaboration of authoritarian regimes. In: European Journal of Political Research, 54(4), pp. 623–638. https://doi.org/10.1111/1475-6765.12100

Yayboke, Erol (2020). Promote and Build: A Strategic Approach to Digital Authoritarianism. Center for Strategic and International Studies (CSIS). Online abrufbar unter: https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism (zuletzt besucht: 22.06.2022).

Datenherrschaft und Kommunikationsgovernance als Demokratieschutz: Perspektiven auf die Plattform- und KI-Regulierung der Demokratien

Matthias C. Kettemann

Die Regeln für die Governance der Daten- und Kommunikationsflüsse spielen eine zentrale Rolle in der Plattformgesellschaft. Während die Mitbestimmung der Bürger*innen an den Regeln, die bestimmte, was gesagt werden darf, als zentrale Forderungen und große Errungenschaft vieler demokratischer Revolutionen gesehen werden kann, ist es um die Teilhabe an kommunikationsbezogenen Entscheidungen auf digitalen Plattformen, in die sich signifikante Teile unserer öffentlichen Diskurse verlagert haben, eher schlecht gestellt. Erprobte demokratische Prinzipien lassen sich nicht ohne Weiteres übersetzen, um die Teilhabe der Nutzer*innen an der Gestaltung privater Selektionsalgorithmen und Moderationspraktiken zu ermöglichen. Die Plattformen selbst sind zum Regelsetzer, Regeldurchsetzer und zum Richter über ihre Entscheidungen geworden. Kommunikationsmacht ohne demokratische Machtkontrolle (also weder checks noch balances) führen zu Spannungen im gesellschaftlichen Diskursgewebe.

Ähnliche Fragen stellen sich auch bei der Regulierung automatisierter Entscheidungsmechanismen und maschinellen Lernens (unscharf, aber populär: „KI"). Wie sollen Staaten vorgehen? Wie können sich Bürger*innen beteiligen?

Angesichts der Vielfalt der wirtschaftlichen, sozialen und kulturellen, bürgerlichen und politischen Rechte, deren Achtung, Schutz und Durchsetzung durch die zunehmende Nutzung digitale Plattformen und von KI berührt werden, besteht ein Bedarf an Prinzipien und Regeln, um die Potenziale dieser Räume und Tools zu realisieren, dabei aber die individuellen Freiheiten zu schützen und gesellschaftlichen Zusammenhalt zu garantieren.

1. Mehr Demokratie auf Plattformen

Die Kommunikationsräume und die kommunikativen Infrastrukturen demokratischer Öffentlichkeiten sind erheblichen Wandlungsprozessen ausgesetzt. In zunehmend von digitalen Plattformen algorithmisch optimierten und rechtlich gestalteten Räumen werden Grundfragen unserer Gesellschaft ausverhandelt. Doch die Staaten – über Gesetze und Gerichte – leisten Widerstand. Im wachsenden Ausmaß wirken private normative Ordnungen und staatliche Rechtsordnungen zusammen in unterschiedlichen, weder allein privatwirtschaftlichen noch staatlichen, sondern hybriden Formen der Governance von Onlinekommunikation. Diese Entwicklung ist auch folgerichtig: Der Interessenausgleich auf Plattformen ist sowohl eine öffentliche Angelegenheit als auch das Ergebnis der Produktgestaltung der Plattformanbieter.

Das Kernproblem dieser bisherigen Ansätze ist – neben ernstzunehmenden und nicht ausgeräumten verfassungsrechtlichen und europarechtlichen Bedenken –, dass die hochkarätig besetzten Gremien nur Entscheidungen über die Rechtswidrigkeit einzelner, vorgelegter Posts treffen und nur begrenzt systemische Probleme adressieren können. Sie dienen weder Diskussion von Maßnahmen, die über die Grenzen strafrechtlicher Verbote hinausgehen (gegenüber sog. legal, but harmful content), noch können sie systemische Fragen adressieren, die einen vorgelegten Einzelfall übersteigen (etwa nach der Ausgestaltung unternehmensinterner Überprüfungsverfahren und Kuratierungsalgorithmen). Jüngst ergangene Gerichtsentscheidungen des BGH sowie verschiedener Instanzgerichte zeigen auch eine generelle Zurückhaltung, sich inhaltlich mit den Ordnungen der Plattformen und ihren Wirkungszusammenhängen auseinanderzusetzen. Die Gerichte fokussieren eher auf die Prozeduralisierung des Rechtsschutzes und verpflichten Plattformen im Rahmen ihrer Haftungsrechtsprechung dazu Löschentscheidungen zu begründen und betroffene User*innen zu informieren.

Das Gesetzgebungspaket aus Digital Services Act und Digital Markets Act als zukünftiger Rahmen für Plattformregulierung in Europa setzt auch Akzente auf die Zugänglichkeit von Informationen über die Gestaltung der Plattformen und die Prinzipien der Kuratierung, und will so zu einem informierten zivilgesellschaftlichen Diskurs über die Rahmenbedingungen der Meinungsbildung im Internet beitragen. Unmittelbare Teilhabemöglichkeiten der Bürger*innen und Nutzer*innen an diesen Systemen werden aber nicht geschaffen. Die Regulierungsstruktur setzt vielmehr auf eine starke Rolle der Kommission sowie nationaler Aufsichtsbehörden, die als Digital Services Coordinator tätig werden.

Nationale Regulierungsbestrebungen und aktuelle Vorschläge auf EU-Ebene adressieren drängende Fragen demokratischer Rückbindung und institutioneller Ausdifferenzierung hybrider Online-Ordnungen derzeit nicht. In diese Lücke zu kurz greifender staatlicher Regulierungsansätze stoßen zahlreiche private Bestrebungen institutioneller Governance-Innovationen, was auch als strategische Positionierung der Unternehmen verstanden werden kann, um durchgreifende Regulierung zu verhindern. Diesen privaten Modellen steht derzeit noch kein schlüssiges öffentliches Gegenmodell gegenüber.

Demokratien können aber die institutionelle Beschränkung der Plattformmacht und die Verbesserung der Legitimität von Ordnungen und algorithmisch-menschlichen Regelungs- und Durchsetzungsarrangements nicht den Plattformen überlassen.

2. Neue Ansätze globaler KI-Regulierung

Während sich Modelle der Rückbindung von Plattformentscheidungen als ein gangbarer Weg zur Reduktion des demokratischen Defizits von Plattformrecht und -praxis abzeichnen (ohne dass schon Einigkeit hinsichtlich Format und Verantwortung dieser Gremien erzielt wurde), steht ein allgemein als sinnvoller angesehener Ansatz an die KI-Regulierung noch aus. Erste Indizien für gangbare normative Wege können der UNESCO-Empfehlung zur Ethik Künstlicher Intelligenz entnommen werden.

Bei der Empfehlung handelt es sich um den ersten global verhandelten völkerrechtlich relevanten Text im Bereich der KI-Ethik. Sie ist nicht nur global, sondern auch inhaltlich holistisch konzipiert. Die Empfehlung bietet den 193 Mitgliedstaaten der UNESCO einen Handlungsrahmen in diesem wichtigen Zukunftsfeld. Zu den UNESCO-Mitgliedstaaten gehören rechtstaatlich solide Staaten wie Deutschland, in denen – via die EU – KI-Normen in Arbeit sind, Staaten wie China, die den Löwenanteil an der KI-Produktion haben und KI bereits in menschenrechtlich herausfordernder Weise nutzen, und Staaten, die weder über grundrechtlichen Schutz vor KI noch über eine nationale KI-Kapazitäten verfügen. Dass China, das im Laufe der Verhandlungen mehrfach kritisch zu bestimmten menschenrechtlichen Festlegungen der Empfehlung positionierte, schlussendlich den Konsens mittrug, wurde von Beobachtern als besonders bemerkenswert bezeichnet.

Die Empfehlung der UNESCO wurde in einem zweijährigen, intensiven und teils kontroversen zwischenstaatlichen Verhandlungsprozess erarbeitet. Dieser Multistakeholderansatz bietet schon allein bedeutende legi-

timatorische Mehrwerte. Durch Einbeziehung verschiedener Stakeholdergruppen folgt die Empfehlung somit einem „Best Practice"-Modell für internationale Normsetzung und bestätigt dieses.

Mit konkretem Bezug auf elf verschiedene Politikfelder, darunter Bildung und Wissenschaft, Kommunikation, Gesundheit sowie Umwelt übersetzt die Empfehlung Prinzipien zu sich aus einer würdesensiblen AI-Nutzung ergebenen politischen Gestaltungsaufgaben. Das Ziel der Empfehlung ist, die KI an den Menschenrechten auszurichten. Sie gibt der KI eine ethische Grundlage, die Menschenrechte und Menschenwürde nicht nur schützt, sondern alle drei Dimensionen des Menschenrechtsschutzes anspricht: Achtung, Schutz und Förderung/Umsetzung.

Der Fokus auf ethische Regeln und nicht primär auf menschenrechtliche Verpflichtungen ist bewusst gewählt. Einerseits hat die UNESCO eine besondere Verantwortung hinsichtlich ethischer Ansätze an die Gestaltung wichtiger gesellschaftlicher Agenden. Andererseits beziehen sich klar konturierte ethische Werte und Grundsätze in verschiedener Weise auf das Recht; sie können bei der Entwicklung und Umsetzung von politischen Maßnahmen und bei der Interpretation von Rechtsnormen helfen, indem sie, wie die Empfehlung es formuliert „im Hinblick auf die rasante technologische Entwicklung Orientierung bieten". Ethik ist nicht ein „Weniger" als Menschenrechte, sondern ein (wenn auch von der Schutzintention in vielen Bereichen deckungsgleiches) Aliud. Ethische Regeln sind anders konzipiert und aufgebaut und werden unterschiedlich, nicht zentral gesteuert, und regelmäßig nicht mit Zwangsgewalt durchgesetzt. Staaten, die menschenrechtliche Verpflichtungen eingehen, sind völkerrechtlich an diese gebunden. Staaten, die sich zu ethischen Verpflichtungen bekennen, können lediglich – aber immerhin – durch internationalen Druck zu verpflichtungskonformen Verhalten veranlasst werden.

Bemerkenswert an dem Text ist der ganzheitliche Fokus auf die verschiedenen Politikfelder, das Bewusstsein, dass diese je unterschiedliche Regulierungsansätze verlangen, sowie der Fokus auf „blind spots" bisheriger KI-Regeln. Dazu gehören der Umweltschutz, die nachhaltige und ressourcenschonende Verwendung von KI, und die Nutzung von KI im Bildungsbereich unter voller Anerkennung des Rechts auf Bildung für alle.

Je nach Handlungsfeld wohnt den empfohlenen Maßnahmen unterschiedlicher Verpflichtungsgrad inne. Zwar stellt die Empfehlung in ihrer Gesamtheit einheitlich „soft law" da, also nicht formal bindendes Recht, doch wurde die Empfehlung in einem mehrjährigen Ausverhandlungsprozess so detailliert verhandelt wie ein völkerrechtlicher Vertrag, sodass sie sich schon insoweit jedenfalls qualitativ von einfachen Resolutionen oder Erklärungen unterscheidet. Die Empfehlung kann nicht vor Gerichten

durchgesetzt werden, jedoch sind die Empfehlungen an Staaten wirkmächtig: von der Beschreibung einzelner Schritte als völkerrechtlich nötig über die Empfehlung konkreter Maßnahmen (wie das *Ethical Impact Assessment (EIA)* für KI-Systeme oder den Aufbau eines Netzwerks unabhängiger *AI Ethics Officer* zur Kontrolle des EIA und anderer Governance-Mechanismen) bis hin zur Aufforderung zur internationalen Zusammenarbeit und Forschung im KI-Bereich und zur mittelindifferenten Aufforderung der Auswahl nötiger Maßnahmen durch Nationalstaaten.

3. Schlussfolgerungen

Das digitale Zeitalter stellt uns vor ganz neue Herausforderungen der Partizipation von Bürger*innen an Entscheidungen, die ihre Rechte und Pflichten betreffen, die aber von privaten Akteuren gefällt werden. Hier ein Mindestmaß an Partizipation sicherzustellen, ist ein wichtiger demokratischer Auftrag, der den Kern der globalen KI- und Plattformregulierungsansätze der Demokratien ausmacht.

Datenherrschaftsrecht ist Demokratieschutz. Eine grundrechtlich sensible Kommunikationsgovernance ist Demokratieschutz. KI-Regulierung durch ethische Richtlinien ist Demokratieschutz. Daher verwundert es nicht, dass in den genannten Bereichen Demokratien, wie skizziert, mit normativen Innovationen voranschreiten.

Im Kern geht es nämlich um nichts Geringeres als um die Gelingensbedingungen für Institutionalisierungen der Rückbindung privater und hybrider Normenordnungen und KI-Nutzungspraktiken an gesellschaftliche Werte. Hier können die Demokratien eine wichtige Vorbildwirkung entfalten.

Dieser Beitrag greift auf Vorarbeiten des Autors zu Plattformbeiräten sowie zur KI-Ethik-Empfehlung der UNESCO zurück.

Autorenverzeichnis

Marco Almada, doctoral researcher at the European University Institute, Florence

Dr. *Ruben Bach*, Lehrstuhl für Social Data Science und sozialwissenschaftliche Methodenlehre, Fakultät für Sozialwissenschaften, Universität Mannheim

Dr. *Stefan Brink*, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Prof. Dr. *Johannes Buchheim*, LL.M. (Yale), Qualifikationsprofessur für Öffentliches Recht und Recht der Digitalisierung (Tenure Track); Direktor des Instituts für das Recht der Digitalisierung (IRDi), Philipps-Universität Marburg

Prof. Dr. *Johannes Buchmann*, Professor für Informatik und Mathematik i.R., TU Darmstadt, Mitglied der Nationalen Akademie der Wissenschaften Leopoldina

Dr. *Ricardo Campos*, Wissenschaftlicher Mitarbeiter und Lehrbeauftragter am Lehrstuhl für Öffentliches Recht, Recht und Theorie der Medien an der Goethe Universität Frankfurt am Main. Direktor des Instituts Legal Grounds (Sao Paulo, Brasilien)

Prof. Dr. *Christian Djeffal*, Professur für Recht, Wissenschaft und Technik; Vorstandsmitglied des Nationalen E-Government Kompetenzzentrums (NEGZ), Technische Universität München, TUM School of Social Sciences and Technology

Prof. Dr. *Astrid Epiney*, LL.M. (EUI Florenz), Professur für Völkerrecht, Europarecht und schweizerisches öffentliches Recht; geschäftsführende Direktorin am Institut für Europarecht, Rektorin, Universität Freiburg /CH

Amaro Grassi, is project and research coordinator for politics, social media and digital democracy in the Department of Public Policy Analysis at Fundação Getulio Vargas, Rio de Janeiro. He holds an MSc in Sociology and is a PhD candidate in Political Science at FGV Rio de Janeiro.

Dr. *Julia Gurol*, Universität Freiburg, Lehrstuhl für Politikwissenschaft mit Schwerpunkt Internationale Beziehungen, Mitglied der Jungen Akademie an der Berlin-Brandenburgischen Akademie der Wissenschaften und der Leopoldina.

Prof. *Ulrich Kelber*, Dipl. Informatiker, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Honorarprofessor am Zentrum für Ethik und Verantwortung (ZEV) der Hochschule Bonn-Rhein-Sieg

Prof. Dr. *Matthias C. Kettemann*, LL.M. (Harvard), Professur für Innovation, Theorie und Philosophie des Rechts, Leiter des Instituts für Theorie und Zukunft des Rechts, Universität Innsbruck; Forschungsprogrammleiter, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut

Prof. Dr. *Frauke Kreuter*, Professur für Statistik und Data Science in den Sozial- und Humanwissenschaften, Institut für Statistik, Fakultät für Mathematik, Informatik und Statistik, LMU München, Co-Direktorin Social Data Science Center, University of Maryland und Mannheim Center for Data Science

Nils Leopold, Volljurist und Rechtsinformatiker; Referent im Grundsatzreferat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Andrea Loreggia, Assistant Professor at the Department of Information Engineering, University of Brescia, Italy

Prof. *Juliano Maranhao*, Professor für Recht und Technologie an der Universtität Sao Paulo, Brasilien.

Privatdozent Dr. *Carsten Ochs*, Postdoc im Fachbereich 05: Gesellschaftswissenschaften/ Fachgebiet Soziologische Theorie der Universität Kassel und Mitarbeiter im BMBF-Projekt 'Forum Privatheit - Demokratieentwicklung, KI & Privatheit

Prof. Dr. *Alexander Peukert*, Professur für Bürgerliches Recht und Wirtschaftsrecht mit Schwerpunkt im internationalen Immaterialgüterrecht, Goethe-Universität Frankfurt am Main

Prof. *Marco Aurélio Ruediger* holds a Ph.D. in Sociology and an MSc in Policy Analysis and Management. He is the Director of the School of Communication, Media and Information and of the Department of Public Policy Analysis at Fundação Getulio Vargas (FGV), Rio de Janeiro

Prof. *Giovani Sartor*, Professor at Faculty of Law at the University of Bologna and at the European University Institute, Florence. Principal Investigator for the ERC (European Research Council) Advanced project COMPULAW.

Prof. Dr. *Indra Spiecker genannt Döhmann*, LL.M. (Georgetown Univ.), Professur für Öffentliches Recht, Informationsrecht, Umweltrecht, Verwaltungswissenschaften; Goethe Universität Frankfurt a.M.; Direktorin KASTEL - Institut für Informationssicherheit und Verlässlichkeit am Karlsruher Institut für Technologie (KI)

Prof. Dr. *Gerald Spindler*, Institut für Wirtschafts- und Medienrecht, Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Multimedia- und Telekommunikationsrecht, Rechtsvergleichung, Georg-August-Universität Göttingen

Dr. *Thorsten Thiel*, Forschungsgruppenleiter "Demokratie und Digitalisierung" am Weizenbaum-Institut für die vernetzte Gesellschaft; Wissenschaftlicher Mitarbeiter Wissenschaftszentrum Berlin (WZB)

Prof. Dr. Dr. h.c. *Thomas Vesting*, Lehrstuhl für Öffentliches Recht, Recht und Theorie der Medien, Johann Wolfgang Goethe-Universität, Frankfurt am Main.

Kira Vogt LL.M., E.MA, Referentin beim Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg

Dr. *Michael Westland*, BA (London), M.Phil., PhD (Cambridge), Ass. Jur. (Berlin), Gründer und Direktor Democratic Futures Foundation gUG (haftungsbeschränkt)