

Oktober 2019 · Dr. Julian Jaursch

Regulatorische Reaktionen auf Desinformation

Wie Deutschland und die EU
versuchen, gegen manipulative
Meinungsmache auf digitalen
Plattformen vorzugehen



Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Falschnachrichten, bewusste Irreführung und Hetze sind keine neuen Phänomene eines digitalen Mediumfelds, sondern uralte gesellschaftliche Probleme. Allerdings erreicht Desinformation im digitalen Raum ein neues Ausmaß, da soziale Netzwerke, Videoportale und Suchmaschinen dafür leicht genutzt und ausgenutzt werden können. Dadurch besteht die Gefahr, dass politische Haltungen verzerrt, extremistische Stimmungen verstärkt und das Vertrauen in gemeinschaftliche Institutionen wie Wahlen, Parlamente und Medien untergraben wird. Dies stellt eine ernst zu nehmende Herausforderung für demokratische Gesellschaften dar.

Auf Länder-, Bundes- und EU-Ebene reagieren politische Entscheidungsträger:innen auf das Desinformationsproblem. Jedoch sind bisherige Regulierungsversuche und politische Lösungsansätze kaum geeignet, um Desinformation einzudämmen. Das Netzwerkdurchsetzungsgesetz (NetzDG) beispielsweise, welches im Kern darauf abzielt, strafrechtlich relevante Inhalte wie einen volksverhetzenden Tweet schneller zu entfernen, ist auf einen Großteil der Desinformation im Netz nicht anwendbar. Dies liegt vor allem daran, dass Desinformation sich oft in einem rechtlichen Grenzbereich bewegt, in dem unklar ist, was von der Meinungsfreiheit gedeckt ist und was rechtswidrig ist.

Neben den Regeln für den Umgang mit potenziell illegalen Inhalten sind auch die bisherigen Maßnahmen der Europäischen Kommission kein passendes Mittel zur Eindämmung von Desinformation. So wurde zum Beispiel im freiwilligen EU-Leitfaden gegen Desinformation für Unternehmen eine Offenlegung politischer Onlinewerbeanzeigen vereinbart. Doch die öffentlich zugänglichen Datenbanken, die Facebook, Google und Twitter dann anboten, waren unausgereift und unvollständig. Sanktionen dagegen sieht der Leitfaden nicht vor. Diese Schwächen der Selbstregulierung hat die EU bereits selbst erkannt und erwägt daher einen „Digital Services Act“ – ein Gesetzespaket, das klare Regeln und Sanktionen für Plattformen festlegen könnte.

In anderen Regulierungsbereichen wie der Medienaufsicht könnten zwar wirksame Maßnahmen gegen Desinformation entstehen. Dies findet aber bisher kaum statt. Ein Beispiel ist der Medienstaatsvertrag, den die deutschen Bundesländer in einem aufwändigen Verfahren ausarbeiten. Laut Entwurf soll er erstmals überhaupt eine gewisse Aufsicht für einige soziale Netzwerke, Suchmaschinen und Videoportale schaffen. Für das Problem

Desinformation könnten zusätzlich die vorgesehenen Verpflichtungen für Unternehmen, ihre Such- und Sortieralgorithmen zu erklären, hilfreich sein. Denn Transparenzvorschriften könnten grundsätzlich für ein besseres Verständnis sorgen, wie das algorithmisch bestimmte Nachrichtenumfeld funktioniert. Die Regeln zur Algorithmentransparenz sind jedoch nicht konkret genug formuliert und das gilt ebenso für die allgemein gehaltene Hinweispflicht zu politischer Onlinewerbung.

Insgesamt ist das Vorgehen zur Eindämmung von Desinformation bisher unkoordiniert und bruchstückhaft. Es ist ein erster Versuch, mit einem gesellschaftlichen Problem umzugehen, das mit Fragen der Meinungsfreiheit, dem Einfluss von Informations- und Kommunikationstechnologien auf die politische Willensbildung, der Schwächung von journalistischem Gatekeeping und der Marktmacht einiger globaler Unternehmen zusammenhängt. Gerade weil so viele schwierige Themenfelder berührt sind, ist es sinnvoll, zukünftig Lösungsansätze zu Desinformation aus unterschiedlichen Rechts- und Politikbereichen zu verbinden.

Zunächst ist es dafür kurzfristig erforderlich, vorhandene Gesetze stärker durchzusetzen, nicht allein im Strafrecht, sondern besonders im Datenschutzrecht. Denn das personalisierte, aufmerksamkeitsgetriebene Nachrichtenumfeld bei sozialen Netzwerken, Videoportalen und Suchmaschinen, in dem sich Desinformation besonders gut verbreitet, funktioniert erst mit einer umfangreichen Datensammlung und Profilbildung. Eine strikte Durchsetzung von Regeln zum Schutz der Privatsphäre, etwa aus der europäischen Datenschutz-Grundverordnung (DSGVO), kann diese Datensammlung zumindest eingrenzen. Für parteipolitische Kommunikation im Internet müssen erst noch klare Vorgaben geschaffen werden, die Parteiengesetz, Medienregulierung und Datenschutzrecht miteinander verknüpfen.

Mittelfristig könnte zum Beispiel bei einer engeren Verzahnung von Datenschutz- und Wettbewerbsrecht, die schon lange zur Diskussion steht, bedacht werden, wie die Daten- und Marktmacht einiger großer Unternehmen die Verbreitung von Desinformation begünstigt. Außerdem lässt sich fragen, wie in Zukunft eine geeignete Aufsicht für digitale Dienste wie soziale Netzwerke und Suchmaschinen ausgestaltet sein muss. Debatten hierzu finden auch in anderen Ländern schon statt. So wird beispielsweise in Frankreich und Großbritannien über eine spezialisierte Behörde für soziale Netzwerke nachgedacht. Diese könnte sich auf die Verbreitungswege von Desinformati-



on fokussieren (statt auf die Entfernung einzelner Inhalte) und beaufsichtigen, ob und wie Unternehmen dazu Prozesse etabliert haben.

Jegliche politischen Lösungsansätze müssen evidenzbasiert sein. Dies bedeutet, dass Forschungseinrichtungen und Behörden das Ausmaß und die Wirkung von Desinformation im digitalen Raum analysieren können müssen. Momentan sind solche Analysen schwerlich machbar, da große Unternehmen Forschenden kaum Einblicke in ihre Daten erlauben. Für sinnvolle Studien müssen Forschung und Aufsicht daher besseren Datenzugang im Einklang mit Datenschutzregeln haben.

Danksagung

Dem gesamten Team der SNV gebührt Dank für die Unterstützung und den Gedankenaustausch in der Anfangsphase des Projekts, insbesondere dem „Team Digitale Öffentlichkeit“, bestehend aus Raphael Brendel, Polina Garaev, Stefan Heumann, Riccardo Ramacci, Alina Rathke, Sebastian Rieger, Alexander Sänglerlaub und Ben Scott. Herzlichen Dank auch an die zahlreichen Gesprächspartner:innen aus Verwaltung, Wissenschaft, Zivilgesellschaft, Medien und Wirtschaft in Workshops und in Cafés, am Telefon und auf Konferenzen, die ihre Expertise, Einschätzungen und Erfahrungen eingebracht haben.



Inhalt

Executive Summary	2
Danksagung	4
Einleitung	6
Wie Microtargeting, Personalisierung und Netzwerkeffekte die Verbreitung von Desinformation erleichtern können	10
Regulatorischer Umgang mit Desinformation	12
Selbstregulierung	14
Inhaltelöschung	16
Medienregulierung	19
Wettbewerb X Datenschutz	22
Fazit	25
Anhang	30
Literaturverzeichnis	31

Einleitung

Drei Tage, Abgeordnete aus elf Parlamenten, 80 Zeugenaussagen: Das „International Grand Committee on Big Data, Privacy and Democracy“, das sich im Mai 2019 in Kanada traf, bot ein umfangreiches parlamentarisches Forum, um über Desinformation im digitalen Raum zu diskutieren.¹ Auch im Bundestag wurden schon die Gefahren parteipolitischer Desinformationskampagnen besprochen. Die Europäische Union setzte bereits Anfang 2018 eine Expertengruppe zum Thema ein. Und die Sonderermittlungen von Robert Mueller zu russischer Desinformation im Wahlkampf zur US-Präsidentenwahl 2016 via Facebook, Instagram, Twitter und YouTube gipfelten in einem gut 400-seitigen Bericht. Dies sind nur einige Belege dafür, dass politische Entscheidungsträger:innen in aller Welt nun seit mehreren Jahren einen passenden Umgang mit Desinformation suchen. Spätestens seit der US-Wahl wird auf mehreren politischen Ebenen über legislative und regulatorische Maßnahmen nachgedacht, um mögliche Gefahren von Desinformation für den gesellschaftlichen Diskurs einzudämmen: von Selbstverpflichtungen für soziale Netzwerke, Suchmaschinen und andere Unternehmen über Vorgaben zur Moderation und Löschung illegaler Inhalte bis hin zu neuen Aufsichtsbehörden.

Das Ringen um passende legislative und regulatorische Maßnahmen im Umgang mit Desinformation gestaltet sich dabei schwierig: Zwar rufen selbst einige US-Unternehmen nach Regulierung auf diesem Gebiet und manche Regierungen haben bereits Gesetze verabschiedet. Doch Desinformation im digitalen Raum wird bisher fragmentarisch angegangen, bedingt durch einen anfänglichen selbstregulatorischen Fokus, auf den viele vereinzelt reaktive Maßnahmen folgten. Die Herausforderungen, die mit Desinformation einhergehen, sind nicht zu unterschätzen: Es geht dabei um Fragen der Meinungsfreiheit, der politischen Willensbildung, der Macht großer Konzerne und des Einflusses von Informations- und Kommunikationstechnologien auf gemeinschaftliche Debatten. Noch befinden sich politische und gesellschaftliche Entscheidungsträger:innen auf der Suche nach Antworten. Daher ist jetzt die Zeit zu prüfen, wie mit legislativen und regulatorischen Ein-

¹ Es waren Abgeordnete aus Costa Rica, Deutschland, Ecuador, Estland, Großbritannien, Irland, Kanada, Marokko, Mexiko, Singapur und St. Lucia anwesend. Standing Committee on Access to Information, Privacy and Ethics, „International Grand Committee on Big Data, Privacy and Democracy“, Standing Committee on Access to Information, Privacy and Ethics, Juni 2019, <https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=10554743>.

griffen die politische Meinungsbildung und der demokratische Diskurs im digitalen Raum gestärkt werden können.

Vor diesem Hintergrund bietet das Papier einen Überblick zum regulatorischen Umgang mit Desinformation in Deutschland und der EU. Es zeigt sowohl bisherige politische Reaktionen auf Desinformationskampagnen auf (zum Beispiel den EU-Aktionsplan) als auch lange geplante Reformen, die Fragen zur Eindämmung von Desinformation berücksichtigen könnten (so etwa zur Medienregulierung).

Zunächst ist ein kurzer Rückblick zum Verständnis von Desinformation hilfreich: Was ist damit gemeint, was soll mit Desinformation erreicht werden und welche Besonderheiten im Zeitalter großer sozialer Netzwerke und Suchmaschinen sind zu berücksichtigen?

Irreführung – egal ob mit falschen Inhalten oder über trügerische Verbreitung. Desinformation sind falsche, ungenaue und irreführende Informationen, die entwickelt und verbreitet werden, um politische Prozesse zu behindern.² Hierbei ist es sehr wichtig zu beachten, dass Irreführung nicht nur durch die Information an sich (die Inhalte einer Nachricht) erreicht werden kann. Neben den Inhalten an sich müssen deren Kontext, Quelle und Verbreitungsweg beachtet werden.³ Auch über die Kontextualisierung und die Art und Weise der Verbreitung lassen sich Menschen täuschen und Meinungsbildungsprozesse behindern. Zum Beispiel können an sich korrekte Informationen aus dem Zusammenhang gerissen werden, etwa wenn Statistiken zu Verbrechen von Eingewanderten nicht in Relation gesetzt werden oder wenn richtige Inhalte manipuliert werden.⁴ Ebenso ist es irreführend, wenn sich Einzelpersonen oder Gruppierungen in sozialen Netzwerken als jemand anders ausgeben, um polarisierende Meinungen zu streuen und zu

2 Lose übersetzt aus European Commission, „A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation“ (Brüssel: European Commission, 12. März 2018), 10, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271; im Englischen bietet sich auch die aktivistische Definition „to disinform“ an, siehe Clare Melford, „Disinformation is an Online Harm“, Global Disinformation Index, 26. Juni 2019, <https://disinformationindex.org/2019/06/disinformation-is-an-online-harm/>.

3 Siehe zu diesem Dreischritt das Konzept „Message - Messenger - Messaging“ bei Michael Meyer-Resende und Rafael Goldzweig, „Online Threats to Democratic Debate: A Framework for a Discussion on Challenges and Responses“ (Berlin: Democracy Reporting International, 26. Juni 2019), https://democracy-reporting.org/wp-content/uploads/2019/06/BP_Threats-to-digital-democracy.pdf.

4 Die SNV-Studie zur Bundestagswahl 2017 zeigt detailliert auf, wie im Vorfeld der Wahl Falschnachrichten, manipulierte Inhalte und kontextlose Statistiken verbreitet wurden, siehe Alexander Sänglerlaub, Miriam Meier, und Wolf-Dieter Rühl, „Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017“ (Berlin: Stiftung Neue Verantwortung, 26. März 2018), https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf.

verstärken. Dies geschah beispielsweise in den USA: Dort gab es Social-Media-Konten von Aktivist:innen zu kontrovers diskutierten Themen wie Polizeigewalt, Rassismus und Migration. Nur stammten diese Konten teilweise nicht aus den USA, sondern aus Russland, und dienten dazu, „Zwietracht im politischen System“ zu säen⁵. Vermeintliche US-Aktivist:innen schalteten darüber hinaus gezielt bezahlte Werbeposts zu umstrittenen Themen, um zu einer weiteren Polarisierung beizutragen. Nicht zuletzt ist eine vorgetäuschte Massenmeinung, basierend auf gefälschten oder gekauften Followern oder manipulierten Suchmaschineneinträgen, ebenfalls eine Täuschung, die den demokratischen Diskurs schädigen kann – so geschehen im Vorfeld der Wahlen zum Europäischen Parlament 2019 zum Thema Migration.⁶

Zwietracht säen und politische Willensbildung behindern. Desinformation ist nicht nur eine Gefahr für Abstimmungen und Wahlkämpfe. Das Thema erfuhr zwar im Zuge des Brexit-Referendums und der Präsidentschaftswahl in den USA eine erhöhte Aufmerksamkeit, aber Desinformation ist nicht unbedingt dazu gedacht, auf Abstimmungsergebnisse Einfluss nehmen: Desinformation dient dazu, die Polarisierung der Gesellschaft anzustacheln und das Vertrauen in demokratische Prozesse und gemeinschaftliche Faktengrundlagen zu untergraben. Auf individueller Ebene werden Bürger:innen durch Desinformation in ihrer freien, selbstbestimmten politischen Willensbildung behindert. Auf gesellschaftlicher Ebene wird so der demokratische Diskurs geschwächt.

Große Suchmaschinen und soziale Netzwerke als Verstärker. In den vergangenen Jahren wurde deutlich, dass sich einige soziale Netzwerke, Suchmaschinen und andere digitale Kanäle besonders für die Verbreitung von Desinformation eignen. Das eingangs erwähnte „Grand Committee“ lud unter anderem Vertreter:innen von Amazon, Apple, Google, Facebook, Microsoft und Twitter vor.⁷ Im Bericht zur US-Wahl 2016 des Sonderermittlers Mueller werden, wie erwähnt, Facebook, Instagram, Twitter und YouTube als Kanäle

5 Übersetzt aus Robert S. Mueller, III, „Report On The Investigation Into Russian Interference In The 2016 Presidential Election“ (Washington, DC: U.S. Department of Justice, März 2019), 4, <https://www.justice.gov/storage/report.pdf>.

6 Trevor Davis, Steven Livingston, und Matt Hindman, „Suspicious Election Campaign Activity on Facebook: How a Large Network of Suspicious Accounts Promoted Alternative Für Deutschland in the 2019 EU Parliamentary Elections“. (Washington, DC: The George Washington University, 22. Juli 2019), <https://smpa.gwu.edu/sites/g/files/zaxdzs2046/f/2019-07-22%20-%20Suspicious%20Election%20Campaign%20Activity%20White%20Paper%20-%20Print%20Version%20-%20IDDP.pdf>; Avaaz, „Far Right Networks of Deceptions: Avaaz uncovers flood of disinformation, triggering shutdown of Facebook pages with over 500 million views ahead of EU elections“ (New York, NY: Avaaz, 22. Mai 2019), <https://avaazimages.avaaz.org/Avaz%20Report%20Network%20Deception%2020190522.pdf>.

7 Standing Committee on Access to Information, Privacy and Ethics, „International Grand Committee on Big Data, Privacy and Democracy“.

russischer Einflussnahme genannt.⁸ Eine britische Parlamentsuntersuchung fokussierte sich auf Facebook.⁹ Diese Dienste können recht kostengünstig und einfach genutzt und ausgenutzt werden, um mit Desinformation bestehende gesellschaftliche Spannungen zu verschärfen. Das ist wichtig zu betonen: Desinformation entsteht nicht wegen dieser Technologien, sie ist kein neues oder rein digitales Phänomen. Desinformation befeuert bestehende gesellschaftliche Herausforderungen, denen sich auch gefestigte Demokratien gegenübergestellt sehen – sei es eine weit verbreitete Abstiegsangst in der Bevölkerung, sei es politische Korruption, seien es ethnische Konflikte.¹⁰

Neu ist hingegen das Ausmaß von Desinformation und das hat auch mit dem Aufstieg einiger sozialer Netzwerke, Suchmaschinen und Videoportalen zu tun: Sie können Debatten und Sichtweisen, die zu gesellschaftlichen Spaltungen und Polarisierung beitragen, verstärken. Deshalb müssen die Funktionsweisen und die Besonderheiten dieser Dienste berücksichtigt werden, wenn über Desinformation im digitalen Raum geredet wird. Facebook, Google, Instagram, Twitter und YouTube beispielsweise arbeiten im Kern nach einer aufmerksamkeitsgetriebenen Logik, in der Wut und Lüge oft besser funktionieren als Freundlichkeit und Wahrheit (siehe Infobox auf der folgenden Seite). Die Aufmerksamkeitsmaximierung, die einige soziale Netzwerke und Suchmaschinen ausmacht, basiert auf einer umfangreichen Datensammlung. Mit diesen Daten lassen sich detaillierte Profile erstellen, die es den Unternehmen ermöglichen, gezielte Werbung („targeted ads“) zu verkaufen. Nebeneffekt sind personalisierte, segmentierte digitale Informations- und Nachrichtenräume weitgehend ohne journalistisches Gatekeeping, die anfällig für die Verbreitung von Desinformation sind.

8 Mueller, III, „Report On The Investigation Into Russian Interference In The 2016 Presidential Election“.

9 House of Commons Digital, Culture, Media and Sport Committee, „Disinformation and ‘fake news’: Final Report“ (London: House of Commons, 14. Februar 2019), <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmds/1791/1791.pdf>.

10 Siehe zu dieser Argumentation auch Ben Scott, „Did Google and Facebook Break Democracy?“, *Progressive Centre UK*, 30. Juli 2019, <https://www.progressivecentre.uk/did-google-and-facebook-break-democracy>; Adam B. Ellick, Adam Westbrook, und Andrew Blackwell, „Operation Infektion: Russian Disinformation from Cold War to Kanye“, *The New York Times*, 12. November 2018, <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html>.

Wie Microtargeting, Personalisierung und Netzwerkeffekte die Verbreitung von Desinformation erleichtern können

Die trügerische Beeinflussung von Personen, aber auch gesellschaftlicher Debatten, ist in der digitalen Öffentlichkeit einfacher denn je. Soziale Netzwerke erlauben es Menschen, Informationen und Unterhaltung nicht nur zu konsumieren, sondern auch zu produzieren.¹¹ Suchmaschinen machen Wissen und Informationen zum politischen Geschehen einfach, schnell und weltweit verfügbar. Das schafft eine enorme Demokratisierung des politischen Diskurses, sodass viel mehr Bürger:innen im Internet an gesellschaftlichen und politischen Debatten teilnehmen können. Abgesehen davon, dass das auch neue Sprachrohre für Extremismus bietet, sorgt dies gleichzeitig für eine verstärkte Segmentierung der Öffentlichkeit: Die Millionen Menschen, die in Deutschland täglich Facebook benutzen¹², können sich ihre Nachrichten- und Informationsräume leichter und stärker personalisieren als je zuvor. Hinzu kommt, dass aufgrund des Aufbaus vieler sozialen Netzwerke (und mangelnder Ressourcen bei traditionellen Medien) oftmals ein journalistisches Gatekeeping fehlt. Also etwa eine Redaktion, die recherchiert, selektiert und korrigiert.

Ohne journalistische Pförtner:innen steht in diesen segmentierten, stark personalisierten Informationsräumen Tor und Tür offen für die Manipulation von Meinungen. Zum Beispiel besteht die Gefahr, dass Nutzende sich eine Echokammer aufbauen, in der ihre bestehenden Sichtweisen bestätigt werden.¹³ Microtargeting¹⁴ erlaubt es kommerziellen und politischen Organisationen, Menschen gezielt mit den Botschaften und Inhalten zu bespielen, die diese Menschen vermutlich besonders rühren und ansta-

11 Vgl. Leonhard Dobusch, „Die Organisation der Digitalität: Zwischen grenzenloser Offenheit und offener Exklusion“, *netzpolitik.org*, 1. Februar 2017, <https://netzpolitik.org/2017/die-organisation-der-digitalitaet-zwischen-grenzenloser-offenheit-und-offener-exklusion/>.

12 In Deutschland ist die Nutzung sozialer Medien für Nachrichten noch vergleichsweise niedrig, aber im Kommen, siehe Nic Newman, „Reuters Institute Digital News Report 2019“ (Oxford: Reuters Institute for the Study of Journalism, 12. Juni 2019), https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-06/DNR_2019_FINAL_0.pdf.

13 Die Wissenschaft kann aufgrund fehlendem Datenzugang bei Unternehmen nur schwer prüfen, ob Echokammern existieren und wie stark sie ausgeprägt. In einigen Studien wurden sie gefunden, siehe die Literaturübersicht bei Jan Philipp Rau und Sebastian Stier, „Die Echokammer-Hypothese: Fragmentierung der Öffentlichkeit und politische Polarisierung durch digitale Medien?“, *Zeitschrift für Vergleichende Politikwissenschaft*, 29. August 2019, 1–19, <https://doi.org/10.1007/s12286-019-00429-1>.

14 Gemeint ist die datenbasierte, gezielte Ansprache einzelner Menschen oder Gruppen.

cheln. Das kann wiederum bestehende gesellschaftliche Spaltungen vertiefen.

Dieses Microtargeting ist Kern der Funktionsweise der meisten weit verbreiteten sozialen Netzwerke und anderen digitalen Angebote: Sie verdienen ihr Geld als Marketingplattformen, die personalisierte Werbeplätze verkaufen. Sie haben dabei weder einen Informationsauftrag noch unterliegen sie einer journalistischen Berufsethik. Die Aufmerksamkeit der Nutzenden ist der alleinige Treiber dieses Systems. Deshalb versuchen Anbieter, Menschen möglichst lange auf ihren Seiten und in ihren Apps zu halten (ihr „Engagement“¹⁵ zu erhöhen), um ihnen Werbung anzeigen zu können. In diesem Sog der Aufmerksamkeitsmaximierung funktionieren Aufregung und Ärger besser als Fakten und Freundlichkeit. Gerade Gefühle der Wut sorgen dafür, dass Inhalte geteilt und andere Ansichten abgelehnt werden.¹⁶ Journalistische Angebote haben es in diesem Umfeld schwieriger. Kombiniert mit der hohen Reichweite und Schnelligkeit vieler sozialer Netzwerke verbreiten sich so die lautesten, krassesten Stimmen der Debatten.¹⁷

Die ungekannte Daten- und Machtkonzentration bei einigen Unternehmen verstärkt diese Tendenzen noch in einem Kreislauf: Je besser Unternehmen die Aufmerksamkeit ihrer Nutzenden einfangen können, desto mehr Menschen nutzen ein soziales Netzwerk oder eine Suchmaschine immer länger, öfter und intensiver, desto besser lernen diese Unternehmen ihre Nutzenden einzuschätzen, desto besser können sie personalisierte Inhalte und Werbung anbieten, desto länger, öfter und intensiver nutzen Menschen diese Angebote. Hieran deutlich, wie wichtig die Datensammlung und die positiven Netzwerkeffekte (je mehr Nutzende ein Angebot hat, desto nützlicher wird es) für viele Unternehmen sind.

15 Der Begriff „Engagement“ stammt direkt aus dem Marketing und bezeichnet Nutzerinteraktion mit digitalen Inhalten, also etwa klicken, liken, folgen, abonnieren.

16 Dag Wollebæk u. a., „Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior“, *Social Media + Society*, 9. April 2019, <https://doi.org/10.1177/2056305119829859>.

17 YouTube und andere Unternehmen führen berechtigterweise an, dass sie zwar ein Interesse haben, Menschen auf ihren Diensten zu halten, aber eben auch ein Interesse, Menschen ein „schönes“ Informations- und Unterhaltungsumfeld zu bieten. Das hat in der Vergangenheit allerdings oft nicht geklappt, weshalb die Kritik weiterhin gültig bleibt, dass krasse Inhalte besonders gut funktionieren. Vergleiche für das Beispiel YouTube Mark Bergen, „YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant“, *Bloomberg*, 2. April 2019, <https://www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant>; Neima Jahromi, „The Fight for the Future of YouTube“, *The New Yorker*, 8. Juli 2019, <https://www.newyorker.com/tech/annals-of-technology/the-fight-for-the-future-of-youtube>; The Economist, „Now playing, everywhere: The tricky task of policing YouTube“, *The Economist*, 4. Mai 2019, <https://www.economist.com/briefing/2019/05/04/the-tricky-task-of-policing-youtube>.

Die einführende Betrachtung zeigt: Eine Diskussion zur regulatorischen Reaktion auf Desinformation kann sich nicht nur auf die Korrektur einzelner falscher Nachrichten beschränken. Hinter dem Phänomen Desinformation im digitalen Raum stecken Fragen zur Datenmacht einiger Konzerne, zum aufmerksamkeitsgetriebenen System vieler sozialer Netzwerke, zu geschwächten journalistischen Gatekeeper:innen und zu fehlenden Regeln für politische Onlinekommunikation. Daher muss bei der Lösungssuche der Blick auf mehrere Rechts- und Politikbereiche gerichtet werden. Wobei es wichtig zu bemerken ist: Regulatorische Maßnahmen müssen gar nicht unbedingt ausdrücklich *gegen* Desinformation oder auch Online-Hetze erdacht werden, sondern können vielmehr auch *für eine Stärkung* der Nutzenden in sozialen Netzwerken, bei Suchmaschinen oder Videoportalen sorgen.

Letzterer Ansatz ist in Deutschland und der EU noch unterentwickelt, bisherige Maßnahmen waren von Selbstregulierung und der Entfernung illegaler Inhalte geprägt. Dies wird im folgenden Überblick näher ausgeführt, in dem mehrere Herangehensweisen analysiert werden.

Regulatorischer Umgang mit Desinformation

Zwei große Desinformationskampagnen im Jahr 2016 in Europa und den USA (zum Brexit-Referendum und zur Präsidentschaftswahl) können als Wendepunkte angesehen werden: Seitdem wird auf beiden Seiten des Atlantiks intensiver darüber nachgedacht, wie regulatorische und legislative Eingriffe Desinformation eindämmen können. Zuvor gab es eine sehr dezente Regulierung von Unternehmen wie Facebook und Google. Es war ihnen weitgehend überlassen, wie sie Desinformation auf ihren Plattformen eindämmten – oder eben nicht. Zudem wurden solche digitalen Technologien lange als (ausschließlich) förderlich für die Kommunikation und die Meinungsbildung angesehen. Prägend war hierfür die Diskussion um die demokratiefördernde Rolle von Facebook, Twitter und YouTube im Arabischen Frühling.¹⁸

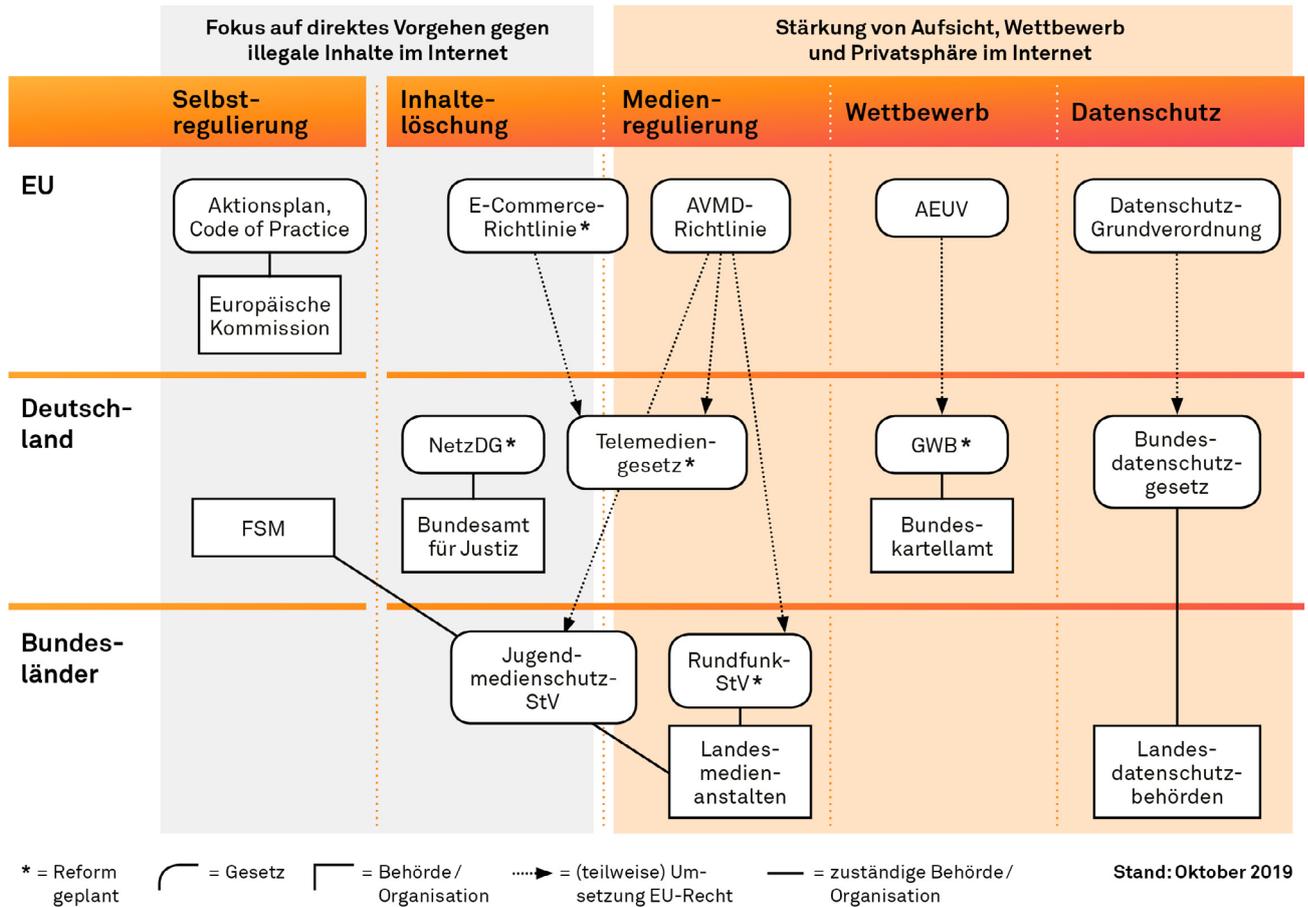
Spätestens nach der US-Wahl 2016 drehte sich diese Sichtweise. Die negativen Auswirkungen sozialer Netzwerke und Suchmaschinen für den demokratischen Diskurs wurden deutlicher. Das neue Ausmaß von Desinformation wurde in der Wissenschaft, der Zivilgesellschaft und auch in der Politik als mögliche Störquelle für die politische Willensbildung erkannt. Reaktive Gegenmaßnahmen entstanden in aller Welt. Dabei befassten sich Regierungen zunächst vornehmlich mit „schädlichen“ Inhalten an sich: Falsche Nachrichten

¹⁸ Maeve Shearlaw, „Egypt five years on: was it ever a ‚social media revolution‘?“, *The Guardian*, 15. Januar 2016, <https://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution>.

ten müssen korrigiert werden, rechtswidrige Beiträge müssen gelöscht werden. Die Bedeutung von Faktenchecks wurde hervorgehoben, ebenso wie die Notwendigkeit, bestehendes Strafrecht auch strikt auf Online-Kommunikation anzuwenden. Dabei wurde sich weiter oft auf die eigenen Maßnahmen der Unternehmen verlassen, die etwa ihre eigenen Regeln zur Inhaltsmoderation und -löschung anpassten oder mit Faktencheck-Organisationen kooperierten. Ein Beispiel für reaktive Maßnahmen dieser Phase ist der Aktionsplan der EU gegen Desinformation, der hauptsächlich freiwillige Selbstverpflichtungen großer Unternehmen umfasst. Das deutsche Netzwerkdurchsetzungsgesetz entfernt sich schon von diesem selbstregulatorischen Ansatz, bleibt aber dabei, vorwiegend auf die Löschung von Inhalten zu setzen.

Drei Jahre nach der US-Wahl hat sich noch nicht viel bewegt. Maßnahmen der Unternehmen selbst, oft ohne regulatorische Vorgaben, bestimmen weiterhin das Vorgehen gegen Desinformation. Hinzu kommt: Viele der Reformen, die in Deutschland ohnehin anstanden, um mit einer Gesellschaft und Wirtschaft im technologischen Wandel umzugehen, sind nicht dafür ausgelegt, die seit spätestens 2016 offenkundigen Gefahren von Desinformation angemessen zu berücksichtigen. Zum Beispiel wurde schon länger über Reformen zur Digitalisierung der Wirtschaft (im Wettbewerbsrecht), zur herausgehobenen Rolle persönlicher Daten (im Datenschutz) oder zur geänderten Medienproduktion und -nutzung (im Rundfunkrecht) diskutiert. Wie solche Überlegungen die Gefahr von Desinformationskampagnen und die bisherigen Reaktionen darauf integrieren können oder sollen, ist unklar.

Insgesamt führt dies zu einem fragmentarischen Umgang mit Desinformation. Im Folgenden wird diese Fragmentierung anhand einer kurzen Analyse verschiedener Herangehensweisen zu Desinformation festgemacht. Die Abbildung auf der nächsten Seite zeigt fünf Bereiche auf, die näher beleuchtet werden: Von Selbstregulierung und Inhaltelöschung bis hin zu Fragen der Medienregulierung, des Wettbewerbsrechts und des Datenschutzes. Es wird jeweils kurz der Hintergrund der Bereiche anhand einer oder mehrerer Maßnahmen erläutert und die Bedeutung für Desinformation hervorgehoben, selbst wenn die jeweilige Maßnahme sich nicht ausdrücklich auf Desinformation bezieht. Auch die dann aufgezeigten Stärken und Schwächen beziehen sich immer nur auf den Umgang mit Desinformation. Sie werden im Fazit aufgegriffen. Zu allen Abkürzungen und erwähnten Gesetzen in der Abbildung finden sich weiterführende Informationen im Text und/oder in der Tabelle im Anhang.



Regulierungsansätze zu Desinformation in Deutschland und der EU

Selbstregulierung

Beispiel und Hintergrund. Das Paradebeispiel für einen selbstregulatorischen Ansatz im Umgang mit Desinformation ist die Reaktion der EU auf die prominenten Desinformationskampagnen von 2016. Die Europäische Kommission stellte Ende 2018 einen Leitfaden gegen Desinformation (Code of Practice)¹⁹ für große soziale Netzwerke und Suchmaschinen sowie einen Aktionsplan²⁰ gegen Desinformation vor. Zuvor hatte eine Expertengruppe Vorschläge zu diesem Thema erarbeitet.²¹ Die Selbstverpflichtungen beziehen

19 European Commission, „EU Code of Practice on Disinformation“, European Commission, 26. September 2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

20 European Commission, „Action Plan against Disinformation“, European Commission, 5. Dezember 2018, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

21 European Commission, „A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation“.

sich auf mehrere Themen wie Medienkompetenz, Inhaltmoderation und politische Werbung. Daher lässt sich Selbstregulierung in diesem Fall als übergreifender Ansatz verstehen.

Im Aktionsplan ist festgelegt, dass der Europäische Auswärtige Dienst mehr finanzielle Ressourcen und mehr Personal für die strategische Kommunikation erhält. Zudem wird ein Frühwarnsystem eingerichtet und es soll Aufklärungskampagnen für Bürger:innen geben. Da sich die Europäische Kommission nicht zur Lage der Desinformation in EU-Mitgliedstaaten äußern kann, wurde der Fokus auf mögliche russische Kampagnen gelegt. Der Aktionsplan umfasst auch die Überwachung des Leitfadens gegen Desinformation für große soziale Netzwerke und Suchmaschinen.²² Inhaltlich geht es bei diesen Selbstverpflichtungen unter anderem darum, gefälschte Konten schnell zu schließen. Darüber hinaus soll das Schalten von politischer Werbung stärker reglementiert werden. Dazu richteten Plattformen beispielsweise Datenbanken für politische Onlinewerbung an, die öffentlich einsehbar sind. Außerdem sollen Unternehmen mit zivilgesellschaftlichen Organisationen zusammenarbeiten und die Forschung unterstützen.

Stärken. Dass es eine EU-weite Antwort auf die Entwicklungen seit 2016 gibt, ist ein wichtiges Signal: Die Europäische Union hat erkannt, dass eine strategische Kommunikation gegen Desinformation nötig ist, ebenso wie eine verstärkte Zusammenarbeit und eine Sensibilisierung der Menschen. Genau diese Punkte werden im Aktionsplan genannt. Zusätzliche Ressourcen und neue Netzwerke können dabei helfen, einige der Probleme von Desinformation anzugehen. Der Code of Practice steht darüber hinaus symbolisch für den Versuch, zusammen mit großen Unternehmen eine Eindämmung von Desinformation zu erreichen.

Schwächen. Die selbstregulatorischen Maßnahmen der EU bleiben vage, dem Leitfaden mangelt es an Durchsetzungs- und Sanktionsmechanismen.²³ Beispiele für diese Schwachstellen finden sich zuhauf: Die vorgegebene „Unterstützung“ der Unternehmen für die Forschung beispielsweise verzichtet auf eine Pflicht zur Öffnung der Datenschnittstellen für Forschende. Das aber ist die Grundlage für sinnvolle wissenschaftliche Studien, die kritisch

²² Unterzeichnende Unternehmen und Industrieverbände sind Facebook, Google, Mozilla, Twitter, die European Association of Communications Agencies (EACA), das Interactive Advertising Bureau (IAB Europe) und die World Federation of Advertisers (WFA).

²³ Für eine Evaluation der EU-Maßnahmen siehe Bruno Lupion, „The EU Framework Against Disinformation: What Worked, What Changed and the Way Forward“ (Berlin: Democracy Reporting International, 30. August 2019), <https://democracy-reporting.org/wp-content/uploads/2019/08/EU-Actions-Against-Disinformation-EP2019-Final.pdf>.

die Maßnahmen der Plattformen begleiten und prüfen können.²⁴ Und dass Unternehmen auch ohne den Kodex an technologischen Lösungen arbeiten, um betrügerische Konten zu löschen, dürfte außer Frage stehen. Neu waren die Datenbanken für politische Onlinewerbung, die im Vorfeld der Wahlen zum Europäischen Parlament 2019 aufgesetzt wurden. Diese waren jedoch unvollständig und von Fehlern geplagt.²⁵ Dagegen konnte die EU nicht viel unternehmen – wegen fehlender Sanktionsmöglichkeiten. Zudem ist es fraglich, ob der ausschließliche Fokus auf russische Einflussnahme der Desinformationsproblematik gerecht wird, wenn klar ist, dass viele Desinformationskampagnen von inländischen Personen und Organisationen betrieben werden. In Deutschland zeigte sich beispielsweise, dass vor der Bundestagswahl 2017 vorrangig Rechtspopulist:innen innerhalb des Landes ihre Mitmenschen in die Irre führten, ohne dass ausländische Staaten direkt eingriffen.²⁶ Die EU war sich dieser Schwachstellen von Anfang an bewusst, heißt es doch im Aktionsplan selbst, dass nach dessen Evaluierung regulatorische Maßnahmen möglich seien. Einige davon werden im nächsten Abschnitt besprochen.

Inhaltelöschung

Beispiele und Hintergrund. Für den Umgang mit rechtswidrigen Inhalten gibt es im Internet bereits etablierte Haftungs- und Lösungsregeln. Solche Inhalte betreffen in Deutschland etwa Volksverhetzung und die Beschimpfung weltanschaulicher oder religiöser Gemeinschaften. Regierungen in aller Welt versuchen seit 2016, die Löschung strafbarer Inhalte besser durchzusetzen. Dieser Ansatz lässt sich nur bedingt auf Desinformation übertragen, da diese nicht immer strafbar ist.²⁷ Eine Auseinandersetzung mit Fragen zur Inhaltmoderation und -löschung ist dennoch auch für den Bereich Desinformation nötig.

²⁴ Zu den Schwierigkeiten für Forschung und Zivilgesellschaft beim Datenzugang siehe Alexander Sänglerlaub, „Der blinde Fleck digitaler Öffentlichkeiten“ (Berlin: Stiftung Neue Verantwortung, 21. März 2019), https://www.stiftung-nv.de/sites/default/files/blinde.fleck_digitale.oeffentlichkeit.pdf.

²⁵ Mozilla Corporation, „Facebook and Google: This Is What an Effective Ad Archive API Looks Like“, *The Mozilla Blog*, 27. März 2019, <https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like>.

²⁶ Sänglerlaub, Meier, und Rühl, „Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017“.

²⁷ Siehe hierzu insbesondere Kapitel 4 und 6 in Christian Mihr und Daniel Moßbrucker, „Regulierung 2.0: Warum soziale Netzwerke, Suchmaschinen & Co. ein Teil der informationellen Grundversorgung geworden sind - und wie sie reguliert werden sollten, um die Meinungs- und Pressefreiheit zu schützen“ (Berlin: Reporter ohne Grenzen, 12. Juni 2018), https://www.reporter-ohne-grenzen.de/uploads/tx_lfnews/media/Reporter-ohne-Grenzen_Regulierung-2.0-Langfassung.pdf.

Die Löschung rechtswidriger Inhalte im Internet funktioniert hauptsächlich über das „Notice and take down“-Verfahren: Soziale Netzwerke, Suchmaschinen und andere Internetdienste müssen rechtswidrige Inhalte löschen – wenn sie davon erfahren. Aktiv müssen sie nicht nach solchen Inhalten suchen. Das ist die Basis für viele Angebote im Internet: Wären soziale Netzwerke, Suchmaschinen, Videoportale und andere digitale Dienste nicht teils von einer Haftung ausgenommen, was Inhalte ihrer Nutzenden betrifft, hätten sich Unternehmen wie Google, Facebook und Twitter wohl kaum entwickeln können. Diese Regelungen und Ausnahmen zur Haftung sind in der E-Commerce-Richtlinie der EU festgehalten und schlagen sich im deutschen Telemediengesetz (TMG) nieder. Auf europäischer Ebene soll ein Digital Services Act die E-Commerce-Richtlinie ersetzen und dabei auch die Haftungsregeln aktualisieren.²⁸ In Deutschland fordert das Netzwerkdurchsetzungsgesetz (NetzDG) große soziale Netzwerke dazu auf, ihren Nutzenden ein Verfahren zum Anzeigen möglicherweise rechtswidriger Inhalte zur Verfügung zu stellen. Darüber gemeldete strafrechtlich relevante Inhalte müssen laut NetzDG innerhalb bestimmter Fristen von den Anbietern gelöscht werden.

Stärken. Illegale Inhalte im Internet zu löschen ist eine konsequente Anwendung geltenden Rechts. Für diese Inhaltelöschung und auch die Inhaltemoderation Strukturen zu finden, ist daher ein positiver Ansatz. Das NetzDG ist dazu eine Ergänzung und Erweiterung der bisherigen Haftungs- und Lösungspraxis und wartet mit einigen neuen Regeln auf: Neben der erwähnten Verpflichtung, Verfahren zur Meldung rechtswidriger Inhalte anzubieten, müssen Unternehmen Ansprechpersonen benennen und über Lösungsmodalitäten berichten. Diese Ansätze sind sinnvoll, denn sie schaffen Regeln für die Strukturen und Prozesse innerhalb der Unternehmen über die Entfernung einzelner Inhalte hinaus. Das kann auch für den Umgang mit Desinformation hilfreich sein, wenn es nämlich unternehmensintern klare, transparente und von außen überprüfbare Vorgaben für die Moderation und Löschung von Inhalten gibt.

Schwächen. Die geltenden Haftungs- und Löschvorschriften aus der E-Commerce-Richtlinie von 2000 haben sich im Großen und Ganzen bewährt, bedürfen aber dennoch einer Überholung angesichts des Aufstiegs sozialer Netzwerke und Suchmaschinen seitdem. Die EU ist selbst von der Notwen-

²⁸ Ursula von der Leyen, „A Union that strives for more: My agenda for Europe“ (Brüssel: European Commission, 16. Juli 2019), 13, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf; ein geleaktes Arbeitspapier zeigt mögliche Eckpunkte eines Digital Services Act auf, siehe Tomas Rudl und Alexander Fanta, „Geleaktes Arbeitspapier: EU-Kommission erwägt neues Gesetz für Plattformen“, [netzpolitik.org](https://netzpolitik.org/2019/geleaktes-arbeitspapier-eu-kommission-erwaegt-neues-gesetz-fuer-plattformen/), 15. Juli 2019, <https://netzpolitik.org/2019/geleaktes-arbeitspapier-eu-kommission-erwaegt-neues-gesetz-fuer-plattformen/>.

digkeit einer Reform überzeugt²⁹ und auch im Koalitionsvertrag von 2017³⁰ wird diese Notwendigkeit erwähnt. Fragen zur Haftung und Inhaltelöschung, besonders mit Blick auf Desinformation, bewegen sich allerdings auf dem schmalen Grat zwischen Meinungsfreiheit und Zensur, was die Debatte um Reformen und Lösungsansätze auf diesem Gebiet schwierig macht.³¹ Selbstverständlich ist es richtig, illegale Inhalte in sozialen Netzwerken nicht zu dulden und deren Löschung konsequent durchzusetzen. Doch gerade Desinformation liegt oft in einem rechtlichen Grenzbereich, in dem schwer abzuschätzen ist, was vom Recht auf freie Meinungsäußerung gedeckt ist und was strafbar ist. Noch problematischer wird es, wenn wie im NetzDG Widerspruchsrechte für Nutzende fehlen (bei der Löschung von Inhalten, die nicht hätten entfernt werden sollen) und die Bestimmung eines Rechtsbruchs auf Unternehmen ausgelagert wird. Zudem sorgt ein Fokus auf Inhaltelöschung nicht dafür, dass Menschen und Gruppen von gezielten, trügerisch manipulierten Botschaften verschont bleiben. Auch führen die NetzDG-Pflichten nicht zwangsläufig dazu, dass Verbreiter:innen illegaler Inhalte strafrechtlich verfolgt werden.³² Nicht zuletzt sind die Regeln für die Transparenzberichte unklar: Diese Berichte der Unternehmen sind aufgrund mangelnder Vorgaben schlecht vergleichbar und teils unvollständig.³³ All dies zeigt, dass der Ansatz der Inhaltelöschung, zumindest wie er aktuell auf rechtswidrige Inhalte angewandt wird, auf viele Fragen zur Desinformation nicht übertragbar ist.

29 Europäische Kommission, „COM(2015) 192 final: Strategie für einen digitalen Binnenmarkt für Europa“, Europäische Kommission, 6. Mai 2015, <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52015DC0192&from=EN>.

30 CDU, CSU, und SPD, „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode“, Christlich Demokratische Union Deutschlands, 12. März 2018, 49; 170, https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1.

31 Beim NetzDG besteht zudem besteht die Gefahr, dass sich autoritär Herrschende in anderen Ländern davon inspirieren lassen und dessen Regeln leicht einsetzen können, um im Name des Vorgehens gegen illegale Inhalte kritische Stimmen zu unterdrücken. Für eine Übersicht des Für und Wider zum NetzDG mit Blick auf Fragen zur Meinungsfreiheit siehe David Kaye, *Speech Police: The Global Struggle to Govern the Internet*, Bd. Columbia Global Reports (New York: Columbia University in the City of New York, 2019); Bundeszentrale für politische Bildung, „Debatte Netzwerkdurchsetzungsgesetz (NetzDG)“, Bundeszentrale für politische Bildung, 16. März 2018, <https://www.bpb.de/dialog/netzdebatte/262660/debatte-netzwerkdurchsetzungsgesetz-netzdg>; Heidi Tworek und Paddy Leerssen, „An Analysis of Germany's NetzDG Law“ (Amsterdam: Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 15. April 2019), https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

32 Mittlerweile werden eigene Sonderdezernate zu Cyberkriminalität eingerichtet, die sich auf die Strafverfolgung von „Hate Speech“ konzentrieren; siehe Max Hoppenstedt, „Strafbare Postings in sozialen Netzwerken: Woher der Hass kommt, ist wirklich nur schwer zu begreifen“, *SPIEGEL ONLINE*, 21. Juni 2019, <https://www.spiegel.de/netzwelt/netzpolitik/netzdg-staatsanwalt-christoph-hebbecke-ueber-hass-in-sozialen-netzwerken-a-1273176.html>.

33 Facebook droht beispielsweise ein Bußgeld, da die Transparenzberichte unvollständig seien; siehe dpa, „Facebook wehrt sich gegen NetzDG-Bußgeld“, *heise online*, 19. Juli 2019, <https://www.heise.de/newsticker/meldung/Facebook-wehrt-sich-gegen-NetzDG-Bussgeld-4475699.html>.

Medienregulierung

Beispiel und Hintergrund. Die Reform der deutschen Medienaufsicht – in Form des geplanten „Medienstaatsvertrags“³⁴ – ist nicht ausdrücklich auf die Eindämmung von Desinformation ausgelegt. Wohl aber sind die bisherigen Rundfunkstaatsverträge dazu da, Nachrichten- und Informationsräume zu schaffen, die den demokratischen Diskurs und die politische Willensbildung nicht behindern, sondern beflügeln. Daher kann der Medienstaatsvertrag als Beispiel dafür dienen, welche Chancen und Risiken aufkommen, wenn ein für analoge Angebote gebauter regulatorischer Rahmen für digitale Angebote angepasst werden soll.

Der Medienstaatsvertrag ist die 23. Änderung des Rundfunkstaatsvertrags, der unter anderem die Aufsicht von Fernsehen, Radio und Onlinemedien in Deutschland regelt. Erstmals wird nun von einem *Medienstaatsvertrag* statt eines *Rundfunkstaatsvertrags* gesprochen. In dieser Umbenennung spiegeln sich die Bestrebungen wider, die deutsche Medienregulierung an das digitale Zeitalter anzupassen. Es soll ein Regelwerk auch für soziale Netzwerke und Suchmaschinen entstehen: Da solche Dienste für Mediennutzende immer wichtiger werden, um an Nachrichten und Informationen zu kommen, möchten die Länder ihren eigenen Kompetenzbereich mit dem Medienstaatsvertrag auch hier geltend machen.³⁵ Denn die Bundesländer sind in Deutschland zuständig für die Aufsicht über Rundfunk und TV sowie „Telemedien“, also Medienangebote im Internet wie etwa Onlineportale von Zeitungen. Eine wichtige Aufgabe dieser Aufsicht betrifft den Jugendmedienschutz, der im Jugendmedienschutz-Staatsvertrag (JMStV) geregelt ist. Dort findet sich auch das System der „regulierten Selbstregulierung“, zu dem beispielsweise der Verein Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM) gehört. Seine Mitglieder sind Unternehmen wie Facebook und Google, die über den Verein eine Beschwerdestelle zu strafbaren und jugendgefährdenden Inhalten betreiben.

Teile des Medienstaatsvertrags, insbesondere in Bezug auf Videoportale wie YouTube, setzen Vorgaben der Richtlinie über audiovisuelle Mediendienste der EU (AVMD-Richtlinie) um. Das ist auch der Grund, warum der Medienstaatsvertrag bis September 2020 fertig sein muss: Die AVMD-Richtlinie muss bis zu diesem Zeitpunkt in nationales Recht umgesetzt werden. Vor-

34 Staatskanzlei Rheinland-Pfalz, „Diskussionsentwurf für einen ‚Medienstaatsvertrag‘“ (2019), https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/MStV-E_Synopse_2019-07_Online_.pdf.

35 Helmut Hartung, „Medienstaatsvertrag: Der Vielfalt verpflichtet“, *Frankfurter Allgemeine Zeitung*, 9. August 2019, <https://www.faz.net/aktuell/feuilleton/medien/medienstaatsvertrag-der-vielfalt-verpflichtet-16324354.html>.

ausgegangen war dem Entwurf des Medienstaatsvertrags eine Bund-Länder-Kommission zur Medienkonvergenz³⁶, die wiederum auf einem umfangreichen Gutachten³⁷ für die Rundfunkkommission der Länder beruhte. Letzteres wurde bereits 2014 veröffentlicht, was zeigt, wie lange die Diskussion um eine Reform der Medienaufsicht für das digitale Zeitalter schon im Gange ist.

Stärken. Da Desinformation immer mehr im digitalen Raum auftritt, ist es ganz grundsätzlich sinnvoll, Aufsichtsmaßnahmen etwa für große soziale Netzwerke und Suchmaschinen zu definieren. Nicht nur in Deutschland wird darüber nachgedacht: So wurden zum Beispiel in Frankreich³⁸ und Großbritannien³⁹ zentrale, auf soziale Netzwerke spezialisierte Behörden vorgeschlagen. Aufgrund der historisch bedingten föderalistischen Struktur der Medienregulierung in Deutschland verortet der Medienstaatsvertrag die Aufsicht über soziale Netzwerke in den Bundesländern.

Einige der im Entwurf vorgeschlagenen konkreten Regeln können bei der Eindämmung von Desinformation hilfreich sein. Ein vielversprechender Ansatz sind die Vorgaben zur Algorithmentransparenz für soziale Netzwerke und Suchmaschinen. Denn eine Offenlegung dazu, wie die Auswahl und Anordnung von Suchergebnissen oder Beiträgen funktioniert, kann bei Nutzenden ein besseres Bewusstsein für das algorithmisch aufbereitete Nachrichtenumfeld schaffen. Die Benennung von Ansprechpersonen ist – ähnlich wie im Netzwerkdurchsetzungsgesetz (siehe oben) – ebenfalls sinnvoll. Beides sind Maßnahmen, die nicht direkt auf möglicherweise rechtswidrige oder irreführende Inhalte abzielen und deren Löschung veranlassen, sondern für mehr Transparenz beim Nachrichtenkonsum sorgen sollen.

³⁶ Bund-Länder-Kommission, „Bericht Bund-Länder-Kommission zur Medienkonvergenz“ (Berlin: Bund-Länder-Kommission, Juni 2016), <https://www.bundesregierung.de/resource/blob/997532/473870/07ba875e860ada4556526641bd9151b6/2016-06-14-medienkonvergenz-bericht-blk-data.pdf?download=1>.

³⁷ Winfried Kluth und Wolfgang Schulz, „Konvergenz und regulatorische Folgen: Gutachten im Auftrag der Rundfunkkommission der Länder“ (Mainz: Rundfunkkommission der Länder, 2014), <https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/Konvergenz-Gutachten.pdf>.

³⁸ Sacha Desmaris, Pierre Dubreuil, und Benoît Loutrel, „Creating a French framework to make social media platforms more accountable: Acting in France with a European vision“ (Paris: French Secretary of State for Digital Affairs, Mai 2019), https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E-1B36873E4&filename=Mission%20Re%CC%81gulation%20des%20re%CC%81seaux%20sociaux%20-ENG.pdf.

³⁹ Department for Digital, Culture, Media & Sport und Home Office, „Online Harms White Paper“ (London: Controller of Her Majesty's Stationery Office, 8. April 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

Schwächen. Ob der Medienstaatsvertrag ausreichend auf das digitale Medienumfeld mit sozialen Netzwerken, Suchmaschinen, Videoportalen und Blogging-Diensten eingeht, ist im aktuellen Entwurf noch offen. Allein schon bei der Einführung neuer oder der Erweiterung bestehender Begrifflichkeiten gibt es Unschärfen und Unklarheiten.⁴⁰ Es wird von Medienplattformen (was ungefähr Netflix meint), Medienintermediären (ungefähr Google und Facebook), Benutzeroberflächen (ungefähr elektronische Programmführer), Video-Sharing-Diensten (ungefähr YouTube) und rundfunkähnlichen Telemedien (ungefähr ARD-Mediathek) gesprochen, wobei die Grenzen verschwimmen und teils noch unklar sind. Insbesondere der letztgenannte Begriff zeigt den grundlegenden Ansatz auf, das bisherige Verständnis von Rundfunk auf soziale Netzwerke, Suchmaschinen und Videoportale auszudehnen. Dass an der Trennung von linearen und nicht-linearen Medien (also etwa Radio versus Streaming-Dienst) festgehalten wird, ist auch den Vorgaben der AVMD-Richtlinie geschuldet.⁴¹ Aber selbst vor diesem Hintergrund wird der Begriff „Rundfunkähnlichkeit“ im deutschen Entwurf dem digitalen Informations- und Nachrichtenumfeld nicht gerecht.⁴²

Regeln zur Transparenz können in vielen Bereichen sinnvoll sein, aber es kommt auf deren Ausgestaltung an. Im Medienstaatsvertrag ist der Mindestanspruch, dass Algorithmentransparenz dabei helfen soll, den Einfluss großer sozialer Netzwerke und Suchmaschinen auf die Meinungsbildung zunächst einmal besser zu verstehen.⁴³ Dafür gibt es insgesamt zwei kurze Paragraphen im Entwurf des Medienstaatsvertrags: einer für Medienplattformen wie Netflix und einer für Medienintermediäre (also soziale Netzwerke und Suchmaschinen). Vorgabe ist jeweils, dass Nutzende unmittelbar und in verständlicher Sprache über die „zentralen Kriterien“ der Such- und Sortieralgorithmen aufgeklärt werden sollen. Für solche Transparenzregeln sind klarere, detaillierte Vorgaben nötig. Denn sonst ergibt sich eine ähnliche Situation wie mit den Transparenzbemühungen, die ohnehin schon beispielsweise bei Facebook und Twitter bestehen: Die Unternehmen klären Nutzende zwar darüber auf, warum sie bestimmte Werbeinhalte sehen, aber diese Informationen sind nur rudimentär und daher wenig hilfreich. Für politische

40 Zu den anfänglichen Schwierigkeiten bei den Definitionen siehe durchgängig Wolfgang Schulz und Stephan Dreyer, „Stellungnahme zum Diskussionsentwurf eines Medienstaatsvertrags der Länder“ (Hamburg: Hans-Bredow-Institut, 26. September 2018), https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/qiuektv_HBI_StellungnahmeMedienstaatsvertrag180926.pdf.

41 Hartung, „Medienstaatsvertrag: Der Vielfalt verpflichtet“.

42 Hermann Rotermund, „Neuer Medienstaatsvertrag – alter Rundfunk“, *CARTA online*, 27. August 2018, <http://carta.info/neuer-medienstaatsvertrag-alter-rundfunk/>.

43 Helmut Hartung, „Das ist ziemlich einmalig‘: Interview mit Prof. Dr. Wolfgang Schulz, Direktor des Hans-Bredow-Instituts für Medienforschung“, *Medienpolitik.net*, 26. September 2018, <https://www.medienpolitik.net/2018/09/medienpolitikdas-ist-ziemlich-einmalig/>.

Werbung in sozialen Netzwerken und Suchmaschinen sieht der Entwurf vor, dass diese gekennzeichnet werden muss.⁴⁴ Darüberhinausgehende Details fehlen, obwohl es konkrete Vorschläge gibt, welche Angaben in welcher Form Nutzenden helfen könnten.⁴⁵

Wettbewerb X Datenschutz

Beispiele und Hintergrund. Seit Jahren wird über eine engere Verzahnung von Wettbewerbs- und Datenschutzbehörden diskutiert, um der wachsenden Daten- und Marktmacht großer sozialer Netzwerke und Suchmaschinen beizukommen.⁴⁶ Dieser Ansatz hat nicht direkt zum Ziel, Desinformation zu unterbinden. Nichtsdestotrotz ist ein Blick auf Wettbewerbs- und Datenschutzregeln wichtig, da diese indirekt zu einer Eindämmung von Desinformation führen können. Das Einfallstor für Desinformation steht in personalisierten, segmentierten Newsfeeds globaler Netzwerke weit offen. Eine Eingrenzung der Datensammlung und der dominanten Position, die gerade Facebook und Google im Online-Werbemarkt innehaben, könnte dieses Einfallstor etwas schließen. Denn die Segmentierung und Personalisierung der Newsfeeds oder Suchmaschinenergebnisse über Such- und Sortieralgorithmen wären ohne umfangreiche Datenanalysen und Profilbildungen nicht möglich (siehe Infobox S. 10 und 11).

Beispielhaft für eine Verknüpfung von Wettbewerbsrecht und Datenschutz lässt sich das Kartellamtsverfahren gegen Facebook in Deutschland anführen. Die Wettbewerbsbehörde untersuchte die Marktmacht Facebooks vor dem Hintergrund der umfangreichen Datensammlung des Unternehmens. Nach einer mehrjährigen Untersuchung kam das Bundeskartellamt zu dem Schluss, dass Facebook eine dominierende Marktposition hat und diese zum Nachteil der Nutzenden missbraucht. Die Nutzenden verlieren

44 Die Medienanstalten, „Stellungnahme der Medienanstalten zum überarbeiteten Diskussionsentwurf der Rundfunkkommission der Länder für einen ‚Medienstaatsvertrag‘“, Die Medienanstalten, 9. August 2019, 10–11, https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Ueber_uns/Positionen/2019_08_09_Stellungnahme_der_Medienanstalten_zum_Medienstaatsvertrag.pdf.

45 Dipayan Ghosh und Ben Scott, „Digital Deceit II: A Policy Agenda to Fight Disinformation on the Internet“ (Washington, DC: New America, 23. Januar 2018), https://d1y8sb8igg2f8e.cloudfront.net/documents/Digital_Deceit_2_Final.pdf.

46 Siehe beispielhaft auf EU-Ebene, in Australien und in Großbritannien: Europäischer Datenschutzbeauftragter, „Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von ‚Big Data‘: Das Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz in der digitalen Wirtschaft“ (Brüssel: Europäischer Datenschutzbeauftragter, März 2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_de.pdf; Australian Competition and Consumer Commission, „Digital Platforms Inquiry - Final Report“ (Canberra: Australian Competition and Consumer Commission, 26. Juli 2019), <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>; Competition and Markets Authority, „Online Platforms and Digital Advertising Market Study“, GOV.UK, 3. Juli 2019, <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>.

laut Wettbewerbsbehörde die Kontrolle über ihre eigenen Daten, auch wenn ihnen dadurch kein direkter finanzieller Schaden entsteht.⁴⁷ Konkret ging es darum, ob und wie Facebook Daten aus seinen Diensten Facebook, Instagram, WhatsApp und aus anderen Quellen zusammenführen darf. Das Bundeskartellamt untersagte diese Praxis. In einem juristischen Verfahren im Anschluss wurde die Umsetzung dieser Entscheidung allerdings zunächst durch das Oberlandesgericht Düsseldorf gestoppt.⁴⁸ Ob das Bundeskartellamt mit seinem Versuch der Verknüpfung von Datenschutz und Wettbewerb Erfolg hat, wird sich erst in den kommenden Monaten und Jahren zeigen: Das endgültige Urteil dürfte noch Monate auf sich warten lassen, der Bundesgerichtshof wird sich mit dem Fall befassen und auch ein Verfahren beim Europäischen Gerichtshof ist möglich.⁴⁹

Stärken. Die weltweit bisher einmalige Verknüpfung von Datenschutz- und Wettbewerbsrecht im Verfahren des Bundeskartellamts steht für den Versuch, die Daten- und Marktmacht von Facebook und anderen dominierenden Digitalunternehmen einzuschränken. Das Kartellamt beruft sich dabei auf die europäische Datenschutz-Grundverordnung (DSGVO). Die DSGVO bietet Möglichkeiten, die Datensammlung – gerade sensibler Daten etwa zu politischer Weltanschauung, Sexualität und Gesundheitszustand – einzugrenzen, die für viele soziale Netzwerke Kern ihres Werbeangebots ist. Um nur ein Beispiel zu nennen: Voreinstellungen bei sozialen Netzwerken müssen so gewählt sein, dass sie möglichst datenschutzfreundlich sind („privacy by default“). Verbunden mit dem Gebot, möglichst wenig Daten zu erheben, kann das Tracking und die Profilbildung eingeschränkt werden. Das verbessert die Chancen, nicht nur Informationen und Beiträge angezeigt zu bekommen, zu denen ein Algorithmus berechnet hat, dass sie zu viel Engagement

47 Zusammengefasst in der Pressemitteilung bei Bundeskartellamt, „Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen“, *Bundeskartellamt*, 7. Februar 2019, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2; vollständige Entscheidung bei Bundeskartellamt, „B6-22/16: Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung“ (Bonn: Bundeskartellamt, 7. Februar 2019), https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html;jsessionid=1758AF99E64A2D1B504758D23E7072EB.1_cid378?nn=3591568.

48 Zusammengefasst in der Pressemitteilung bei Michael Börsch, „Facebook: Anordnungen des Bundeskartellamts möglicherweise rechtswidrig und deshalb einstweilen außer Vollzug“, *Oberlandesgericht Düsseldorf*, 26. August 2019, http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/index.php; vollständiger Beschluss bei Oberlandesgericht Düsseldorf, „Beschluss VI-Kart 1/19 (V) In der Kartellverwaltungssache 1. Facebook Inc., 2. Facebook Ireland Ltd., 3. Facebook Deutschland GmbH, Antragstellerinnen und Beschwerdeführerinnen, Verfahrensbevollmächtigte:... gegen Bundeskartellamt, Antragsgegner und Beschwerdegegner“, *Oberlandesgericht Düsseldorf*, 26. August 2019, http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-V_.pdf.

49 PBE/DPA, „Gericht verpasst Kartellamt im Verfahren gegen Facebook einen Dämpfer“, *SPIEGEL ONLINE*, 26. August 2019, <https://www.spiegel.de/netzwelt/apps/bundeskartellamt-gegen-facebook-oberlandesgericht-duesseldorf-bremst-a-1283736.html>.

der Nutzenden führen – etwa indem Wut oder andere Emotionen besonders stark angesprochen werden.⁵⁰

Schwächen. Im Datenschutz gibt es mit der DSGVO ein kürzlich verabschiedetes Regelwerk, um gegen eine unrechtmäßige Datensammlung vorzugehen. Doch gestaltet sich deren Durchsetzung schwierig, da Datenschutzbehörden dafür oft die Ressourcen fehlen. Im Gegensatz dazu haben Kartellbehörden traditionell eine starke Durchsetzungskraft. Ihnen mangelt es jedoch an einem für das digitale Zeitalter passenden Rechtsrahmen, obwohl die Behörden selbst eine starke Expertise zur Digitalisierung der Wirtschaft aufgebaut haben.⁵¹ Diese institutionellen Schwächen hat das Kartellamtsverfahren gegen Facebook aufgezeigt. Das behindert indirekt auch die Eindämmung von Desinformation auf großen Plattformen. Mit Blick auf das Wettbewerbsrecht ist eine Reform geplant. Hierzu hat das Bundeswirtschaftsministerium die Kommission „Wettbewerbsrecht 4.0“ ins Leben gerufen, die in ihrem Bericht neben verbessertem Datenzugang für Bürger:innen und mögliche Wettbewerber auch eine „institutionalisierte Vernetzung“ verschiedener Aufsichtsbehörden empfiehlt.⁵² Bis solche oder ähnliche Reformen kommen, bleibt es allerdings beim geltenden Rechtsverständnis, das von einer Trennung von Kartellrecht und Datenschutz ausgeht.

Insgesamt bringt der Überblick zu den dargestellten Ansätzen im Umgang mit Desinformation strukturelle Schwächen zum Vorschein. Geprägt ist dieser Umgang von reaktiven Maßnahmen nach 2016, die zunächst hauptsächlich aus Selbstregulierung und verschärften Vorgaben zur Inhaltelöschung bestanden. In anderen Rechts- und Politikbereichen bilden sich nun erst langsam darüber hinaus gehende Ansätze aus. Die geplanten Reformen der Medienaufsicht und des Wettbewerbsrechts sind hierfür Beispiele. Dabei wird aber kein ganzheitlicher Blick auf Desinformation geworfen, was den Umgang damit dementsprechend lückenhaft bleiben lässt. Im folgenden Fazit werden einige der Schwachstellen aufgegriffen und als mögliche zukünftige Betätigungsfelder für legislative und regulatorische Maßnahmen besprochen.

50 Weitere Beispiele aus der DSGVO sind Regeln zur Zweckbindung, Transparenz- und Informationspflichten und Datenschutz bei Kindern. Auch eine Erweiterung der Datenschutz-Folgenabschätzung könnte hilfreich sein.

51 Rupprecht Podszun, „Nach dem Facebook-Verfahren: Der Kartellrechts-Clash“, *Legal Tribune Online*, 13. September 2019, <https://www.lto.de/recht/hintergruende/h/facebook-verfahren-bkarta-ausbeutung-marktbeherrschung/>.

52 Kommission Wettbewerbsrecht 4.0, „Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft“ (Berlin: Bundesministerium für Wirtschaft und Energie, 9. September 2019), 5, https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=4.

Fazit

*Wir brauchen nur weniger welches
Und etwas mehr jenes
Eine Gleichung wie diese löst nicht einmal der Klassenprimus
Weltretten 4-
- Volker Racho*

Die im Papier aufgezeigten Aktivitäten verdeutlichen einerseits, dass sich ein Problembewusstsein für Desinformation in der Politik und bei Unternehmen entwickelt. Andererseits offenbaren sie Schwierigkeiten in der Eindämmung von Desinformation: Selbstregulierung hat nicht funktioniert, was die Eigeneinschätzung der EU zum Aktionsplan bestätigt. Eine Übertragung des Ansatzes zur Löschung von Inhalten, wie es bisher klarer Schwerpunkt bei rechtswidrigen Inhalten war, ist unpassend. Auch geplante regulatorische Vorhaben wie die Reform der Medienaufsicht sind den Gefahren von Desinformation nicht angemessen. So entsteht ein lückenhaftes regulatorisches Umfeld. Davon profitieren Personen und Organisationen, die Desinformation verbreiten möchten.

Demokratische Gesellschaften sind den Gefahren von Desinformation jedoch nicht machtlos ausgeliefert. Auch das wurde im Papier deutlich. Auf allen politischen Ebenen gibt es legislative und regulatorische Vorhaben, die dabei helfen können, Desinformation einzudämmen. Dabei ist weniger ein Kampf *gegen* irreführende und illegale Inhalte an sich von Bedeutung. Stattdessen ist etwas mehr Einsatz *für* ein digitales Informationsumfeld nötig, in dem Bürger:innen sich frei und selbstbestimmt ihre politische Meinung bilden können. Dazu gehören Transparenzregeln für Unternehmen ebenso wie Maßnahmen zur Stärkung der Privatsphäre und eine passende Aufsicht. Und obwohl dies nicht der Schwerpunkt des Papiers ist: Selbstverständlich sind auch der Ausbau der Nachrichten- und Informationskompetenz sowie die Förderung von Journalismus wichtig.⁵³ Werden die hier aufgezeigten Herangehensweisen zusammengedacht, lassen sich einige übergreifende Punkte für mögliche zukünftige Aktivitäten identifizieren.

Nicht nur auf Selbstregulierung verlassen. Der Code of Practice der EU hat Symbolcharakter, leistet aber wenig mehr als das. Obwohl die EU ihn als Erfolg ausgibt⁵⁴, ist sie sich gleichzeitig bewusst, wie begrenzt selbstregulatorische Maßnahmen sind. Im dazugehörigen Aktionsplan heißt es deshalb,

⁵³ Die SNV behandelt dies in separaten Projekten zur Stärkung digitaler Öffentlichkeit.

⁵⁴ European Commission, „JOIN(2019) 12 final: Report on the implementation of the Action Plan Against Disinformation“ (Brüssel: European Commission, 14. Juni 2019), https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf.

dass auch regulatorische Maßnahmen vorgeschlagen werden könnten, wenn sich bei der Evaluation nach einem Jahr keine Fortschritte zeigen. Die mögliche Reform der E-Commerce-Richtlinie zu einem Digital Services Act könnte diese angedachten Regulierungen umfassen. Das NetzDG und der Anspruch des Bundeskartellamts unterstreichen die Einstellung politischer und regulatorischer Entscheidungsträger:innen, dass Selbstregulierung nicht mehr ausreicht. Soziale Netzwerke und Suchmaschinen etwa, die ihr Geld als Werbeplattformen verdienen, aber gleichzeitig die politische Willensbildung vieler Menschen mitsteuern, brauchen für diese Nebenwirkung ihrer Arbeit als Werbevermarkter klare Regeln. Das mag heute in Deutschland besonders für Facebook, Google, Instagram und YouTube gelten, kann sich aber in naher Zukunft auf ganz andere Angebote beziehen. Auch das muss bei möglichen regulatorischen Schritten bedacht werden.

Transparenzregeln näher definieren. In vielen der bisherigen Maßnahmen geht es um Transparenz: zum Beispiel im Medienstaatsvertrag mit seinen Transparenzregeln für Algorithmen, im Aktionsplan zu politischer Werbung und im NetzDG mit Blick auf die Benennung von Ansprechpersonen und die Berichtspflicht für Unternehmen. Für Nutzende kann ein Einblick in die Funktionsweise von sozialen Netzwerken und Suchmaschinen hilfreich sein. Noch wichtiger sind solche Einblicke für die Forschung, um die Eigenheiten und Auswirkungen digitaler Dienste zu verstehen und diese Erkenntnisse für die Gesellschaft zugänglich zu machen. Dafür müssen Transparenzregeln klarer sein, etwa müssen Kriterien zur Offenlegung und Nachvollziehbarkeit von Algorithmen detaillierter definiert sein. Zudem muss es Forschenden möglich sein, mit Daten der sozialen Netzwerke und Suchmaschinen zu arbeiten.⁵⁵ Mit aussagekräftigen Studienergebnissen können dann politische Entscheidungsträger:innen evidenzbasierte Entscheidungen treffen. Momentan müssen sich Forschung und Politik oft auf Einzelfallstudien verlassen oder sind auf freiwillige Initiativen der Unternehmen verlassen, um an Daten zu kommen. Das funktioniert bisher nicht besonders gut.⁵⁶ Auch die Berichte mit Zahlen zu gelöschten Inhalten, die im NetzDG vorgeschrieben sind, stoßen auf Kritik, weil sie uneinheitlich und unvollständig sind.⁵⁷ Wichtig ist es, bei Transparenzfragen eine Wechselwirkung mit dem Datenschutz zu beachten: Forderungen nach Transparenz für Forschende dürfen nicht aus

⁵⁵ Sänglerlaub, „Der blinde Fleck digitaler Öffentlichkeiten“.

⁵⁶ Katie Paul, „Funders Threaten to Quit Facebook Project Studying Impact on Democracy“, *Reuters*, 28. August 2019, <https://www.reuters.com/article/us-facebook-election-research-idUSKCN1VI04F>.

⁵⁷ Moritz Koch und Dietmar Neuerer, „Netzwerkdurchsetzungsgesetz: Die Bundesregierung erreicht im Kampf gegen Hate-Speech im Netz nur wenig“, *Handelsblatt*, 6. August 2019, <https://www.handelsblatt.com/politik/deutschland/netzwerkdurchsetzungsgesetz-die-bundesregierung-erreicht-im-kampf-gegen-hate-speech-im-netz-nur-wenig/24874984.html>.

fadenscheinigen Datenschutzgründen abgelehnt werden und Datenschutz darf nicht aufgeweicht werden, um Forschung zu ermöglichen. Die DSGVO hält prinzipiell Wege offen, die eine anonymisierte, aggregierte Datenauswertung für die Forschung erlaubt.

Transparenz ist auch bei parteipolitischer Onlinekommunikation nötig. Der Aktionsplan spielt auf politische Werbung im Internet an und der Digital Services Act könnte dazu klare Regeln für die EU beinhalten. Aktuell sind Bürger:innen auf die freiwilligen Maßnahmen der Unternehmen angewiesen, die letztere über die Jahre entwickelt haben. Kritik an dieser selbstregulatorischen Praxis und konkrete Verbesserungsvorschläge für Regulierung existieren bereits.⁵⁸ Dafür müssen Ansätze aus dem Datenschutz und der Medienregulierung kombiniert werden, ebenso muss in Deutschland das Parteiengesetz beachtet werden. Idealerweise ließen sich aber unter Berücksichtigung länderspezifischer Wahlgesetze tatsächlich europäische Regeln finden.

Rechtsdurchsetzung verbessern. Bevor neue Gesetze für die digitale Öffentlichkeit geschaffen werden, sollten erst mal bestehende Gesetze strikt angewandt werden. Das war der Hintergrund des Netzwerkdurchsetzungsgesetzes mit Blick auf das Strafrecht. Statt auf das Strafrecht wäre aber ein Fokus auf das Datenschutzrecht hilfreich. Auf den ersten Blick mag es nicht offensichtlich sein, was Datenschutz mit Desinformation zu tun hat: Die DSGVO ist nicht dafür ausgelegt, flächendeckend strafrechtlich relevante Inhalte aus dem Internet zu entfernen. Wendet sich der Blick hingegen der datengetriebenen Funktionsweise von Facebook, Google, Twitter, YouTube und anderen Unternehmen zu, können Datenschutzregeln sehr wohl zur Eindämmung von Desinformation beitragen (siehe oben unter „Wettbewerb X Datenschutz“). Die Forderungen nach besserer Rechtsdurchsetzung im Datenschutz sind keinesfalls neu oder kontrovers, allein es fehlen die Ressourcen. Seit Jahren beklagen Verantwortliche in den Datenschutzbehörden der Länder zu wenig Personal und finanzielle Mittel. Gerade weil Datenschutzrechte im Zeitalter Überwachungskapitalistischer Unternehmen wie Facebook und

58 Dipayan Ghosh und Ben Scott in Anja Zimmer, Hrsg., *Smart Regulation for Digital Media Pluralism* (Berlin: Medienanstalt Berlin-Brandenburg, 2019), https://mediapolicylab.de/files/content/document/Policy%20Statements/White_Book_MPL_July2019.pdf; Jochen König und Juri Schnöller, „Wie digitale Plattformen sich um Transparenz bemühen“, *Politik & Kommunikation*, 9. Juli 2019, <https://www.politik-kommunikation.de/ressorts/artikel/wie-digitale-plattformen-sich-um-transparenz-bemuehen-1923588873>; für eine ausführliche Betrachtung aus britischer Perspektive mit Schlussfolgerungen auch für Deutschland und die EU siehe Michela Palese und Josiah Mortimer, Hrsg., *Reining in the Political 'Wild West': Campaign Rules for the 21st Century* (Electoral Reform Society, 2019), <https://www.electoral-reform.org.uk/latest-news-and-research/publications/reining-in-the-political-wild-west-campaign-rules-for-the-21st-century/>.



Google⁵⁹ eine noch höhere Bedeutung erlangen, ist es daher wichtig, Expertise und Ressourcen für deren Durchsetzung bereitzustellen.

Koordination verbessern und Aufsicht ganzheitlich denken. Auf absehbare Zeit werden Reformen auf verschiedenen politischen Ebenen in diversen Rechtsbereichen – von der Medienaufsicht über Inthaltmoderation bis hin zum Wettbewerbsrecht den Umgang mit Desinformation und auch Online-Hetze prägen. Um bei diesem fragmentarischen Ansatz möglicherweise gegenläufige Ziele und Entscheidungen zu verhindern, ist eine verbesserte Koordinierung der jeweiligen Behörden untereinander sinnvoll. Das bezieht sich etwa auf die Verzahnung von Wettbewerbs- und Datenschutzrecht. Ein anderes Beispiel ist der Datenschutz für Kinder: Dieser wird aktuell im Jugendmedienschutz und in der DSGVO behandelt, ohne dass es eine institutionalisierte Abstimmung dazu gibt. Auch eine engere Zusammenarbeit deutscher Behörden und Ministerien mit europäischen Partnern ist hilfreich, um nach Möglichkeit EU-weite gemeinsame Standards zu etablieren. Der Digital Services Act könnte dazu Abhilfe schaffen. Hierbei muss allerdings auf länderspezifische Kontexte geachtet werden, zum Beispiel mit Blick auf Internetnutzung, Mediensystem und Aufsichtsstruktur. Deutschlands Medienaufsicht etwa ist aus gutem Grund staatsfern und föderalistisch aufgebaut.

Auch im Angesicht dieser historisch bedingten Notwendigkeiten in Deutschland lohnt es sich, über zukünftige Formen der Aufsicht speziell für soziale Netzwerke und Suchmaschinen nachzudenken. Die Idee einer „Internetintendanz“ etwa beinhaltet unter anderem eine Kontrollinstanz für Fragen der Desinformation.⁶⁰ Wie oben erwähnt (siehe Medienregulierung) wurde in Frankreich der Regierung nach monatelanger Recherche bei Facebook eine zentrale Aufsichtsbehörde für soziale Netzwerke vorgeschlagen. Auch in Großbritannien wird darüber diskutiert. Interessanterweise verglichen die französischen Expert:innen ihren Vorschlag mit der Finanzmarktregulierung: Der Blick ist dort auf Prozesse (nicht Produkte) gerichtet und es gibt eine übergreifende Aufsichtsbehörde für den Markt. Ähnlich ist es bei der Pharmaregulierung. Das primäre Ziel der Aufsicht ist es jeweils nicht, das einzelne Finanzprodukt oder das einzelne Medikament aus dem Verkehr zu ziehen, sondern dafür Sorge zu tragen, dass von vornherein innerhalb der Unter-

⁵⁹ Shoshana Zuboff, *Das Zeitalter des Überwachungskapitalismus* (Frankfurt am Main: Campus Verlag, 2018).

⁶⁰ Christoph Bieber, Leonhard Dobusch, und Jörg Müller-Lietzkow, „Die Internetintendanz“, *Medienkorrespondenz*, 28. April 2019, <https://www.medienkorrespondenz.de/leitartikel/artikel/die-internetintendanz.html>.



nehmen geeignete Compliance-Prozesse und Strukturen etabliert sind, um möglichen Schaden von den Bürger:innen abzuwenden.

Einige dieser Maßnahmen sind kurzfristig anzugehen, andere erfordern langfristige, strukturelle Reformen. Zum Beispiel sind Überlegungen zu einer separaten Aufsicht für soziale Netzwerke mit grundgesetzlichen Fragen verbunden, die kaum schnell und einfach zu klären sind. Bestimmte Bereiche bieten sich hingegen sofort für regulatorische und legislative Aktivitäten an. Die DSGVO konsequent anzuwenden wäre eine solche Sofortmaßnahme. Ebenfalls ist es sinnvoll, möglichst bald über klare Regeln für politische Onlinekommunikation nachzudenken. Auch wenn in Deutschland die Gefahr von Desinformation über politische Online-Werbung noch gering ist und nicht dramatisiert werden sollte, ist absehbar, dass politische Kommunikation sich noch stärker in den digitalen Raum verlagert.

Werden solche kurzfristigen und langfristigen Lösungsansätze zusammengedacht, entsteht eine holistische Policy-Agenda, die den Gefahren von Desinformation gerecht wird. Andernfalls wird das Problem der Desinformation weiter durch einen fragmentarischen regulatorischen Umgang verschlimmert.

Regulatorische Maßnahmen und Möglichkeiten zur Eindämmung von Desinformation



Ebene	Europäische Union				Deutschland (Bund)			Deutschland (Bundesländer)	
	Selbstreg.	Datenschutz	Inhalte	Inhalte	Inhalte	Inhalte	Wettbewerb	Inhalte	Medienaufsicht
Name und Abkürzung	Code of Practice und Aktionsplan	Datenschutz-Grundverordnung (DSGVO)	Richtlinie über audiovisuelle Mediendienste (AVMD-R)	E-Commerce-Richtlinie, evtl. zukünftig Digital Services Act (DSA)	Netzwerkdurchsetzungsgesetz (NetzDG)	Telemediengesetz (TMG)	Gesetz gegen Wettbewerbsbeschränkungen (GWB)	Jugendmedienschutz-Staatsvertrag (JMStV)	Rundfunkstaatsvertrag (RStV), evtl. zukünftig Medienstaatsvertrag
Expliziter Verweis auf Desinformation	Ja	Nein	Nein	Nein (aber via Haftung indirekt auf rechtswidrige Inhalte)	Nein (aber auf rechtswidrige Inhalte wie Volksverhetzung)	Nein (aber via Haftung indirekt auf rechtswidrige Inhalte)	Nein	Nein (aber auf jugendgefährdende Inhalte wie Gewaltverherrlichung)	Nein
Wirksam seit	2018	2018	2010	2000	2017	2007	1957	2002	1987
Status	Evaluation 2019/2020	Evaluation 2020	Zuletzt geändert 2018, muss bis 2020 in Mitgliedstaaten umgesetzt sein	Novellierung 2020	Novellierung 2019/2020 geplant	Zuletzt geändert 2019	Zuletzt geändert 2018, Novellierung geplant	Zuletzt geändert 2016	Zuletzt geändert 2018, Novellierung bis September 2020
EU-Bezug	Ja, EU-eigene Maßnahme	Ja, EU-eigene Maßnahme, in D v. a. im Bundesdatenschutzgesetz BDSG) umgesetzt	Ja, EU-eigene Maßnahme	Ja, EU-eigene Maßnahme	Nein	Ja, da teilweise Umsetzung E-Commerce-Richtlinie	Ja, da teilweise von Vertrag über die Arbeitsweise der Europäischen Union (AEUV) bestimmt	Umsetzung AVMD offen	Ja, da in geplanter Fassung teilweise Umsetzung AVMD-R
Ausgangspunkt	Europäische Kommission	Europäische Kommission	Europäische Kommission	Europäische Kommission	Bundesmin. d. Justiz und f. Verbraucherschutz	Bundesmin. für Wirtschaft und Energie	Bundesmin. für Wirtschaft und Energie	Staatskanzleien der Bundesländer	Staatskanzleien der Bundesländer
Kernpunkte mit Bedeutung für Desinformation	Code of Practice: Selbstverpflichtungen für Unternehmen zu Onlinewerbung, Zusammenarbeit mit Zivilgesellschaft, Forschung Aktionsplan: Mehr Ressourcen und Personal für strategische Kommunikation; Aufbau Frühwarnsystem	Eindämmung Datensammlung und Profilbildung und Rechte für Internutzende (Betroffenenrechte), u. a. Rechte auf Auskunft, Löschung, Berichtigung, Datenportabilität; Vorgaben für datenschutzfreundliche Voreinstellungen; Zweckbindung	Vorgaben für unabhängige nationale Medienaufsicht , in neuester Fassung mit Fokus auf Videoportale	Haftungsregeln bzw. -ausnahmen für Internetprovider bzgl. rechtswidriger Inhalte In DSA evtl. EU-weite Regeln für Inhalte-moderation, Reform Haftungsregeln für soziale Netzwerke und Suchmaschinen; Regeln für pol. Werbung; spezialisierte Aufsichtsbehörde	Basierend auf Strafrecht Vorgaben für soziale Netzwerke für Anzeige rechtswidriger Inhalte , die innerhalb best. Fristen gelöscht werden müssen; Benennung von Ansprechpersonen für Behörden; Berichtspflicht	Haftungsregeln bzw. -ausnahmen für Internetprovider bzgl. rechtswidriger Inhalte	Eindämmung Marktmacht , in letzter Änderung v. a. Anpassung für Digitalunternehmen durch Ausweitung Fusionskontrolle; Erweiterung des Faktorenkataloges für Marktmacht	Vorgaben für unzulässige bzw. entwicklungsbeneinträchtigende Inhalte ; Zuständigkeit für Einrichtungen der Freiwilligen Selbstkontrolle, z. B. Multimedia-Diensteanbieter (FSM)	Aufsicht über TV, Rundfunk, Telemedien In geplanter Fassung neue Definitionen und Regeln Algorithmentransparenz u. a. für Suchmaschinen, Videoportale, soziale Netzwerke

Literaturverzeichnis

Australian Competition and Consumer Commission. „Digital Platforms Inquiry - Final Report“. Canberra: Australian Competition and Consumer Commission, 26. Juli 2019. <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.

Avaaz. „Far Right Networks of Deceptions: Avaaz uncovers flood of disinformation, triggering shutdown of Facebook pages with over 500 million views ahead of EU elections“. New York, NY: Avaaz, 22. Mai 2019. <https://avaazimages.avaaz.org/Avaaz%20Report%20Network%20Deception%2020190522.pdf>.

Bergen, Mark. „YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant“. Bloomberg, 2. April 2019. <https://www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant>.

Bieber, Christoph, Leonhard Dobusch, und Jörg Müller-Lietzkow. „Die Internetintendanz“. Medienkorrespondenz, 28. April 2019. <https://www.medienkorrespondenz.de/leitartikel/artikel/die-internetintendanz.html>.

Börsch, Michael. „Facebook: Anordnungen des Bundeskartellamts möglicherweise rechtswidrig und deshalb einstweilen außer Vollzug“. Oberlandesgericht Düsseldorf, 26. August 2019. http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/index.php.

Bundeskartellamt. „B6-22/16: Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung“. Bonn: Bundeskartellamt, 7. Februar 2019. https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html;jsessionid=1758AF99E64A2D1B504758D23E7072EB.1_cid378?nn=3591568.

———. „Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen“. Bundeskartellamt, 7. Februar 2019. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2.

Bundeszentrale für politische Bildung. „Debatte Netzwerkdurchsetzungsgesetz (NetzDG)“. Bundeszentrale für politische Bildung, 16. März 2018. <https://www.bpb.de/dialog/netzdebatte/262660/debatte-netzwerkdurchsetzungsgesetz-netzdg>.

Bund-Länder-Kommission. „Bericht Bund-Länder-Kommission zur Medienkonvergenz“. Berlin: Bund-Länder-Kommission, Juni 2016. <https://www.bundesregierung.de/resource/blob/997532/473870/07ba875e860ad-a4556526641bd9151b6/2016-06-14-medienkonvergenz-bericht-blk-data.pdf?download=1>.

CDU, CSU, und SPD. „Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD. 19. Legislaturperiode“. Christlich Demokratische Union Deutschlands, 12. März 2018. https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1.

Competition and Markets Authority. „Online Platforms and Digital Advertising Market Study“. GOV.UK, 3. Juli 2019. <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study>.

Davis, Trevor, Steven Livingston, und Matt Hindman. „Suspicious Election Campaign Activity on Facebook: How a Large Network of Suspicious Accounts Promoted Alternative Für Deutschland in the 2019 EU Parliamentary Elections“. Washington, DC: The George Washington University, 22. Juli 2019. <https://smpa.gwu.edu/sites/g/files/zaxdzs2046/f/2019-07-22%20-%20Suspicious%20Election%20Campaign%20Activity%20White%20Paper%20-%20Print%20Version%20-%20IDDP.pdf>.

Desmaris, Sacha, Pierre Dubreuil, und Benoît Loutrel. „Creating a French framework to make social media platforms more accountable: Acting in France with a European vision“. Paris: French Secretary of State for Digital Affairs, Mai 2019. https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E1B36873E4&filename=Mission%20Re%CC%81gulation%20des%20re%CC%81seaux%20sociaux%20-ENG.pdf.

Department for Digital, Culture, Media & Sport, und Home Office. „Online Harms White Paper“. London: Controller of Her Majesty’s Stationery Office, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

Die Medienanstalten. „Stellungnahme der Medienanstalten zum überarbeiteten Diskussionsentwurf der Rundfunkkommission der Länder für einen ‚Medienstaatsvertrag‘“. Die Medienanstalten, 9. August 2019. https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Ueber_uns/Positionen/2019_08_09_Stellungnahme_der_Medienanstalten_zum_Medienstaatsvertrag.pdf.

Dobusch, Leonhard. „Die Organisation der Digitalität: Zwischen grenzenloser Offenheit und offener Exklusion“. netzpolitik.org, 1. Februar 2017. <https://netzpolitik.org/2017/die-organisation-der-digitalitaet-zwischen-grenzenloser-offenheit-und-offener-exklusion/>.

dpa. „Facebook wehrt sich gegen NetzDG-Bußgeld“. heise online, 19. Juli 2019. <https://www.heise.de/newsticker/meldung/Facebook-wehrt-sich-gegen-NetzDG-Bussgeld-4475699.html>.

Ellick, Adam B., Adam Westbrook, und Andrew Blackwell. „Operation Infektion: Russian Disinformation from Cold War to Kanye“. The New York Times, 12. November 2018. <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html>.

Europäische Kommission. „COM(2015) 192 final: Strategie für einen digitalen Binnenmarkt für Europa“. Europäische Kommission, 6. Mai 2015. <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52015DC0192&from=EN>.

Europäischer Datenschutzbeauftragter. „Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von ‚Big Data‘: Das Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz in der digitalen Wirtschaft“. Brüssel: Europäischer Datenschutzbeauftragter, März 2014. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_de.pdf.

European Commission. „A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation“. Brüssel: European Commission, 12. März 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271.

———. „Action Plan against Disinformation“. European Commission, 5. Dezember 2018. https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

———. „EU Code of Practice on Disinformation“. European Commission, 26. September 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

———. „JOIN(2019) 12 final: Report on the implementation of the Action Plan Against Disinformation“. Brüssel: European Commission, 14. Juni 2019. https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf.

Hartung, Helmut. „Das ist ziemlich einmalig‘: Interview mit Prof. Dr. Wolfgang Schulz, Direktor des Hans-Bredow-Instituts für Medienforschung“. Medienpolitik.net, 26. September 2018. <https://www.medienpolitik.net/2018/09/medienpolitikdas-ist-ziemlich-einmalig/>.

— — —. „Medienstaatsvertrag: Der Vielfalt verpflichtet“. Frankfurter Allgemeine Zeitung, 9. August 2019. <https://www.faz.net/aktuell/feuilleton/medien/medienstaatsvertrag-der-vielfalt-verpflichtet-16324354.html>.

Hoppenstedt, Max. „Strafbare Postings in sozialen Netzwerken: ‚Woher der Hass kommt, ist wirklich nur schwer zu begreifen‘“. SPIEGEL ONLINE, 21. Juni 2019, <https://www.spiegel.de/netzwelt/netzpolitik/netzdg-staatsanwalt-christoph-hebbecke-ueber-hass-in-sozialen-netzwerken-a-1273176.html>.

House of Commons Digital, Culture, Media and Sport Committee. „Disinformation and ‘fake news’: Final Report“. London: House of Commons, 14. Februar 2019. <https://publications.parliament.uk/pa/cm201719/cmselect/cm-cumeds/1791/1791.pdf>.

Jahromi, Neima. „The Fight for the Future of YouTube“. The New Yorker, 8. Juli 2019. <https://www.newyorker.com/tech/annals-of-technology/the-fight-for-the-future-of-youtube>.

Kaye, David. Speech Police: The Global Struggle to Govern the Internet. Bd. Columbia Global Reports. New York: Columbia University in the City of New York, 2019.

Kluth, Winfried, und Wolfgang Schulz. „Konvergenz und regulatorische Folgen: Gutachten im Auftrag der Rundfunkkommission der Länder“. Mainz: Rundfunkkommission der Länder, 2014. <https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/Konvergenz-Gutachten.pdf>.

Koch, Moritz, und Dietmar Neuerer. „Netzwerkdurchsetzungsgesetz: Die Bundesregierung erreicht im Kampf gegen Hate-Speech im Netz nur wenig“. Handelsblatt, 6. August 2019. <https://www.handelsblatt.com/politik/deutschland/netzwerkdurchsetzungsgesetz-die-bundesregierung-erreicht-im-kampf-gegen-hate-speech-im-netz-nur-wenig/24874984.html>.

Kommission Wettbewerbsrecht 4.0, „Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft“. Berlin: Bundesministerium für Wirtschaft und Energie, 9. September 2019. https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=4.

König, Jochen, und Juri Schnöller. „Wie digitale Plattformen sich um Transparenz bemühen“. Politik & Kommunikation, 9. Juli 2019. <https://www.politik-kommunikation.de/ressorts/artikel/wie-digitale-plattformen-sich-um-transparenz-bemuehen-1923588873>.

Leyen, Ursula von der. „A Union that strives for more: My agenda for Europe“. Brüssel: European Commission, 16. Juli 2019. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

Lupion, Bruno. „The EU Framework Against Disinformation: What Worked, What Changed and the Way Forward“. Berlin: Democracy Reporting International, 30. August 2019. <https://democracy-reporting.org/wp-content/uploads/2019/08/EU-Actions-Against-Disinformation-EP2019-Final.pdf>.

Melford, Clare. „Disinformation is an Online Harm“. Global Disinformation Index, 26. Juni 2019. <https://disinformationindex.org/2019/06/disinformation-is-an-online-harm/>.

Meyer-Resende, Michael, und Rafael Goldzweig. „Online Threats to Democratic Debate: A Framework for a Discussion on Challenges and Responses“. Berlin: Democracy Reporting International, 26. Juni 2019. https://democracy-reporting.org/wp-content/uploads/2019/06/BP_Threats-to-digital-democracy.pdf.

Mihr, Christian, und Daniel Moßbrucker. „Regulierung 2.0: Warum soziale Netzwerke, Suchmaschinen & Co. ein Teil der informationellen Grundversorgung geworden sind - und wie sie reguliert werden sollten, um die Meinungs- und Pressefreiheit zu schützen“. Berlin: Reporter ohne Grenzen, 12. Juni 2018. https://www.reporter-ohne-grenzen.de/uploads/tx_lfnews/media/Reporter-ohne-Grenzen_Regulierung-2.0-Langfassung.pdf.

Mozilla Corporation. „Facebook and Google: This Is What an Effective Ad Archive API Looks Like“. The Mozilla Blog, 27. März 2019. <https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like>.

Mueller, III, Robert S. „Report On The Investigation Into Russian Interference In The 2016 Presidential Election“. Washington, DC: U.S. Department of Justice, März 2019. <https://www.justice.gov/storage/report.pdf>.

Newman, Nic. „Reuters Institute Digital News Report 2019“. Oxford: Reuters Institute for the Study of Journalism, 12. Juni 2019. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-06/DNR_2019_FINAL_0.pdf.

Oberlandesgericht Düsseldorf. „Beschluss VI-Kart 1/19 (V) In der Kartellverwaltungsache 1. Facebook Inc., 2. Facebook Ireland Ltd., 3. Facebook Deutschland GmbH, Antragstellerinnen und Beschwerdeführerinnen, Verfahrensbevollmächtigte:... gegen Bundeskartellamt, Antragsgegner und Beschwerdegegner“. Düsseldorf: Oberlandesgericht Düsseldorf, 26. August 2019. http://www.olg-duesseldorf.nrw.de/behoerde/presse/Presse_aktuell/20190826_PM_Facebook/20190826-Beschluss-VI-Kart-1-19-_V_.pdf.

Palese, Michela, und Josiah Mortimer, Hrsg. Reining in the Political 'Wild West': Campaign Rules for the 21st Century. London: Electoral Reform Society, 2019. <https://www.electoral-reform.org.uk/latest-news-and-research/publications/reining-in-the-political-wild-west-campaign-rules-for-the-21st-century/>.

Paul, Katie. „Funders Threaten to Quit Facebook Project Studying Impact on Democracy“. Reuters, 28. August 2019. <https://www.reuters.com/article/us-facebook-election-research-idUSKCN1VI04F>.

pbe/dpa. „Gericht verpasst Kartellamt im Verfahren gegen Facebook einen Dämpfer“. SPIEGEL ONLINE, 26. August 2019. <https://www.spiegel.de/netz-welt/apps/bundeskartellamt-gegen-facebook-oberlandesgericht-duesseldorf-bremst-a-1283736.html>.

Podszun, Rupprecht. „Nach dem Facebook-Verfahren: Der Kartellrechts-Clash“. Legal Tribune Online, 13. September 2019. <https://www.lto.de/recht/hintergruende/h/facebook-verfahren-bkarta-ausbeutung-marktbeherrschung/>.

Rau, Jan Philipp, und Sebastian Stier. „Die Echokammer-Hypothese: Fragmentierung der Öffentlichkeit und politische Polarisierung durch digitale Medien?“ Zeitschrift für Vergleichende Politikwissenschaft, 29. August 2019, 1–19. <https://doi.org/10.1007/s12286-019-00429-1>.

Rotermund, Hermann. „Neuer Medienstaatsvertrag – alter Rundfunk“. CAR-TA online, 27. August 2018. <http://carta.info/neuer-medienstaatsvertrag-alter-rundfunk/>.

Rudl, Tomas, und Alexander Fanta. „Geleaktes Arbeitspapier: EU-Kommission erwägt neues Gesetz für Plattformen“. netzpolitik.org, 15. Juli 2019. <https://netzpolitik.org/2019/geleaktes-arbeitspapier-eu-kommission-erwaegt-neues-gesetz-fuer-plattformen/>.

Sängerlaub, Alexander. „Der blinde Fleck digitaler Öffentlichkeiten“. Berlin: Stiftung Neue Verantwortung, 21. März 2019. https://www.stiftung-nv.de/sites/default/files/blinde.fleck_.digitale.oeffentlichkeit.pdf.

Sängerlaub, Alexander, Miriam Meier, und Wolf-Dieter Rühl. „Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017“. Berlin: Stiftung Neue Verantwortung, 26. März 2018. https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf.

Schulz, Wolfgang, und Stephan Dreyer. „Stellungnahme zum Diskussionsentwurf eines Medienstaatsvertrags der Länder“. Hamburg: Hans-Bredow-Institut, 26. September 2018. https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/qiuektv_HBI_StellungnahmeMedienstaatsvertrag180926.pdf.

Scott, Ben. „Did Google and Facebook Break Democracy?“ Progressive Centre UK, 30. Juli 2019. https://www.progressivecentre.uk/did_google_and_facebook_break_democracy.

Shearlaw, Maeve. „Egypt five years on: was it ever a ‚social media revolution‘?“ The Guardian, 15. Januar 2016. <https://www.theguardian.com/world/2016/jan/25/egypt-5-years-on-was-it-ever-a-social-media-revolution>.

Staatskanzlei Rheinland-Pfalz. „Diskussionsentwurf für einen ‚Medienstaatsvertrag‘“. (2019). https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Mediapolitik/MStV-E_Synopse_2019-07_Online_.pdf.

Standing Committee on Access to Information, Privacy and Ethics. „International Grand Committee on Big Data, Privacy and Democracy“. Standing Committee on Access to Information, Privacy and Ethics, Juni 2019. <https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=10554743>.

The Economist. „Now playing, everywhere: The tricky task of policing YouTube“. The Economist, 4. Mai 2019. <https://www.economist.com/briefing/2019/05/04/the-tricky-task-of-policing-youtube>.

Tworek, Heidi, und Paddy Leerssen. „An Analysis of Germany’s NetzDG Law“. Amsterdam: Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 15. April 2019. https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

Wollebæk, Dag, Rune Karlsen, Kari Steen-Johnsen, und Bernard Enjolras. „Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior“. Social Media + Society, 9. April 2019. <https://doi.org/10.1177/2056305119829859>.

Zimmer, Anja, Hrsg. Smart Regulation for Digital Media Pluralism. Berlin: Medienanstalt Berlin-Brandenburg, 2019. https://mediapolicylab.de/files/content/document/Policy%20Statements/White_Book_MPL_July2019.pdf.

Zuboff, Shoshana. Das Zeitalter des Überwachungskapitalismus. Frankfurt am Main: Campus Verlag, 2018.



Dr. Julian Jaursch

Oktober 2019

Regulatorische Reaktionen auf Desinformation

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expert:innen Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über den Autor

Julian Jaursch ist Leiter des Projekts „Stärkung digitaler Öffentlichkeit | Policy“. Er analysiert und evaluiert bestehende Ansätze, wie die digitale Öffentlichkeit gestärkt werden kann, und identifiziert mögliche regulatorische Maßnahmen zu deren Schutz. Ziel des Projekts ist es, konkrete Handlungsempfehlungen für politische und gesellschaftliche Entscheidungsträger:innen zu entwickeln.

So erreichen Sie den Autor

Dr. Julian Jaursch

Projektleiter Stärkung digitaler Öffentlichkeit | Policy

jjjaursch@stiftung-nv.de

+49 (0)30 81 45 03 78 93

[@jjjaursch](#)



Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80

F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de

info@stiftung-nv.de

Design:

Make Studio

www.make-studio.net

Layout:

Johanna Famulok

Grafik:

Anne-Sophie Stelke

www.annesophiestelke.com



Dieser Beitrag unterliegt einer CreativeCommons-Lizenz (CC BY-SA). Die Vervielfältigung, Verbreitung und Veröffentlichung, Veränderung oder Übersetzung von Inhalten der Stiftung Neue Verantwortung, die mit der Lizenz „CC BY-SA“ gekennzeichnet sind, sowie die Erstellung daraus abgeleiteter Produkte sind unter den Bedingungen „Namensnennung“ und „Weiterverwendung unter gleicher Lizenz“ gestattet. Ausführliche Informationen zu den Lizenzbedingungen finden Sie hier:

<http://creativecommons.org/licenses/by-sa/4.0>