2019 / Manipulation und Mobilisierung im Netz / TRANSNATIONALE SICHERHEITSRISIKEN

↓ EMPFEHLUNGEN

1. Hassrede einschränken, aber Freiheitsrechte garantieren Die Bundesregierung soll Maßnahmen auf VN- und EU-Ebene wie den Aktionsplan der VN gegen Hassrede unterstützen. Generell sollten internationale Initiativen jedoch nur befürwortet werden, wenn sie die Freiheit schützen und übermäßige staatliche Eingriffe vermeiden.

2. Gesetzliche Regulierung nur auf Basis gesicherter Erkenntnisse und konzeptioneller Klarheit Ohne das Verständnis von Wirkungszusammenhängen und ohne konzeptionelle Klarheit bei Rechtsbegriffen sollte es keine Gesetzesinitiativen gegen extremistische Inhalte oder Hasskommentare geben.

3. Novellierung des NetzDG Das Netzwerkdurchsetzungsgesetz (NetzDG) überlässt sozialen Netzwerken die Erstbeurteilung über die Rechtswidrigkeit von Inhalten. Das kann zu übermäßigem Löschen führen. Stattdessen sollte mehr Gewicht auf die Ermittlung der Urheber strafrechtlich relevanter Äußerungen gelegt werden.

4. Transparenzregeln beim Einsatz von Algorithmen Algorithmen bestimmen die Priorisierung von Nachrichten bei Diensten wie Facebook oder Google. Ihr Zustandekommen muss einer rechtsstaatlichen Kontrolle unterliegen und Auswirkungen auf Wahlkämpfe müssen transparent gemacht werden.

5. Impressumspflicht und Transparenz bei politischer Werbung Die Anonymität im Internet sollte nicht leichtfertig eingeschränkt werden. Bei politischer Werbung im Internet empfehlen wir eine umfassende Impressumspflicht und leicht einsehbare Angaben, wer für die Werbung bezahlt hat und wem welche Werbung angezeigt wird.

6. (Daten-)Schutz des Einzelnen Gezielte politische Werbung über soziale Netzwerke basiert auf der Verwendung von Nutzerprofilen. Nur strikte Datenschutzregelungen können eine Barriere gegen individuell zugeschnittene und manipulative Werbung bilden.

7. Stärkung von Medienkompetenz Die Maßnahmen gegen Manipulation und Mobilisierung im Internet setzen überwiegend auf Kontrolle oder auf Symbolik. Nachhaltiger und besser ist eine breite politische Bildungsarbeit und die Vermittlung von Medienkompetenz auf allen Ebenen des Bildungssystems.

8. Öffentlich-rechtliche Grundinformation im Internet Wir empfehlen den Aufbau eines öffentlich-rechtlichen Fördersystems zur Gewährleistung von Grundinformation im Internet – analog zum Auftrag des öffentlich-rechtlichen Rundfunks. Dies kann über die Unterstützung von Recherchenetzwerken und journalistischen Plattformen geschehen.

TRANSNATIONALE SICHERHEITSRISIKEN / Manipulation und Mobilisierung im Netz /

Flucht und Migration, Klimawandel, der internationale Terrorismus oder externe Versuche von Wahlmanipulation sind Themenfelder genuin transnationalen Charakters. Meinungen über Bedrohungslagen gehen auseinander und stehen oft im Widerspruch zu verfügbaren Daten. Technologische Innovationen, die Kommunikationsverhalten grundlegend verändern, verschärfen diesen Befund. Dies ist eine zentrale Herausforderung für die innere Friedensfähigkeit liberaler Demokratien und für die globale Politik.

5.1 ↙ Aktuelle Trends

Transnationale Risiken für Sicherheit und Frieden können als Gefahren definiert werden, „die nicht von einem einzelnen Land ausgehen und auch nicht auf einzelne Länder beschränkt bleiben, sondern über Territorialgrenzen hinweg wirksam werden können“ (→ BICC/HSFK/IFSH/INEF 2018, Kapitel Transnationale Sicherheitsrisiken: 127). Sie sind gleichermaßen Bedrohungen für den inneren Frieden von Gesellschaften und für Kooperationen zwischen Akteuren der globalen Politik. Sie zeichnen sich häufig durch einen hohen Grad an Unbestimmtheit und Ungewissheit aus und umfassen ein breites Spektrum realer und/oder wahrgenommener Bedrohungen.

Anzahl der Terroropfer rückläufig, Gewaltniveau weiter hoch

Ein Beispiel ist der Terrorismus: 2017 kamen insgesamt 26.400 Menschen durch terroristische Anschläge ums Leben. Die meisten Angriffe gingen auf das Konto islamistischer Gruppen, allen voran des sogenannten Islamischen Staats (IS), der Taliban und der Al-Shabaab. Die militärische Schwächung des IS vermag zu erklären, dass die Anzahl der Anschlagsopfer 2017 im dritten Jahr in Folge rückläufig war (University of Maryland/National Consortium for the Study of Terrorism and Responses to Terrorism 2018). Das Gewaltniveau bleibt im Vergleich zu früheren Jahrzehnten dennoch hoch und ist, wie an den Rechtfertigungen für internationales politisches und militärisches Eingreifen beispielsweise in der Sahelregion zu sehen ist, eine der Triebfe-

dern für internationales Handeln → **1**. Das Ausmaß der Gewalt variiert erheblich zwischen verschiedenen Weltregionen. Die mit Abstand meisten Opfer waren im Irak, Afghanistan, Nigeria und Syrien zu beklagen. Obwohl die Anschlagshäufigkeit im Irak und in Syrien zuletzt abnahm, finden mehr als die Hälfte aller Terrorattacken weltweit noch immer in diesen vier Ländern statt. Ganz anders stellt sich das Bild in Westeuropa dar: 2017 halbierte sich hier die Zahl der Todesopfer (81) gegenüber dem Vorjahr (168). Dieser Abwärtstrend dauerte 2018 an.

Rechtsextreme Gewalt nimmt zu

Im Vergleich dazu steigt die Anzahl rechtsextremistisch motivierter Terroranschläge oder Anschlagsvorbereitungen (→ Institute for Economics & Peace 2018). Zwischen 2010 und 2014 erwirkte der Generalbundesanwalt in Deutschland sechs Haftbefehle gegen Personen, die der Vorbereitung oder Ausführung einer schwerwiegenden fremdenfeindlichen Straftat verdächtigt wurden – im Zeitraum 2015-2018 waren es bereits 35.[1]

Bedrohungsempfinden und reale Gefahr unterscheiden sich

Transnationale Sicherheitsrisiken eignen sich aufgrund ihrer komplexen und langen Wirkungsketten und der daraus resultierenden Ungewissheit in ganz besonderer Weise für Versuche, Ängste zu schüren und die öffentliche Meinungsbildung gezielt zu beeinflussen. Das subjektive Empfinden entspricht dabei nicht immer objektiven Befunden – sofern solche überhaupt möglich sind. Am ehesten gehen Wahrnehmung und aktuelle Ereignisse beim Klimawandel Hand in Hand. 2017 bat das US-amerikanische Meinungsforschungsinstitut Pew Research Center 40.000 Menschen in 38 Staaten darum, acht mögliche Bedrohungen in eine Rangfolge zu bringen. In sechs von sieben untersuchten lateinamerikanischen Ländern sowie in vier von sechs Staaten Sub-Sahara-Afrikas stand demnach der Klimawandel an erster Stelle – also in eben jenen Regionen, die am stärksten von extremen Wetterereignissen betroffen sind. In Russland und den USA nahm der Klimawandel hingegen eine vergleichsweise nachrangige Stellung ein (→ Poushter/Manevich 2017).

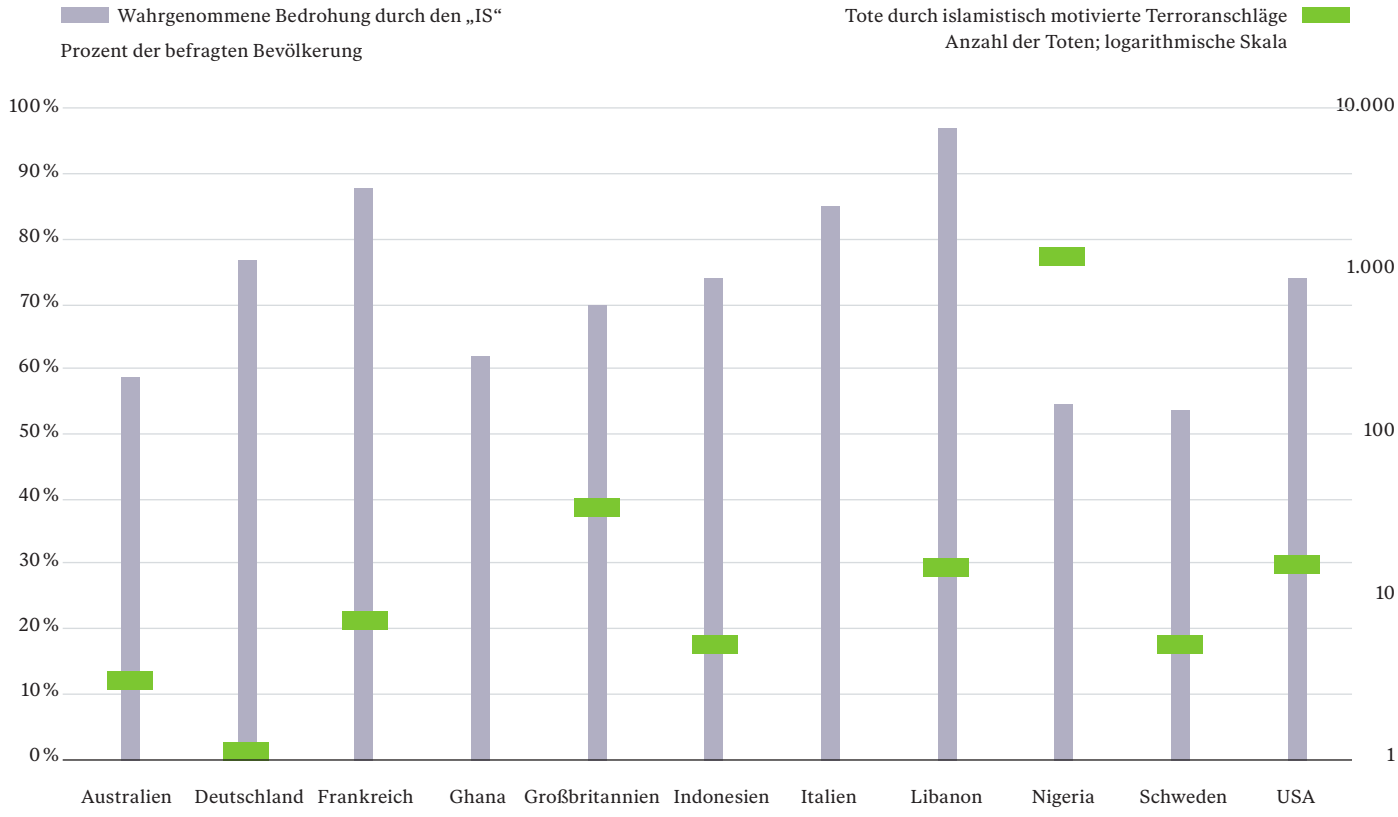
Angstempfinden und Bedrohungswirklichkeit korrelieren beim Thema Terrorismus nur bedingt. Zwar spiegelt sich der Rückgang islamistischer Anschläge in Deutschland und Westeuropa über die vergangenen Jahre auch in Gefährdungsumfragen wider. Führte „Terrorismus“ 2017 den Angstindex des Infocenters der R+V Versicherung an (→ BICC/HSFK/IFSH/INEF 2018, Kapitel Transnationale Sicherheitsrisiken), rutschte er 2018 auf Platz fünf (→ R+V Versicherung 2018). Der Sicherheitsreport 2019 des Instituts für Demoskopie Allensbach kommt zu einem ähnlichen Ergebnis: demnach fühlten sich 2016 45 % der befragten Bürger vom „Terrorismus“ bedroht – 2018 waren es nur noch 28 %. Jedoch offenbaren Ländervergleiche deutliche Unterschiede zwischen subjektivem Empfinden und tatsächlichen terroristischen Gewaltereignissen – einfache Zusammenhänge gibt es in diesem Zusammenspiel nicht (→ **34** /141 für einige illustrative und selektive Beispiele zur bedingten Korrelation und objektiver Bedrohung – gemessen am Indikator „Todesopfer“ – durch den Islamischen Staat (IS) und den islamistischen Extremismus anhand von Daten aus dem Jahr 2017). Das Bedrohungs-

empfinden zum Terrorismus entwickelt sich über Zeit und wird durch transnationale Ereignisse beeinflusst. In den R+V Umfragen zur Angst der Deutschen vor Terrorismus schlagen sich Ereignisse wie die Anschläge in Frankreich im Jahr 2015 auf Charlie Hebdo und auf das Stade de France/Bataclan sowie in Belgien im Jahr 2016 nieder: das Bedrohungsempfinden erhöhte sich von 42 % der Bevölkerung im Jahr 2014 auf 73 % im Jahr 2016. Auf diesem hohen Niveau verharrte es dann nach dem Anschlag auf dem Breitscheidplatz Ende des Jahres 2016 in Berlin.

Ähnliche Diskrepanzen zwischen Empfinden und Bedrohungslage zeigen sich beim Thema Flucht und Migration. Die Zahl der Geflüchteten nimmt weltweit zwar von Jahr zu Jahr zu → **2** /77, und für die Geflüchteten selbst sind die Gefahren real: Von Januar 2015 bis Januar 2019 verloren insgesamt 25.471 Migranten während der Reise ihr Leben (→ IOM 2019a). Für die Aufnahmeländer variiert die Belastung allerdings stark. Laut UNHCR beträgt das Verhältnis zwischen Staatsbürgern und Vertriebenen im Libanon etwa 6:1. Die Länder der Europäischen Union sind von derartigen Relationen weit entfernt. Seit ihrem Höhepunkt 2015 nahm die Zuwanderung aus außereuropäischen Regionen hier kontinuierlich ab: von 390.432 Migranten (2016) auf 186.768 (2017) und zuletzt auf 144.166 (→ IOM 2019b). Zudem ist die verbreitete Annahme, die Zuwanderung erhöhe deutlich das Risiko terroristischer Anschläge, irreführend (→ BICC/HSFK/IFSH/INEF 2018, Kapitel Transnationale Sicherheitsrisiken).

34 Terroristische Bedrohung durch den Islamischen Staat und islamistischen Extremismus im Jahr 2017

Quelle → **5** /157



Dennoch belegt die Furcht vor „Spannungen durch Zuzug von Ausländern“ im Angstindex 2018, wie schon 2016 und 2017, den dritten Platz (→ R+V Versicherung 2018). Die Daten des Pew Research Center zeigen überdies, dass Ängste vor Einwanderung besonders in jenen Gesellschaften vorherrschen, die den geringsten Anteil von Menschen mit Migrationshintergrund an der Gesamtbevölkerung aufweisen – so insbesondere in osteuropäischen Ländern wie Polen oder Ungarn (→ Poushter/Manevich 2017; Statista 2019). Die verbreitete Wahrnehmung, dass Zuwanderung die Sicherheit bedroht, birgt das Potenzial, den inneren Frieden einer Gesellschaft zu gefährden – vor allem dann, wenn der Regierung nicht zugetraut wird, diese vermeintliche Gefahr in den Griff zu bekommen (→ BICC/HSFK/IFSH/INEF 2018, Kapitel Transnationale Sicherheitsrisiken). Der Angstindex 2018 unterstreicht die Befürchtung einer „Überforderung der Politiker“ (Platz 4) sowie einer „Überforderung der Behörden durch Flüchtlinge“ (Platz 2) – beides Kategorien, die erst 2015 und 2016 im Zuge der „Flüchtlingskrise“ Eingang in die Umfragen fanden. Ungeachtet der abnehmenden Zuwanderung halten sie sich weiterhin auf Spitzenpositionen.

Was erklärt das Auseinanderfallen zwischen objektiver Gefährdung und subjektivem Angstempfinden, besonders im Kontext von Migration und Terrorismus? Politische und wissenschaftliche Diskurse weisen in diesem Zusammenhang häufig auf die Bedeutung digitaler Informationsvermittler (Intermediäre) wie Facebook oder Google hin. Unterschieden werden kann dabei zwischen Analysen dazu, wie die virtuelle Welt Wahrnehmungen von Unsicherheit neu ordnet (siehe Diskussionen um Filterblasen, Echokammern oder Algorithmisierung), und Analysen darüber, wie verschiedene Akteure in dieser virtuellen Welt kommunizieren, emotionalisieren und manipulieren (beispielsweise Diskussionen um die Beeinflussung von Wahlen oder um die Mobilisierungsmöglichkeiten zur Gewalt). Dieses Kapitel fokussiert auf virtuelle, transnationale Gefahren für die liberale Demokratie. Deren innere Friedensfähigkeit war und ist eine der wesentlichen Triebfedern zur multilateralen Ausgestaltung der internationalen Friedens- und Sicherheitsinstitutionen. Die aktuell oft beschworene Krise multilateraler Institutionen und internationaler Kooperationsfähigkeit hängt auch mit diesen neuen Formen der Manipulation und Mobilisierung im Internet zusammen.

5.2 ↙ Strategien der Manipulation und Mobilisierung im Internet

Medien haben in Demokratien eine zentrale Funktion als Informationsvermittler sowohl für die Bürger als auch für ihre regierenden Repräsentanten. Sie bieten öffentliche Foren, um politische Forderungen und Entscheidungen zu begründen, zu legitimieren oder auch zu kritisieren. In vernetzten Informationsgesellschaften spielen hierbei zunehmend die sozialen Netzwerke eine Rolle. Aber auch demagogische Aussagen und Falschmeldungen, beleidigende und menschenverachtende Kommentare sowie direkte Gewaltaufrufe verbreiten sich über sie schnell. Es ist zu vermuten,

Im Umgang mit gesellschaftlicher Polarisierung kommt sozialen Netzwerken eine wichtige Rolle zu

dass die sozialen Netzwerke dazu beitragen, politische und gesellschaftliche Polarisierungen zu verschärfen. Hier sind insbesondere zwei Fragen von Bedeutung: Wie nutzen Akteure diese Medien zur Verbreitung politischer Botschaften und wie gestalten Intermediäre die Informationsumgebung ihrer Nutzer und nehmen damit selbst Einfluss auf das Informationsgeschehen?

STRATEGISCHE INFORMATIONSVERBREITUNG UND MANIPULATIONSVERSUCHE

Wahlkampfführende politische Gruppierungen, Parteien und Kandidaten können mithilfe sozialer Netzwerke genau zugeschnittene Botschaften an ausgesuchte Teile der Wahlbevölkerung senden. Sie haben sich insbesondere in den USA mithilfe von großen Internetfirmen und Auskunfteien Daten über die Wählerschaft beschafft, ausgewertet und vor allem in hoch umkämpften Wahlkreisen die Wähler gezielt entsprechend ihrer politischen Einstellungen angesprochen (microtargeting). Mit der Verwendung von sogenannten dark ads sind sie noch einen Schritt weitergegangen: verschiedene Zielgruppen wurden vom gleichen Absender mit unterschiedlichen, auf sie persönlich zugespitzten Inhalten beliefert.

Wählergruppenspezifische Werbung ist kein neues Phänomen. Aber sie hat eine neue Dimension erreicht, indem sie datengestützte Techniken nutzt, die eine schnelle und auf individuelle Einstellungen zugeschnittene Verbreitung von Informationen ermöglichen. Intermediäre wie Facebook und Google sind an dieser Entwicklung maßgebend beteiligt. Sie verfügen nicht nur über eine detaillierte Nutzerdatenbank, sondern bieten ihren Kunden aus der Politik ein breites Spektrum digitaler Marketingtools und -techniken, um Nutzer gezielt anzusprechen. Große öffentliche Aufmerksamkeit erregten Berichte über die Tätigkeit der britischen Firma Cambridge Analytica im Rahmen des Wahlkampfs von Donald Trump im Jahr 2016. Cambridge Analytica legte auf Basis von teils offenbar unrechtmäßig erlangten Daten Persönlichkeitsprofile von schätzungsweise 220 Mio. US-Amerikanern an. Über diese Profile konnten ihre Kunden die Wahlberechtigten individuell ansprechen. Zwar beurteilen viele Experten die angeblich wahlentscheidende Wirkung des Analyse-Modells von Cambridge Analytica skeptisch; dennoch steht es exemplarisch für eine in ihren Wirkungen bislang noch wenig verstandene Herausforderung für die Durchführung freier und fairer Wahlen.

Cambridge Analytica und die US-Wahlen

Auch in Europa gab es Bemühungen, soziale Netzwerke für politische Kampagnen zu nutzen, so etwa im Rahmen der Brexit-Abstimmung. Viele über die Netzwerke verbreitete Anzeigen enthielten falsche oder irreführende Informationen. Alle größeren deutschen Parteien haben im Bundestagswahlkampf 2017 microtargeting betrieben und Wähler über individualisierte Wahlwerbung angesprochen. Die gezielte Verbreitung politischer Werbebotschaften über die sozialen Netzwerke hat in Deutschland noch nicht das Ausmaß und die Intensität wie in den USA erreicht, wo die Datenschutzbestimmungen deutlich mehr erlauben; doch auch hierzulande sind diese Entwicklungen

keineswegs unproblematisch. Da die gezielte Ausspielung politischer Werbung über die sozialen Netzwerke zuvor erstellte Profile von Nutzern verwendet, sollten alle Versuche, das hohe Datenschutzniveau zu untergraben – etwa im Zuge der Ausgestaltung der ePrivacy-Verordnung –, unterbunden werden.

Aber nicht nur die Verbreitung von Werbebotschaften durch politische Organisationen und Public-Relations-Agenturen ist ein Problem. Zum Gesamtbild gehört auch die von vielen staatlichen und nichtstaatlichen Gruppierungen lancierte „Computerpropaganda", die ohne Billigung der Social-Media-Betreiber verbreitet wird. Während des US-Wahlkampfes 2016 und vor der Brexit-Abstimmung wurden in den sozialen Netzwerken über gefälschte Nutzerkonten eine Unmenge polarisierender Botschaften und Falschmeldungen verbreitet. Diese sollten Diskussionen manipulieren, Verunsicherungen und Vorurteile schüren, die Ansichten politischer Gegner bloßstellen und eine vermeintliche Unterstützung der eigenen Position auf Twitter, Facebook oder Instagram simulieren. Es ist unklar, ob und in welchem Maße dahinter Geheimdienste, auf eigene Faust vorgehende politische Aktivisten oder Hacker mit kommerziellen Motiven stehen. Ganz unabhängig von solchen sogenannten fake accounts können bei Facebook zudem sogenannte Fanseiten erstellt werden, die kein Impressum verlangen. Diese Anonymität ist problematisch – vor allem im Kontext von Wahlen und Diffamierungskampagnen. Wünschenswert wäre es deshalb, eine umfassende Impressumspflicht gesetzlich festzulegen und internationale Regelungen einzuführen, die zwischen domain privacy und nötiger Transparenz abwägen.

Fake accounts, social bots und Wahlmanipulation

Eine Studie des Internet-Instituts der Universität Oxford hat gezeigt, dass über gefälschte Nutzerkonten betriebene social bots ebenfalls eine immer wichtigere Rolle in Wahlkämpfen und Krisensituationen einnehmen (→ Woolley/Howard 2017). Diese automatisch generierten Programme täuschen bei bestimmten Meldungen oder Tweets eine größere Verbreitung vor. Die Absicht besteht darin, die Aufmerksamkeit für ausgewählte Themen zu steigern. Die algorithmische Relevanzermittlung sozialer Netzwerke, wie sie beispielsweise von Facebook betrieben wird, verstärkt die auf diese Weise hervorgerufenen Verzerrungseffekte zusätzlich.

Im April 2017 räumte Facebook ein, dass es Versuche gegeben habe, im Vorfeld der amerikanischen Präsidentschaftswahlen über gefälschte Accounts die öffentliche Meinung zu beeinflussen. Ein halbes Jahr später gab das Unternehmen bekannt, dass versucht worden sei, über gekaufte Anzeigen gesellschaftliche Spaltungen in den USA voranzutreiben, etwa bei Themen wie Einwanderung und Waffenbesitz. Facebook vermutete Einflussversuche aus Russland (→ Stamos 2017). Im Oktober 2018 veröffentlichte Twitter zehn Mio. Nachrichten von 3.841 Accounts, hinter denen sich offenbar die staatliche Internet Research Agency aus Russland verbarg. Über diese Nutzerkonten wurde auch versucht, Einfluss auf die öffentliche Meinung in Deutschland zu nehmen (→ Holland 2018). In seiner Anklageschrift vom Februar 2018 gegen 13 russische Staatsbürger legte US-Sonderermittler Robert Mueller detailliert dar, wie die

Internet Research Agency unter falschen Identitäten versuchte, mittels Werbung über Facebook, Instagram und andere soziale Netze die Gegner Donald Trumps zu schwächen und der mit den Demokraten sympathisierenden Wählerschaft nahezulegen, der Wahl fernzubleiben. Facebook und Twitter haben inzwischen zahlreiche verdächtige Nutzerkonten gelöscht.

HERAUSFORDERUNG DIGITALE HASSKULTUREN

Durch seine Veränderlichkeit und die niedrigen Einstiegshürden erzeugt das Internet sogenannte „Schwarmeffekte". Ohne solche Effekte würden beliebte Internet-Plattformen wie Wikipedia oder YouTube nicht existieren. Problematisch sind sie dann, wenn sie sich in digitalen Hasskulturen manifestieren. Diese sind durch einen ausgeprägten Antipluralismus, die Zurückweisung liberaler Wertvorstellungen sowie das Fehlen einer aufgeklärten Diskussionskultur gekennzeichnet. Da sich Schwarmstrukturen im Internet klassischen Vorstellungen von Gruppenmitgliedschaften mit ideologisch geschlossenen Überzeugungen entziehen, sind die aus ihnen hervorgehenden Verhaltensweisen weniger vorhersehbar.

Radikale Ideologen nutzen „Schwarmeffekte" des Internets aus

Strategisch denkende Akteure haben den Charakter digitaler Schwarmstrukturen erkannt und versuchen, diese für sich nutzbar zu machen. Sie organisieren politische Kampagnen, um die sich temporäre Gemeinschaften bilden, deren Diskurse die Grenzen zwischen alltäglichen Äußerungen und ideologischer Propaganda aufheben.

Ein beliebtes Mittel sind sogenannte Memes: zumeist humoristische Bild-Text-Collagen mit politischen Botschaften, die sich besonders gut über soziale Netzwerke verbreiten und im digitalen Kontext zunehmend textbasierte Kommunikation ersetzen. Für Strategen aus dem rechtsextremen Spektrum sind sie der zentrale Teil eines „Informationskriegs", in dem die Voraussetzungen für eine Rechtswende geschaffen werden sollen (→ Precht 2019).

Eine weitere Strategie ist die Veröffentlichung privater Informationen im Internet, die betroffene Personen oder Gruppen bloßstellen oder einschüchtern soll. Immer häufiger stecken politische Motive hinter diesem sogenannten doxing (→ Douglas 2016). Der wohl bekannteste doxing-Fall in Deutschland ist die Verbreitung privater Daten hunderter Personen des öffentlichen Lebens durch den 20-jährigen Johannes S. im Dezember 2018. Sowohl seine Auswahl des betroffenen Personenkreises als auch sein Verhalten deuten auf eine rechtsextreme Motivation.

Ein weiterer Fall war das rechtsextreme Online-Netzwerk Reconquista Germanica (RG). Im Vorfeld der Bundestagswahlen 2017 sorgte die Gruppierung mit dem Versuch für Aufsehen, Online-Diskurse zu unterwandern, die Anhänger demokratischer Parteien einzuschüchtern und zur Wahl der Alternative für Deutschland (AfD) zu animieren (→Ebner/Davey 2017). Die Planung und Verbreitung von Falschinformationen, die

Erstellung und Verbreitung beleidigender oder rassistischer Memes, das Kapern von Hashtags sowie die gezielte Manipulation von Diskussionsverläufen auf Internetforen gehören, ebenso wie das ‚doxing', zum Repertoire der RG.

Diese Beispiele zeigen, dass digitale Hasskulturen nicht ungesteuert, aber auch nicht vollständig organisiert sind. Ihr fluider Charakter macht es oft schwer, die mit ihnen verbundenen Strategien und ihre Herkunft zu identifizieren und zu verstehen. Sie haben indessen Auswirkungen auf die Bereitschaft anderer Nutzer, ihre politische Meinung zu äußern. Einer repräsentativen Studie zufolge beteiligt sich fast die Hälfte der hessischen Bevölkerung nicht an Diskussionen im Netz – und zwar unter anderem aus Angst, mit Hassreden konfrontiert zu werden (→ IDZ/Campact 2018). In Zeiten, in denen die Informationsgewinnung und das Kommunikationsverhalten der jungen Generationen bevorzugt über digitale Kanäle geschieht, ist dies eine bedenkliche Entwicklung.

5.3 ↙ Wirkungsmechanismen von Manipulations- und Mobilisierungsversuchen

Was lässt sich zur Wirksamkeit der beschriebenen Strategien sagen? Zu unterscheiden sind Versuche, die auf ein bestimmtes Ereignis zielen, etwa die Beeinflussung von Wahlen, und Versuche, die auf die strukturelle Veränderung von politischen Einstellungen gerichtet sind. Einzelne Postings können zudem lediglich zuspitzen oder verzerren, sie können falsche Behauptungen aufstellen, aber auch Hassbotschaften enthalten und zur Gewalt aufrufen.

In der Forschung herrscht weitgehend Konsens darüber, dass die bekannten Versuche, organisiert in die sozialen Netzwerke hineinzuwirken, für den Ausgang der letzten amerikanischen Präsidentschaftswahl nicht entscheidend waren. Es lassen sich aber Hinweise finden, dass sie bereits vorhandene gesellschaftliche Polarisierungen verstärken und unter bestimmten Voraussetzungen Radikalisierung fördern können (Lischka/Stöcker 2017) → **35** /147. Was konkrete Effekte angeht, liegen bisher jedoch keine eindeutigen Ergebnisse vor.

Nicht jede Nachricht findet zudem ein größeres Publikum. Die Verbreitung von Mitteilungen unterliegt komplizierten Prozessen der Aufmerksamkeitsgewinnung und Informationsverteilung. Das Interesse von Facebook besteht zum Beispiel darin, Nutzer möglichst lange auf dem Portal zu halten, um mehr Werbung platzieren zu können. Um das zu erreichen, nutzt das Unternehmen seine detaillierten Kenntnisse über die Interessen der Nutzer. Die Verteilung von Informationen erfolgt also nicht entlang inhaltlicher Relevanz auf Grundlage journalistischer Kriterien, sondern entlang des individuell möglicherweise Interessanten auf Basis des vorherigen Nutzerverhaltens

35 Radikalisierung im Internet

Es ist eine gängige Annahme, dass zwischen Radikalisierung und der Nutzung sozialer Netzwerke ein enger Zusammenhang besteht. Wissenschaftliche Studien sind jedoch zu unterschiedlichen Ergebnissen gelangt. Ein methodisches Problem besteht darin, dass virtuelle und reale Lebenswirklichkeiten verschmelzen und damit die spezifischen Online-Faktoren einer Radikalisierung schwer zu bestimmen sind.
Unbestritten ist, dass nicht mehr allein Islamisten, sondern auch Kräfte des äußeren rechten Spektrums besonders präsent und aktiv in den sozialen Netzwerken sind. Unklar ist hingegen das „Warum": Nutzen rechte Kräfte die sozialen Netzwerke nur besonders strategisch (zum Beispiel durch „Armeen" von Online-Aktivisten oder sogenannten bots, die Stimmungen zu beeinflussen versuchen)? Bieten diese Medien eine Gelegenheitsstruktur, die besonders vorteilhaft für ihre Manipulationen sind (zum Beispiel durch die Anonymität des Netzes, die Dehumanisierung und Enthemmung begünstigt)? Gehört es gar zu den Eigenschaften des Internets, dass sich dessen Nutzer selbst manipulieren (zum Beispiel durch die Begünstigung simplifizierender und emotionalisierender Inhalte, die den Affekten entsprechen, die bspw. der Rechtspopulismus adressiert)? Die Artikulation von (Be-)Drohungen spielt aber in jedem Fall eine große Rolle in sozialen Netzwerken und ein Zusammenhang mit der Rechtfertigung von Gewalthandeln ist plausibel.
Erklären lässt sich dies zum einen durch eine veränderte Verteilung von Informationen. Traditionelle journalistische Qualitätskontrollen haben an Einfluss eingebüßt und nicht-professionelle Quellen, insbesondere auch solche, die Falschmeldungen in die Welt setzen, größere Verbreitung erfahren. Zum anderen spielt eine veränderte Informationsgeografie eine Rolle, bei der Nachrichten über Unglücksfälle oder Verbrechen, die zuvor auf lokale Medien beschränkt blieben, über die digitalen Medien überregionale oder gar globale Verbreitung finden können.
Solche Ereignisse rücken damit näher an die Medienrezipienten heran, scheinen sich zu häufen und können sich so auf das Bedrohungsempfinden auswirken. Dieser Effekt kann über die strategische Verbreitung und Zuspitzung bestimmter Nachrichten verstärkt werden. Oft werden diese mit Handlungsaufforderungen verbunden. Nimmt man all diese Faktoren zusammen, so ist es durchaus einleuchtend, dass einzelne Individuen oder Gruppen zur Überzeugung gelangen können, selbst gegen die vermeintliche Bedrohung vorgehen und für Sicherheit sorgen zu müssen.

(→ Lischka/Stöcker 2017). Untersuchungen zeigen überdies, dass ungewöhnliche Inhalte auf größeres Interesse stoßen und deshalb mehr Reichweite erlangen. Dazu zählen insbesondere polarisierende Botschaften und Falschmeldungen. Gerade solche Beiträge hat Facebook in der Vergangenheit stärker beworben (→ Vosoughi et al. 2018).

Demokratische Willensbildung vs. fragmentierte Netz-Öffentlichkeiten

Wenn die Auswahlkriterien, nach denen Wählern personalisierte Wahlwerbung zugespielt wird, unbekannt bleiben, greift das deutlich in den demokratischen Willensbildungsprozess ein. Eine transparente Kommunikation, die als konstitutiv für die demokratische Meinungsbildung gilt, ist damit nicht gegeben, und in den sozialen Netzwerken bilden sich fragmentierte, konkurrierende und oft transnationale Öffent-

lichkeiten. Die gezielte Ansprache bestimmter Gruppen oder einzelner Individuen ersetzt so den allgemeinen öffentlichen Diskurs – im besseren Falle durch Informationen, die auf ein Profil zugeschnitten sind; im schlechteren in Form von Falschmeldungen und Hassbotschaften.

5.4 ↙ Gegenmaßnahmen und ihre Schwächen[2]

VERSUCHE DER EINDÄMMUNG DURCH DIE ONLINE-PLATTFORMEN

Angesichts der Diskussionen um Desinformationen (fake news), Hassrede und Manipulationen durch bots und gefälschte Nutzerprofile kündigten die großen Online-Plattformen eine Reihe von Maßnahmen an (und führten sie zum Teil bereits ein), die diesen Problemen entgegenwirken sollen.

Die Anbieter von Online-Diensten setzen hierbei einerseits an technischen Lösungen an, andererseits an einigen wenigen Transparenzregeln. Die technischen Veränderungen betreffen zuvorderst die Steuerungsmechanismen der Algorithmen. Facebook räumt eigenen Angaben zufolge nun „bedeutungsvollen Interaktionen“ Vorrang ein, wie dem Kommentieren oder Teilen von Beiträgen von Freunden und der Familie. Das kann aber Filterblasen verstärken. Zudem optimiert Facebook Inhalte weiterhin so, dass die Nutzer möglichst lange auf der Plattform bleiben. Seltener angezeigt werden öffentliche Inhalte wie Nachrichten-Beiträge, Videos oder Botschaften von Unternehmen. Nachrichtenquellen werden zudem nach neuen Relevanzkriterien eingestuft – so präferiert Facebook die Einschätzungen repräsentativ ausgewählter und stetig wechselnder Gruppen von Menschen auf Facebook und lokale Nachrichtenquellen, um die Verbreitung von Falschinformationen und problematischen Posts einzudämmen. Da Algorithmen alleine nur sehr schwer Desinformationen von zutreffenden Nachrichten unterscheiden können, greift Facebook seit Anfang 2017 in über 20 Ländern auf Drittanbieter zurück, die häufig geteilte Meldungen auf deren Wahrheitsgehalt prüfen sollen. Dieses Verfahren ist allerdings nicht unumstritten. Sowohl die Transparenz der Prüfkriterien als auch die politische Neutralität der jeweiligen Drittanbieter wird bemängelt. Im September 2018 ergänzte Facebook sein Repertoire für den Kampf gegen Wahlbeeinflussung nochmals. Das Unternehmen kündigte die Einrichtung eines sogenannten „War Rooms“ an, in dem ein Team von ca. 20 Personen Kampagnen, über die Falschmeldungen verbreitet werden könnten, mittels Analyseprogrammen entdecken und Gegenmaßnahmen einleiten soll.

Facebook und Google reagieren mit veränderten Algorithmen und lassen Nachrichten überprüfen

Google stellte im Februar 2019 ein Konzept vor, das ebenfalls auf die Änderung von Algorithmen fokussiert. Zum einen sollen Ranking-Algorithmen die Qualität von Mitteilungen auf Google News, Google Search und YouTube bestimmen und Artikel entsprechend priorisieren. Neben einer solchen Gewichtung der Informationsqualität

sollen intelligente Systeme sogenannte „bösartige Akteure“, die Nutzer etwa täuschen und Falschinformationen verbreiten wollen, entdecken und deren Inhalte entsprechend herabstufen. Zudem will Google den Nutzern mehr Kontextinformationen zur Verfügung stellen, etwa in Form von Links zu weiteren Beiträgen, um ihnen bessere Einschätzungen zu ermöglichen und keine YouTube-Videos mehr empfehlen, die verschwörungstheoretische oder irreführende Inhalte transportieren → **37** /149.

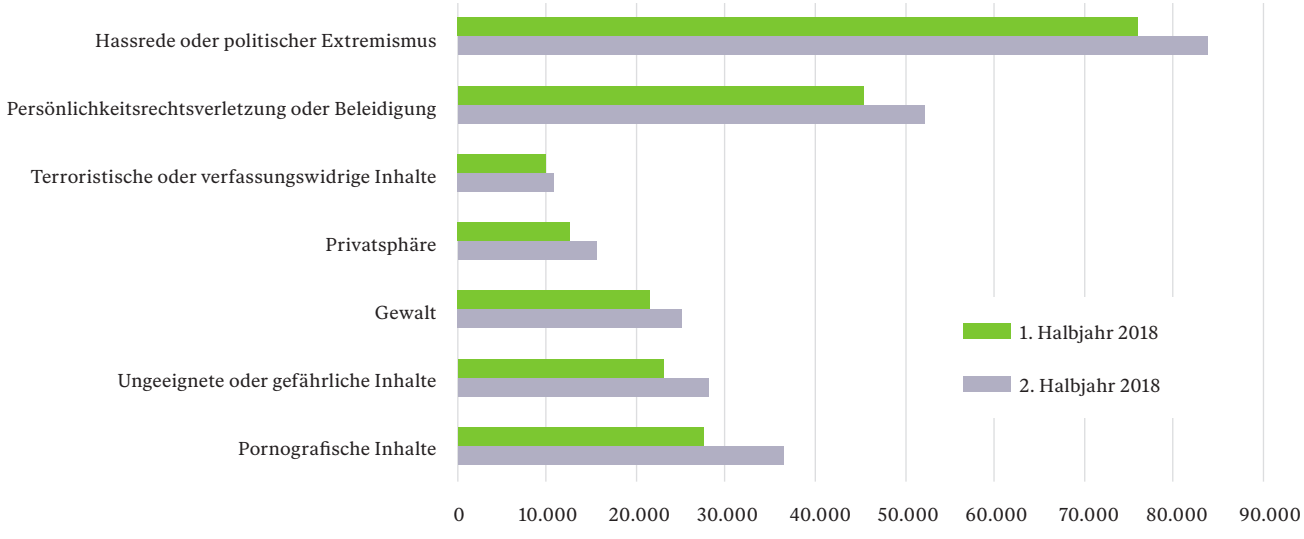
Facebook und Twitter kündigten zudem mehr Transparenz bei politischen Werbeanzeigen an. Bei Twitter soll politische Werbung nur noch über zertifizierte Accounts geschaltet werden können. Darüber hinaus sollen Informationen über die Sponsoren der Werbung, über die Zielgruppen und die Anzahl der Aufrufe eine Woche lang im sogenannten ads transparency center abfragbar sein.

Auch Facebook eröffnet seinen Nutzern die Möglichkeit, sich alle Anzeigen anzuschauen, die bei Facebook, Instagram und Messenger sowie bei Partner-Diensten geschaltet werden. Sichtbar soll auch sein, zu welchem Zeitpunkt und unter welchem Namen eine Facebook-Seite angelegt worden ist, wer die Werbung finanziert hat und an welche Zielgruppen sie sich richtet. In einem Archiv will das Unternehmen Wahlanzeigen und Anzeigen zu politischen Themen sieben Jahre lang vorhalten.

Diese technischen Maßnahmen und Transparenzversuche gehen in die richtige Richtung, bleiben aber den kommerziellen Interessen der Unternehmen untergeordnet. Es regt sich deshalb der Wunsch nach stärkerer staatlicher Regulierung, die idealerweise international abgestimmt sein sollte, um Umgehungsversuchen entgegenwirken zu können.

37 Gemeldete Inhalte bei YouTube, aufgeschlüsselt nach Beschwerdegrund

Quelle → **5** /157



STAATLICHE GEGENMAßNAHMEN

Gegenwärtig konzentrieren sich staatliche Bemühungen vor allem auf die Unterbindung von Terrorpropaganda, Hetz- oder Hasskommentaren. Die bislang auf nationaler, europäischer und internationaler Ebene ergriffenen Gegenmaßnahmen zielen im Schwerpunkt auf strukturelle Regulierung, etwa durch Kontrollmaßnahmen, bewegen sich aber meist auf einer rein deklaratorischen Ebene. Darüber hinaus gibt es gerade bei den präventiven Ansätzen im Bereich der politischen Bildung Verbesserungsbedarf.

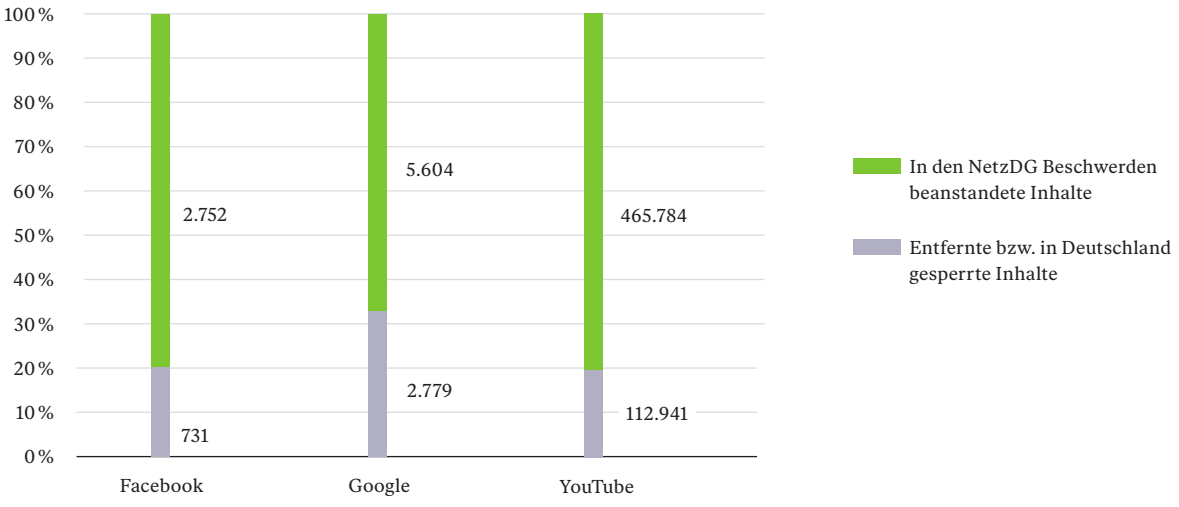
Die Debatte um strukturelle Regulierungen und Kontrollmaßnahmen fokussiert sich in Deutschland auf das am 1. Januar 2018 in Kraft getretene NetzDG. Es sieht Bußgelder für Social Media-Unternehmen vor, wenn sie kein wirksames Verfahren für den Umgang mit Beschwerden über rechtswidrige Inhalte nachweisen können. Als rechtswidrig gelten gemäß NetzDG und durch dessen Verweise auf das Strafgesetzbuch unter anderem Hassinhalte. Das Gesetz soll jedoch auch die Verbreitung bestimmter Formen von Desinformationen unterbinden. Gemeint sind Tatbestände wie landesverräterische Fälschung, Verleumdung und Fälschung beweiserheblicher Daten → **37**/150. Da die Anbieter selbst entscheiden müssen, ob ein Inhalt „offensichtlich rechtswidrig" bzw. „rechtswidrig" ist, besteht grundsätzlich die Gefahr des „overblocking". Statt auf kurze Löschfristen sollte deshalb mehr Gewicht auf die schnelle Ermittlung der Urheber von strafrechtlich relevanten Äußerungen gelegt werden (→ Buermeyer 2017).

NetzDG bedarf einer Novellierung

37 Über das NetzDG-Meldeformular übermittelte Beschwerden und Löschungen im Jahr 2018

Quelle → **5** /157

Prozent der jeweiligen übermittelten Beschwerden
1. und 2. Halbjahr



Mit dem Fokus allein auf die sozialen Netzwerke beantwortet das NetzDG die Frage des „Wer?" bislang nur in Teilen, denn ausgenommen sind „Plattformen mit journalistisch-redaktionell gestalteten Angeboten, die vom Diensteanbieter selbst verantwortet werden" sowie „Plattformen, die zur Individualkommunikation oder zur Verbreitung spezifischer Inhalte bestimmt sind". Hinzu kommen nach wie vor Unklarheiten des „Wie?", d.h. wie wirksame Verfahren aussehen, wie sie transparent und nachvollziehbar gestaltet und wie sie überprüft werden sollen. Eine Präzisierung dieser nur in Teilen beantworteten Fragen verlangt nach einer Novellierung des NetzDG.

Auf EU-Ebene gibt es weitere Vorhaben und Maßnahmen. Im Juni 2015 richtete die EU bei Europol die Internet Referral Unit (IRU) ein. Inhalte sozialer Netzwerke können von einem EU-IRU-Analysten, einem Mitgliedstaat oder einem Dritten, der über eine operative Vereinbarung mit Europol und ein eigenes IRU-System verfügt, markiert werden – der entsprechende Inhalt wird dann geprüft und ggf. werden Maßnahmen zur Löschung eingeleitet. Weiterhin schuf die EU Einrichtungen zur Bekämpfung gezielter Desinformationen. Im März 2015 rief sie beispielsweise die East StratCom Task Force ins Leben. Sie analysiert und berichtet über Desinformationstrends, korrigiert Falschinformationen und soll das Bewusstsein im Hinblick auf Desinformationskampagnen schärfen, die vom russischen Staat und russischsprachigen Medien ausgehen könnten.

Spannungsverhältnis zwischen Standards der Unternehmen und dem rechtlichen Rahmen

Die EU-IRU und das NetzDG stellen lediglich Markierungs- und Verweissysteme dar. Letztlich ist es Sache der Online-Anbieter, die betroffenen Inhalte zu entfernen. Der EU-IRU steht kein EU-weites Berichtssystem zur Verfügung. Darüber hinaus kann sich Europol bei der Entfernung von Inhalten bisher nur auf die Gemeinschaftsstandards der jeweiligen Internetunternehmen und nicht auf die EU-Definition von „terroristischen Straftaten" verlassen. Dieses Spannungsverhältnis zwischen dem nationalen/supranationalen Rechtsrahmen einerseits und den Nutzungsbedingungen der Social-Media-Unternehmen andererseits hat Konsequenzen. So fand etwa Facebook einen Weg, das NetzDG dadurch zu umgehen, dass es seine Nutzer ermutigt, Inhalte nicht nach den Bestimmungen des NetzDG anzuzeigen, sondern als Verstoß gegen Gemeinschaftsstandards zu melden (→ Echikson/Knodt 2018).

Staaten, die EU sowie internationale Organisationen und Einrichtungen versuchten bisher, Schwächen bei Kontrolle und Durchgriff mit deklaratorischen Maßnahmen, Dialogforen und Selbstverpflichtungen auszugleichen. Beispiele hierfür sind das EU-geführte EU Internet Forum, das branchengeführte Global Internet Forum to Counter Terrorism (GIFCT) oder auch der United Nations Plan of Action on Hate Speech. Diese Foren und Selbstverpflichtungen setzen sich zum Ziel, Wege und Maßnahmen zu erarbeiten, um gegen manipulative Inhalte, die etwa Radikalisierung und Terrorismus Vorschub leisten könnten, vorzugehen. Gleichzeitig sollen zivilgesellschaftliche Akteure dazu befähigt werden, effektive Gegenreden im Internet zu platzieren.

Die EU-Kommission hat im September 2018 den Entwurf zu einer Verordnung vorgelegt, die allen auf dem Gebiet der EU tätigen Online-Firmen vorschreiben würde, „terroristische Inhalte“ unverzüglich von ihren Plattformen zu nehmen. Wenn die Anbieter von einer zuständigen Behörde über entsprechende Inhalte informiert werden, müssten sie diese innerhalb einer Stunde entfernen oder den Zugang zu ihnen deaktivieren. Die Dienste müssten zudem präventiv dafür sorgen, dass derartige Inhalte nicht in ihren Angeboten auftauchen. Bei Verstößen würden den Anbietern Bußgelder von bis zu vier Prozent ihres jährlichen Umsatzes drohen. Der stärkere Fokus auf behördliche Meldungen ist begrüßenswert. Wie auch beim NetzDG bleiben aber Herausforderungen hinsichtlich der Rolle der Intermediäre und der Transparenz der Verfahren bestehen.

HERAUSFORDERUNGEN UND VORSCHLÄGE

Die hier exemplarisch beschriebenen Eingriffe und Selbstverpflichtungen werfen alle, wenn auch in unterschiedlichem Maße, sehr grundsätzliche Fragen zu Grundrechten auf: Inwieweit wird die Meinungsfreiheit beschränkt? Wird Zensur geübt (intendiert oder unintendiert)? Wo sind womöglich Fehlanreize in die Gesetzestexte eingebaut, die zu einem vorauseilenden sogenannten overblocking von Inhalten führen?

Regulierung darf Meinungsfreiheit nicht gefährden

Es gibt zudem keine konzeptionelle Klarheit bei den Kernbegriffen: Wo liegt die Grenze zwischen Hassrede und Satire? Wie kann man Desinformationen von unproblematischen Meinungsäußerungen unterscheiden? Zwar sind es letztendlich Gerichte, die über die Rechtmäßigkeit zu entscheiden haben – das NetzDG ist jedoch so angelegt, dass es diese Abwägung zunächst den Plattformbetreibern überlässt.

In diesem Zusammenhang geben die Entwicklungen bei der automatisierten Entfernung von Inhalten Anlass zur Sorge. Es ist für die großen Online-Unternehmen verlockend, sich aus Kosten- und Machbarkeitsgründen mehr und mehr auf eine automatisierte Erkennung illegaler Inhalte zu verlassen. Der Verordnungsentwurf der EU-Kommission zu den „terroristischen Inhalten” ist zum Beispiel ohne automatisierte Filtertechnologien kaum umzusetzen. Sämtliche Maßnahmen, die auf die Entfernung von Inhalten zielen, laufen Gefahr, in das Grundrecht der freien Meinungsäußerung einzugreifen. Zurückhaltung – insbesondere von staatlicher Seite – ist hier deshalb immer geboten.

Weiterhin besteht das Problem von Ausweichstrategien im transnationalen Raum. Gelöschte Inhalte tauchen auf einer anderen Plattform wieder auf oder Aktivitäten werden in das sogenannte darknet oder auf Dienste verlegt, die nicht dem NetzDG unterliegen, etwa die Messenger-Apps.

Statt auf die Kontrolle von Inhalten zu setzen, sollten bevorzugt Maßnahmen ergriffen werden, die die Transparenz erhöhen. Dies betrifft die Anbieter von Online-Diensten ebenso wie Staaten. Die Anbieter haben nur erste Schritte zu mehr Transparenz eingeleitet, etwa hinsichtlich der Verfahren des Rankings von Informationen und der dahinterliegenden Algorithmen. Die Datensätze, die Analysekategorien sowie die Logik und die Parameter, auf die die Algorithmen optimiert werden, sollten perspektivisch einer rechtsstaatlichen Kontrolle unterzogen werden. Dies könnte etwa in Form unabhängiger regelmäßiger Überprüfungen unter Wahrung der Geschäftsgeheimnisse der Anbieter geschehen. Wir empfehlen die Einrichtung einer unabhängigen Agentur auf EU-Ebene, der gegenüber Social Media Anbieter zur (vertraulichen) Offenlegung ihrer Algorithmen verpflichtet sind, um im EU-Raum operieren zu dürfen.

Transparenz über Funktionsweise der Algorithmen erhöhen

Bei internationalen Maßnahmen sollte die Bundesregierung sehr genau darauf achten, nicht den Zensur- und Kontrollbestrebungen illiberaler Staaten Tür und Tor zu öffnen. Ein Beispiel für die notwendige Differenzierung sind zwei parallele Prozesse in den Vereinten Nationen (VN): zum einen treibt Russland eine Open-ended Working Group (OEWG) voran (A/RES/73/27), die auf den Schutz souveräner nationaler Interessen bei der Regulierung des Internets zielt. Dieses Vorgehen ist kritisch zu sehen. Unterstützenswerter ist der Regelbildungsprozess der Group of Governmental Experts (GGE), die unter Federführung der USA bis mindestens ins Jahr 2021 (A/RES/73/266) an Grundlinien für eine gemeinschaftsorientierte und völkerrechtlich basierte Internetregulierung arbeiten wird (→ Kettemann 2019).

Auch Parteien und politische Gruppierungen können mehr tun. Ein erster Schritt zur Schaffung von mehr Transparenz in Bezug auf Wahlwerbung wäre die Abgabe von Selbstverpflichtungen politischer Parteien und ihrer Kandidaten dazu, auf die Verbreitung bestimmter Informationen über Online-Plattformen zu verzichten. Dazu zählen falsche, erfundene oder gestohlene Informationen, manipulierte Videos und der Einsatz von social bots zur Bloßstellung politischer Gegner. Ein Ansatz in diese Richtung ist die Erklärung der Transatlantic Commission on Election Integrity.

Regierungen können nicht nur durch negative Anreize eingreifen, sondern positiv gestalten: Beispielsweise könnte in Deutschland die vielfältige Landschaft der politischen Bildungsträger noch stärker genutzt werden, um Medienkompetenzen zu vermitteln. Noch wichtiger ist, Medien- und Debattenkompetenzen auf allen Ebenen der Bildung – von der frühkindlichen bis zur berufsbegleitenden – zu verankern, also in Lehrplänen und Lehreraus- und -weiterbildungen. Wenn traditionelle Medien bei der Vermittlung von Grundinhalten zunehmend an Einfluss verlieren, muss darüber nachgedacht werden, wie die öffentlich-rechtliche Pflicht zur informationellen Grundversorgung auch im Digitalen umgesetzt werden kann. Eine bloße Ausweitung der öffentlich-rechtlichen Rundfunkstruktur ist vermutlich ein zu einfacher und zu kurzer Weg. Vielmehr müsste der bottom-up-Logik des Internets entsprechend eine Vielzahl an Formaten und Institutionen dauerhaft öffentlich gefördert werden – von Recherchenetzwerken über kleinteilige und auch lokale journalistische Tätigkeiten. So kann auch der Staat aktiver, positiver und umfassender mit den gegenwärtigen Herausforderungen für die Stabilität der liberalen Demokratie umgehen.

Medienkompetenz als zentrales Ziel von Bildung

SCHLUSSFOLGERUNG

Manipulations- und Mobilisierungsversuche durch extremistische und populistische Akteure von Innen und Außen treffen liberale Demokratien in ihrem Kern: sie schwächen Konfliktlösungs- und innere Friedensfähigkeit. Offen zugängliche Informationen und der Austausch von Argumenten bleiben Grundpfeiler demokratischer Willensbildung. Es gibt drei wesentliche Herausforderungen: 1) strategische nichtstaatliche, aber teils auch staatliche Akteure, die mit relativ geringem Aufwand öffentliche Diskurse manipulieren, Falschmeldungen lancieren und Polarisierungstendenzen verstärken; 2) Verstärkereffekte durch das Schwarmverhalten von Nutzern sozialer Netzwerke und die Fluidität der zahlreichen Plattformen; 3) intransparente Algorithmen, die bei der Verbreitung aber auch dem Blockieren von Themen inzwischen eine entscheidende Rolle einnehmen und die menschliche Urteilskraft immer weiter in den Hintergrund drängen. Staat und Zivilgesellschaft sind aber nicht machtlos. Sie können Transparenz über Quellen und Verfahren einfordern. Die Grundlagenforschung kann Klarheit bei den Rechtsbegriffen schaffen und aufzeigen, welche Wirkungen von der Kommunikation in sozialen Netzwerken ausgehen. Entscheidungen darüber, wie reguliert wird, sollten nicht übereilt getroffen und auf Grund der transnationalen Reichweite der Netzwerke international abgestimmt werden. Die Bundes- und Landesregierungen können den Bereich der primären Prävention stärken, indem sie die Medienkompetenz erhöhen – und zwar sowohl durch Projektangebote der politischen Bildung als auch durch den dauerhaften Ausbau von Kompetenzen auf allen Ebenen des Bildungssystems. In dieser aktiven, vorsorgenden Gestaltung liegen die größten Chancen zur Wahrung des inneren Friedens und Stärkung der liberal-demokratischen Ordnung gegenüber transnationalen Risiken durch die Möglichkeiten des Internets.

1 Eigene Erhebung aus Pressemitteilungen der Generalbundesanwaltschaft, 2015-2018.

2 Dieser Abschnitt hat sehr von Kommentierungen durch Matthias Kettemann, Niklas Rakowski und Thorsten Thiel profitiert. Wir danken ihnen dafür.

Autorinnen und Autoren

Reem Ahmed
IFSH – Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Stephen Albrecht
IFSH – Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Dr. Marc von Boemcken (Koordination)
BICC – Bonn International Center for Conversion

Maik Fielitz
IFSH - Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Dr. Julian Junk (Koordination)
HSFK – Leibniz Institut Hessische Stiftung Friedens- und Konfliktforschung

PD Dr. Martin Kahl (Koordination)
IFSH - Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Holger Marcks
IFSH - Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Manjana Sold
HSFK - Leibniz Institut Hessische Stiftung Friedens- und Konfliktforschung

Quellenverzeichnis

Bonn International Center for Conversion (BICC)/Leibniz-Institut Hessische Stiftung Friedens- und Konfliktforschung (HSFK)/ Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH)/Institut für Entwicklung und Frieden (INEF) 2018: Friedensgutachten 2018. Kriege ohne Ende. Mehr Diplomatie, weniger Rüstungsexporte, Berlin et al.

Buermeyer, Ulf 2017: Facebook-Justiz statt wirksamer Strafverfolgung?, in: https://www.lto.de/recht/hintergruende/h/netzwerkdurchsetzungsgesetz-netzdg-facebook-strafverfolgung-hate-speech-fake-news/; 24.3.2017.

Douglas, David M. 2016: Doxing: A Conceptual Analysis, in: Ethics and Information Technology 18, 199–210.

Ebner, Julia/Davey, Jacob 2017: The Fringe Insurgency. Connectivity, Convergence and Mainstreaming of the Extreme Right, London.

Echikson, William/Knodt, Olivia 2018: Germany's NetzDG: A Key Test for Combatting Online Hate, in: https://www.ceps.eu/publications/germany%E2%80%99s-netzdg-key-test-combatting-online-hate; 28.02.2019.

Holland, Martin 2018: Russische Trolle in Deutschland: Per Twitter die öffentliche Meinung vergiften, heise.de, 24.10.2018, https://www.heise.de/newsticker/meldung/Russische-Trolle-twitterten-auf-Deutsch-als-normale-Nutzer-und-lokale-Boten-4200551.html; 28.02.2018.

IDZ/Campact 2018: #Hass im Netz. Der schleichende Angriff auf unsere Demokratie - Eine repräsentative Untersuchung in Hessen, Jena.

Institute for Economics & Peace 2018: Global Terrorism Index 2018. Measuring the Impact of Terrorism, Sydney.

IOM (Internationale Organisation für Migration) 2019a: Missing Migrants. Tracking Deaths along Migratory Routes, in: https://missingmigrants.iom.int/; 28.02.2019.

IOM (Internationale Organisation für Migration) 2019b: Flow Monitoring Europe, in: http://migration.iom.int/europe?type=arrivals; 20.03.2019.

Kettemann, Matthias C. 2019: Internationale Regeln für soziale Medien: Menschenrechte wahren und Desinformation bekämpfen. Global Governance Spotlight 2/2019. Stiftung Entwicklung und Frieden, Bonn.

Lischka, Konrad/Stöcker, Christian 2017: Digitale Öffentlichkeit - Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen. Arbeitspapier im Auftrag der Bertelsmann Stiftung, Gütersloh.

Poushter, Jacob/Manevich, Dorothy 2017: Globally, People Point to ISIS and Climate Change as Leading Security Threats. Concern about Cyberattacks, World Economy also Widespread, in: https://www.pewglobal.org/2017/08/01/globally-people-point-to-isis-and-climate-change-as-leading-security-threats/; 28.02.2019.

Precht, Jørn 2019: Verbreitung populistischer Narrative in den Kommentarspalten des sozialen Netzwerks Facebook, in: Müller, Michael/Precht, Jørn (Hrsg.): Narrative des Populismus, Wiesbaden, 93–114.

R+V Versicherung 2018: Die Ängste der Deutschen 2018, in: https://www.ruv.de/presse/aengste-der-deutschen; 28.02.2019.

Stamos, Alex 2017: An Update on Information Operations on Facebook, September 6, 2017, https://newsroom.fb.com/news/2017/09/information-operations-update/; 28.02.2019.

Statista 2019: Europäische Union: Anteil ausländischer Staatsangehöriger an der Gesamtbevölkerung in den Mitgliedsstaaten im Jahr 2017, in: https://de.statista.com/statistik/daten/studie/73995/umfrage/auslaenderanteil-an-der-bevoelkerung-der-laender-der-eu27/; 28.02.2019.

University of Maryland/National Consortium for the Study of Terrorism and Responses to Terrorism 2018: Global Terrorism in 2017. Background Report, Maryland.

Vosoughi, Soroush/Roy, Deb/Aral, Sinan 2018: The Spread of True and False News Online, in: Science 359: 6380, 1146–1151.

Woolley, Samuel C./Howard, Philip N. 2017: Computational Propaganda Worldwide: Executive Summary, in: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf; 28.02.2019.

Abbildungen / Grafiken / Tabellen