



#btw21 im Netz

Wie wir unsere Demokratie zukünftig vor digitalen
Bedrohungen schützen können

Interviews mit Anna-Lena von Hodenberg (HateAid), Chloe Colliver
& Helena Schwertheim (ISD), Julian Jaurisch (Stiftung Neue Verantwortung), uvm.

Herausgeberschaft

Reset.



Ben Scott
Executive Director bei Reset

#btw21 im Netz: Wie wir unsere Demokratie zukünftig vor digitalen Bedrohungen schützen können

„Der Zustand einer Demokratie bemisst sich am Herzschlag ihrer politischen Öffentlichkeit“, sagte einst der Philosoph und Soziologe Jürgen Habermas. Doch wie klingt der Herzschlag einer Demokratie, deren Diskurse durch Hass und Desinformation vergiftet sind? Die Bundestagswahl 2021 markierte in der bundesdeutschen Geschichte mitten in der Pandemie eine Zäsur: Noch nie war ein Wahlkampf in Deutschland so digital. Das Netz ist längst für die Hälfte der Wählenden die wichtigste Informationsquelle, doch beteiligt sich nur ein Bruchteil von Ihnen auch an politischen Diskussionen. Gerade die persönlichen Erfahrungen mit Hass und Desinformationen, vor allem bei den unter 34-jährigen, zeigt, warum das so ist. Somit wird in der digitalen Öffentlichkeit ein extrem verzerrtes Bild der Realität vermittelt. Verzerrt durch das Vorherrschen von extremen Ansichten und Unsinn, von dem Social-Media-Konzerne gelernt haben, dass sie damit die Aufmerksamkeit, die sie für den Verkauf von Werbung benötigen, besser erregen können. Wie ein altes Sprichwort besagt: „Eine Lüge kann um die halbe Welt reisen, während die Wahrheit ihre Schuhe anzieht“. Und das gilt für viele Themen von der öffentlichen Gesundheit in der Pandemie bis zum Klima.

In diesem Report haben wir zahlreiche Expert:innen um ihre Einschätzung gebeten, wie sicher das Netz als demokratischer Raum für politische Debatten war. Ob es um den Einsatz von politischer Werbung in sozialen Netzwerken oder die Verbreitung von Desinformationen zu Parteien und Kandidat:innen geht, zeigen die Einschätzungen der Expert:innen ein geeintes Bild: Ein in weiten Teilen funktionierendes demokratisches System, mit vertrauenswürdigen klassischen Medien oder politischen Kampagnen, die von gegenseitigem Respekt geprägt waren. Und große Desiderate in der Regulierung, Verantwortungsübernahme und Rechtsdurchsetzung gerade bei den sozialen Netzwerken.

Die Demokratie muss tun, was sie schon immer getan hat, wenn die Interessen des Marktes Amok laufen und das Gemeinwohl gefährdet ist: öffentliches Recht zum Schutz der Menschen erlassen. In Europa besteht nun mit dem Digital Services Act (DSA) sowie dem Digital Markets Act (DMA) die einmalige Chance, den Herzschlag auch unserer politischen Öffentlichkeit zu schützen und die bisher fehlenden Regulierungslücken mit Bedacht und Weisheit zu schließen. Aus den vielen Erfahrungen, empirischen Befunden und Einschätzungen einer Vielzahl von NGOs, Wissenschaftler:innen, Journalist:innen und Expert:innen haben wir zusammen mit dem Leibniz-Institut für Medienforschung | Hans-Bredow-Institut ein Policy-Book entwickelt, das diesen politischen Gestaltungsprozess mit Anregungen und Ideen füttert, auch für die kommende Bundesregierung.

Inhalt

Kapitel I

Die #btw21 und das Netz aus
Sicht der Expert:innen 4

Hass im Netz:
Anna-Lena von Hodenberg (HateAid) 5

Desinformation:
Chloe Colliver & Helena Schwertheim
(*Institute for Strategic Dialogue*) 7
Karolin Schwarz (*Expertin für Desinformation
und Rechtsextremismus im Netz*) 9

Politische Aufsicht:
Marie-Therese Sekwenz (*Sustainable
Computing Lab*) & Julian Jaurisch
(*Stiftung Neue Verantwortung*) 11
Matthias C. Kettemann & Vincent Hofmann
(*Leibniz-Institut für Medienforschung |
Hans-Bredow-Institut*) 14

Rolle der Parteien im Wahlkampf:
Isabelle Borucki (*Freie Universität Berlin*)
& Ulrike Klinger (*Universität Siegen*) 17

Ausländische Beeinflussung:
Anneli Ahonen (*Institut for Strategic Dialogue*) 19

Blick der Gesellschaft auf die Plattformen:
Alexander Sänglerlaub (*futur eins*) 21

Politische Werbung:
Laura Edelson (*New York University*)
& Sam Jeffers (*Who Targets Me*) 24
Christian Bock (*SumOfUs*) 26

Kapitel II

Rechtliche Einführung 28

Der Rechtsrahmen der Plattformen 29

Europäischer Rechtsrahmen 31

Kapitel III

Für ein besseres Internet morgen –
Handlungsoptionen für heute 33

I. Einsatz für eine ambitionierte Ausgestaltung
des Digital Service Act der EU 34

II. Einsatz für ambitionierte Rechtsvorschriften
der EU zu Transparenz in der politischen Werbung 37

III. Verbesserung des Wettbewerbs auf EU-Ebene
und in Deutschland 39

VI. Einführung eines digitalen
Gewaltschutzgesetzes 41

V. Ausweitung der Kapazitäten von Behörden
und Parteien 43

VI. Weiterentwicklung des
Medienkonzentrationsrechts 45

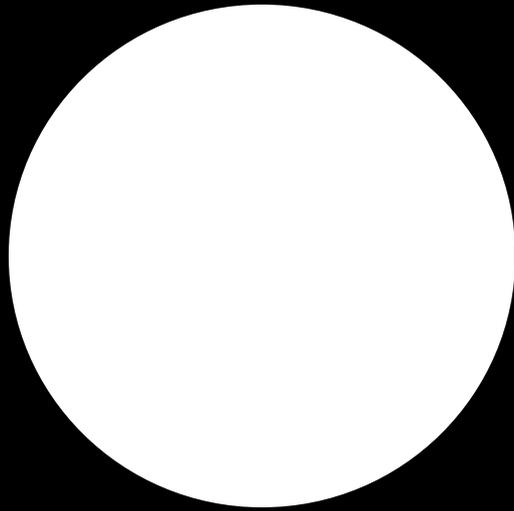
VII. Ausweitung des Bildungsangebots
im Digitalbereich 47

VIII. Verschärfung des Jugendmedienschutzes 49

IX. Fortentwicklung des Datenschutzes 51

X. Mehr Transparenz und Kontrolle
von Algorithmen 53

Impressum 55



I

Die #btw21 und das
Netz aus Sicht der
Expert:innen

Ganz klar, die Plattformen müssen das NetzDG durchsetzen

Foto: Andrea Heinsohn



Annalena von Hodenberg
Geschäftsführerin von HateAid

Anna-Lena von Hodenberg, seit wann gibt es die weltweit ziemlich einzigartige Beratungsstelle für Betroffene digitaler Gewalt?

HateAid wurde 2018 von Fearless Democracy, Campact, einem Volljuristen und mir gegründet, weil Betroffene allein gelassen wurden und kaum Strafverfolgung stattfand. Mittlerweile hat die gemeinnützige Organisation ca. 40 Mitarbeiter:innen, darunter Jurist:innen und Sozialpädagog:innen. Wir beraten Betroffene, unterstützen sie bei der Durchsetzung ihrer Rechte, indem wir Zivilprozesse finanzieren, und vertreten deren Interessen auf nationaler und internationaler Ebene. Wir finanzieren uns durch Spenden und die Entschädigungszahlungen aus den Prozessen, die wir gewinnen.

Was haben Sie im Vorfeld der Bundestagswahl 2021 beobachtet?

Wir haben gemeinsam mit Reset eine Datenanalyse auf Facebook gemacht. Da haben wir potentiell illegale oder rechtswidrige Inhalte auf Facebook gesucht. Es waren so Kommentare wie, eine Politikerin sei ein „Fickfehler, die hätte man besser über die Mauer gespritzt“, „Ich kotz auf dich du grüne fotze“ oder „Weg mit der alten Schlampe“. Die haben wir auf Basis der Community-Standards oder des Netzwerkdurchsetzungsgesetzes gemeldet und dann verfolgt, ob Facebook sie löscht und auf welcher Grundlage.

Die Community-Standards sind deren recht weit gefasste Allgemeine Geschäftsbedingungen mit relativ viel Interpretationsspielraum. Daher hat Deutschland als erstes Land in Europa ein Gesetz eingeführt, das den

Umgang dieser Plattformen mit illegalen Inhalten reguliert – das Netzwerkdurchsetzungsgesetz (NetzDG). Es bestimmt anhand eines Straftatenkatalogs, dass potentiell illegale Inhalte gelöscht werden müssen, und zwar innerhalb von 24 Stunden. Oder innerhalb von sieben Tagen, wenn die rechtliche Bewertung anspruchsvoller ist. Wir haben daher untersucht, ob das NetzDG von Facebook eingehalten wird.

Was war das Ergebnis?

In den meisten Fällen wurde nicht nach deutschem Recht, also dem NetzDG, sondern nach internen Regeln gelöscht. Und in etwa der Hälfte der Fälle auch nicht nach den Community-Standards von Facebook. Obwohl unsere Juristin von HateAid all die Inhalte als potentiell rechtswidrig eingestuft hat.

Das haben wir auch dem Bundesamt für Justiz mitgeteilt, das die Einhaltung des NetzDG überwacht und prüft, ob es sich um einmalige oder strukturelle Verstöße handelt. All das haben wir publik gemacht. Die Süddeutsche Zeitung hat darüber berichtet. Und wir haben es weiter gestreut an die Staatsanwaltschaften, Professor:innen und Regierungskreise in Deutschland und Europa, mit denen wir in Kontakt stehen.

Erschien aus der Perspektive von HateAid die digitale Gewalt im Vorfeld der Bundestagswahl anders als zuvor?

Ob es mehr Hasskommentare während dieser Bundestagswahl gab als bei der letzten, können wir von HateAid nicht sagen, weil es dazu keine Studien gibt, die das qualitativ und wissenschaftlich fundiert nachweisen. Dazu müsste man Langzeitmessungen machen und es

>

war das erste Mal, dass man so genau beobachtet hat, wie digitale Gewalt in diesem Kontext nach NetzDG von Facebook gelöscht wird.

Das wurde vorher noch nie in dieser Weise und unter diesen Bedingungen angeschaut. Die Leaks des Wall Street Journals haben gezeigt, dass bei Facebook einige Nutzer:innen als VIPs, bzw. Personen des öffentlichen Lebens eingestuft werden, auf die die Community-Standards nicht angewendet werden.

Das haben wir auch bei den Hasskommentare in Bezug auf Politiker:innen gesehen, die so gut wie nie gelöscht wurden. Man nennt das White-listing. Dazu können Donald Trump gehören, Angela Merkel oder Annalena Baerbock. **Es ist naheliegend, anzunehmen, dass es während der Bundestagswahl 2021 sehr viel mehr auch digitalen Hass gegen Politikerinnen und Politiker, Journalisten und Journalistinnen gab als je zuvor.**

Wie wurden die Daten für die HateAid-Analyse erhoben?

Meiner Oma würde ich die künstliche Intelligenz, mit der das geschieht, als Sieb beschreiben. Man schmeißt einen Haufen Kommentare in ein Sieb mit unterschiedlich großen Löchern und die besonders fetten und potenziell illegalen Hasskommentare bleiben eben hängen. Die haben unsere Juristinnen dann alle einzeln analysiert und sie wurden bei Facebook gemeldet und die Löschung regelmäßig nachverfolgt. **Aber jeder sechste von uns beanstandete Post blieb stehen.**

HateAid beanstandet aber auch das Melde-Prozedere als zu kompliziert und irreführend.

Im Prinzip haben die Menschen ein gutes Gefühl dafür, welche Inhalte mit dem Recht auf freie Meinungsäußerung konform gehen und welche nicht. Auch ohne ein Studium des StGB ist klar, dass Androhungen von Tod und Vergewaltigung gemeldet werden können und die „blöde Kuh“ vielleicht eher nicht. Aber man muss sich bei der Verletzung des Persönlichkeitsrechts, vor allem bei Beleidigungen immer den Kontext genauer anschauen. Wir haben

beobachtet, dass „Weg mit der alten Schlampe“ gelöscht wurde, aber „Weg mit dem Arschloch“ nicht. Das ist nicht nachvollziehbar.

Was hat Sie an den Ergebnissen der Analyse überrascht?

Es hat uns überrascht, wie wenig Facebook ein großes dem Netzwerk durchsetzungsgesetz Folge leistet und wir sind gespannt, wie das Bundesamt für Justiz darauf reagiert. Denn wenn man ein Gesetz hat – das wir begrüßen – und wenn man dieses Gesetz aber nicht anwendet, dann muss man sagen: Es ist gescheitert.

Was sind oder wären dann Ihre Forderungen?

Ganz klar, die Plattformen müssen das NetzDG durchsetzen. Es ist deutsches Recht und daran sind sie gebunden. Wenn sie das nicht tun, muss die Bundesregierung dafür sorgen, dass das passiert und wenn das nicht reicht, müssen sie es ändern. Von Facebook fordern wir, dass sich die Plattform auch an ihre eigenen Community-Standards hält. **Wenn Hasskommentare stehen gelassen werden, normalisiert sich Gewalt. Opfern wird demonstriert: Du musst das aushalten, und Tätern: Weiter so!**

Das NetzDG und HateAid sind in Deutschland einzigartig. Was empfehlen Sie aus Ihrer Erfahrung anderen Ländern in der EU oder sogar weltweit?

Wir empfehlen allen, die öffentlichen Räume im Netz zu beobachten und sicherer zu machen. Die Betreiber der Plattformen haben ein intrinsisches Interesse, Hass, Gewalt und Desinformation stehen zu lassen. Denn sie verdienen daran. Weil Erregung die Menschen anzieht. Sie kommen und bleiben auf den betreffenden Seiten.

Es gibt da ein hohes Verkehrsaufkommen. Und deswegen inserieren hier die Werbekunden. So wird mit Gewalt Gewinn gemacht. Das kann und muss man als Gesellschaft regulieren, indem man Regeln aufstellt, die man aber auch durchsetzen muss. Es wäre wichtig, dass das auch in anderen Ländern

transparent, zum Thema gemacht und verfolgt wird und wir alle müssen den Blick nach Brüssel richten, denn da werden solche grundlegenden Gesetze momentan verhandelt und entschieden.

Diese Hoffnung verbinden Sie mit dem Digital Services Act?

Aber auch die Befürchtung, dass der DSA verwässert wird und damit unsere recht progressive nationale Gesetzgebung ausgehebelt wird. Momentan gibt es starke Kräfte, die beispielsweise die Meldefristen ablehnen. Dadurch gäbe es kaum noch Druckmittel, auf die man bei der Durchsetzung der Gesetze rekurrieren könnte. Wir finden es befremdlich, welchen schlechten Ruf das NetzDG in Brüssel hat. Betroffenen aus Frankreich, Belgien und anderen Ländern geht es noch viel schlechter als uns. Sie haben gar keine Handhabe. Und die Gefahr des Overblocking, die man ernst nehmen muss, hat sich bisher nicht bewahrheitet.

Es gab ja große Befürchtungen und Kritik diesbezüglich. Aber wir sehen alle, es ist eher umgekehrt: Es wird viel zu wenig gelöscht, was eigentlich illegal ist. Und wir wollen die sozialen Medien doch zu einem gerechteren und besseren Ort machen, an dem wir uns alle viel auseinandersetzen und streiten können – aber eben ohne, dass Menschen Angst haben müssen, Gewalt zu erfahren.

HateAid ist die erste Beratungsstelle Deutschlands gegen Hass im Netz. Die 2018 gegründete Organisation wurde von den NGOs Campact und Fearless Democracy ins Leben gerufen. www.hateaid.org

Transparenz in die Systeme der Unternehmen bringen

Foto: Privat



Helena Schwertheim
Institute for Strategic Dialogue

Was konnten Ihr während der Bundestagswahl hinsichtlich Desinformation und Verschwörungstheorien beobachten?

Helena Schwertheim: Wir hatten ein Team von Analyst:innen, das täglich die einschlägigen Social-Media-Kanäle beobachtet hat. Als Haupttrend konnten wir vor allem viel mehr Desinformationen bei rechtsextremen und verschwörungstheoretischen Gruppierungen beobachten. In diesen Gruppen wurden insbesondere verschiedene Narrative hinsichtlich eines etwaigen Wahlbetrugs im Vorfeld der Wahlen diskutiert. Eines der zentralen Narrative, welches auch von offiziellen AfD-Kanälen und Querdenker-Gruppen verbreitet wurde, bezog sich wie schon bei den US-Wahlen auf möglichen Briefwahl-Betrug.

Ein weiteres Narrativ, das von den gleichen Gruppierungen verbreitet wurde, war die angebliche Diskriminierung nicht geimpfter Personen. Ein weiteres Narrativ richtete sich gegen Einwanderung. So konnten wir beobachten, dass die AfD viele Inhalte erstellte, die afghanische Einwanderer:innen im Allgemeinen in ein sehr negatives Licht rücken. Es gab Manipulationen von Daten der Einwanderungsstatistik, um diese Menschen als Vergewaltiger und Kriminelle darzustellen und sich gleichzeitig als Beschützer zu präsentieren.

Gab es überraschende Beobachtungen?

Chloe Colliver: Die Ergebnisse sind vor dem Hintergrund unserer Beobachtungen anderer Wahlen relativ vorhersehbar gewesen. Die von uns identifizierten Desinformationen haben in diesem Jahr leicht zugenommen. Dies liegt vor allem daran, dass die Eintrittsschwelle für Personen, die an der Verbreitung von Desinformationen beteiligt sind, niedriger geworden ist. Das Ausmaß der Bedrohungen und ihr Potential, auch offline Schaden anzurichten, scheint sich während der Pandemie

verschärft zu haben. Im Allgemeinen gibt es in Deutschland aber keine derart dramatische Verbreitung von Verschwörungstheorien, wie wir es bei beispielsweise bei den US-Präsidentenwahlen 2020 gesehen haben.

Was sind die Erklärungen dafür, dass wir in Deutschland eine andere Situation haben?

Chloe Colliver: Das hat verschiedene Gründe. Die stark polarisierten Medien in den USA, einschließlich der Rundfunkmedien, schaffen ein Ökosystem, in dem es keine gemeinsame Realität mehr zwischen links und rechts gibt. Wohingegen wir in Deutschland zu einem gewissen Grade eine Zentralisierung sowohl der Medien als auch des politischen Parteienspektrums beobachten. Ich denke, es sind kontextuelle Faktoren, die dazu führen, dass die Gesellschaft in den USA anfälliger für eine Verbreitung von Extremismus und Desinformation ist, als die deutsche.

Helena Schwertheim: In den USA gab es einen Präsidenten, der diese betrügerischen Narrative propagierte. In Deutschland haben wir zwar Politiker:innen der AfD. Diese lagen in den Umfragen allerdings bei nur etwa 10 Prozent. Ein weiterer Grund könnte sein, dass es auf gesellschaftlicher und politischer Ebene mehr Widerstand gegen diese Art von Manipulationen gibt. Und natürlich spielt in diesem Zusammenhang auch das Wahlsystem in Deutschland eine Rolle, das eben kein Mehrheitswahlsystem ist.

Es gab dennoch Medienberichte über Desinformation und Hass, die sich insbesondere gegen die Grünen und ihre Spitzenkandidatin richteten. Diesbezüglich gab eine Studie von ISD Germany. Könnten Ihr diese Studie kurz vorstellen und erläutern, was Ihr beobachtet habt?

Foto: Privat



Chloe Colliver
Institute for Strategic Dialogue

>

Helena Schwertheim: Wir haben eine Studie durchgeführt, in der wir Daten der 100 meist-geteilten Facebook-Posts bzw. meistgelesenen Telegram-Posts über die Spitzenkandidat:innen, Annalena Baerbock, Armin Laschet und Olaf Scholz für den Zeitraum von Februar bis Juli 2021 verwendet haben, um den Hass und die Desinformation gegen sie zu untersuchen.

Dabei fanden wir heraus, dass alle drei Kandidat:innen zum Ziel digitaler Angriffe wurden. Annalena Baerbock wurde im Vergleich zu den anderen Kandidaten jedoch deutlich häufiger zum Ziel der Angriffe mit Verschwörungsmäthen. In derartigen Kommentaren wurde auch immer wieder auf ihr Geschlecht verwiesen und ihre persönliche Integrität angegründert.

Hatten die digitale Gewalt und die Verschwörungstheorien gegen die Kandidat:innen Auswirkungen auf die Entwicklung der Umfragewerte der jeweiligen Partei?

Chloe Colliver: Das ist ohne weitere Forschungsinformationen sehr schwer zu beurteilen. Desinformation und Belästigung gegen Annalena Baerbock haben eine gewisse Schwelle der Aufmerksamkeit erreicht, die die Meinung eines breiten Publikums im Vorfeld der Wahl beeinflusst haben könnte. Die effektivsten Formen der Desinformation sind oft diejenigen, die Elemente der Wahrheit enthalten.

Und genau das war bei den Angriffen gegen Politiker:innen in den letzten Monaten der Fall. Die Sorge, die ich angesichts der Anfeindungen gegen Politiker:innen habe, ist aber nicht so sehr, dass sie den Wahlausgang beeinflussen. Vielmehr befürchte ich, dass durch die Anfeindungen bestimmte Kandidat:innen davon abgehalten werden, sich überhaupt zu äußern, öffentlich aufzutreten oder sich als Kandidat:in aufstellen zu lassen.

Wie bewertet Ihr den Zusammenhang zwischen Desinformation und Verschwörung auf der einen Seite und Belästigung und digitaler Gewalt auf der anderen Seite?

Chloe Colliver: Diese beiden Dinge können sehr unterschiedlich sein. Verschwörungstheorien und Desinformation

gab es schon immer, vor allem innerhalb extremistischer Gruppierungen. Politiker:innen, Journalist:innen und Menschen in einflussreichen Positionen sind schon lange Ziel von Verschwörungstheorien. Dagegen ist die Tatsache, dass Belästigungen und Desinformationen als Waffe eingesetzt werden, ein neueres Phänomen: **Kandidat:innen und Politiker:innen, insbesondere Frauen, werden mittlerweile sehr viel häufiger mittels Diffamierungs- und Verleumdungskampagnen angegriffen.** Sie sind durch öffentliche Social-Media-Plattformen viel zugänglicher als früher.

Die Europäische Kommission hat einen Entwurf für den Digital Service Act (DSA) vorgelegt, der im nächsten Jahr verabschiedet werden soll. Was ist Eure Meinung bezüglich des DSA?

Chloe Colliver: Der DSA bietet einen umfassenden Rahmen für die Verbesserung des Schutzes der Nutzer:innen in vielerlei Hinsicht. Besonders hervorheben möchte ich in diesem Zusammenhang die Möglichkeit, Transparenz in die Systeme der Unternehmen zu bringen und Systeme zur Risikominderung einzusetzen. Der DSA befasst sich also nicht nur mit der Entfernung von Inhalten, sondern auch mit der Frage, inwiefern algorithmische Systeme Schäden oder Sicherheitsprobleme auf Plattformen verstärken können. Dazu gehört auch eine Verpflichtung, Inhalte von den Plattformen zu entfernen, die nach den jeweiligen nationalen Rechtsordnungen illegal sind.

Was den Datenzugang für Forscher:innen im Rahmen des DSA betrifft, wollen wir sicherstellen, dass nicht nur akademische Einrichtungen, sondern auch zivilgesellschaftliche Gruppen, Forscher:innen und Journalist:innen in gewissem Maße mit einbezogen werden. Damit würde es mehr öffentliche Rechenschaftspflicht für diese Plattformen außerhalb der direkten Regulierung geben. Über eine Programmierschnittstelle zugängliche Daten sollten dabei auch öffentlich zugängliche Kommentare und nicht nur ursprüngliche Beiträge enthalten. Sinnvoll wäre es zudem, Plattformen dazu zu bringen, aggregierte Informationen darüber zu veröffentlichen, wie Nutzer:innen zu einem Inhalt im Internet gelangen, zum Beispiel über Empfehlungssysteme

oder eine direkte Suche. Damit könnten wir auch besser verstehen, wie Plattformen Nutzer:innen zu verschiedenen Informationen leiten.

Welches sind Eure Kernpunkte für die nächste deutsche Regierungskoalition?

Helena Schwertheim: Die wichtigste Aufgabe wird es sein, einen Datentreuhänder zu haben, der zwischen den Plattformen sowie Forscher:innen, Akademiker:innen und der Zivilgesellschaft im öffentlichen Interesse vermittelt. In der Vergangenheit gab es bereits Organisationen mit einem solchen Auftrag, dort mangelte es jedoch an Befugnissen und richtiger Umsetzung.

Es besteht daher die Notwendigkeit, einen Datentreuhänder zu benennen und mit den richtigen Kompetenzen auszustatten. Eine weitere Empfehlung ist es, in Zukunft mehr Sorgfaltspflichtverfahren gegen Desinformation, insbesondere geschlechtsspezifische Desinformation einzuführen.

Welche Plattformen waren Eurer Meinung nach im Zusammenhang mit der Bundestagswahl von besonderer Bedeutung?

Helena Schwertheim: Wir konnten beobachten, dass auf Plattformen, die unter das NetzDG fallen, wie zum Beispiel Facebook, Twitter und Instagram, weniger „extreme“ Inhalte zu finden waren. Stattdessen haben sich diese Plattformen zu Rekrutierungsplattformen für ein Publikum entwickelt, das anschließend dann auf andere Plattformen wie Telegram oder Videoplattformen wie Youtube abwanderte.

Derartige Plattformen, genauso wie kleinere Nischenplattformen, sind vergleichsweise schwieriger zu überwachen. Man kann das Phänomen mit einem Ballon-Effekt beschreiben. Dreht man den Ballon in eine Richtung, entweicht die Luft einfach woanders hin. Deshalb brauchen wir eine ganzheitliche Herangehensweise an Desinformation und Hassrede. **Telegram hat sich insbesondere im Zuge der Corona-Pandemie zu einer Brutstätte für extremistische Inhalte entwickelt.**

Noch immer reagieren Politik und Institutionen zu langsam



Foto: Andi Weiland

Karolin Schwarz
Journalistin und Expertin für
Desinformation und
Rechtsextremismus im Netz

Wie stellte sich das Phänomen Desinformation im diesjährigen Bundestagswahlkampf dar? Wer verbreitete besonders viele Desinformation über wen und über welche Kanäle?

Falschmeldungen im Bundestagswahlkampf betrafen sowohl den Ablauf der Wahl selbst als auch die Kandidat:innen. Bereits im Spätherbst 2020 – fast ein Jahr vor der Bundestagswahl – wurden erste Beiträge aus den Reihen der AfD und von „Ein Prozent“, lanciert, die das Vertrauen in die Briefwahl angreifen sollten. Auffällig waren auch Falschmeldungen über Annalena Baerbock, bereits kurz nach Bekanntgabe ihrer Kandidatur. Der Bundestagswahlkampf hat aber auch gezeigt, dass nicht nur die Kanzlerkandidat:innen das Ziel von Desinformation sind, sondern auch prominente Köpfe der Parteien, wie Markus Söder.

Wenig überraschend spielte Telegram eine wichtige Rolle als Ausgangspunkt für Falschmeldungen, die dann auf andere Plattformen getragen wurden. Facebook, Twitter und andere Massenplattformen sind nach wie vor wichtige Werkzeuge, nicht immer aber Ursprung von Falschmeldungen. Sie werden vor allem genutzt, um die breite Masse zu erreichen. Auch über den Audio- und Video-Weg wurden Falschmeldungen verbreitet. Beispielsweise über Podcasts (Ein Prozent) oder Sprachnachrichten auf Telegram, Videos auf YouTube (Die Basis zur Landtagswahl in Sachsen-Anhalt) oder auf alternativen Videoplattformen wie Bitchute und Wirtube.

Gab es Unterschiede zur Wahl 2017? Lässt sich sagen, ob es mehr oder weniger Desinformationen gab?

Viele Falschmeldungen, die 2017 populär waren, gab es in abgewandelter Form auch 2021: Meldungen über radierbare Stifte in den Wahlkabinen, abgeschnittene Ecken an Wahlzetteln, angeblich politisch motivierte Wahlhel-fende. Ein paar Unterschiede gab es durchaus: Falschmeldungen zur Wahl wurden mit Verschwörungsmmythen und Falschbehauptungen über COVID-19 verknüpft, der Angriff auf die Briefwahl begann schon fast ein Jahr vor der Bundestagswahl und mit einem Beitrag auf BILD TV wurden mehrere Verschwörungsmmythen und falsche Behauptungen auch einem breiteren Publikum zugänglich gemacht. Ob es mehr Falschmeldungen gab, lässt sich nicht seriös quantifizieren, allein schon wegen der Masse der Plattformen nicht.

Welche Rolle spielen die Social-Media-Plattformen? Hast Du den Eindruck, dass sie mit ganzer Kraft gegen Desinformation vorgehen?

Insgesamt kann man sagen: In den vergangenen Jahren hat man sich einige Gedanken über Falschmeldungen im Vorfeld von Wahlen gemacht. Grundsätzlich hätte es aber mehr Informationen zum Ablauf der Wahlen (Wann steht der Gewinner fest, etc.) geben können, sowie Informationen über einige immer wiederkehrende Falschmeldungen (fehlende Siegel, abgeschnittene Ecken, Stifte). Auch Informationen in einfacher Sprache wären wichtig.

Aus den Erkenntnissen von 2017 wissen wir, dass Desinformationen erst große Reichweiten erlangen, wenn auch klassische Medien versagen. Welche Rolle spielten 2021 klassische Medien bei der Verbreitung von Desinformation?

Die Bild, in Gestalt von BILD TV und Claus Strunz, Julian Reichelt und Hans-Ulrich Jörges, haben unbelegte Behauptungen und Verschwörungsmethoden über die Briefwahl Raum gegeben. Zudem: Insgesamt dauerte es bis zum Erscheinen von Faktenchecks im Vorfeld der Bundestagswahl wiederum teilweise recht lange.

Welche Akteure sind besonders aktiv bei der Verbreitung?

Auch 2017 waren heimische Akteur:innen schon ein wichtiger Einfluss. Nicht zuletzt hat sich das an den wiederkehrenden „Wahlbeobachter“-Kampagnen von Ein Prozent oder Gruppierungen wie Reconquista Germanica gezeigt. Auch Falschmeldungen über Geflüchtete und Migrant:innen haben 2017 eine wichtige Rolle im Wahlkampf gespielt. Auch 2021 war das der Fall. Auf Telegram interagieren Rechtsextreme inzwischen tagtäglich mit COVID-Leugner:innen und -Verharmloser:innen und Verschwörungsideolog:innen. Falschbehauptungen über abgeschnittene Ecken an Wahlzetteln lassen sich teilweise ursprünglich dem Reichsbürger- und Souveränistenmilieu zuordnen. Beeinflussung ausländischer Akteur:innen spielte auch 2021 eine Rolle. Dabei sollte nicht nur russische Einflussnahme, sondern auch medienaktivistische Projekte wie die Epoch Times sowie rechtsradikale Meinungsmedien aus Österreich betrachtet werden.

Hat sich beim Kampf gegen Desinformation etwas signifikant zur letzten Bundestagswahl verändert?

Erfreulicherweise ist das Büro des Bundeswahlleiters auch in diesem Jahr proaktiv auf Twitter unterwegs gewesen und hat dort Falschmeldungen widerlegt. Ansonsten ließ sich auch 2021 wieder eine Mischung aus Hilflosigkeit und Ignoranz beobachten. Noch immer reagieren Politik und Institutionen – mit einigen wenigen erfreulichen

Ausnahmen – sehr langsam auf Falschmeldungen. Das Fact-Checking von Correctiv am Wahltag und in den Tagen zuvor war sichtbar und schnell. In den Wochen davor haben viele Faktencheck-Projekte teilweise allerdings sehr lange gebraucht, um wirkmächtige Mythen (z. B. Falschmeldungen über die Wahl in Sachsen-Anhalt) zu widerlegen – auch das kann allerdings an einer mangelnden Sensibilisierung von Institutionen liegen, die für Faktenchecks häufig befragt werden müssen. In verschiedenen Gesprächen mit Politiker:innen vor der Wahl war eine hinreichende Sensibilisierung für das Problemfeld eher die Ausnahme denn die Regel.

Was müsste in Deutschland passieren, damit wir das Phänomen besser in den Griff bekommen?

Das alles zeigt letztendlich: Es braucht langfristige Strategien, die auch über den Tag der Wahl hinausgehen und Angriffe auf demokratische Prozesse, darunter auch Wahlen, als langfristiges Problem betrachten. Darüber hinaus kann das Problem nicht allein über Sanktion gelöst oder vermindert werden. Es braucht guten Journalismus, Sensibilisierung und Trainings in Institutionen und in der Politik und nachhaltige Konzepte in der Erwachsenenbildung.

Außerdem braucht es mehr länderübergreifende Kooperation, im Journalismus wie im Bereich von Politik, Institutionen und Bildung. Das hat nicht zuletzt die Infodemie gezeigt, die letztendlich auch im Lichte ihrer politischen Dimension betrachtet werden muss. Das Misstrauen in Wissenschaft, wichtige Gesundheitspolitiker:innen, Ärzt:innen und andere erzeugt auch Misstrauen in demokratische Prozesse. Diese Dinge dürfen nicht isoliert betrachtet werden. Aus diesem Spektrum wird längst nicht nur mehr die Pandemie gelegnet, sondern auch die Existenz des HI-Virus. Und die nächste große Desinformations-Katastrophe beginnt gerade erst. Die Klimawandelleugner:innen gruppieren sich gerade erst. Die Reaktion auf diese Art der Desinformation und Verschwörungsideologien wird auch beeinflussen, wie wir als Gesellschaft mit dem Problem umgehen können.

... es bringen halt die besten Regeln auf dem Papier nichts, wenn sie nicht durchgesetzt werden

Foto: Privat



Marie-Therese Sekwenz
Sustainable Computing Lab

Warum brauchen wir Regeln für einen fairen digitalen Wahlkampf?

Marie-Therese Sekwenz: Nach Skandalen wie Cambridge Analytica und dem Brexit – also im Speziellen seit wir Microtargeting haben – ist es eben so, das ich in meiner digitalen Realität etwas anderes wahrnehme als Du. Das bedeutet, dass politische Werbung direkt auf mich zugeschnitten werden kann. Das gab es vorher nicht. Erinnern wir uns an das Fernsehen: Dort erreicht die gleiche Message alle zur gleichen Zeit. Bei Facebook und Co. kann ich die Werbung auf alle einzelnen Zielgruppen spezifisch zuschneiden. Das ist problematisch, weil die Nutzer in vulnerablen Momenten angesprochen werden können. Durch die Menge an Daten die über einen Nutzer vorhanden ist, können sehr granulare Informationen über ihn, oder sie gesammelt werden, um deren Verhalten zu beeinflussen. Ggf. werben sogar die gleichen Parteien mit verschiedenen Botschaften zum gleichen Thema. Das ist eine völlig neue Qualität. Insofern steht außer Frage, das wir politische Werbung im Digitalen mindestens genauso regulieren müssen, wie politische Werbung im analogen Raum.

Wie können wir die Parteien zur Verantwortung ziehen, um einen fairen digitalen Wahlkampf zu gewährleisten?

Julian Jaurisch: Zumindest für diesen Wahlkampf war die einzige realistische Möglichkeit eine Selbstverpflichtung. Marie hat es erwähnt: Sei es Intransparenz, sei es Microtargeting – noch ist es nicht so, dass gesetzlich diese Themen adressiert wären. Die Selbst-

verpflichtungen können Gesetze nicht ersetzen. Sie waren für den aktuellen Wahlkampf aber die zweitbeste Option.

Wir hätten uns gewünscht, dass die Parteien von sich aus sagen: „Wir haben 2021 im Digitalen einen anderen Wahlkampf als mit Plakaten und Ständen auf dem Marktplatz. Das hat andere Chancen, aber auch andere Risiken. Dessen sind wir uns bewusst und wir als Parteien, als diejenigen, die digitale Werbung schalten und die zur Meinungsbildung beitragen, übernehmen dafür Verantwortung, indem wir für Transparenz sorgen, gegen digitale Gewalt eintreten und für hohe Datenschutzstandards sorgen.“ Das wäre die Signalwirkung von einer gemeinsamen Selbstverpflichtung der Parteien gewesen.

Wie haben die Parteien auf eure Idee einer Selbstverpflichtung reagiert?

Julian Jaurisch: Wir haben mit „Campaign Watch“ ein Bündnis aus 22 Organisationen geschmiedet – von Gewerkschaften bis Universitäten, Zivilgesellschaft bis Menschenrechtsorganisationen. Da steckt also eine breit gefächerte Koalition von Menschen und Organisationen dahinter.

Wir waren uns auch bewusst, dass wir teilweise sehr weitreichende Vorschläge anbieten. Unser Ziel war es, die Parteien dafür zu sensibilisieren, dass sie aktiv werden müssen und vor allem Verantwortung übernehmen. Wir haben u. a. eine Einschränkung von Microtargeting, klare Kennzeichnungspflichten für alle bezahlten Inhalte – inklusive InfluencerInnen –, Einhaltung von Datenschutz und aktive Moderation auf

Foto: Sebastian Heise



Julian Jaurisch
Stiftung Neue Verantwortung

>

den eigenen Social-Media-Seiten gegen Antisemitismus, gegen Rassismus, gegen Sexismus vorgeschlagen.

Zu einer gemeinsamen Selbstverpflichtung kam es zwar nicht, aber alle Parteien, außer der AfD, haben sich zumindest eigene Selbstverpflichtungen gegeben. Guckt man sich diese an, sind dort definitiv einige Vorschläge von Campaign Watch aufgenommen worden. Das ist ein wichtiger Erfolg. Und der zweite Erfolg, den ich nennen würde, ist, dass es viele Veranstaltungen, Analysen, Monitorings zu digitaler Gewalt, zu Desinformation, zu Einsatz von Social Media generell, Kampagnen zu Microtargeting gab, dass sowohl in der Politik als auch in der Gesellschaft das Thema deutlich stärker auf der Agenda war als 2017, was fairer Wahlkampf online bedeutet.

Sind das Wege zur Plattformregulierung oder müssten wir nicht längst bei der Plattformregulierung angekommen sein?

Julian Jaurisch: Wir hatten in unserem Bündnis bei Campaign Watch zuerst überlegt, ob wir die Selbstverpflichtung gemeinsam für Parteien und Plattformen formulieren. Das war z. B. in den Niederlanden gelungen, da haben die Parteien und die großen Plattformen sich auf eine gemeinsame Selbstverpflichtung geeinigt. Das haben wir für Campaign Watch indirekt gelöst, in dem wir für Plattformregulierung Vorschläge eingebaut haben: Parteien müssen von den Plattformen Transparenz einfordern und auf die Einhaltung der Plattform eigenen Sorgfaltspflichten zur Moderation von Beiträgen dringen. Langfristig gesehen halte ich es nicht für sinnvoll, sich bei den Plattform auf Selbstverpflichtung zu verlassen. Wir brauchen Gesetze, Selbstverpflichtung bringen so gut wie nichts, das haben die vergangenen Jahre gezeigt.

Zum Beispiel gibt es seit 2018 einen Verhaltenskodex zu Desinformation, den große Plattformen unterzeichnet haben. Das war super, um überhaupt einmal Plattformen und Europäische Kommission an einen Tisch zu bringen,

aber dadurch, dass die Verpflichtungen sehr vage waren, es keine Sanktionen gab und alles auf Freiwilligkeit beruhte und ohne Monitoring ablief, hat es aus meiner Sicht wenig gebracht. Der Kodex soll nun überarbeitet werden, das ist sicher wichtig. Dennoch: Klare gesetzliche Regeln sind in vielen Fällen, die wir hier gerade besprochen haben, unabdingbar.

Marie, ihr habt zudem eine Risikoprüfung für die Plattformen durchgeführt. Kannst du uns beschreiben, was es damit auf sich hat und zu welchem Ergebnis ihr gekommen seid? Eine ähnliche Idee ist ja auch im kommenden Digital Services Act beschrieben.

Marie-Therese Sekwenz: Wir haben uns zuerst den abgesteckten Rechtsrahmen für die Plattformen angeschaut – also z. B. das deutsche NetzDG oder das österreichische Kommunikationsplattformengesetz – und diese rechtlichen Rahmen um die privatrechtlichen Community-Standards ergänzt, um zu sehen, was wird abgedeckt, wo sind Überschneidungen und was ist überhaupt konkret geregelt. Das war der erste Teil der Risikoanalyse.

Der zweite Teil betrifft den Wahlkontext, also Kategorien, die wir gefasst haben, um Desinformation zu unterscheiden und zu unterteilen. Dabei haben wir uns Fragen gestellt wie: Was passiert, wenn ein Post z. B. gegen einen Politiker oder eine Politikerin trollt und wie oft kommt das vor? Gibt es Verschwörungstheorien in den Daten etc. Bei der Dritten Kategorie handelt es sich um den Versuch, „electoral rights“ im Netz zu beurteilen. Hier war für uns z. B. interessant, ob die Legitimität der Wahl an sich angezweifelt wird, ob der Wahlprozess angegriffen wird, oder falsche Informationen z. B. über die Schließung der Wahllokale verbreitet werden.

Interessant war, dass wir schon relativ schnell an dem Punkt waren, wo das Recht nicht mehr greift, aber die Community Standards für die meisten problematischen Posts als quasi

zweiter rechtlicher Layer auch nicht mehr weitreichend genug waren, um dem problematischen Content von der Plattform entfernen zu können. Also konnten wir schnell feststellen, dass wir mehr und andere Regeln brauchen, die z. B. im Speziellen den Kontext der Wahl online schützen.

Wie kann die Unabhängigkeit von solchen Prüfungen gewährleistet werden?

Julian Jaurisch: Ich habe noch keine Antwort auf diese Frage, aber ich finde, das ist genau die Frage, die zu stellen ist. Wie es bisher ist, kann es jedenfalls nicht sein, dass die Aufgabe bei den Plattformen liegt. Es braucht unabhängige Prüfungen von außen mit eigenen Datenzugängen. Das, was wir in dieser Wahl erlebt haben, dass unabhängiger Forschung einfach der Datenzugang oder das Add-On mit fadenscheinigen Argumenten von Facebook abgedreht wird, darf sich nicht wiederholen.

Klar ist, Unabhängigkeit muss in irgendeiner Weise sichergestellt werden, aber wer das machen soll und auf welche Weise, ist für mich aus dem jetzigen Entwurf des Digital Services Act der EU-Kommission noch nicht ersichtlich.

Es wird immer wieder über eine europäische Regulierungsbehörde geredet, würde die etwas bringen?

Julian Jaurisch: Aus meiner Sicht ist die Aufsichtsfrage im DSA noch ziemlich unterbelichtet oder wird nicht so richtig angegangen, weil sich zu sehr auf Haftungsfragen oder Sorgfaltspflichten konzentriert wird. Die sind wichtig, aber es bringen halt die besten Regeln auf dem Papier nichts, wenn sie nicht durchgesetzt werden.

Das sehen wir etwa bei der DSGVO. Wir haben hier ein relativ progressives Datenschutzrecht, das den Bürger:innen wirklich etwas bringen könnte, aber die Durchsetzung scheitert oftmals daran, dass entweder die Behörden nicht gut genug ausgestattet sind, um es durchzusetzen. Oder aber die Verfahren bzw. das Hin- und Her-Geschiebe von

Verantwortlichkeiten so komplex ist, dass man am Ende einen Flaschenhals bei einer bestimmten Behörde hat, die nicht willens oder nicht mit genug Ressourcen ausgestattet ist, durchzugreifen. Im Fall der DSGVO ist das eben Irland, um es ganz konkret zu machen und deshalb wäre mein Wunsch oder ist meine Hoffnung, dass dieses Thema Aufsicht und Aufsichtsstrukturen im DSA mehr Aufmerksamkeit erfährt.

Langfristig halte ich eine europäische Behörde, die unabhängig von Parteien und Politik ist und sehr spezielle Expertise mit Blick auf Plattformen hat, für sinnvoll. Viele der neuen Regeln im DSA sind noch unerprobt, zum Beispiel, was Risikoberichte angeht, was die Transparenz von algorithmischen Empfehlungssystemen angeht, was Audits für große Tech-Konzerne angeht. Hier muss technische Expertise aufgebaut und gebündelt werden. Eine starke, zentrale EU-Stelle, die auf Augenhöhe mit milliardenschweren Konzernen agieren kann, würde außerdem das mögliche Problem von nationalen Flaschenhälsen bei der Durchsetzung angehen.

Welche Forderung in Form von Plattformregulierung würdest du an die deutsche Bundesregierung richten?

Marie-Therese Sekwenz: **Wo wir uns fast alle einig sind, ist mehr Transparenz, vor allem bezogen auf die algorithmischen Entscheidungen.** Datenzugänge würden uns helfen, mehr Verständnis zu den Mechanismen auf den Plattformen zu durchdringen, z. B. wie viel bleibt stehen bei der Moderation der Inhalte? Wie gut arbeiten die KIs auf den Plattformen – wie gut die Menschen?

Es braucht einen ganzen Satz an neuen Regelungen, um die digitalen Räume besser zu schützen. Sollte hier der DSA hinter den Erwartungen bleiben, muss die neue Bundesregierung eben vorangehen.

Haben wir noch Zeit, die liberale Demokratie zu schützen?

Julian Jaurisch: Den Untergang der liberalen Demokratie sehe ich zumindest nicht für übermorgen, aber eben auch genauso wenig mit einem einzigen Gesetz gestoppt. Es braucht gute Gesetze mit funktionierender Rechtsdurchsetzung und unabhängiger Aufsicht. Dabei bedarf es eines Balanceakts zwischen verschiedenen demokratischen Werten und Rechten, aber eben auch des Schutzes vor Hass und Desinformation. Am Ende braucht es ein Gesamtpaket: besserer Qualitätsjournalismus, mehr Nachrichtenkompetenz, mehr politische Bildung, und eben als ein Puzzleteil auch Regulierung und Aufsicht. Das alles muss ineinander greifen.

Campaign Watch: *Das Bündnis aus NGOs, Zivilgesellschaft und Wissenschaft rief während des Wahlkampfes politische Parteien dazu auf, sich eine Selbstverpflichtung für den Online-Wahlkampf – vor allem im Hinblick auf politische Werbung – aufzuerlegen.*
www.campaign-watch.de

Die Plattformen müssen hinnehmen, dass wir gesellschaftlich Mindestanforderungen an ihre Geschäftspraktiken stellen

Foto: HBI (Hans-Bredow-Institut)



Matthias C. Kettemann
Leibniz-Institut für Medienforschung |
Hans-Bredow-Institut

Wie haben die Social-Media-Plattformen sich mit ihren Diensten auf die Bundestagswahl vorbereitet?

Matthias C. Kettemann: Die Plattformen haben schon seit geraumer Zeit beginnend in den USA vor den letzten Wahlen erkannt, dass die Onlinekommunikation im Wahlkontext besonders schützenswert ist. Das ist nicht nur eine ökonomische Entscheidung. Es ist auch eine Entscheidung, die unmittelbar Demokratierelevanz besitzt. Teilweise sogar, so könnte man argumentieren, ist sie völkerrechtlich geboten, weil die gesellschaftlichen Bestimmungsprozesse besonders schützenswert sind. Nicht nur vor ausländischen Einflüssen, sondern auch vor internen Verfälschungen.

Wahlkommunikation ist historisch gesehen viel, viel mehr reguliert, als Kommunikation im Nichtwahlkontext. Plattformen haben eine sehr kurze Geschichte in der Regulierung, deswegen sind sie noch sehr erratisch. Dennoch wurden verschiedene Regeln aufgestellt, die wir in unserem ersten Papier dazu zusammengefasst haben. Im Kern geht es darum, den Schutz der Integrität der Wahlen zu sichern, beispielsweise durch koordiniertes Vorgehen gegen Desinformation.

Generell sieht man eine Art Konsens der Plattformen, dergestalt, dass sie ihre Rolle als Kommunikationsort für staatsbürgerliche Prozesse, für demokratie-relevante Prozesse viel ernster nehmen. So haben sie aus dem Desaster von 2016 gelernt, indem sie in den USA jetzt

ein bisschen nachgezogen und Wahlwerbung kurz vor der Wahl für einige Zeit verboten haben.

Wie sieht es aus insgesamt mit dem rechtlichen Rahmen aus, in dem sich die Plattformen nun während des Bundestagswahlkampfes bewegt haben?

Vincent Hofmann: Der hat sich jetzt konkret für den Bundestagswahlkampf nicht sehr stark geändert. Im Prinzip ist er derselbe wie vor vier bis fünf Jahren, seit dem Inkrafttreten des NetzDG. Was sich ein bisschen geändert hat, sind weitere Verpflichtungen für Plattformen hinsichtlich strafrechtlicher Inhalte, die aber teilweise auch erst im nächsten Jahr in Kraft treten werden. Die Plattformen sind jedenfalls weiterhin verpflichtet, bestimmte, klar rechtswidrige Inhalte innerhalb von einem Tag zu löschen und nur einfach rechtswidrige Inhalte innerhalb von sieben Tagen. Daran hat sich nichts geändert.

Das Hauptproblem sind jedoch nur bedingt die rechtswidrigen Inhalte, von denen es viele gibt. Es gibt aber auch eine Menge problematischer Inhalte, die nicht gleich rechtswidrig sind. Bei denen haben die Plattformen wesentlich mehr Freiraum, auf diese einzuwirken, sie zu verstärken, sie zu amplifizieren, zu deamplifizieren, sie zu verbieten. So haben wir z. B. Urteile des Bundesgerichtshof, die bestätigen, dass die Plattformen engere Grenzen ziehen dürfen, als es das Gesetz vorsieht.

Foto: Privat



Vincent Hofmann
Leibniz-Institut für Medienforschung |
Hans-Bredow-Institut

>

Das heißt: Plattformen dürfen mehr verbieten, als via Gesetz verboten ist. Dies läuft neuen Tendenzen etwa in Brasilien, Polen, Florida oder Texas entgegen, wo Plattformen gezwungen werden, alles was legal ist online zu halten. Das wäre allerdings ein zu starker Eingriff in deren Autonomie und wirtschaftliche Freiheit. So hat auch der Bundesgerichtshof entschieden: Plattformen dürfen AGB aufstellen und nach ihnen löschen. Sie sind aber verpflichtet, bestimmte Verfahrensrechte zu beachten. Dazu gehört zum Beispiel, dass Personen informiert werden müssen, warum ihre Inhalte gelöscht werden.

Wie ist die neue Richtlinie von Facebook zur koordinierten Schädigung der Gesellschaft zu bewerten?

Matthias C. Kettemann: Der Beitrag kann einen sehr großen Effekt haben, vor allem in Richtung Querdenker. Diese koordinierte Schädigung der Gesellschaft durch authentische Gruppen sind quasi der zweite Köcher. Der erste Köcher, den Facebook und andere Plattformen haben, ist das Vorgehen gegen unauthentische Inhalte und unauthentische Profile. Hierbei handelt es sich um gefakte Profile, die z. B. von Serverfarmen aus St. Petersburg gesteuert werden. Aber das Problem sind natürlich auch authentische Personen. Viele Menschen schreiben eben falsche Sachen, einige sogar unter Klarnamen. Hier ist es gut, dass Facebook Leadership zeigt – spät, aber doch – und gegen diese authentischen Personen auch vorgeht. Trotzdem zeigen die Enthüllungen zu Facebook aber auch, dass das Unternehmen bei der Anwendung seiner Richtlinien nicht alle Nutzer:innen

gleich behandelt und besonders Promis und Politiker:innen weitgehend immunisiert sind.

Viele der Probleme sind auch erst dadurch gekommen, dass Facebook Gruppen vernetzt hat, die nicht vernetzt werden sollten. Wenn etwa ein Empfehlungsalgorithmus bildhaft gesprochen den Impfgegnern sagt: „Hey, die Querdenker mögen die Regierung auch nicht, vernetzt euch mal mit denen!“ ist das mit Blick auf die Sicherung rationaler Kommunikation und Meinungsbildung doch eher ungünstig.

Wie kommt es, dass ein Unternehmen sich dazu entscheidet, nur Accounts einer bestimmte Gruppe zu löschen, aber andere Accounts dann wiederum nicht, die zum Teil ähnliche Inhalte verbreiten?

Matthias C. Kettemann: Die Plattformen schauen derzeit, wo die Probleme liegen und zurzeit ist es so, dass Probleme im Bereich Desinformation in Deutschland primär von Accounts herrühren, die ein Verhältnis zur AfD aufweisen. Ich persönlich fände es besser, wenn die Plattformen viel stärker und kohärenter vorgehen. Die Frage ist, ob die Durchsetzung der Regeln gegenüber allen auf dieselbe Weise schon eine Rechtspflicht ist. Man kann so zumindest argumentieren, wenn man sich etwa die Entscheidungen vom Oversight Board anschaut. Da geht der Trend ganz klar in die Richtung, zu sagen, dass Facebook und die anderen Plattformen sich stärker an ihre internen Regeln halten müssen.

Wie können denn Plattformen wie Messengerdienste zur Verantwortung gezogen werden?

Matthias C. Kettemann: Im Hinblick auf Telegram und andere größere Individualkommunikationsdienste, die inzwischen etwas öffentliches, quasi facebookähnliches anbieten, ist es höchste Zeit, dass das NetzDG durchgesetzt wird. Bei kleineren Plattformen wäre eine Erweiterung des NetzDG nicht mehr vom Wortlaut gedeckt. Dafür müsste dann erst klar ausgelegt werden, dass auch ganz kleine Plattformen davon umfasst sind. Über das NetzDG hinausgehend glaube ich, dass wir langsam zu einem Punkt kommen, wo ein Mindestmaß an Transparenz erwartet wird. Von den Plattformen kann man rechtlich erwarten, dass genauso wie Standards an Fahrradhersteller bestehen, sich Plattformen gefallen lassen müssen, dass wir gesellschaftlich – nicht juristisch – Mindestanforderungen an ihre Geschäftspraktiken stellen. Das ist jetzt noch keine Antwort aus dem Recht. Das heißt, das sind Themen, wo wir noch in den nächsten Jahren viele Entwicklungen sehen werden.

Kommen wir zur politischen Werbung im Bundestagswahlkampf. Wie haben sich die Parteien verhalten hinsichtlich der Leitlinien, die das Bündnis Campaign Watch aufgestellt hat?

Vincent Hofmann: Im Leitfaden von Campaign Watch gab es bestimmte Targeting-Parameter, die festgelegt wurden. Hier gab es „Unproblematische“, die man auch an einem Wahlkampfstand mitbekommen hätte: Geografie oder Alter. Überraschend fand ich, dass die Parteien mehr oder minder ausdrücklich gesagt haben, dass sie weitere Parameter wie

Interessen, Geschlecht oder gesprochene Sprachen nutzen werden, um ihre Zielgruppe anzusprechen. Hier haben sie sich explizit nicht an den Leitfaden von Campaign Watch gehalten.

Ähnlich war es mit Bots. DIE LINKE, SPD, Grüne haben darauf verzichtet. Diese Parteien, haben sich in ihrer Selbstverpflichtung dazu geäußert. Bei der AfD gab es eine eher undurchsichtige Antwort. Ein klares Nein gegen Social Bots war es definitiv nicht.

Ist eine gemeinsame Selbstverpflichtung etwas, was in der nächsten Legislatur angegangen werden sollte oder muss man vor allem auf die Plattformen schauen?

Vincent Hofmann: Wenn sich die Parteien auf gemeinsame Spielregeln im Wahlkampf einigen, wäre das sicherlich sinnvoll. Wichtig wäre dann, dass man Mechanismen wie Datenzugänge und Transparenz hat, mit deren man prüfen kann, ob die Parteien sich daran halten. Das kann eine sinnvolle Vorstufe vor regulatorischen Eingriffen sein. Der Wahlkampf hat zudem gezeigt, dass politische Werbung nicht unser Hauptproblem ist. Deutschland ist auch hier im Vergleich zu den USA relativ verschont geblieben ist, wie schon im letzten Wahlkampf.

Was sind die wichtigsten Punkte, um digitale Bedrohung im Netz anzugehen?

Matthias C. Kettemann: Keine Überraschungen hier: Mehr Investitionen in digitale Bildung. Das heißt mehr Investitionen in den Aufbau von Kompetenzen der Bürger:innen unabhängig von ihrer

Erwerbsbiografie oder ihrem sozioökonomischen Status. Eine Immunisierung der Gesellschaft gegen Desinformation kann man in der Gestalt erreichen.

Auch wäre ein kohärentes Vorgehen bei politischer Onlinewerbung notwendig. Das NetzDG sollte zudem breiter auch auf die Individualkommunikationsplattformen angewandt werden und deren Dienste, bei denen eine:r Nutzer:in viele andere erreichen kann. Zudem: Das Investment für digitalen Opferschutz sollte erhöht werden.

Sie teilen gar nicht gerne

Foto: Bea Roth



Isabelle Borucki

Forschungsgruppenleiterin an der NRW School of Governance der Universität Duisburg-Essen

Was habt ihr im Bundestagswahlkampf 2021 gemacht?

Isabelle Borucki: Wir haben in einem politik- und kommunikationswissenschaftlichen Projekt versucht, die Parteien und ihre Wahlkämpfe auf Social Media zu beobachten: Was machen die Parteien da, was die Kandidierenden und wie ist die Resonanz? Es war quasi ein Live-Monitoring des Wahlkampfs durch ein wissenschaftliches Team, das von Ulrike und mir geleitet wurde und an dem Studierende mitarbeiteten.

Wir haben im Wesentlichen Kurzanalysen geliefert, auf einer Website versammelt und damit der interessierten Öffentlichkeit zur Verfügung gestellt. Kurz vor dem Wahlsonntag kam beispielsweise ein schöner Countdown von Ulrikes Team, das Topleaderboard auf Social Media, wo man sehen konnte, welche Politikerin da in Bezug auf Postings und Interaktion führte. Die wissenschaftliche Auswertung beginnt aber erst jetzt nach dem Wahlkampf.

Ulrike Klinger: Das war im Grunde Wissenschaftskommunikation, das heißt, wir machen politische Daten aktuell transparent und vermitteln sie der Öffentlichkeit als Open-Source-Materialsammlung. Wissenschaftlich verwertbar ist das noch nicht, das könnten Fachzeitschriften nicht publizieren, es ist viel zu simpel.

Normalerweise würden wir während eines Wahlkampfs noch nichts veröffentlichen, sondern erst einmal schauen, an welche Daten kommen wir ran und wie werten wir sie anschließend zu welchen Fragen wissenschaftlich aus? Aber diesmal dachten wir, das ist eine Wahl, die ganz anders ist als alle anderen in der Geschichte der Bundesrepublik, und auch weil die letzten Wahlkämpfe in verschiedenen Ländern teilweise suboptimal gelaufen sind, versuchen

wir, da ein bisschen Transparenz reinzubringen und unseren Beitrag zu leisten, damit nachvollziehbarer wird, wie der Wahlkampf auf Social Media läuft.

Wie kamt ihr an die Daten?

Ulrike Klinger: Mit CrowdTangle greifen wir auf Facebook-Daten zu. In den Nutzungsbedingungen steht aber schon, dass man diese Daten nicht für die Lehre verwenden darf. Außerdem haben wir dank Reset einen Premium-Zugang zu BrandWatch, damit greifen wir auf Twitterdaten zu. Die kriegt man auch direkt über eine Datenschnittstelle, aber nicht in einem Format, mit dem auch Studierende arbeiten können. In diesem Projekt konnten also Studierende mit Daten arbeiten, zu denen sie sonst nie Zugang hätten, weil der Zugang zu teuer oder ganz unmöglich ist, oder eben nicht für die Lehre verwendet werden darf. Mit diesen Datenportalen kann man Wort- oder Emoji-Wolken machen und Häufigkeitsauszählungen wie: Was sind die am häufigsten geteilten Links? Welche Postings performen besonders gut oder schlecht? All die Analysen, die Studierende für unser gemeinsames Projekt machten, haben wir dann auf die [Website*](#) gestellt und sie so Journalistinnen und der Öffentlichkeit in open source zugänglich gemacht. Zusätzlich bekamen wir Daten von CitizenBrowser, so dass wir nun mit Daten arbeiten konnten, die wir sonst als Wissenschaftlerinnen eher nicht bekämen.

Was kostet denn so was?

Ulrike Klinger: Über die Academic Twitter Schnittstelle kommt man kostenlos an Rohdaten, wenn man akkreditiert wurde. Dafür braucht man aber schon einige methodische Vorkenntnisse, das ist nicht für Laien gemacht. Mit Crowdtangle bekommt man kostenlos Zugang zu den

Foto: Jan Kopankiewicz



Ulrike Klinger

Professorin für Digitale Demokratie an der European New School of Digital Studies (ENS) der Europa-Universität Viadrina

* www.zahlen-zur-wahl.de

Posts von öffentlichen Facebook-Accounts, auch da muss man akkreditiert sein. Im Moment sind das weltweit nur ca. 1000 Forscher:innen.

Wenn man keine Akkreditierung hat und nicht mit Scraping-Tools oder Datenschnittstellen arbeiten kann, muss man die Daten kaufen. Das ist recht teuer, auch Dienste, die kleine Voralysen anbieten, da ist man für ein Jahresabo schnell im fünfstelligen Bereich. Bei den anderen Plattformen ist es überwiegend recht aussichtslos.

Einige Medien wie die Süddeutsche Zeitung, Zeit, Spiegel, Tagesspiegel arbeiten mit Datenjournalisten, aber die meisten kleineren, lokalen Zeitungen oder Sender können sich das nicht leisten. Daher ist diese Form der Wissenschaftskommunikation, auch wenn sie auf einem simplen Level operiert, bestimmt ganz hilfreich. Wir stellen aufbereitete Daten zur Verfügung, mit denen Journalist:innen oder Lehrer:innen dann arbeiten können. Wir hoffen, damit zur Transparenz des Wahlkampfes für die Öffentlichkeit und die Gesellschaft.

Wie kooperativ waren die Plattformen gegenüber Forscher:innen wie euch?

Ulrike Klinger: Sie teilen gar nicht gerne. Facebook geht momentan sogar recht aggressiv gegen Forscher:innen vor – zum Beispiel gegen einen unserer geplanten Kooperationspartner, das AdObservatory der NYU. Dort war für die US-Wahl ein Tool entwickelt worden, mit dem man beobachten kann, an wen sich die Facebook-Werbungen der Parteien richten. Targeting-Analysen also. Das sollte für die Bundestagswahl angepasst werden. Doch dann hat Facebook den Kolleginnen den Zugang gesperrt. Auch Algorithm Watch war kürzlich gezwungen, ein Forschungsprojekt zu beenden, bei dem es um den Instagram-Algorithmus ging, weil Facebook rechtliche Schritte angedroht hatte. Wissenschaftliche Projekte und NGOs können sich rechtlich nicht mit einem milliardenschweren Konzern wie Facebook anlegen. Der Preis für die Gesellschaft ist, dass sie wichtige Dinge über die öffentliche Kommunikation auf den Plattformen nicht erfahren wird.

Isabelle Borucki: Auf Facebook kann sich jeder die Werbebibliothek anschauen, über eine Datenschnittstelle darauf

zugreifen und sich die dort hinterlegten Daten ziehen, um sie zu analysieren. Allerdings scheint die Werbebibliothek nicht vollständig zu sein, dafür gibt es in der wissenschaftlichen Literatur Hinweise. Das zu beleuchten und genauer zu untersuchen, war geplant, konnte aber nicht mehr realisiert werden aufgrund der Tatsache, dass unseren Kooperationspartnern der Zugang geschlossen wurde.

Ulrike Klinger: Dabei hat die Kooperation zwischen den Projekt-Teams toll funktioniert. Normalerweise würden wir konkurrierend arbeiten, aber hier haben wir uns super ausgetauscht zwischen der European New School und dem Weizenbaum-Institut, für die ich die Projektleitung habe, und mit dem Leibniz Institut für Medienforschung in Hamburg und weiteren Kolleg:innen an anderen Instituten.

Isabelle Borucki: ...Wie an der NRW School of Governance mit meinem Projekt "Digitale Parteienforschung", und der Professur an der Universität Siegen, die ich gerade vertrete. Aber unser eigentliches Interesse – nämlich zu bewerten, wer von den Parteien postet wie viel, von wem lässt man es sich bezahlen und an wen werden die Posts gerichtet und vielfältig und wie viele Impressionen bekommen diese Posts – das konnten wir nicht realisieren. Das hat Facebook verhindert.

Mit welcher Begründung?

Ulrike Klinger: Es ist eine recht komplexe rechtliche Debatte. Im Kern geht es dabei um den Schutz der Privatsphäre. Das ist eigentlich begrüßenswert. Aber man fragt sich schon, ob es sinnvoll ist, die Privatsphäre von Parteien, die öffentlich kommunizieren und Werbung schalten, vor den Blicken von Wissenschaftler:innen zu schützen, zumal in einem Wahlkampf.

Wie ist der Online-Wahlkampf denn nun nach eurer Beobachtung gelaufen?

Ulrike Klinger: Im Großen und Ganzen recht erwartbar – es gab kaum Überraschungen, die vom Forschungsstand abweichen. Das ist übrigens eine gute Nachricht. Wir müssen das natürlich noch auswerten, aber vorläufig sehe

ich viel Personalisierung, Negative Campaigning, auch die Kampagnen und Angriffe auf weibliche Kandidaten alles andere als ungewöhnlich, leider. Erstaunlich fand ich, dass die Facebook-Seite der SPD mit Geoblocking arbeitet, also in vielen Ländern nicht verfügbar war. Das wundert mich, denn Social Media sind ja eine wichtige Informationsquelle für Wahlberechtigte im Ausland. Dadurch sind die Facebook-Posts der SPD übrigens nicht im Datenarchiv von Crowdtangle enthalten, das erschwert unsere Arbeit und trägt nicht eben zu Transparenz bei. Also: erwarbar, aber nicht langweilig! Ich bin gerade in den USA und hier wäre man froh über Kandidat:innen, die sich vielleicht nicht sonderlich spektakulär aufführen, sondern ganz überwiegend rational und zivilisiert miteinander umgehen.

Aber Affekte regieren schon auch, in den sozialen Medien?

Isabelle Borucki: Ich teile den Eindruck, dass es mehr personalisiertes Negative Campaigning gab. Das bedeutet, man attackiert den politischen Gegner nicht wegen seiner Inhalte, sondern persönlich und stellt heraus weswegen die Konkurrentin unmöglich ist, nach dem Motto: „Baerbock kann es nicht, der Laschet lacht dumm.“

Ulrike Klinger: Der bei weitem am meisten kommentierte und geteilte Post während der Bundestagswahl war von der AfD, die am meisten mit Affekten, Personalisierung und Negativität arbeitet: Da sieht man Annalena Baerbock, der in einer Fotomontage ein Kopftuch verpasst wurde, und darüber steht: Einwanderungsministerium. Vollkommen absurd, aber im Netz erfolgreich.

Anzeichen dafür, dass sich Akteure, die mit der amerikanischen Rechten in Verbindung stehen, in die Themen und den Wahlkampfprozess einmischten



Foto: Privat

Anneli Ahonen

Institute for Strategic Dialogue

Konnte man während der Bundestagswahl 2021 Versuche ausländischer Einflussnahme beobachten?

In der öffentlichen Debatte über ausländische Einflussnahme vor der Wahl ging es hauptsächlich um die Aktionen Russlands, während andere Länder wie China, Iran oder die Türkei fast nicht auftauchten. **Bisher ist klar, dass staatlich unterstützte russische Quellen schon früh versucht haben, die Grünen und Annalena Baerbock zu diskreditieren.** Ihr Hauptaugenmerk lag in der Untergrabung des Vertrauens in die Maßnahmen der Regierung hinsichtlich COVID-19 sowie die Effizienz und Sicherheit der Impfstoffe. Viele nichtstaatliche Akteure verfolgten die gleichen Ziele.

Die deutliche Warnung der Regierung vor Cyberangriffen und dem damit verbundenen Risiko von Desinformations- und Beeinflussungsoperationen zeigte, dass die Regierung die Bedrohung ernst nimmt. Sie brachte die Angriffe mit der Hackergruppe Ghostwriter und dem russischen Militärgesamtdienst in Verbindung und sagte, sie habe Beweise für Versuche, sensible Informationen vor allem von deutschen Politikern zu erlangen. Damit haben die Debatte und die Verwirrung über die Art dieser Angriffe ein gewisses Ende gefunden.

Es gibt jedoch auch viele offene Fragen. Wurden die möglicherweise erlangten sensiblen Informationen dann in Desinformationskampagnen verwendet, um Entscheidungsträger:innen, politische Kandidat:innen oder Wähler:innen zu

beeinflussen? Ghostwriter hat bereits früher Einflusskampagnen in Polen, Litauen und Lettland durchgeführt. Wenn diese Kampagnen in Deutschland stattgefunden haben, hatten sie dann Auswirkungen auf die Wahl? Wie hoch ist die Wahrscheinlichkeit, dass diese Art von Kampagnen auch gerade noch weitergeführt werden?

Welche Techniken werden von ausländischen Akteur:innen am häufigsten eingesetzt?

Was wir derzeit aus Deutschland wissen: Cyberangriffe auf Politiker:innen im Vorfeld der Wahl einerseits und staatlich unterstützte russische Medien andererseits, die einer bestimmten Partei oder einem Kandidaten besondere, negative Aufmerksamkeit widmen, sind Techniken, die auch schon früher beobachtet wurden.

Was war im Rahmen Eurer Beobachtungen zur Bundestagswahl 2021 besonders überraschend?

Es war überraschend zu sehen, wie viel Publikum russische staatlich unterstützte Quellen in Deutschland mit aggressiven und provokativen Social-Media-Strategien gewinnen konnten – das alles unter Verletzung der Richtlinien der Social-Media-Plattformen. Daher ist es sinnvoll, sich immer wieder daran zu erinnern, dass die russischen Staatsmedien vollständig von den Social-Media-Plattformen abhängig sind, um ihr Publikum in Deutschland zu erreichen. Ich habe mit besonderem Interesse

verfolgt, wie diese ausländischen Bedrohungen von der Regierung an die Öffentlichkeit kommuniziert wurden.

Die Frage, die mich am meisten interessiert ist, ob deutsche Wähler:innen genügend öffentlich zugängliche Informationen darüber haben, ob und wie ein ausländischer Staat versucht, ihre Wahlentscheidungen zu beeinflussen. Hier haben die deutschen Medien, Faktenprüfer, Nichtregierungsorganisationen und Forscher gezeigt, wie eine starke Zivilgesellschaft das öffentliche Bewusstsein für die Versuche ausländischer staatlicher Einflussnahme effektiv erhöhen kann.

Sowohl die deutsche Regierung als auch die EU reagierten mit öffentlichen Erklärungen. Das ist zwar ein wichtiges Signal, allerdings muss es dann auch Konsequenzen für derartige Handlungen geben.

Welche Rolle spielen die Plattformen in Bezug auf ausländische Beeinflussung?

YouTube hat nach der Wahl die deutschen Kanäle von Russia Today (RT) unter Berufung auf seine COVID-19-Richtlinien gelöscht. Die deutschsprachigen Inhalte und Artikel von Russia Today werden aber weiterhin auf anderen Plattformen wie Facebook und Twitter verbreitet. Hier stellt sich auch die Frage, warum das alles erst nach der Wahl geschah bzw. erst nach 1,5 Jahren aktiver Förderung von Inhalten, die die COVID-19-Maßnahmen der Regierung in Frage stellen und Anti-Vaxx-Nachrichten und Verschwörungstheorien fördern.

Was sind die größten Herausforderungen hinsichtlich der Bekämpfung ausländischer Einflussnahme?

Abgesehen von den bereits erwähnten Herausforderungen besteht eine der Herausforderungen darin, dass es keinen Grund zu der Annahme gibt, dass derartige Aktivitäten aufgehört haben.

Welche Forderungen (an die deutsche und europäische Politik) und welche Lösungen ergeben sich daraus?

Russlands Beeinflussungsversuche auf westliche Wahlen – von den USA 2016, 2018, 2020 bis hin zum Brexit, der französischen Präsidentschaftswahl, der katalanischen Abstimmung und nun auch in Deutschland – sind im Großen und Ganzen zum „business as usual“ geworden, das ein erhebliches Umdenken sowohl für die EU-Mitgliedsstaaten auf nationaler Ebene als auch für die EU als Ganzes erfordern wird. Allerdings wird es ohne eine transparentere Politik der Social-Media-Plattformen und einen verbesserten Zugang zu Daten für unabhängige Forscher:innen sehr schwierig sein, festzustellen, wie die Plattformen vom Ausland aus genutzt werden.

Das **Institute for Strategic Dialogue (ISD)** ist eine unabhängige, gemeinnützige Organisation, die sich für den Schutz der Menschenrechte und die Umkehrung der steigenden Flut von Polarisierung, Extremismus und Desinformation weltweit einsetzt.
www.isdglobal.org/about

Nachrichteninkompetente Gesellschaften, die Propaganda für bare Münze nehmen

Foto: Andrea Russo



Alexander Sänglerlaub
Direktor und Co-Gründer des
Think & Do Tanks futur eins

Hass, Desinformation und die digitale Debattenkultur während des Bundestagswahlkampfes 2021

www.reset.tech/resources/social-media-in-germany-effects-on-the-culture-of-debate-disinformation-and-hate

In repräsentativen Online-Befragungen hat reset unter der Leitung von Alexander Sänglerlaub zusammen mit dem Meinungsforschungsinstitut pollytix drei Reports veröffentlicht, in denen über 3.000 Wähler:innen zu ihren Erfahrungen mit Hass im Netz oder Desinformationen im Wahlkampf befragt wurden.

Ihr habt im Wahlkampf zusammen mit pollytix die wahlberechtigten Bundesbürger:innen zu verschiedensten Themen befragt. Was genau wolltet ihr wissen?

Wir wollten wissen, wie die Wählerinnen und Wähler da draußen im Land die Stimmung in den Sozialen Medien im Wahlkampf einschätzen. Da ging es nicht nur um die Wahrnehmung von Hass und Desinformation oder ganz generell um den Zustand der digitalen Debattenkultur, sondern auch, welche Erfahrungen die Menschen selbst mit Hass und Hetze gemacht haben oder welche Desinformationen eigentlich geglaubt werden. Gibt es überhaupt eine Problemwahrnehmung? Und wenn ja, was folgt daraus? Und wie ergeht es denen, die zahlreiche Erfahrungen mit Hass gemacht haben. Ziehen sich die Menschen aus den Diskursen zurück? All das haben wir mit einer repräsentativen Befragung von über 3.000 deutschen Wähler:innen, die online sind, versucht herauszufinden.

Beginnen wir mit der Debattenkultur!

Uns hat hier vor allem interessiert, welchen Einfluss Social Media auf unsere Demokratie und unsere Debatten hat. Das wurde kontrovers gesehen: 48% sehen keine Bereicherung unserer Debatte, 43% schon. Auffällig ist hier auch der Geschlechterbias: Männer bewerten den Einfluss auf unsere demokratischen Debatten etwas besser als Frauen. Interessant ist aber, dass sich nur ein Bruchteil der Befragten überhaupt auf Social Media in politische Debatten einbringt: Gerade einmal nur 15 Prozent der Befragten tun dies aktiv und regelmäßig. Wer sind nun diese 15 Prozent? Hier gibt es ein Ungleichgewicht, weil hier vor allem Junge, Männer und aber

auch beispielsweise Anhänger der AfD überrepräsentiert sind. **Daran erkennen wir, dass die Debatten auf Facebook & Co. nicht den Querschnitt der Gesellschaft darstellen, sondern ein Zerrbild.** Das ist eine wichtige Erkenntnis vor allem für den Journalismus: Debatten in sozialen Netzwerken sind nicht repräsentativ für die Bevölkerung, diesem Trugschluss darf man nicht aufsitzen.

Es wird also auch von den Leitmedien und der Politik aus den ‚Sozialen‘ Medien ein unverhältnismäßiges Zerrbild der gesellschaftlichen Stimmung transportiert?

Absolut, zumal sich Zweidrittel der Befragten einen weniger aggressiven Wahlkampf im Netz wünschen. Sie empfinden den Ton als zu rau. Jede:r Zweite sagt das. Und das hat natürlich Auswirkungen: drei von vier Wähler:innen halten sich in Diskussionen online bewusst zurück. Eine deutliche Mehrheit bleibt in den politischen Online-Debatten passiv. Sie schweigt. Etwa die Hälfte der Wähler:innen – das haben wir in den Nachwahlbefragungen gesehen – hat sogar bewusst versucht, politischen Themen in sozialen Netzwerken zu entgehen.

Welche Plattformen hattet ihr im Visier?

Bei der Nutzung haben wir nach allen gefragt: Youtube, Facebook, Instagram, TikTok, Snapchat, Twitter usw. Sie werden je nach Alter allerdings sehr unterschiedlich genutzt und das macht die Ergebnisse spannend. Die Jungen nutzen oft mehrere Plattformen sehr intensiv und gleichzeitig: Instagram, Snapchat, TikTok, doch nutzt nur jede:r Zweite der 18–34jährigen noch Facebook. Auffällig in der Mediennutzung ist

>

allerdings auch, dass z. B. Anhänger:innen der AfD überdurchschnittlich Telegram oder die BILD-Zeitung nutzen.

Schauen wir nur auf die Debattenkultur, ist es interessant zu sehen, dass 69% sagen, die Lokalzeitungen hätten einen positiven Einfluss auf die Debattenkultur, auch die Öffentlich-Rechtlichen kommen mit 67 Prozent auf sehr gute Werte. Nur 21 Prozent sagen, dass Facebook eine positive Wirkung auf unsere Debattenkultur hätte, bei Twitter sind es 20 Prozent. Dahinter folgt als Schlusslicht nur noch die Bild-Zeitung mit 17 Prozent. Das ist insofern interessant, weil Facebooks Algorithmen gar nicht so weit weg sind von der Aufmerksamkeitsökonomie von Boulevardzeitungen.

Die Sozialen Medien sind die Boulevardzeitung von heute?

Genauso aufgeregt und affektgeladen mit dem Surplus, dass die Algorithmen Wut und andere Affekte eben besonders triggern und weiterverbreiten, um die Menschen auf den Plattformen zu halten. Faktizität oder Qualität der Information spielen bei den Algorithmen keine Rolle – auch das ist fast wie beim Boulevard (lacht).

Die Folgen sind weniger lustig. Dadurch, dass soziale Netzwerke gerade für politische Debatten ein ziemlich toxisches Umfeld liefern, führt dazu, dass Frauen, Minderheiten, LGBTQIA+ und viele andere Menschen sich aufgrund des rauen, offensiven oder offen gewalttätigen Diskurses aus dem Debattenraum zurückziehen und ihre Stimmen dadurch verstummen. Das ist ein ziemliches Armutszeugnis für eine Demokratie, deren Diskussionsräume so massiv von Plattformen bestimmt werden, die mal mit einem anderen Versprechen angetreten sind. Selbst die Menschen, die auf Facebook sind, glauben nach unserer Umfrage nicht daran, dass es gut ist für die Debattenkultur: Nur 28 Prozent glauben das, bei Twitter steht es immerhin fast 50 zu 50.

Doch es wird noch dramatischer: 51 Prozent der Wähler:innen geben zu, das es sich negativ auf ihr psychisches Wohlbefinden auswirke, wenn sie zu viel Zeit auf Social Media verbringen.

Ein Großteil sagt zudem, dass sie versuchen zu detoxen, es aber nicht schaffen! Bei den Jungen sind es sogar fast 60 Prozent der 18–34jährigen, die sagen, dass es auf ihre Psyche schlägt, und 40 Prozent, dass es schwierig ist, sich von den Plattformen zu lösen.

Auch in den durch Frances Haugen geleakten Dokumente von Facebook, wozu ja auch Instagram und WhatsApp gehören, wurde klar, dass Instagram genau weiß, dass seine Suchtmechanismen per Algorithmus so wirken. Demnach wussten sie schon seit 2019, dass die Nutzung von Instagram beispielsweise bei einem von drei minderjährigen Mädchen eine gestörte Körperwahrnehmung noch verschlimmert und dass jugendliche Instagram-User häufiger unter Ängsten und Depressionen leiden.

Wäre ich Verbraucherschützer, müsste ich wohl darüber nachdenken, ob man Warnhinweise anbringen müsste, die in regelmäßigen Abständen den Menschen mögliche Folgen ins Bewusstsein rufen – wie auf Zigarettenschachteln.

Immerhin: Jeweils 85 Prozent der Befragten antworteten auf die Frage, ob Hass und Desinformation ein Problem für die Gesellschaft seien: Ja! Und auch dreiviertel der Menschen sagen: Das muss gelöst werden, von Politik und Plattformen. Sei es durch mehr Regulierungen oder bessere Strafverfolgungsbehörden. Wir sehen da einen klaren Auftrag der Wählerinnen und Wähler an die neue Regierung.

Kommen wir zum Hass in eurer Studie. Habt ihr euch auch mit den Tätern beschäftigt?

Nach denen haben wir nicht gefragt, sondern danach, wer welche Hassereifahrungen im Netz macht und das sind besorgniserregende Zahlen. Junge Frauen zwischen 18 und 34 kriegen nicht nur besonders viel ab, 38 Prozent haben persönliche Erfahrungen gemacht. 93 Prozent erachten den Hass im Netz in dieser Altersgruppe als Problem. Er bezieht sich vor allem auf Frauen, Menschen mit Migrationshintergrund und Menschen, die nicht heterosexuell sind. Jede dritte Frau zwischen 18 und 34

wurde im Netz schon sexuell belästigt; 28 Prozent quer durch alle Altersgruppen wurden schon beleidigt; 11 Prozent, dass private Daten gegen ihren Willen verbreitet wurden. Von den Jüngeren wurden 64 Prozent schon beleidigt und sexuelle Belästigung trifft jede Dritte zwischen 18 und 34. Es trifft übrigens weniger Männer, aber manchen trifft es auch.

Was wolltet ihr zu Desinformation wissen?

Wir wollten wissen, wie der Umgang mit Desinformationen im Netz ist. Drei von vier Befragten trauen sich immerhin zu, Desinformation zu erkennen. Klingt erst einmal gut, doch das ist leider nur die Selbsteinschätzung. [Aus unserer Studie zur digitalen Informations- und Nachrichtenkompetenz aus dem März 2021](#) wissen wir allerdings, dass es genau umgekehrt ist: Gerade einmal 22% der Deutschen haben de facto eine hohe Nachrichtenkompetenz, fast die Hälfte allerdings keine oder nur eine sehr geringe. Wir überschätzen uns demnach nicht nur in Umfragen, sondern sind als Gesellschaft weitaus schlechter mit Desinformation angemessen umzugehen, als wir annehmen.

Was war im Wahlkampf '21 in dieser Hinsicht besonders?

Wir haben dann noch nach der Zustimmung zu bestimmten Verschwörungsnarrativen gefragt, die während des Wahlkampfs verstärkt kursierten und diese Zahlen machen besonders nachdenklich. 28 Prozent glaubten, dass die Grünen das Autofahren komplett verbieten wollen, 21 Prozent sagten immerhin teils-teils. Oder 23 Prozent glauben, Muslime wollten in Deutschland einen Gottesstaat errichten und 31 Prozent sind sich da nicht ganz sicher. Auch hier sind es wieder übermäßig viele AfD-Anhänger:innen, die das glauben. Dazu gehörte, auch der Glaube an das Narrativ, dass wohl etwas was mit der Briefwahl nicht stimmen werde oder dass es keine menschengemachte Klimakrise gäbe, dass Corona ein Vorwand für die Unterdrückung der Menschen sei – das sagten immerhin

noch 17 Prozent und weitere 16 waren unentschieden. Im Schnitt stimmten ein Viertel bis ein Fünftel diesen Verschwörungsnarrativen zu.

Was sind eure Schlussfolgerungen daraus?

Hass und Desinformation beeinflussen die Debattenkultur und gefährden die Demokratie, zum einen, weil sich die Menschen aus den demokratischen Diskursen zurückziehen, zum anderen, weil sie falsch informiert unter Umständen schlechte Entscheidungen treffen – schauen wir doch nur auf die Impfquote jetzt in der Pandemie.

Es braucht mehr Nachrichtenkompetenz, die geschult werden kann. Hass muss von den Plattformen und den Staatsanwaltschaften schneller verfolgt und gelöscht werden. Es braucht aber auch mehr Fact-Checking. Im letzten Bundestagswahlkampf 2017 gab es auf 30 Millionen Nutzer:innen von Facebook gerade einmal – drei – Fact-Checker. 2021 sind es bei Correctiv, der dpa und AFP zwar ein paar mehr, aber wohl vermutlich immer noch zu wenig. Alles in allem müssen wir als Gesellschaften mal langsam zu Potte kommen, unsere Diskursräume – und die Menschen dort drin, besser zu schützen. Oder wir nehmen eben eine zunehmend vom Hass zersetzte und desinformierte Gesellschaft als gegeben.

Zu Beginn jeder technischen Neuerung gibt es einen Hype. Ist der Rausch allmählich vorbei und es kommt der Kater?

In der Technikgeschichte gab es fast immer die technikaffinen Pioniere, welche die Utopien proklamierten und dann kam langsam der Rest der Gesellschaft nach. Dann kommen auch zunehmend die Probleme und Verwerfungen ans Tageslicht, die eine neue Technik mit sich bringen kann.

Auch bei der Regulierung sind wir schneckenlangsam. Schauen wir zum Beispiel ins Medienrecht, wie wir das mit dem Privatfernsehen gemacht haben, als es in den Achtzigern entstand: Vor einem Werbeblock kommt ein ordentlicher Disclaimer, der sagt: Jetzt kommt Werbung! In einer Nachrichtensendung

heißt es bei einem Kommentar: Jetzt folgt die Meinung von XY! Wenn politische Werbung kommt: Für diesen Wahlwerbespot sind die Parteien verantwortlich! All das haben wir im digitalen Raum in der Deutlichkeit nicht.

Welche Entwicklungen haben wir denn verschlafen? Wo könnten wir aus der alten Medienwelt noch etwas für die digitale lernen?

Die Erfahrung des Nationalsozialismus und von Goebbels' Schnauze war eben auch, einen öffentlich-rechtlichen Rundfunk einzuführen, der staatsfern ist. Gerade wir in Deutschland sollten schmerzlich wissen, was es bedeutet, wenn Medien als mächtige Propagandamaschinen missbraucht werden. So gab es 1961 das erste Rundfunkurteil des Bundesverfassungsgerichts, das Parteien verbot, Rundfunk zu machen. Heute aber haben wir mit Twitter, Facebook, YouTube für Parteien die Möglichkeit, starke Propaganda in die Welt zu schießen, ohne uns zu fragen, ob das für die Demokratie eine Bereicherung ist, wenn ein Donald Trump mit 90 Millionen Followern seine Meinungen und Desinformationen in die Welt posaunt.

Ist es klug, Extremisten auch noch einen Lautsprecher in die Hand zu drücken? Gerade in Amerika haben wir gesehen, wohin das führen kann: Zum Sturm aufs Kapitol. Erst danach wurde Trump der Lautsprecher abgestellt und Twitter hat ihn geblockt. Vielleicht zu spät. Andere propagieren aber nach wie vor munter weiter und treffen eben auf nachrichteninkompetente Gesellschaften, die Propaganda für bare Münze nehmen.

Es geht hier nämlich um mächtige ‚Werkzeuge‘, wie Waffen oder Autos



Foto: Privat

Sam Jeffers
Co-Gründer und Executive Director
von Who Targets Me

Was konntet Ihr bei Eurer Untersuchung hinsichtlich der Verbreitung von Desinformationen in sozialen Netzwerken beobachten?

Sam Jeffers: Günstige Online-Werbung bietet neuen Marktteilnehmer:innen die Möglichkeit, sich bei einer Wahl Gehör zu verschaffen. Das bringt eine Reihe von Risiken mit sich, wie beispielsweise ausländische Einflusskampagnen, aber auch Angriffe zahlreicher unbekannter Quellen.

Insgesamt versuchen wir mit unseren politischen Empfehlungen sicherzustellen, dass Menschen soziale Netzwerke verantwortungsbewusst nutzen. Etwas plakativ ausgedrückt: **Wir sollten den Menschen nicht am ersten Tag die Schlüssel zum Lamborghini geben, sondern zunächst sicherstellen, dass sie die Fahrprüfung mit einem langsameren Auto bestanden haben.**

Was gibt es diesbezüglich über Deutschland zu sagen?

Sam Jeffers: Ob es sich um Desinformationen und Fehlinformationen handelt, hängt von ihrer Definition ab. Für Kritiker:innen einer politischen Partei ist es einfach zu sagen: „Mir gefällt nicht, was die Gegner sagen“ und es dann als Lüge zu bezeichnen.

Laura Edelson: Die Menschen in die Irre zu führen, ist ein Teil des Ganzen, aber meine größere Sorge liegt bei der Art und Weise, wie Plattformen zur Polarisierung beitragen: Ja, die AfD ist in der Lage, ein unglaubliches Engagement auf Plattformen zu erreichen. Ich erinnere mich zum Beispiel noch, als Alice Weidel während der Flutkatastrophe eine Regenjacke trug und dabei mit freiwilligen Helfer:innen sprach und Anteilnahme zeigte.

Direkt dahinter auf Platz 2 aber waren die Grünen. Die äußeren Enden des politischen Spektrums profitieren also unverhältnismäßig stark von den Anreizen der Online-Kommunikation, da die „extremsten“ Meinungen für alle am spannendsten sind.

In meinen Augen ist das das Interessante an den Grünen. Die Grünen produzieren nicht wirklich qualitativ hochwertige Inhalte: Sie posten in der Regel nicht häufig und haben auch sonst keinen regelmäßigen Posting-Zeitplan. Aber sie haben sich im Vergleich zu den etablierten Parteien besser eingebracht, was meines Erachtens mehr mit ihrer Politik als mit ihrem Auftritt zu tun hat.

Sam Jeffers: Man kann allerdings sehen, dass sie für die Größe ihrer Partei in Relation mehr Geld ausgegeben haben als andere Parteien.

Laura Edelson: Das hängt auch mit den Finanzierungsstrukturen der politischen Parteien in Deutschland zusammen. Die Tatsache, dass neuere Parteien (noch) nicht über eine große Mitgliederbasis verfügen, macht Online-Engagement mit dem Ziel der Spendensammlung nochmal wichtiger für diese Parteien.

Inwieweit konntet Ihr in eurem Projekt zur Bundestagswahl politische Online-Werbung untersuchen?

Laura Edelson: **Ich wurde am 2. August gesperrt. Das deutsche Ad Observatory sollte am Mittwoch, dem 4. August starten.**

Konntet Ihr die Daten analysieren?

Laura Edelson: Wir können aufgrund unserer Sperrung leider nur von Beobachtungen berichten. Die AfD hat in



Foto: Privat

Laura Edelson
Wissenschaftliche Mitarbeiterin
an der New York University

Sachen Werbung bessere Arbeit geleistet: die Partei produzierte qualitativ hochwertige Inhalte, ihre Strategie war insgesamt konsistenter. Interessant war auch, dass die AfD meines Wissens die einzige Partei war, die mittels Werbung um Spenden gebeten hat. Das ist interessant, da es nach meiner Kenntnis keinen rechtlichen Grund gibt, warum Parteien in Deutschland nicht auch über diesen Weg um Spenden werben sollten. Es ist nur eine soziale Norm, dass sie das nicht tun. Mich hat interessiert, inwieweit diese soziale Norm Bestand hat. Soweit ich das beurteilen kann, scheint sie mit Ausnahme der AfD eingehalten worden zu sein.

Wie kann es mehr Transparenz bei politischen Anzeigen geben, ohne die Privatsphäre der Nutzer:innen zu gefährden?

Laura Edelson: Anzeigen enthalten weder Namen der Nutzer:innen, noch andere persönliche Informationen. Anzeigen können und sollten daher öffentlich sein.

Sam Jeffers: Es gibt dieses eine, sehr spitzfindige Argument, das Facebook in Bezug auf Transparenz vorbringt: Wenn man eine Anzeige sieht und weiß, worauf sie abzielt und dann sieht, dass jemand unter der Anzeige kommentiert hat, kann man davon ausgehen, dass diese Person bestimmte Interessen angegeben hat.

Laura Edelson: Dieses Argument ist Blödsinn. Wenn man jemandem zeigt, wonach die Werbung ausgewählt wurde, kann die Person ebenfalls sehen, dass seine Freunde sie teilen oder kommentieren. Daher gibt es bei der Veröffentlichung von Informationen über die Zielgruppenansprache keine zusätzliche Verletzung der Privatsphäre.

Welche Herausforderungen gibt es beim Austausch von Daten zwischen Plattformen und Forscher:innen?

Laura Edelson: Es gibt ein ernstes Problem hinsichtlich Desinformationen, Hass und allgemein polarisierenden Inhalten auf Facebook. Bei Google ist es offen gesagt noch schlimmer im Hinblick auf die Transparenz. Daher muss es einen viel breiteren Zugang zu Tools

wie CrowdTangle geben. Vor allem brauchen wir Zugang zu Kommentaren.

Eine Sache, die Twitter und auch Google meiner Meinung nach richtig machen, ist, dass zum Beispiel Twitter eine Richtlinie für Werbung in sozialen Netzwerken hat: Personen können nur nach Geocode, Alter und Geschlecht angesprochen werden – wobei hier anzumerken ist, dass Twitter definitiv Probleme bei der Umsetzung der Richtlinie hat. Ich glaube, dass die Richtlinie aus der Tatsache resultiert, dass man kein Vertrauen in die eigenen Fähigkeiten hat, politische Anzeigen gründlich und verantwortungsvoll zu überprüfen. Ich wünschte, so würden sich mehr Plattformen verhalten: wenn man etwas nicht sicher gestalten kann, sollte man es lieber ganz lassen.

Es geht hier nämlich um mächtige „Werkzeuge“, wie Waffen oder Autos. Dabei haben wir die Regeln für den Straßenverkehr noch nicht hinreichend ausgearbeitet. Ich möchte nicht, dass Leute, die politische Anzeigen schalten, schon jetzt unglaublich schnelle Autos fahren, obwohl wir die Regeln für den Straßenverkehr nicht kennen. Das heißt nicht, dass es nie schnelle Autos geben darf. **Doch bis wir herausgefunden haben, wie diese Werkzeuge sicher eingesetzt werden können und sollten, denke ich, dass wir sie im Moment einfach ganz weglassen sollten.**

Welche Forderungen habt Ihr und welche Lösungen könnten sich daraus ergeben?

Sam Jeffers: Eine genaue Überprüfung der Werbetreibenden und eine angemessene Transparenz bei derartigen Überprüfungen.

Laura Edelson: Politische Werbetreibende, die eine bestimmte Größe überschreiten, sollten ein Due-Diligence-Verfahren durchlaufen müssen. Die Plattformen sollten für jeden großen politischen Werbetreibenden, der 10.000 € überschreitet, dieselben KYC-Anforderungen (Know Your Customer) stellen.

Zudem sollte die gesamte politische Werbung transparent bleiben und Journalist:innen, Akademiker:innen sowie unabhängigen gemeinnützigen Forscher:innen muss der Zugang zu CrowdTangle oder etwas Ähnlichem ermöglicht werden. Facebook sollte

zudem verpflichtet werden, offenzulegen, wie viel Geld sie für die Einhaltung der Gesetze in den verschiedenen Ländern ausgeben.

Eine Idee ist, dass Algorithmen von Dritten geprüft werden müssen, um sicherzustellen, dass sie keinen Schaden anrichten. Ähnlich wie Banken in den USA, die über eine FDIC-Versicherung verfügen, von einem externen Prüfer geprüft werden müssen.

Sam Jeffers: Wir versuchen auch, Moderationsmethoden in die Transparenzstandards zu integrieren. Bei jeder Anzeige sollte angegeben werden, ob sie von einem Menschen geprüft wurde oder nicht.

Eine weitere schwer umzusetzende Regel ist die Begrenzung der Anzahl der Anzeigen, die insgesamt geschaltet werden dürfen. Die FDP hat im letzten Monat in Deutschland ca. 2000 Anzeigen geschaltet. Wenige Anzeigen verringern den Anreiz, zahlreiche Daten zu sammeln und AB-Tests durchzuführen. Das würde einen großen Teil des Drucks nehmen. Wir sind zwar nicht für ein Verbot, aber wir versuchen sicherzustellen, dass Werbung auf eine verantwortungsvolle, weniger technikgetriebene Weise erfolgt.

Laura Edelson: In den USA haben wir auch das Problem, dass viele falsche oder verleumderische Inhalte verbreitet werden. Das habe ich hier in dem Ausmaß nicht gesehen, weil die Akteure in Deutschland meines Erachtens (noch) nicht so weit gehen wollen. Eine Idee wäre trotzdem, dass an die wiederholte Schaltung von Anzeigen mit falschen Informationen bestimmte Konsequenzen geknüpft werden.

*Mit dem Tool **Who Targets Me** lässt sich Transparenz in Geschäft der politischen Online-Werbung auf Facebook bringen, indem über 50.000 Menschen mittels Datenspende ihre Werbedaten mit der NGO teilen. www.whotargets.me/en*

New York University | Tandon School of Engineering: *Das Ad Observatory sollte ähnlich wie Who Targets Me politische Online-Werbung transparent offenlegen. Kurz bevor dem Start weigerte sich Facebook Daten mit dem Tool zu teilen. www.adobservatory.org*

Es gibt ein systemisches Problem im Werbesektor



Foto: Privat

Christian Bock
Senior Campaigner
bei SumOfUs

Was haben Sie im Rahmen der Bundestagswahl gemacht?

Wir haben untersucht, welche Firmen Anzeigen schalten auf Webseiten, die Desinformation, Hass und Hetze verbreiten. Das haben wir zusammen mit Reset und Global Disinformation Index gemacht. Die Leute von GDI schauen sich Webseiten an, auf denen Desinformationen und Hassrede verbreitet werden. Da geht es um antisemitische oder rassistische Inhalte, die Leugnung des Klimawandels bis hin zu Desinformation bezüglich der Bundestagswahl oder der Verunglimpfung von Parteien und Kandidierenden.

Das ist die ganze Bandbreite des rechten bis rechtsextremen und verschwörungsmythischen Reichsbürger:innen-Spektrums. Welche Werbung ist auf diesen Webseiten platziert? **Es zeigte sich, dass erstaunlich viele große Unternehmen, auch sehr viele deutsche bis hin zu Dax-Unternehmen wie Allianz, BMW oder Deutsche Bank, auf diesen Webseiten Werbung schalten.**

Warum?

Die machen das zumeist nicht selber und gezielt. Sondern es läuft über Agenturen, die Anzeigenpakete schalten. Vermutlich beauftragt die Marketingabteilung eines Unternehmens so eine Agentur. Die arbeiten häufig über sogenannte AdTech-Firmen, Google hat beispielsweise eine hauseigene AdTech-Firma oder auch der Springer-Verlag. Die platzieren dann diese Banner auf Webseiten und die Unternehmen kriegen das gar nicht mit.

So kommt es vor, dass beispielsweise ein großes Unternehmen zum Pride Month sein Logo in Regenbogenfarben einfärbt, aber gleichzeitig Werbung

schaltet auf Webseiten, in denen LGBTQ+-feindliche Inhalte verbreitet werden. Also haben wir eine Kampagne gestartet, um die Unternehmen darauf hinzuweisen und davon abzubringen, weiter Werbung auf solchen Seiten zu schalten.

Wussten die Verantwortlichen davon?

Wir sind erst mal wohlwollend davon ausgegangen, dass die Unternehmen das nicht mit Absicht machen. Also haben wir die Konzerne angeschrieben und sie darauf hingewiesen, ihnen auch die Nachweise gezeigt und dann die Forderungen der Kampagne gezeigt. Die niedrigschwelligste Forderung war, dass sie doch bitte diese Werbung umgehend da runternehmen sollen.

Wie haben die Unternehmen reagiert?

Der Großteil hat relativ rasch geantwortet und sich bedankt für den Hinweis und betont, dass es nicht mit den eigenen Werten d'accord geht. Sie würden nun ihre Blocklisten genauer unter die Lupe nehmen. Blocklisten versammeln die Webseiten, auf denen sie Werbung nicht schalten wollen. Die müssen regelmäßig aktualisiert werden. Also, sorry, is wohl durchgerutscht, wir ändern das. Das gab es relativ häufig. Aber einige Unternehmen haben gar nicht reagiert. Erst nachdem wir die Geschichte dem SPIEGEL gegeben haben.

Und damit ist die Sache erledigt?

Nein! Wir können und wollen ja nicht den ganzen Tag damit verbringen, die Recherchearbeit der Unternehmen zu übernehmen. Das ist ja ein systemisches Problem innerhalb des Werbesektors. Daher ist das nächste Ziel, das auch

auf einer systemischen Ebene anzugehen. Das wären eine Selbstverpflichtung des Zusammenschlusses der Werbeindustrie und der Werbetreibenden oder eine gesetzliche Regulierung und Zwangsverpflichtung über den Digital Services und den Digital Markets Act auf EU-Ebene.

Hat nicht der Verein der Werbeindustrie, GARM, schon eine Liste mit problematischen Inhalten, wo keine Werbung geschaltet werden sollte?

Ja, in GARM sind viele große Unternehmen und auch Plattformen, auf denen Werbung geschaltet wird. Aber bislang gilt Desinformation noch nicht als problematische Kategorie von Inhalten. Das wollen wir erreichen.

Können die genau eingrenzen, was Desinformation ist?

Wie das im Einzelfall dann gemacht wird, da bin ich ehrlich gesagt in der technischen Umsetzung auch überfragt. Ich kann mir vorstellen, dass es über bestimmte Schlüsselwörter funktioniert. So arbeitet auch GDI.

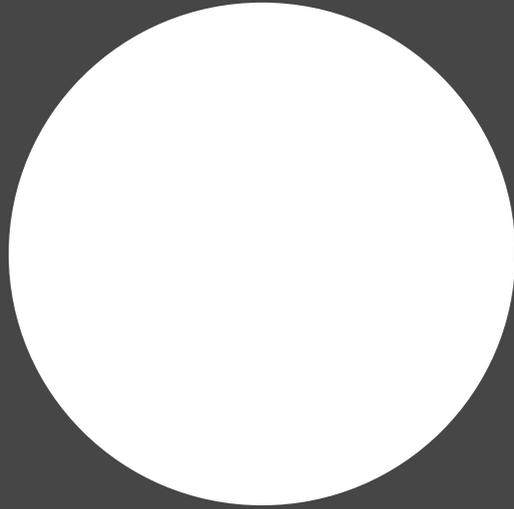
Haben euch die Ergebnisse überrascht, die ihr zu Tage gefördert habt?

Zynische Antwort: Auch im Netz ist man von nichts mehr überrascht. Aber wir staunen, dass Desinformation nicht als Problem wahrgenommen wird in dieser Industrie. Welche fatalen Auswirkungen Desinformation hat, konnte man spätestens im Zusammenhang mit der letzten US-Präsidentenwahl sehen, als Falschinformationen und Aufhetzerei dazu führten, dass Rechtsterroristen das Capitol stürmten. Spätestens da muss eigentlich für alle ersichtlich geworden sein, wie groß die Gefahr für die Demokratie ist, wenn auf Druck der großen Plattformen, die da daran verdienen, nicht ernsthaft vorgegangen wird gegen Falsch- und Desinformation.

Muss man sich da nicht international vernetzen?

Unbedingt! Das Internet ist international, die großen Unternehmen operieren international und auch die Regelungen und ethischen Kodizes müssten es sein. Das war nur ein Anfang und man muss überall an die Parteien herantreten und die Selbstverpflichtung zu einem fairen digitalen Wahlkampf einfordern. Das hat in Deutschland schon ganz gut geklappt. Wenn auch nicht auf ganzer Linie. Manche haben sich bitten lassen und die AfD reagierte gar nicht.

Die Kampagnenorganisation **SumOfUs** versucht ein Gegengewicht zur wachsenden Macht von Unternehmen zu setzen. Während des Wahlkampfes setzte sie sich u. a. dafür ein, das weniger Werbung von deutschen Unternehmen auf verschwörungsgläubigen Webseiten landet. sumofus.org



II

Rechtliche Einführung

Welche Rechtsnormen in der
Netzkommunikation gelten

Normen der Netzkommunikation:

Der Rechtsrahmen der Plattformen

Ein Raum des Rechts

Von wegen rechtsfreier Raum: Die Aktivitäten auf und von Online-Plattformen stehen im Mittelpunkt regulatorischer Veränderungen, die den Beginn einer neuen Regulierungsphase des Internets markieren. Sowohl Gerichte als auch Gesetzgeber formen die Pflichten und Rechte von Nutzer:innen und Plattformen neu. Die EU ist besonders aktiv bei der Regulierung des digitalen Raumes und hat einige ambitionierte Gesetzesvorhaben gestartet. Doch auch wenn diese Vorhaben gewichtige Probleme lösen wollen, bleiben Schwachstellen und Regelungslücken. Um diese identifizieren zu können, bietet dieses Kapitel einen kurzen Überblick über die aktuellen Entwicklungen von Rechtsprechung und Gesetzgebung rund um die Position der Online-Plattformen.

Rechtsprechung

Der BGH urteilte Ende Juli 2021, dass Plattformen im Rahmen ihrer Nutzungsbedingungen auch legale Inhalte verbieten können. Die Netzwerke können die Grenze des auf ihrer Plattform Erlaubten enger ziehen als der Staat, weil die Sanktionen der Netzwerke deutlich weniger schwer wiegen als beispielsweise staatliches Strafrecht. Allerdings müssten sich die Netzwerke ihrer besonderen Bedeutung für die öffentliche Meinungsbildung und -äußerung entsprechend verhalten. Dieser Sonderrolle müssten sie in der Form Rechnung tragen, dass sie die von Moderationsentscheidungen betroffenen Nutzer:innen informieren und die Möglichkeit der Stellungnahme einräumen. Der BGH verdeutlichte damit die Bedeutung der Netzwerke für die Meinungsbildungs- und Meinungsäußerungsfreiheit und gab zu erkennen, dass solcher Verantwortung im Rahmen legaler Inhalte, nur durch grundrechtewahrende Verfahren genügt werden kann.¹ Eine ähnliche Begründung liefert das LG Köln in einer am 11.10.2021 ergangenen Eilentscheidung über zwei Videos auf YouTube. Die Videos der Aktion „#allesaufdeutsch“, setzten sich unter anderem mit der Coronapolitik auseinander. Kritiker:innen werfen der Aktion die Verbreitung von

Verschwörungsmythen vor. Das LG Köln entschied im Rahmen des Verfahrens zum vorläufigen Rechtsschutz, dass die zwei Videos wieder zugänglich gemacht werden müssen. Als Begründung nannte das Gericht die fehlende Erklärung der Maßnahmen. YouTube hätte den Betroffenen im Rahmen der Löschung deutlich machen müssen, welche Teile des Videos genau Grund für die Löschung waren und gegen welche Nutzungsbedingungen diese Teile verstoßen würden. Eine pauschale „Begründung“, das gesamte Video verstoße gegen die Nutzungsbedingungen, sei insbesondere bei längeren Videos problematisch. Mit der Löschung des gesamten Videos würden auch zulässige Teile entfernt.

Ebenfalls weichenstellend war der Beschluss des Bundesverfassungsgerichts zum Account der rechtsextremen Partei „III. Weg“. ² Facebook löschte das Profil der Partei wegen Verstößen gegen Strafgesetze und Nutzungsbedingungen. Das BVerfG entschied im Eilverfahren, dass Facebook bis zur Europawahl 2019 die Seite wieder verfügbar machen müsse. Dies begründete das BVerfG mit den umfassenden Rechtsfragen bezüglich des Verhältnisses der Partei als Nutzerin und dem Netzwerk und der Rolle der Grundrechte der Partei in diesem Verhältnis. Die Folgen einer aufrechterhaltenen Sperre der Partei auf Facebook wögen schwerer als die Aufhebung der Sperre bis zur Europawahl, entschied das BVerfG 2019. 2021 wiederholte sich der Fall in gleicher Konstellation. ³ Diesmal entschieden sowohl das BVerfG als auch das Pfälzische Oberlandesgericht, dass die Partei keinen Anspruch auf Wiederherstellung des Profils auf Facebook habe. Dies lag jedoch an der fehlerhaften Zuordnung der Partiseite an eine Privatperson.

Gesetzlicher Rahmen der Plattformkommunikation

Neben diesen wegweisenden Gerichtsentscheidungen wurde auch der gesetzliche Rahmen für Plattformen in Deutschland und der EU ausgeweitet bzw. soll demnächst ausgeweitet werden. National geschah dies vor allem durch das NetzDG aus dem Jahr 2017 und den neuen MStV aus dem Jahr 2020.

¹BGH, Urteile vom 29. Juli 2021 – III ZR 179/20 und III ZR 192/20

²Bundesverfassungsgericht - Presse - Verpflichtung zur Entsperrung eines Facebook-Accounts im einstweiligen Rechtsschutz.

³<https://www.zeit.de/news/2021-09/22/iii-weg-ohne-anspruch-auf-entsperrung-von-facebook-seite>.

● Rechtliche Einführung

NetzDG

Am 1. Oktober 2017 trat das Netzwerkdurchsetzungsgesetz (NetzDG) in Kraft. Das Gesetz soll die Durchsetzung staatlichen Rechts in sozialen Netzwerken mit mindestens zwei Millionen im Inland registrierten Nutzer:innen verbessern und zur konsequenten Löschung strafbarer Inhalte führen. Hintergrund war die zunehmende Verbreitung illegaler Inhalte im digitalen Raum und die Erfahrungen aus dem US-Wahlkampf 2016.⁴

Kern des NetzDG ist die Pflicht für soziale Netzwerke, „offensichtlich rechtswidrige Inhalte“ nach Meldung durch Nutzer:innen binnen 24 Stunden entfernen zu müssen. „Rechtswidrige Inhalte“ müssen nach 7 Tagen von der Plattform gelöscht werden. Außerdem müssen die Netzwerke Beschwerdemöglichkeiten einrichten und regelmäßig einen Bericht über die erfolgten Löschungen nach dem NetzDG veröffentlichen.

Allerdings müssen Inhalte nach dem NetzDG nur dann gelöscht werden, wenn durch die Veröffentlichung bestimmte Straftaten begangen wurden. § 1 Abs. 3 NetzDG nennt unter anderem die Aufforderung zur Straftat, die Beleidigung oder das Verbreiten von Zeichen verfassungsfeindlicher Organisationen. Insbesondere Desinformationen erfüllen allerdings selten den Tatbestand solcher Straftatbestände.

2021 wurde das NetzDG im Rahmen des Gesetzespakets zur Bekämpfung von Rechtsextremismus und Hasskriminalität ergänzt. Nun müssen die Netzwerke sowohl den gemeldeten Inhalt als auch die Daten der verantwortlichen Nutzer:innen an das Bundeskriminalamt (BKA) weiterleiten. Gewichtige Gründe sprechen allerdings dafür, dass diese im Februar 2022 in Kraft tretende neue Pflicht nicht verfassungskonform sein könnte. Vor allem ist die Hürde, wann die Netzwerke die Daten an das BKA übermitteln müssen, sehr niedrig.

Medienstaatsvertrag

An die Stelle des alten Rundfunkstaatsvertrages (RStV) trat am 7. November 2020 der Medienstaatsvertrag (MStV). Mit diesem soll der rechtliche Rahmen an die fortschreitende Digitalisierung der Medienlandschaft angepasst werden.⁵ Wie schon der neue Name des Staatsvertrages verrät, ist der auf den Rundfunk fokussierte Medienbegriff des alten RStV durch einen neuen Begriff ersetzt worden. § 2 Nr. 14 MStV führt den Begriff „Medienplattform“ ein. Dieser umfasst alle Dienste, die mediale Inhalte zu einem Gesamtangebot aufarbeiten, unabhängig von der verwendeten Technologie.

Daneben umfasst der MStV auch sog. Medienintermediäre (§ 2 Nr. 16 MStV), welche ohne Zusammenfassung zu einem Gesamtangebot auch journalistisch-redaktionelle Inhalte sortieren und allgemein zugänglich präsentieren. Darunter fallen bspw. Suchmaschinen oder soziale Netzwerke.⁶

Ein Ziel des MStV ist es, Meinungsvielfalt und kommunikative Chancengleichheit in der Medienlandschaft sicherzustellen.⁷ Erreicht werden soll dieses Ziel durch umfassende Pflichten für Medienintermediäre, soweit sie einen Einfluss auf die öffentliche Meinungsbildung haben.⁸ In diesem Fall sind sie unter anderem zur Offenlegung der Funktionsweise ihrer Algorithmen verpflichtet und dürfen diese nicht so festlegen, dass einzelne journalistisch-redaktionelle Inhalte systematisch und ohne Rechtfertigung benachteiligt werden (§§ 93 Abs. 1, 94 Abs. 1). Auch müssen Social Bots als solche gekennzeichnet werden (§ 18 Abs. 3). Die Prüfung von Verstößen liegt bei den Landesmedienanstalten, die Anzeigen für vermutliche Verstöße von Medienintermediären erhalten können.

● *Vincent Hofmann und Matthias C. Kettemann*

⁴Vgl. BT-Drs. 18/12356, S. 1, <http://dipbt.bundestag.de/dip21/btd/18/123/1812356.pdf>.

⁵BeckOK InfoMedienR/Martini, MStV Präambel, Rn. 43.

⁶Vgl. Intermediäre, <https://www.die-medienanstalten.de/themen/intermediaere>.

⁷Vgl. Begr. zum MStV, LT-Drs. N 18/6414, 89, https://www.landtag-niedersachsen.de/drucksachen/drucksachen_18_07500/06001-06500/18-06414.pdf.

⁸BeckOK InfoMedienR/Martini, MStV Präambel, Rn. 45, <https://beck-online.beck.de/Bcid/Y-400-W-BECKOKINFOMEDIEN-G-MSTV-NAME-PRAEAMBEL-GI-C>.



Europäischer Rechtsrahmen

Neben den nationalen, bereits erlassenen Gesetzen, stehen einige europäische Regulierungsvorhaben in den Startlöchern.

Europäischer Aktionsplan für Demokratie

Der Europäische Aktionsplan für Demokratie ist ein im Dezember 2020 vorgestelltes Rahmenprojekt der EU-Kommission. Dieses hat die Stärkung der Zivilgesellschaft und den krisenfesteren Ausbau der europäischen Demokratien zum Ziel. Diese Ziele sollen durch mehrere Verordnungen und Maßnahmen erreicht werden, welche in drei Teilbereiche untergliedert sind: Förderung freier und fairer Wahlen, Ausbau der Medienfreiheit und Bekämpfung von Desinformation.

Eine wichtiger Bestandteil sollen Legislativvorschläge zur Gewährleistung von mehr Transparenz bei gesponserten politischen Inhalten („politische Werbung“) sein, flankiert von entsprechenden Unterstützungsmaßnahmen und Leitlinien für politische Parteien und Mitgliedstaaten.

Digital Services Act (DSA)

Am 15. Dezember 2020 stellte die EU-Kommission ihren Entwurf des Digital Services Act (DSA) vor. Der DSA soll als Nachfolger der E-Commerce Richtlinie einen Beitrag zu einer sicheren und vertrauenswürdigen Online-Kommunikation in Form einer EU-Verordnung leisten (Art. 1 Abs. 2 lit. b).⁹

Der Entwurf des DSA sieht insbesondere für Online Plattformen weitreichende Änderungen vor. Online Plattformen sind Dienste, welche Inhalte von Nutzer:innen speichern und öffentlich verbreiten. Darunter zählen Marktplätze oder Soziale Netzwerke. Diese haften dem Entwurf nach unverändert für illegale Inhalte, sobald sie von diesen Kenntnis erlangen. Um eine solche Kenntniserlangung zu ermöglichen, muss ein effizientes Beschwerdemanagement gewährleisten, dass Meldungen über mutmaßlich illegale Inhalte schnell und zuverlässig bearbeitet werden. Hier lassen sich Ähnlichkeiten zum deutschen NetzDG erkennen.¹⁰ Auch sollen die Transparenzpflichten ausgeweitet werden: Diese müssen unter anderem einen jährlichen Bericht über die erfolgten Modera-

tionsmaßnahmen veröffentlichen. Art. 24 des Entwurfs enthält die Verpflichtung der Online-Plattformen, Informationen über die angezeigte Online-Werbung transparent zu gestalten. Für den Nutzer soll bei jeder einzelnen Werbung klar, eindeutig und in Echtzeit erkennbar sein, ob und wessen Werbung angezeigt wird. Zudem müssen die wichtigsten Parameter für die Bestimmung der Zielgruppe einsehbar sein. Damit soll personalisierte Werbung und insbesondere das zu Wahlkampfzwecken genutzte, kontrovers diskutierte Microtargeting transparenter werden.

Noch weitergehende Pflichten sieht der Entwurf des DSA für „Very Large Online Platforms“ (VLOPs) vor. Darunter werden „systemrelevante“ Plattformen mit mind. 45 Mio. monatlichen aktiven Nutzern in Europa verstanden. Die Kommission misst solchen Plattformen einen besonderen Einfluss auf öffentliche Debatten zu und sieht in ihnen wichtige Informationsquellen im Rahmen öffentlicher Meinungsbildung. Ebenfalls sieht die Kommission Risiken in der Reichweite dieser Plattformen, wie die Verbreitung illegaler Inhalte, Manipulationen oder Einschränkungen bei der Grundrechtsausübung, insbesondere der freien Meinungsäußerung.¹¹ Der DSA sieht mögliche Maßnahmen zur Minimierung dieser Risiken vor, z. B. die öffentlich zugängliche Archivierung aller geschalteten Werbeanzeigen (Art. 30), eine verstärkte Inhaltsmoderation (Art. 27) sowie die Pflicht zur jährlichen Durchführung einer unabhängigen Prüfung, ob die Vorgaben aus dem DSA eingehalten wurden (Art. 28).¹²

Die Themen Fake News und Desinformation, sofern sie nicht ohnehin unter illegale Inhalte fallen, sind in der DSA hingegen kaum geregelt.¹³

Digital Markets Act (DMA)

Der gleichzeitig mit dem DSA vorgestellte Entwurf des Digital Markets Act (DMA) richtet sich gegen die Geschäftspraktiken so genannter Gatekeeper. Dies sind Unternehmen, welche

⁹Europäische Kommission, 2020/0361 (COD), S. 49, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0825&from=de>.

¹⁰Berberich/Seip, Der Entwurf des Digital Service Act, GRUR-Prax 2021, 4 (5), <https://beck-online.beck.de/Bcid/Y-300-Z-GRURPRAX-B-2021-S-4-N-1>.

¹¹Ibid

¹²Europäische Kommission, 2020/0361 (COD), S. 68, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0825&from=de>.

¹³Berberich/Seip, Der Entwurf des Digital Service Act, GRUR-Prax 2021, 4 (7), <https://beck-online.beck.de/Bcid/Y-300-Z-GRURPRAX-B-2021-S-4-N-1>.

● Rechtliche Einführung

eine große Zahl von Kund:innen mit einer großen Zahl von Unternehmen zusammenbringen und einen signifikanten Einfluss auf den EU-Binnenmarkt über eine gewisse Dauer ausüben (Art. 3 Abs. 1 DMA-E). Dazu zählen auch die im Rahmen der Meinungsbildung zu politische Wahlen besonders relevanten sozialen Netzwerke. Die großen Netzwerke genießen ihre Vormachtstellung insbesondere durch die enormen Datenmengen ihrer Nutzer:innen, welche ihnen ein optimales Produktangebot ermöglichen. Um diese datenbasierte Vormachtstellung aufzulösen, sollen Gatekeeper in der Verwendung der Daten beschränkt und zur Weitergabe der Daten verpflichtet werden. So dürfen u. a. die von gewerblichen Nutzer:innen gewonnenen Daten nicht im Wettbewerb mit diesen Nutzer:innen verwendet werden. Auch müssen Daten zum Verhalten von Kund:innen in Zukunft an die Unternehmen weitergereicht werden, welche das Produkt verkauft haben.

und sozial abträglich und transparent die Sichtbarkeit genommen werden und die normative Vormachtstellung einiger weniger Konzerne durch Verfahrens- und Transparenzregeln reduziert werden. Die Nutzer:innen sollen wissen, welche Standards gelten, wie diese umgesetzt werden und wie sie sich gegen Löschungen wehren können. Dies sichert die Grundrechte der Nutzer:innen und wahrt das demokratische und demokratisierende Potential der Onlinekommunikationsräume.

● *Vincent Hofmann und Matthias C. Kettemann*

Data Governance Act (DGA)

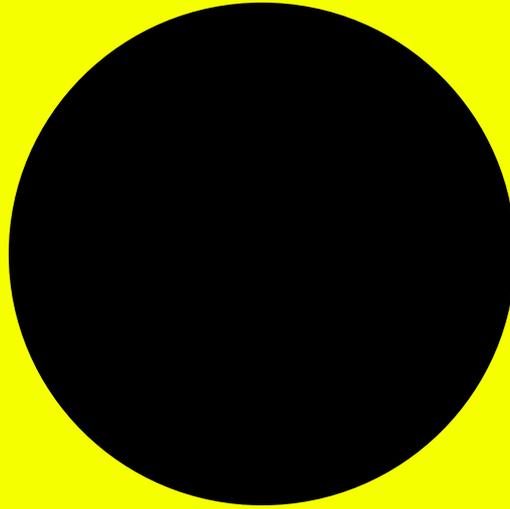
Der seit 2018 durch die Datenschutzgrundverordnung (DSGVO) gestärkte Datenschutz brachte neben seinen Vorteilen für Verbraucher:innen auch bedeutende Hemmnisse für Unternehmen. So gaben 2020 in einer Umfrage des Branchenverbandes Bitkom gut die Hälfte der befragten Unternehmen an, durch die DSGVO in ihrer Innovationskraft beschränkt zu sein.¹⁴ Die mit der DSGVO einhergehenden Erschwernisse sollen durch den Data Governance Act (DGA), dessen überarbeitete Fassung Anfang Dezember 2021 vorgestellt werden wird, vermindert werden. Unter Wahrung der Standards der DSGVO soll insbesondere das Vertrauen der Nutzer:innen in die Sicherheit der Verarbeitungsprozesse personenbezogener Daten gestärkt und so die Möglichkeit zur Datenverwendung durch Unternehmen und Forschungseinrichtungen erhöht werden.¹⁵

Fazit

Auch wenn insbesondere die europäischen Gesetzesvorhaben als durchaus ambitioniert bezeichnet werden können, ist das Verhältnis zu den nationalen Netzregeln, wie dem NetzDG, und den Regelungen auf Landesebene, wie dem MStV, teilweise noch unklar. Dabei steht mit den Regulierungsvorhaben einiges auf dem Spiel. Nur mit ausgereiften Normen kann das Regelungsziel der neuen Gesetze erreicht werden: Rechtswidrige Inhalte sollen vom Netz genommen

¹⁴Bitkom, "Jedes 2. Unternehmen verzichtet aus Datenschutzgründen auf Innovationen,, <https://www.bitkom.org/Presse/Presseinformation/Jedes-2-Unternehmen-verzichtet-aus-Datenschutzgruenden-auf-Innovationen>.

¹⁵Europäische Kommission, "Proposal for a Regulation on European Data Governance (Data Governance Act,, <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-data-governance-data-governance-act>.



III

Für ein besseres Internet morgen – Handlungsoptionen für heute

Das Leibniz-Institut für Medienforschung | Hans-Bredow-Institut hat den Prozess der Sammlung der folgenden Handlungsoptionen koordiniert. Die unten genannten Organisationen haben mit ihren Forschungen zur Identifikation der Handlungsoptionen beigetragen. Eine Nennung bedeutet nicht, dass die Organisation alle Optionen unterstützt.

**CYBERSECURITY
FOR DEMOCRACY**

Stiftung
Neue
Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

**DEMOCRACY
REPORTING
INTERNATIONAL**

**Hate
Aid**

**CARDIFF
UNIVERSITY**
Crime and Security
Research Institute
Sefydliad Ymchwil
Trosedd a Diogelwch

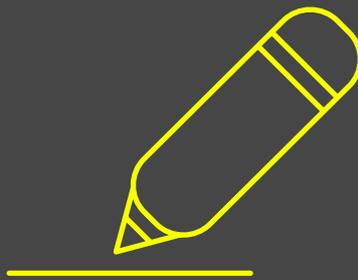
**COUNTER
EXTREMISM
PROJECT**

ISD Institute
for Strategic
Dialogue

NRW School of Governance
www.nrw-school.de

I.

*Einsatz für
eine ambitionierte
Ausgestaltung des Digital
Services Act der EU*



● 10 Handlungsoptionen für heute

Effektive Durchsetzung durch die Einführung einer starken europäischen Plattformaufsicht mit Sitz in Brüssel.

Bisher sieht der Entwurf des DSA eine Aufgabenteilung bezüglich der Plattformaufsicht vor. Hauptsächlich zuständig sind die nationalen Koordinator:innen für digitale Dienste. Diese bilden zusammen das Europäische Gremium für digitale Dienste nach Art. 47 DSA-E, welches jedoch nur koordinierend und unterstützend tätig ist. Die Kommission darf bei sehr großen Online Plattformen („very large online platforms“, VLOP) zwar einschneidende Maßnahmen wie Befragung oder Überwachung einleiten sowie Buß- und Zwangsgelder verhängen. Dies kann jedoch erst erfolgen, wenn der nationale Koordinator erfolglos zum Einschreiten aufgefordert wurde. Am Beispiel der irischen Datenschutzbehörden haben wir sehen müssen, dass dies nicht ausreicht.

Sinnvoll erscheint: die Umkehr der bisher vorgesehenen Systematik dahingehend, dass primär ein europäischer Koordinator für digitale Dienste für die Plattformaufsicht zuständig ist, welcher mit Unterstützung von hierarchisch untergeordneten nationalen Koordinator:innen agiert.

Einführung verpflichtender, unabhängiger Folgenabschätzungen für Plattformen hinsichtlich ihrer Auswirkungen auf Menschenrechte und Aufnahme von Geschlechtergleichheit, Diskriminierungsfreiheit und Jugendschutz als explizite Schutzziele in die Risikobewertungen

Bisher sieht Art. 26 Abs. 1 lit. b DSA-E für VLOP eine verpflichtende Risikobewertung vor. Diese umfasst direkt oder über einen Verweis auf die entsprechenden Normen der EU-Grundrechtecharta Geschlechtergleichheit, Diskriminierungsfreiheit und Jugendschutz. Ein allgemeiner Verweis auf die Verpflichtung zur Achtung der Menschenrechte fehlt. Im Gegensatz zur Überprüfung nach Art. 28 kann die Risikobewertung von den Netzwerken selbst durchgeführt werden. Eine unabhängige Stelle muss hier nicht eingeschaltet werden.

Sinnvoll erscheint: Art. 26 DSA-E dahingehend zu ändern, dass die Folgenabschätzung wie die Überprüfung nach Art. 28 von unabhängigen Stellen durchgeführt wird und diese Stellen darüber hinaus (siehe Forderung 1) g) nicht von den Netzwerken beauftragt werden dürfen. Der Katalog der Risikoabwägung sollte um die allgemeine Formulierung „und die Rechte der EU-Grundrechtecharta“ ergänzt werden.

Verpflichtung von Online-Plattformen zum Einsatz ihrer AGB zum Schutz der Nutzer:innen.

Bisher kann man als Nutzer:in Social-Media-Plattformen nicht dazu bringen, ihre eigenen Gemeinschaftsstandards durchzusetzen und beispielsweise Profile von (gewaltorientierten) extremistischen Akteuren oder Hass-Organisationen zu löschen, solange diese keine Straftaten (nach NetzDG) auf der Plattform verüben. Social-Media-Plattformen brechen somit ein „Schutzversprechen“, dass sie ihrerseits in den AGBs formulieren. Der Entwurf des DSA eröffnet die Möglichkeit, dass Social-Media-Plattformen ihre AGB auch zum Schutz ihrer Nutzer durchsetzen müssen. Art. 12 Abs. 2 regelt, dass Anbieter bei Anwendung ihrer vertraglichen Regelungen „sorgfältig“ und u. a. „objektiv“ vorgehen müssen.

Sinnvoll erscheint: die Klarstellung, dass die Regelungen auch „effektiv“ zum Schutz der Nutzer:innen anzuwenden sind.

Beibehaltung der Risikokategorie der vorsätzlichen Manipulationen der Dienste sehr großer Plattformen mit nachteiligen Auswirkungen u. a. auf die gesellschaftliche Debatte, Wahlprozesse und öffentliche Sicherheit (Art. 26 Abs. 1 lit c DSA-E).

Haftung für algorithmisch empfohlene illegale und schädliche Inhalte

Bisher Der DSA-E sieht vor, „Soziale Medien“ und Videosharing Plattformen weiterhin von der Haftung für Nutzer:innen generierte schädliche oder illegale Inhalte freizustellen, selbst wenn diese Inhalte von den Plattformen an andere Nutzer:innen empfohlen werden. Insbesondere bei Gatekeeper-Plattformen wird jedoch jede Form von Content auf die Verwertbarkeit für kommerzielle Zwecke hin analysiert (content recognition systems). Die großen Plattformen wissen also das, was sie wissen wollen.

Sinnvoll erscheint: den DSA-E dahingehend anzupassen, dass Unternehmen die a) content recognition systems einsetzen und b) Nutzer:innen generierte Inhalte anderen Nutzer:innen empfehlen, für die Empfehlung illegaler und schädlicher Inhalte haftbar gemacht werden können (Aktive Rolle).

● 10 Handlungsoptionen für heute

Einbeziehung von unabhängigen Expert:innen der Zivilgesellschaft und Wissenschaft in die Erarbeitung von Risikominderungsmaßnahmen sehr großer Plattformen diese sollten ausdrücklich Maßnahmen zur verbesserten sachlichen wie personellen Ausstattung der Moderations- und Sicherheitsteams sowie zur Beschränkung von irreführenden und entmächtigenden Designmerkmalen einbeziehen.

Bisher ist der Katalog in Art. 27 Abs. 1 DSA-E als „kann“-Vorschrift formuliert und sieht entsprechend lediglich eine Empfehlung, aber keine Pflicht zur Ergreifung bestimmter Maßnahmen vor (das Ergreifen von Maßnahmen ist verpflichtend).

Sinnvoll erscheint: dass Art. 27 Abs. 1 DSA-E derart umgestaltet wird, dass die VLOP auf Maßnahmen zur verbesserten sachlichen wie personellen Ausstattung der Moderations- und Sicherheitsteams sowie zur Beschränkung von „Deceptive Patterns“, irreführender Designmerkmale nur dann verzichten dürfen, wenn dies durch Erkenntnisse der Risikobewertung gerechtfertigt ist. Die Bewertung und Erarbeitung von Abhilfemaßnahmen muss unter Einbeziehung von Expert:innen der Zivilgesellschaft und Wissenschaft unter ethischen Gesichtspunkten erfolgen.

Einbeziehung zusätzlicher Informationen in Transparenzberichte wie Auskünfte zur Dauer und Intensität der Exposition gegenüber Desinformation und illegalen Inhalten.

Bisher umfassen die Vorgaben für die Transparenzberichte nach Art. 13 Abs. 1 DSA-E nur die Pflicht zur Offenlegung der Art der Maßnahme und der Dauer bis zum Ergreifen der Online-Plattform.

Sinnvoll erscheint: dass Plattformen verpflichtet werden, präzisere Daten zur Inhalte-Moderation herauszugeben. Auskünfte zur Dauer und Intensität der Exposition gegenüber (und des Engagements mit) Desinformation und illegalen Inhalten sollten in den Katalog in Art. 13 Abs. 1 DSA-E aufgenommen werden.

Risikobasierte Ausweitung der Risikobewertungen und Transparenzkriterien hinsichtlich Empfehlungssystemen auf kleinere Plattformen, sofern potentiell größere Auswirkungen, insbesondere auf Wahlen, vorliegen.

Bisher differenziert der DSA nur nach der Größe der Plattformen. Diese werden je nach Zahl der Nutzer:innen stärker oder schwächer reguliert.

Sinnvoll erscheint: Die starren, an der Zahl der Nutzer:innen orientierten Grenzen im DSA werden der tatsächlichen Bedrohungslage nicht gerecht. Dieses System der differenzierten

Regulierung sollte durch ein durchlässiges System ergänzt werden, welches auf von unabhängigen Stellen durchgeführten Risikoanalysen fußt.

Wahrung der Unabhängigkeit von Audits, indem prüfende Stellen vom geplanten Europäischen Rat für digitale Dienste beauftragt werden.

Bisher sieht Art. 28 Abs. 1 DSA-E für VLOP vor, dass diese einen jährlichen Bericht durch eine unabhängige Stelle erstellen lassen. Diese Stelle wird durch die VLOP selbst bestellt und bezahlt.

Sinnvoll erscheint: Um die Abhängigkeit der prüfenden Stelle von der zu prüfenden Plattform zu reduzieren, muss die Vergabe der Prüfungsaufträge durch den nationalen Koordinator für digitale Dienste oder das Europäische Gremium für digitale Dienste erfolgen.

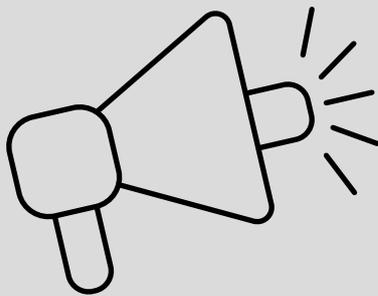
Einführung einer verpflichtenden Programmierschnittstelle sehr großer Plattformen zur Datenbereitstellung für Untersuchungen systemischer Risiken durch unabhängige Expert:innen aus Wissenschaft, Medien und Zivilgesellschaft – dabei sollten auch Kommentare unter Beiträgen unter Einhaltung des Datenschutzes zugänglich werden.

Bisher sieht der DSA zwei Arten der Pflicht zur Datenbereitstellung vor. In Art. 31 Abs. 2 ist die Pflicht zur Bereitstellung von Daten auf Verlangen der Koordinator:innen für digitale Dienste geregelt. In Art. 31 Abs. 4 ist geregelt, dass zugelassenen und mit akademischen Einrichtungen verbundene Forscher:innen Zugang zu Daten erhalten können. Welche Daten dies genau sind und welche Hürden Forscher:innen für die Zulassung nehmen müssen, ist noch nicht geregelt. Dies wird nach Art. 31 Abs. 5 in delegierten Rechtsakten erfolgen, sprich nachträglich ausgestaltet werden.

Sinnvoll erscheint: Art. 31 DSA-E muss um die Pflicht für VLOP zur Einführung einer technischen Schnittstelle für Forscher:innen ergänzt werden. Es muss klargestellt werden, dass auch Kommentare unter Beiträgen unter Einhaltung des Datenschutzes über die Schnittstelle erreichbar sein müssen. Ebenfalls muss die Anforderung des Anschlusses an eine akademische Einrichtung geändert werden, sodass auch Medien und Zivilgesellschaft erfasst sind. Gleichzeitig muss der Datenschutz gewahrt werden. Die Anträge auf Zugänge müssen daher detaillierte und glaubwürdige Angaben über die Notwendigkeit des Zugangs, das bestehende Datenschutzkonzept und den Nachweis über die Fähigkeit zur Umsetzung enthalten.

II.

Einsatz für ambitionierte Rechtsvorschriften der EU zu Transparenz in der politischen Werbung



● 10 Handlungsoptionen für heute

Einführung klarer Definitionen und verbesserter Transparenzregeln.

Bisher sieht Art. 24 DSA-E gewisse Transparenzpflichten für Online-Werbung vor. Dies umfasst den Umstand, dass es sich um bezahlte Werbung handelt, von wem diese bezahlt wird und die „wichtigsten Parameter“, welche zur Auswahl der Werbung für die einzelne Nutzer:in geführt haben. Insbesondere Art. 24 lit. c enthält die sehr unbestimmte Formulierung „aussagekräftige Informationen über die wichtigsten Parameter“. Sowohl das Merkmal „aussagekräftig“ als auch „wichtigste Parameter“ sind sehr weich formuliert und dürften zu einem Leerlaufen der Vorschrift führen.

Sinnvoll erscheint: Die Begriffe aus Art. 24 DSA-E müssen geschärft werden, um die Grenze einer zu allgemeinen „Erklärung“ der Parameter zu verhindern.

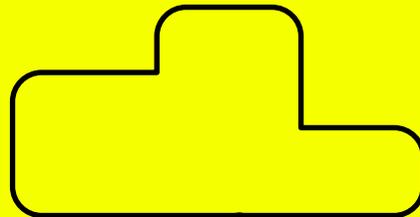
Einführung einer Kennzeichnungspflicht für alle Formen bezahlter politischer Werbung und von Regeln zur Begrenzung des Microtargeting.

Bisher sieht der DSA-E für Werbung nur genannte Transparenzpflichten (Art. 24) und eine Werbe-Datenbank (Art. 30) vor. Außerdem soll die Kommission nach Art. 36 darauf hinwirken, dass die Plattformen untereinander weitergehende Standards für Werbung beschließen.

Sinnvoll erscheint: Der auf Eigenverantwortung setzende Ansatz nach Art. 36 DSA-E kann keine Lösung für den Kern des Geschäftsmodells der Plattformen, die Werbung, sein. Microtargeting sollte auf die unsensiblen Merkmale „Alter“ und „Lokalität“ beschränkt werden.

III.

Verbesserung des Wettbewerbs auf EU- Ebene und in Deutschland



● 10 Handlungsoptionen für heute

Ambitionierte Ausgestaltung des Digital Markets Act der EU u. a. durch strenge Vorgaben für Gatekeeper hinsichtlich der Zusammenführung personenbezogener Daten unterschiedlicher Dienste – dazu gehört eine Abfrage der Einwilligung der Nutzer:innen auf der Grundlage von klaren und umfassenden Informationen.

Bisher sieht Art. 5 Abs. 1 DMA-E vor, dass eine solche Zusammenführung grundsätzlich untersagt ist, außer es liegt eine Wahl bzw. Einwilligung gemäß der DSGVO vor. Die Einwilligung kann mithin nur zweckgebunden erteilt werden. Weitere Anforderungen an den Umfang der Informationen vor der Einwilligung bestehen nicht.

Sinnvoll erscheint: eine Regelung der Mindestanforderungen, die an die zu erteilenden Informationen zu stellen sind, bevor eine etwaige Einwilligung erteilt wird. Dies soll sicherstellen, dass wenig aussagekräftige Begriffe wie „umfassende Information“ zur Aushöhlung der Norm führen.

Prüfung von Möglichkeiten zur Entflechtung sehr großer Plattform im Rahmen des GWB, sofern der DMA dies nicht vorsieht.

Bisher sieht Art. 16 Abs. 1 DMA-E die Befugnis der Kommission vor, alle strukturellen Maßnahmen zu ergreifen, die auf die Einhaltung der Pflichten des Gatekeepers hinwirken. Dazu kann auch eine Abspaltung bestimmter Konzernteile zählen, dies wird aufgrund des schweren Eingriffs in Freiheiten des Unternehmens der letzte Schritt eines Verfahrens sein. Solche strukturellen Maßnahmen sieht das GWB heute auch bereits in § 32 Abs. 2 als letztes Mittel der Durchsetzung vor.

Sinnvoll erscheint: dass vielversprechende Instrumente auch genutzt werden und das nationale Kartellrecht auch weiterhin neben dem DMA als Mittel gegen große Plattformen eingesetzt werden kann.

Einführung einer gesetzlichen Verpflichtung zur Datenportabilität und Interoperabilität

Bisher ist nur das Recht auf Datenportabilität in Art. 20 DSGVO verankert und umfasst das Recht, die bereitgestellten, personenbezogenen Daten zu erhalten und einem anderen Verantwortlichen zu übermitteln, sofern die Verarbeitung auf einer qualifizierten Einwilligung beruht und automatisiert erfolgte. Dies soll nach der DSGVO auch interoperabel möglich sein. Der DMA-E sieht in Art. 6 Abs. 1 lit. f die Pflicht für Gatekeeper zur

Sinnvoll erscheint: die Einführung eines datenschutzwahrenden Rechts auf Interoperabilität bei bedeutender Infrastruktur wie Messengerdiensten sowie die verpflichtende Einführung eines einfachen Systems zur Datenportabilität. Datenschutzwahrend muss dabei bedeuten, dass voreingestellt und in der gesamten Infrastruktur der Datenschutz priorisiert werden muss.

Einführung eines öffentlichen und wirtschaftlich unabhängigen Datentreuhänders mit einem robusten politischen Mandat, auch zur Durchsetzung des Datenzugangs.

Bisher sind zwar unabhängige Datentreuhänder in Art. 9 ff. DGA vorgesehen, die die Daten nicht selbst kommerziell nutzen dürfen. Dies ist allerdings weder mit einem politischen Mandat verbunden noch ist nach derzeitigem Stand Aufgabe der Datentreuhänder, Datenzugänge durchzusetzen.

Sinnvoll erscheint: daher die Einrichtung öffentlicher, unabhängiger Datentreuhänder auf EU-Ebene deren Mandat insbesondere effektive Mittel wie Strafen zur Durchsetzung der Pflicht zur Einführung eines Datenzugangs umfasst.

IV.

Einführung eines digitalen Gewaltschutzgesetzes



● 10 Handlungsoptionen für heute

Ermöglichung vereinfachter und schneller Klagemöglichkeiten für Betroffene bei Zivilprozessen

Bisher gibt es für Opfer digitaler Gewalt keine vereinfachten Möglichkeiten, Zivilklage gegen Täter:innen zu erheben. Dies richtet sich allgemein nach der Zivilprozessordnung (ZPO) und dem Gerichtsverfassungsgesetz (GVG).

Sinnvoll erscheint: ein der Schnelligkeit des Internets angepasste Verfahren für Opfer von Gewalt, das in ersten Schritten auf den Schutz der Opfer vor künftigen Taten gerichtet sein muss. Dabei sollten die Besonderheiten wie kurze Speicherzeiten von Nutzungs- und Bestandsdaten berücksichtigt werden.

Sicherstellung des Zeugenschutzes bereits bei der Anzeigeerstattung durch Schutz der Privatanschrift von Verletzten und Zeug:innen

Bisher wird die Anschrift der Verletzten und Zeug:innen bei Vernehmungen ohne Anwesenheit des/der Beschuldigten grundsätzlich in den gem. § 68 I StPO aufgenommen. Nur unter besonderen Umständen kann davon abgewichen werden.

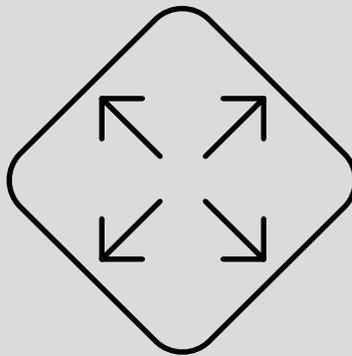
Sinnvoll erscheint: eine Wahlmöglichkeit der Betroffenen, ihre eigene Anschrift oder die eines Rechtsbeistands anzugeben.

Einführung einer Abgabe von Plattformen an Unterstützungs- und Beratungsangebote für Betroffene sowie an Meldestellen

Sinnvoll erscheint: eine verbindliche Regelung zur finanziellen Unterstützung von Unterstützungs- und Beratungsangeboten durch Plattformen.

V.

*Ausweitung der
Kapazitäten von Behörden
und Parteien*



● 10 Handlungsoptionen für heute

Evaluation der Arbeit des Bundeswahlleiters hinsichtlich des Erkennens und Bekämpfens von Desinformation und darauf basierend Bereitstellung von Ressourcen, um das Angebot anzupassen und gegebenenfalls auszuweiten.

Bisher sind die Aufgaben des Bundeswahlleiters im Bundeswahlgesetz und detaillierter in der Bundeswahlordnung geregelt.

Sinnvoll erscheint: die Bundeswahlordnung durch eine Evaluation im Nachgang einer Bundestagswahl zum Umgang des Bundeswahlleiters bezüglich des Erkennens und Bekämpfens von Desinformation zu erweitern.

Ausreichende Bereitstellung von Ressourcen der politischen Parteien für offene Kommunikation und die Moderation ihrer Social-Media-Seiten

Bisher wird die Moderation der Social Media Seiten von den Parteien selbst organisiert und verwaltet.

Sinnvoll erscheint: die Ausweisung finanzieller Mittel speziell für diesen Zweck sowie die Verpflichtung der Parteien zur Moderation ihrer Social Media-Seiten.

Zentralisierung der Datenschutzaufsicht für die Wirtschaft beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Bisher ist die datenschutzrechtliche Kontrolle privatwirtschaftlicher Unternehmen gem. § 40 Abs. 1 Bundesdatenschutzgesetz Aufgabe der Landesdatenschutzbehörden.

Sinnvoll erscheint: die datenschutzrechtliche Kontrolle privatwirtschaftlicher Akteure direkt an den Bundesdatenschutzbeauftragten bzw. eine bei diesem zu schaffende Einheit zu übertragen.

Ausweitung der personellen und sachlichen Ausstattung der Strafverfolgungsbehörden

Bisher steigt die Zahl von Fällen im Zusammenhang mit Hasskriminalität im Internet stetig an. Die 2022 in Kraft tretende Pflicht der Plattformen, als Verstoß gegen das NetzDG gemeldete Inhalte und die dazugehörigen Nutzungsdaten an das BKA auszuleiten, wird die Zahl der Fälle noch weiter erhöhen.

Sinnvoll erscheint: Strafverfolgungsbehörden auf die besonderen Herausforderungen von Straftaten im Internet, insbesondere solcher im NetzDG aufgeführter Straftaten vorzubereiten.

Dazu zählt auch die Einführung von Schwerpunktstaatsanwaltschaften mit ausreichender personeller Kapazität zur Bearbeitung der Vielzahl an Strafanzeigen. Statt weitreichenden Speicher- und Ausleitungspflichten erscheinen punktuelle und effektive Lösungen (wie die Login-Falle), die schon im geltenden Recht verankert ist, sinnvoll.

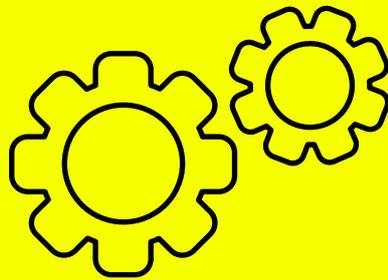
Die Einstufung als „Gefährliche Personen und Organisationen“ sollte eine systemische Perspektive einnehmen und auch das Verhalten von Nutzer:innen außerhalb der Plattformen mit einbeziehen.

Bisher limitieren Policy-Dialoge mit dem Fokus auf Selbstregulierung wie das EU Internet Forum und der Christchurch Call for Action ihren Fokus auf das Verhalten von Nutzer:innen auf der jeweiligen Social-Media-Plattform. Viele (gewaltorientierte) extremistischen Akteure haben deshalb ihre Strategie angepasst und verüben keine Straftaten mehr auf den Plattformen, nutzen diese aber um ihre Online-Shops zu promoten und um Anhänger:innen anzuwerben.

Sinnvoll erscheint: Die beispielsweise in den aktuellen Facebook-Gemeinschaftsstandards ausgeführte eher systemische Perspektive auf „Gefährliche Personen und Organisationen“, die auch das Verhalten von Nutzer:innen außerhalb der Plattformen mit einbezieht, sollte bei Policy-Dialogen wie dem EU Internet Forum und dem Christchurch Call for Action integriert werden.

VI.

Weiterentwicklung des Medienkonzentrationsrechts



● 10 Handlungsoptionen für heute

Unterstützung der Bemühungen der Länder, ein novelliertes praktikables Medienkonzentrationsrecht zur Verhinderung vorherrschender Meinungsmacht im digitalen Zeitalter einzuführen.

Bisher regelt der Medienstaatsvertrag in den §§ 59–68 vielfaltssichernde Maßnahmen. Diese gelten jedoch nur für privaten Rundfunk und mithin nicht für Online-Dienste.

Sinnvoll erscheint: die Bemühungen der Länder zur Übertragung der vielfaltssichernden Vorschriften auch auf Online-Dienste voranzubringen.

Insbesondere Prüfung von Möglichkeiten zur Stärkung regionaler Angebote oder der Förderung qualitativer Inhalte über neue Eingriffsbefugnisse der Kommission zur Ermittlung der Konzentration im Medienbereich

Bisher kann die Kommission nach dem Entwurf des DMA Gatekeepern bei vielfaltsgefährdenen Praktiken Abhilfemaßnahmen aufzwingen.

Konkret fordern wir: diese Abhilfemaßnahmen auch um die Förderung regionaler Angebote zu ergänzen.

VII.

Ausweitung des Bildungsangebots im Digitalbereich



● 10 Handlungsoptionen für heute

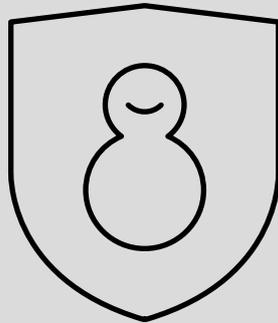
Umfassende Umsetzung der Strategie „Bildung in der digitalen Welt“ der Kultusministerkonferenz und Ausweitung der Förderung der Nachrichten- und Informationskompetenz aller Bürger:innen

Bisher werden die Nachrichtenkompetenzen junger Menschen mitunter als „beunruhigend“ beschrieben (Stanford History Education Group). Eine Studie der SNV ergab, dass nur 22 % der Teilnehmenden über hohe Kompetenzwerte zum Thema Nachrichten verfügten. Insbesondere das Vertrauen in einen unabhängigen Journalismus ist relativ schwach ausgeprägt. An die sogenannte „Lügenpresse“ glaubte rund ein Viertel der Befragten.

Sinnvoll erscheint: die Ausweitung der Erwachsenenbildung für digitale Nachrichten- und Informationskompetenz, etwa am Arbeitsplatz, in Bibliotheken oder Volkshochschulen sowie online beispielsweise bei Plattformen und auf Nachrichtenseiten. Außerdem die Verbesserung und den Ausbau der Angebote für Kinder und Jugendliche durch Plattformen, Schulen und Vereine. Für beides müssen staatliche Stellen und/oder Fonds großer digitaler Plattformen den Ausbau und die Finanzierung solcher Angebote sicherstellen.

VIII.

Verschärfung des Jugendmedienschutzes



- 10 Handlungsoptionen für heute

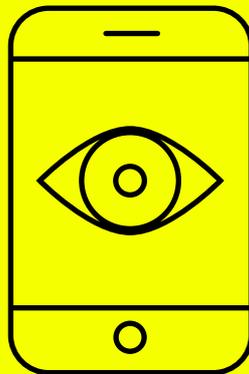
Übernahme der Vorsorgemaßnahmen des Jugendschutzgesetzes zur Wahrung von Schutzzielen für Kinder und Jugendliche auf EU-Ebene

Bisher trägt auf europäischer Ebene vor allem die **Richtlinie für audiovisuelle Mediendienste** dem Jugendschutz Rechnung. Demnach sollen Zugangskontrollen eingerichtet und so verhindert werden, dass Minderjährige mit Inhalten in Kontakt kommen, die sie in ihrer Entwicklung gefährden könnten. Das Jugendschutzgesetz geht hier weiter und führt einen Katalog mit Vorsorgemaßnahmen auf, welche Anbieter von Online Diensten zu beachten haben. Dazu zählen unter anderem die Pflicht zur Bereitstellung der AGB in kindgerechter Sprache oder die Voreinstellung, dass Profile von Minderjährigen in Suchen nicht auffindbar sind.

Sinnvoll erscheint: Äquivalente zu den wirksamen Vorsorgemaßnahmen des JuSchG auch auf europäischer Ebene in Rechtssetzungsprozesse einzubringen.

IX.

Fortentwicklung des Datenschutzes



● 10 Handlungsoptionen für heute

Ergänzung der DSGVO um spezifische ambitionierte Regelungen zu Profiling-Verfahren digitaler Plattformen, sofern sich eine hinreichend wirkungsvolle europäische Lösung in absehbarer Zeit als nicht realistisch erweisen sollte.

Bisher ist Profiling in der DSGVO in vielen Teilen der Verarbeitung personenbezogener Daten gleichgestellt. Eine über diese Gleichstellung hinausgehende Begrenzung speziell von Profiling findet sich jedoch nicht in der DSGVO. Als große Ausnahme greift dabei die Zustimmung der Nutzer:innen, welche jedoch oft unbedacht erteilt wird.

Sinnvoll erscheint: eine Begrenzung von Profiling-Verfahren durch digitale Plattformen beispielsweise durch absolute Beschränkung der Verwendung bestimmter sensibler Daten, kürzere Speicherzeiten sowie besondere Anforderungen an die Zustimmungspflichten.

Verbesserung des Schutzes sensibler personenbezogener Datenkategorien wie ethnisch Herkunft, Religion, sexuelle Orientierung oder politische Ansichten.

Bisher ist die Verarbeitung dieser Datenkategorie gem. Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Es gibt jedoch einige Ausnahmen.

Sinnvoll erscheint: u. a. eine Konkretisierung bezüglich der Anforderungen an die Art und den Umfang der zur Profilbildung herangezogenen Daten, der zulässigen Tiefe der zu Zwecken einer Profilbildung erfolgenden Schlussfolgerungen, und vor allem der Zwecke, für die Profilbildungen zulässigerweise eingesetzt werden dürfen. Außerdem müssen absolute Verbote wie z. B. die Verwendung von Profilen bei der Bewerber:innenauswahl, wenn diese aus Daten aus dem Privatleben gewonnen wurden und von Profilbildungen bei besonders sensiblen personenbezogenen Daten, etwa in Zusammenhang mit Emotionserkennungssoftware und biometrischen Daten eingeführt werden.

Einführung praktikabler Einwirkungsmöglichkeiten für Nutzer:innen auf die über sie gebildeten Profile, einschließlich der Möglichkeit zur Löschung, Korrektur, Überprüfung und Herausgabe aller über sie gespeicherten Daten.

Bisher müssen durch die Nutzer:innen bereitgestellte Daten auf Anfrage gemäß Art. 20 I DSGVO übermittelt werden. Ein

Recht auf Löschung ergibt sich aus Art. 17 DSGVO. Ein Recht auf Berichtigung der Daten ergibt sich gem. Art. 16 DSGVO nur bei unrichtigen Datensätzen.

Sinnvoll erscheint: die bereits rechtlich geschaffenen Möglichkeiten von Löschung und Auskunft durch einfache Verfahren zu erleichtern. Der Anspruch auf Berichtigung soll in einen Anspruch auf Abänderung umgestaltet werden. Dies würde bedeuten, dass die Nutzer:innen auch richtige Daten durch unrichtige Daten ersetzen können.

X.

***Mehr Transparenz und
Kontrolle von Algorithmen***



● 10 Handlungsoptionen für heute

Empfehlungssysteme sollten standardmäßig nicht auf der Verarbeitung sensibler Datenkategorien wie politischen Ansichten beruhen.

Bisher ist im Art. 29 Abs. 1 DSA-E nur die Offenlegung der wichtigsten Parameter des Empfehlungssystems für VLOPs vorgeschrieben. Außerdem muss dem Nutzer:in mindestens eine Empfehlungslogik angeboten werden, die nicht auf einem wertenden Profil beruht (Profiling). Dies bedeutet dann auch den Ausschluss sensibler Datenkategorien, was jedoch nicht zwingend die standardmäßige Art der Empfehlungsalgorithmen ist.

Sinnvoll erscheint: daher, das Verhältnis umzukehren. Empfehlungssysteme dürfen standardmäßig nicht auf Profiling beruhen und andere, sensible Datenkategorien anwenden. Nutzer:innen müssen solche auf Profiling beruhende Systems stattdessen aktiv auswählen.

Prüfung von Möglichkeiten zur Beendigung des sogenannten Engagement Based Ranking

Bisher sieht der DSA-E in Art. 27 Abs. 1 lit. a vor, dass VLOPs als Risikominderungsmaßnahme auf Basis der Risikobewertung auch eine Umstellung der Empfehlungslogiken anstreben können. Außerdem sind VLOPs zur Transparenz bezüglich der „wichtigsten Parameter“ ihrer Empfehlungslogik gem. Art. 29 Abs. 1 DSA-E verpflichtet. Eine vollständige Offenlegung der zur Empfehlung führenden Faktoren oder gar ein Verbot von Engagement als Faktor ist nicht vorgesehen.

Konkret fordern wir: eine Prüfung, ob das sogenannte Engagement Based Ranking gesetzlich unterbunden werden kann.

Impressum

Luminate Ltd.

Director: Ben Scott
36–38 Hatton Garden, Holborn,
London EC1N 8EB, United Kingdom

E-Mail:

Luminate Ltd.: hello@luminategroup.com
Reset: hello@reset.tech

Webseite:

Luminate Ltd.: www.luminategroup.com
Reset: www.reset.tech

Register: Companies House, United Kingdom

Recht: UK

Company Nr.: 11125848

Die Interviews führten für Reset: Nataly Bleuel,
Mauritius Dorn, Merle Heine, Alexander Sänglerlaub

Titelbild: REUTERS / CHRISTIAN MANG - stock.adobe.com

Gestaltung: nach morgen, Studio für digitale Produkt-
und Markenentwicklung, www.nachmorgen.de