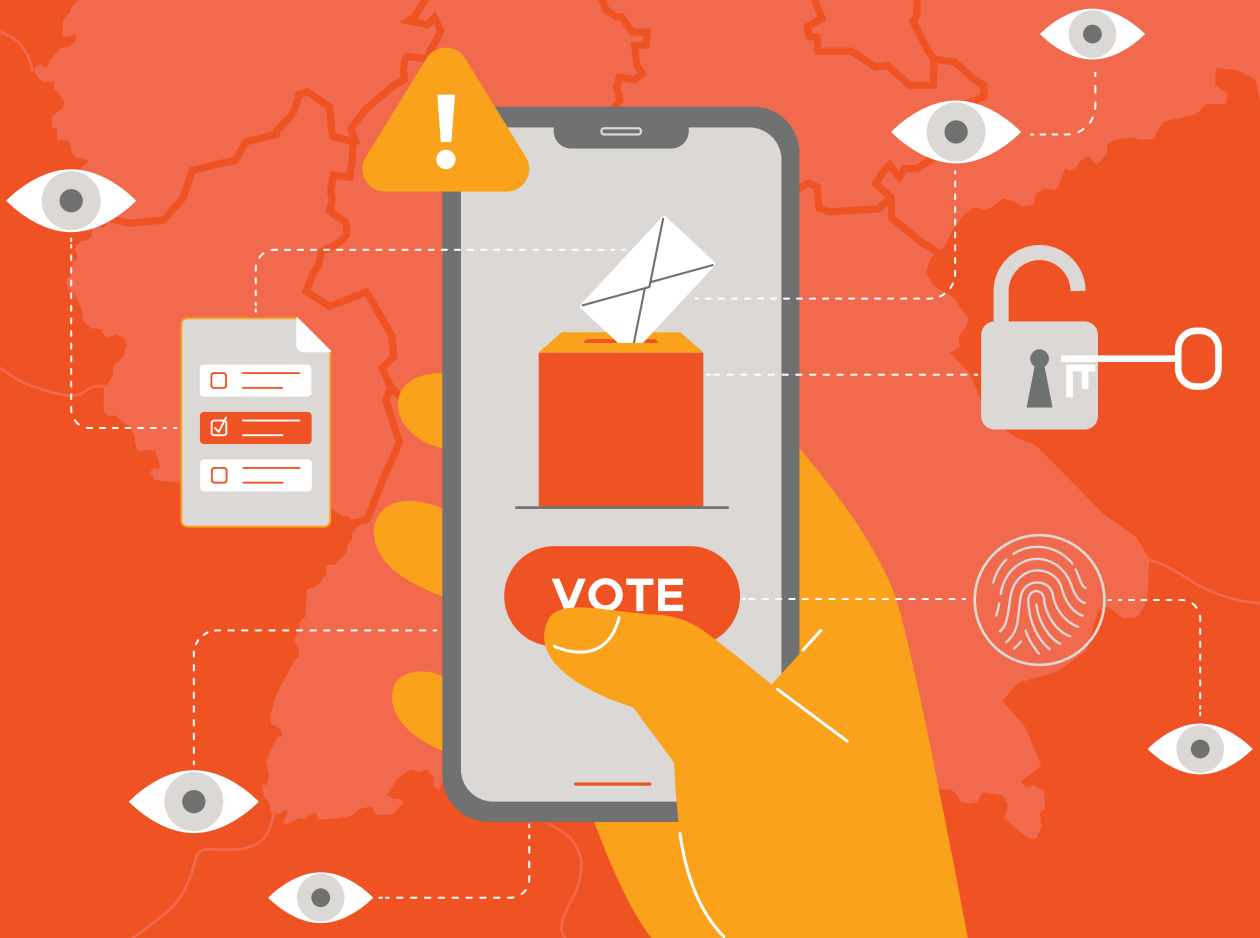
DEMOCRACY
REPORTING
INTERNATIONAL

Bewertung der Online-Risiken für die Bundestagswahl



Bewertung der Online-Risiken für die Bundestagswahl

DEMOCRACY
REPORTING
INTERNATIONAL

Über Democracy Reporting International

Democracy Reporting International (DRI) stärkt die Demokratie durch die Gestaltung der Institutionen, die sie nachhaltig machen. Wir unterstützen lokale Wege der Demokratieförderung mit unparteiischen Analysen und guten Praktiken und erwecken internationale Standards zum Leben. Wir arbeiten mit lokalen Akteuren zusammen, um unseren gemeinsamen demokratischen Raum in einer polarisierten Welt zu schützen und zu erweitern, und sind unabhängig von politischen Meinungen oder persönlichen Überzeugungen. Erfahren Sie mehr unter: http://www.democracy-reporting.org

Anerkennung

Dieser Bericht wurde von Erik Meyer verfasst, mit Beiträgen von Michael Meyer-Resende und Helena Schwertheim. Die Ergebnisse des Berichts basieren auf den Experten-Roundtables, die von DRI am 20. April und 27. April 2021 veranstaltet wurden. Forset gestaltete das Layout dieser Publikation.

Datum: Juni 2021

Dieser Bericht ist Teil eines von Reset finanzierten Projekts. Sein Inhalt gibt nicht unbedingt die Position von Reset wieder.

Diese Veröffentlichung ist unter einer Creative Commons Attribution Non-Commercial 4.0 International Lizenz verfügbar.

Inhalt

1. Zusammenfassung

Während der Corona-Pandemie ist Deutschland digitaler geworden. Der Wahlkampf zur Bundestagswahl 2021 wird in einem bislang ungekannten Ausmaß dort stattfinden, wo viele Wählerinnen und Wähler in den letzten Monaten ihr Leben organisiert, sich informiert und sich ausgetauscht haben: in Messenger-Diensten, sozialen Netzwerken und auf Video-Plattformen.

Bekanntermaßen gibt es online bei der politischen Kommunikation spezifische Risiken. Die Bundestagswahlen 2021 sind für Akteure der Desinformation aus verschiedenen Gründen besonders wichtig. Das Ende der Ära Merkel und eine weitere Schwächung der ehemaligen Volksparteien verspricht eine Neuausrichtung der deutschen Politik. Die politischen Verwerfungen durch die Corona-Pandemie erhöhen die Gefahren des politischen Extremismus.

Durch einige Faktoren werden Risiken, die sich bei Wahlen in anderen Demokratien gezeigt haben, reduziert. Dazu gehören:

- Das Wahlrecht zum Bundestag: Im Gegensatz zum klassischen Mehrheitswahlrecht ergibt sich keine Möglichkeit, das Gesamtergebnis durch gezielte Beeinflussung in wenigen Wahlkreisen zu manipulieren.
- Der gesetzliche Rahmen ist in manchen Bereichen stärker ausgeprägt als in anderen Demokratien; vor allem das NetzDG verpflichtet Plattformen, gegen strafbare Inhalte vorzugehen.
- Medien, die journalistischen Qualitätsansprüchen genügen, haben in Deutschland bei der Meinungsbildung noch eine höhere Wichtigkeit als in anderen Demokratien. Das Vertrauen in diese Medien ist vergleichsweise hoch.

Andere Faktoren erhöhen die Risiken für einen fairen Online-Wahlkampf in folgenden Bereichen:

Bezahlte Onlinewerbung:

- Die Ausgaben für bezahlte politische Onlinewerbung steigen, aber es gibt in diesem Bereich wenig Transparenz. Zum einen, weil die Gesetzgebung im Bereich der Parteien- und Wahlkampffinanzierung sehr schwach ist, zum anderen, weil auch die Online-Anbieter (in ihren „Werbearchiven“) nur begrenzte Informationen zur Verfügung stellen. Im Übrigen gibt es viele Grauzonen wie die Pflichten von Influencern.
- Politische Werbung, die an spezielle Gruppen versendet wird (Microtargeting), mindert das Prinzip der politischen Verantwortung: Es lässt sich nicht mehr nachvollziehen, wem welche Versprechen gemacht werden.
- Bezahlwerbung ist auch dort problematisch, wo sie genutzt wird, um die Verbreitung von Desinformation zu fördern, zum Beispiel, wenn sie Nutzer*innen auf pseudo-journalistische Medien lenkt, die propagandistische Zwecke verfolgen oder falsche Nachrichten verbreiten.

Hassrede:

- Die Verbreitung von Hassrede (strafbare Inhalte, die sich gegen Personen oder Gruppen richten) wird zwar durch das NetzDG erschwert, findet aber weiterhin viele Online-Wege. Sie richtet sich oft gegen Frauen und Minderheiten.
- Kampagnen zur Mobilisierung zu gewalttätigen Aktionen, um Aufmerksamkeit zu erzielen (Beispiel: Der versuchte Sturm in den Reichstag). Die Plattformen haben dieser Gefahr bis vor kurzem wenig Aufmerksamkeit geschenkt.
- Eine restriktive Interpretation des NetzDG führt dazu, dass wichtige Verbreitungskanäle keinen besonderen Verpflichtungen unterliegen. Auf der Plattform Telegram werden zum Beispiel offensichtlich antisemitische Inhalte an große Gruppen verteilt.

Desinformation:

- Kontroverse Themen, zu denen es eine Polarisierung gibt, die in Demokratien normal ist, werden ins Extreme gezogen und dadurch verzerrt.
- Die Wahrnehmung dessen, was politisch wichtig ist, wird manipuliert: Sei es durch automatisierte Konten, die einem Thema oder einer Behauptung künstliche Reichweite verschaffen, oder durch koordinierte Aktionen von echten Nutzer*innen, die eine spontane öffentliche Erregung suggerieren wollen.
- Desinformation zum Wahlvorgang: Die AfD importiert die Strategie eines großen Teils der US-amerikanischen Republikanischen Partei, indem sie suggeriert, die Briefwahl würde zum systematischen Betrug missbraucht.
- Ungeschickte behördliche oder journalistische Kommunikation wird oft für Desinformation missbraucht.

Cyber-Angriffe gegen Behörden oder gegen Online-Versammlungen (Beispiel: CDU-Parteitag im Januar) dienen der Desinformation. Sie verbreiten ein Gefühl der Bedrohung und des Durcheinanders, um das Vertrauen in demokratische Prozesse zu schwächen.

Ausländische Einflussnahme:

Die EU berichtet, dass Deutschland die wichtigste Zielscheibe russischer Desinformationskampagnen in Europa ist. Auch China wird in diesem Zusammenhang zunehmend erwähnt. Die Zuordnung von Desinformationskampagnen zu ausländischen Akteuren sollte allerdings vorsichtig erfolgen, um diese Akteure nicht als wichtiger oder mächtiger darzustellen, als sie sind.

Ausländische Desinformation bedient sich der oben genannten Methoden der Desinformation oder der Verbreitung von Hassrede. Spezifische zusätzliche Risiken ergeben sich aus der Verbreitung von illegal erworbenen Informationen (zum Beispiel Daten aus dem Hacking-Angriff auf den Bundestag) und die spezielle Ansprache von Bürger*innen mit Migrationshintergrund.

Am Ende des Berichts empfehlen wir kurzfristige Maßnahmen, um die verschiedenen Risiken für die Bundestagswahl zu reduzieren.

2. Hintergrund

Am 20. April 2021 hielt Democracy Reporting International (DRI) einen Runden Tisch mit einschlägigen Akteur*innen der Zivilgesellschaft ab, um Risiken des Online-Wahlkampfs für die Bundestagswahl in diesem Jahr zu besprechen. Für Expertise und Kommentare bedanken wir uns bei den Repräsentant*innen von:

- Alliance of Democracies Foundation
- Bundestagsfraktion Bündnis 90/Die Grünen
- CeMAS – Center für Monitoring, Analyse und Strategie
- European New School of Digital Studies
- German Marshall Fund
- Leibniz-Institut für Medienforschung, Hans-Bredow-Institut
- HateAid
- Institute for Strategic Dialogue (ISD)
- John-F.-Kennedy-Institut für Nordamerikastudien der Freien Universität Berlin
- Stiftung Neue Verantwortung (SNV)
- Tactical Tech

Am 27. April 2021 wurden die daraus resultierenden Schlussfolgerungen zusammenfassend präsentiert und in einem weiteren Kreis diskutiert. Neben den bereits genannten wissenschaftlichen Einrichtungen und zivilgesellschaftlichen Organisationen waren weitere Akteur*innen vertreten:

- AlgorithmWatch
- Heinrich-Böll-Stiftung
- Stiftung Mercator
- Oxford Internet Institute
- Auswärtiges Amt
- EU East StratCom Task Force

Zusätzlich präsentierten Vertreter*innen der Landesmedienanstalten aus Baden-Württemberg und Berlin-Brandenburg sowie von Plattformen (Facebook, Twitter) ihre Einschätzungen und diesbezüglichen Vorhaben. Die folgende Darstellung gibt wesentliche Aspekte dieser Diskussionen wieder, repräsentiert aber nicht unbedingt die Meinungen aller Beteiligten.

In 2020 entwickelte DRI das Digital Democracy Risk Assessment, ein Instrument, um die Anfälligkeit nationaler Wahlen für Online-Manipulationen einzuschätzen. Es bietet einen konzeptionellen Rahmen, einen Leitfaden für Benutzer*innen und ein Dashboard mit Daten für die 27 EU-Mitgliedsstaaten und das Vereinigte Königreich. Der konzeptionelle Rahmen umfasst vier Dimensionen, in denen Wahlen für Online-Manipulationen anfällig sein können: Staat, Politik, Medien und Gesellschaft. Dieser Bericht gibt einen Überblick über die Risiken für die Bundestagswahl, die sich aus diesen vier Dimensionen ergeben. Dabei erstreckten sich die Diskussionen am Runden Tisch sowie die diskutierten Risiken oft auf mehrere Dimensionen gleichzeitig.

3. Politischer Kontext der Bundestagswahl 2021

Deutschland ist aufgrund der geopolitischen Lage und seines Einflusses in der Europäischen Union ein politischer Akteur von globaler Bedeutung. Innenpolitische Entwicklungen sind daher für viele ausländische Akteur*innen von Interesse.

Die Bundestagswahlen 2021 sind aus verschiedenen Gründen besonders signifikant:

- Das Ende der Ära Merkel und eine mögliche Neuausrichtung der deutschen Politik.
- Eine weitere Verschiebung des Parteiensystems zulasten der ehemaligen Volksparteien.
- Ein verstärkter globaler Wettbewerb zwischen demokratisch verfassten Staaten und autoritären Systemen.
- Die politischen Verwerfungen durch die Corona-Pandemie, inklusive stärkerer Polarisierung und – bei einer Minderheit – grundsätzlicher Ablehnung des Regierungshandelns bzw. Leugnens, dass die Pandemie eine Gefahr ist.
- Verstärkter politischer Extremismus, der sich auch, aber nicht nur, aus der Ablehnung von Maßnahmen zur Pandemie-Bekämpfung speist. Durch die AfD hat Rechtsextremismus eine Präsenz im Bundestag. In diesem Zusammenhang sind die Demokratie insgesamt delegitimierende Diskursverschiebungen festzustellen.
- Auch die politische Kommunikation hat sich während der Pandemie weiter in Online-Formate verlagert. Deshalb wird die Wahlkampfkommunikation der Parteien unabhängig von der konkreten pandemischen Lage stärker als 2017 online stattfinden und dort Ansatzpunkte für eine politische Auseinandersetzung liefern, die zunehmend im Netz geführt wird.

3.1 Medialer Kontext: Zur aktuellen Relevanz politischer Online-Kommunikation

Durch den Corona-bedingten Digitalisierungsschub ist die Bedeutung von Online-Angeboten für die Meinungsbildung in Deutschland weiter stark gewachsen: „Fast jeder zweite (45%) nutzt mittlerweile täglich Suchmaschinen, soziale Netzwerke und Instant-Messenger-Dienste, um sich über das Zeitgeschehen zu informieren“, resümiert eine Auswertung der Medienanstalten für das zweite Halbjahr 2020.[1] Diese Entwicklung betrifft die informierende Nutzung allgemein, aber auch explizit politische Kommunikation etwa bei Facebook, Instagram und Twitter ist relevant. Ein Fünftel der deutschen Bevölkerung ab 14 Jahren nimmt dort regelmäßig politische Botschaften wahr.[2] Die ARD/ZDF-Onlinestudie 2020 belegt grundsätzlich eine steigende Nutzungsentwicklung auch bei Diensten, die der Individualkommunikation zugerechnet werden: Etwas mehr als zwei Drittel der Bevölkerung (68 %) nutzen nun täglich Messenger wie WhatsApp.[3]

Laut der Umfrage des Eurobarometers 2019 vertrauen 47 % der deutschen Bürger*innen den Medien.[4] Dies mag zwar niedrig erscheinen, ist aber im Vergleich zu anderen EU-Ländern ein moderates Vertrauensniveau (höheres Vertrauen wird in Portugal mit 66 % verzeichnet, das geringste Vertrauen in Griechenland mit 20 %).[5]

3.2 Strukturell wirksame Rahmenbedingungen

STAAT: WAHLSYSTEM

Die personalisierte Verhältniswahl zum Bundestag ist weniger anfällig für intransparente Einflussnahme durch Desinformationskampagnen als reine Mehrheitswahlen. Durch dieses Repräsentationsprinzip ist es etwa nicht direkt möglich, allein durch Mobilisierung einer geringen Stimmenzahl in umkämpften Wahlkreisen einen entscheidenden Einfluss auf die proportionale Zusammensetzung des Parlaments auszuüben. Hinzu kommt ein Vielparteiensystem mit vielen Möglichkeiten der Koalitionsbildung, so dass eine „Entweder-oder-Wahl“ vermieden wird. Insofern werden Faktoren reduziert, die Manipulationsoptionen eröffnen. Einflussnahme ist vor diesem Hintergrund eher auf grundsätzlicher Ebene zu erwarten mit dem Ziel, das Vertrauen in den demokratischen Prozess zu untergraben.

MEDIEN: REGULIERUNG VON INFORMATIONSINTERMEDIÄREN

Die gesetzlichen Rahmenbedingungen für politisch relevante Online-Kommunikation sind in Deutschland in mancher Hinsicht restriktiver ausgestaltet als in anderen Demokratien. Zentral für diese Einschätzung ist das Netzwerkdurchsetzungsgesetz (NetzDG), das Anbieter sozialer Netzwerke im Kampf gegen die Verbreitung von illegalen Inhalten zur Einhaltung von Mindeststandards verpflichtet. Allerdings bleibt die Wirkung umstritten: Kritiker*innen sehen durch Overblocking die freie Meinungsäußerung bedroht, da die Plattformen zur Vermeidung von NetzDG-Verfahren ihre Gemeinschaftsstandards restriktiv(er) implementieren. Positiv lassen sich die Sensibilisierung für problematische Inhalte sowie der verstärkte Einsatz von Ressourcen zur Selbstregulierung resümieren. Eine unabhängige Evaluation der diesbezüglichen Praxis von Content-Moderation und Deplatforming steht aus, weil dafür notwendige Daten nicht vollumfänglich verfügbar sind.

Eine weitere Regulierung erfolgt durch Vorschriften im Medienstaatsvertrag, der den Landesmedienanstalten eine Aufsichtsfunktion über Intermediäre gibt. Allerdings ist in diesem Kontext kein systematisches Monitoring zu erwarten, sondern die Reaktion auf Fälle, die etwa durch Beschwerden bekannt werden. Das Interesse gilt dabei vor allem Inhalten, die besondere Aufmerksamkeit erlangen oder Reichweiten erzielen.

In Bezug auf Wahlen wird die Umsetzung der Kennzeichnungspflicht politischer Werbung auch bei der Kooperation mit Influencern eine vordringliche Rolle spielen, ebenso, dass die Kennzeichnung politischer Werbung durchgängig intakt bleibt, auch wenn als Anzeigen ausgewiesene Inhalte von Nutzer*innen weiter geteilt werden. Eine weitere Herausforderung stellt für die Landesmedienanstalten nun die

1. Die Medienanstalten, „Informierende Mediennutzung so hoch wie nie – Internetnutzung legt weiter zu“, 29. April 2021, https://www.die-medienanstalten.de/service/pressemitteilungen/meldung/informierende-mediennutzung-so-hoch-wie-nie-internetnutzung-legt-weiter-zu
2. Die Medienanstalten, „Informierende Mediennutzung so hoch wie nie – Internetnutzung legt weiter zu“, 29. April 2021, https://www.die-medienanstalten.de/service/pressemitteilungen/meldung/informierende-mediennutzung-so-hoch-wie-nie-internetnutzung-legt-weiter-zu
3. Beisch und Schäfer, „Internetnutzung mit großer Dynamik: Medien, Kommunikation, Social Media“, Media Perspektiven 9/2020, https://www.ard-zdf-onlinestudie.de/files/2020/0920_Beisch_Schaefer.pdf
4. Vgl. die Angabe zum Vertrauen in die Medien im Dashboard des Digital Democracy Risk Assessment zu „Medien“ (https://digitalmonitor.democracy-reporting.org/risk-assessment), das auf den von der EU-Kommission erhobenen Umfragedaten des Eurobarometers basiert (https://data.europa.eu/euodp/en/data/dataset/S2253_91_5_STD91_ENG).
5. Vgl. die Angabe zum Vertrauen in die Medien im Dashboard des Digital Democracy Risk Assessment zu „Medien“ (https://digitalmonitor.democracy-reporting.org/risk-assessment), das auf den von der EU-Kommission erhobenen Umfragedaten des Eurobarometers basiert (https://data.europa.eu/euodp/en/data/dataset/S2253_91_5_STD91_ENG)

Kontrolle der Einhaltung journalistischer Sorgfaltspflichten bei bislang nicht berücksichtigten Online-Medien dar.[6] Hier wurden 2021 erste „Alternativmedien“ mit Verstößen konfrontiert, allerdings besteht verfahrenstechnisch kaum Aussicht auf eine kurzfristige Sanktionierung.

POLITIK: PARTEIEN- UND WAHLKAMPFFINANZIERUNG

Während die in Deutschland praktizierte Form staatlicher Parteienfinanzierung aus vergleichender Perspektive positive Aspekte aufweist, attestieren internationale sowie zivilgesellschaftliche Organisationen vor allem bei Parteispenden und Wahlkampffinanzierung ein Regulierungsdefizit sowie Reformbedarf besonders im Hinblick auf die Transparenz. So müssen Spenden erst ab 10.000 Euro mit Namen und Anschrift der Geber*innen in den Rechenschaftsberichten der Parteien aufgeführt werden. Diese werden jedoch nur einmal jährlich vorgelegt. Erst Spenden ab 50.000 Euro müssen Parteien dem Bundestagspräsidium sofort anzeigen und darauf folgt eine Veröffentlichung. Demgegenüber fordern etwa die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) und die Staatengruppe gegen Korruption (GRECO) des Europarates eine gesonderte, zeitnahe Rechenschaftspflicht zur Wahlkampffinanzierung.

POLITIK: VERTRAUEN IN POLITISCHE PARTEIEN

Politische Parteien sind eine weitere wichtige demokratische Institution sowie Schlüsselakteure im Wahlkampf. Je geringer das Vertrauen in Parteien ist, desto offener können die Wähler*innen für Desinformationen über Parteien und Politik sein. Laut der Umfrage des Eurobarometers 2019 vertrauen 29 % der deutschen Bürger*innen den politischen Parteien in ihrem Land (ohne Angabe dazu, welchen Parteien).[7] Dies mag zwar niedrig erscheinen, ist aber im Vergleich zu anderen EU-Ländern ein hohes Maß an Vertrauen (der höchste Wert wird in Dänemark mit 48 % verzeichnet, der niedrigste in Großbritannien mit 8 %).[8] Diese Daten stammen aus der Zeit vor der Covid-19-Pandemie.

GESELLSCHAFT: VERTRAUEN IN DIE REGIERUNG

Ein gewisses Vertrauen der Bürger*innen in die gewählte Regierung ist wichtig für den sozialen Zusammenhalt und für die Leistungsfähigkeit einer Regierung. Die Schwächung des Vertrauens in Regierung und Parteien ist oft ein Kernziel von Desinformationskampagnen und Online-Interventionen, die darauf abzielen, die Gesellschaft zu polarisieren. Laut der Umfrage des Eurobarometers 2019 vertrauen 45 % der deutschen Bürger*innen ihrer Regierung, was im Vergleich zu anderen EU-Ländern moderat, aber nicht hoch ist (die Spanne reicht in dieser Umfrage von 63 % in den Niederlanden bis zu 13 % in Kroatien).[9] Auch bei diesem Wert spielt die Erhebung vor der Covid-19-Pandemie und den staatlichen Reaktionen darauf eine Rolle, was die Daten weniger aussagekräftig macht.

6. Landesanstalt für Medien NRW, „In den Blick genommen: Journalistische Sorgfaltspflichten im Netz“, 12. Februar 2021, https://www.medienanstalt-nrw.de/presse/pressemitteilungen-2021/2021/februar/in-den-blick-genommen-journalistische-sorgfaltspflichten-im-netz.html
7. Vgl. die Angabe zum Vertrauen in die Medien im Dashboard des Digital Democracy Risk Assessment zu „Politics: Trust in Political Parties“ (https://digitalmonitor.democracy-reporting.org/risk-assessment/), das auf den von der EU-Kommission erhobenen Umfragedaten des Eurobarometers basiert (https://data.europa.eu/euodp/en/data/dataset/S2253_91_5_STD91_ENG)
8. Vgl. die Angabe zum Vertrauen in die Medien im Dashboard des Digital Democracy Risk Assessment zu „Politics: Trust in Political Parties“ (https://digitalmonitor.democracy-reporting.org/risk-assessment/), das auf den von der EU-Kommission erhobenen Umfragedaten des Eurobarometers basiert (https://data.europa.eu/euodp/en/data/dataset/S2253_91_5_STD91_ENG).
9. Vgl. die Angabe zum Vertrauen in die Medien im Dashboard des Digital Democracy Risk Assessment zu „State: Trust in National Government“ (https://digitalmonitor.democracy-reporting.org/risk-assessment/), das auf den von der EU-Kommission erhobenen Umfragedaten des Eurobarometers basiert

3.3 Die Risiken in zentralen Handlungsfeldern politischer Online-Kommunikation

Politische Onlinewerbung

Bezahlte politische Werbung in Online-Formaten ist in der Regel nicht transparent. Es ist unmöglich oder schwierig herauszufinden, wer für was bei welchen Online-Angeboten und in welchem Ausmaß Werbung kauft und an welche Zielgruppen sie ausgespielt wird sowie anhand welcher Angaben diese Zielgruppen angesprochen werden. Auch wenn einige Plattformen wie Twitter und TikTok nach eigenem Ermessen keine für Wahlen relevante politische Werbung mehr anbieten, bleibt eine beträchtliche Grauzone, in der von Kandidierenden und Parteien immer größere Summen aufgewendet werden. Exemplarisch lässt sich dies an der steigenden Anzahl von und den Ausgaben für Anzeigen bei Facebook und Instagram verfolgen.[10] Die Forderung nach mehr Transparenz ist hier gleichzeitig eine Voraussetzung für die Analyse der Auswirkungen, die durch externes Monitoring und wissenschaftliche Forschung bislang nicht vollständig erschlossen werden können.

Abgesehen von der mangelnden Transparenz bestehen folgende Risiken:

- Verstöße gegen die Datenschutzgrundverordnung (DSGVO), zum Beispiel wenn Wähler*innen nach politischer Orientierung klassifiziert werden. Die Organisation Tactical Tech hat das globale Geschäft mit politisch signifikanten persönlichen Daten in mehreren Berichten durchleuchtet.[11]
- Extremistische Kräfte, die durch bezahlte Werbung versuchen, bestimmte Schichten der Wählerschaft zu demobilisieren oder zu mobilisieren.
- Bezahlwerbung, die Nutzer*innen auf pseudo-journalistische Angebote führt, die journalistischen Standards offensichtlich nicht genügen und stattdessen Desinformation oder Propaganda verbreiten.
- Verstöße gegen Wahlkampffinanzierung, weil Ausgaben nicht deklariert werden und auch nicht öffentlich nachvollzogen werden können.
- Verarmung der politischen Debatte und politischer Verantwortlichkeit durch Microtargeting von Botschaften: Da Argumente oder Versprechen für viele unsichtbar bleiben und hochgradig fragmentiert versendet werden, werden sie nicht öffentlich diskutiert. Die öffentliche Verantwortlichkeit von Parteien für ihre Positionen und Versprechen wird dadurch geschwächt.
- Der rechtliche Rahmen für politische Onlinewerbung ist schwach. Es gibt keine Verpflichtung der Parteien oder Kandidierenden, ihre Ausgaben für Onlinewerbung zeitnah zu veröffentlichen und Informationen darüber bereitzustellen. Die Stiftung Neue Verantwortung reklamiert: „Für Postwurfsendungen gibt es klare Vorgaben, welche demografischen Daten von wem genutzt werden dürfen. Für das verhaltensbasierte Microtargeting im Internet bestimmen es Plattformen meist allein, wie sie das Targeting politischer Werbung handhaben.“[12]

10. Fieber, „Wie Deutschlands Parteien auf Facebook Politik machen - und warum die AfD so erfolgreich ist”, 15. April 2021, https://web.de/magazine/politik/deutschlands-parteien-facebook-politik-afd-erfolgreich-35712388
11. Für weitere Informationen siehe: https://ourdataourselves.tacticaltech.org/projects/data-and-politics/
12. Jaursch, „Regeln für faire digitale Wahlkämpfe”, Stiftung Neue Verantwortung, 8. Juni 2020, https://www.stiftung-nv.de/sites/default/files/regeln_fur_faire_digitale_wahlkampfe.pdf

- Die DSGVO verbietet zwar grundsätzlich die „Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen“ hervorgehen (§ 9), aber hier gibt es erhebliche Unklarheiten, zum Beispiel wenn solche Merkmale indirekt aus anderen Eigenschaften einer Person abgeleitet werden. Es gibt auch keinen klaren Schutz gegen Werbung, die auf Einschätzung psychologischer Eigenschaften beruht (siehe § 22 DSGVO zu Profiling).

- Der schwache rechtliche Rahmen spiegelt sich in einer fehlenden institutionellen Verankerung wider. Keine staatliche Instanz beobachtet systematisch politische Werbung online. Diese Aufgabe bleibt nicht-staatlichen Akteuren überlassen.

Online-Hassrede und gesetzeswidrige Inhalte

„Hassrede“ ist ein Sammelbegriff für strafbare Äußerungen, vor allem Volksverhetzung (§ 130 Strafgesetzbuch – StGB), Bedrohung oder auch Beleidigung und Verleumdungen im Sinne des StGB. Für manche Studien wird ein erweiterter Begriff von „hateful speech“ verwendet. Es geht grundsätzlich nicht um polemische oder extrem kritische Äußerungen, die in der politischen Auseinandersetzung gang und gäbe sind.

Das Problem der Hassrede in Online-Öffentlichkeiten hat eine explizit politische Dimension. Sie zielt oft darauf ab, Diskussionen extrem zu polarisieren, Nutzer*innen abzuschrecken oder zum Schweigen zu bringen. Hassrede im Netz hat direkte Auswirkungen auf psychisches Wohlbefinden und kann zu Gewalttaten anstiften, wie es auch bei der Ermordung des Kasseler Regierungspräsidenten Walter Lübcke (CDU) deutlich geworden ist. Studien der Amadeu Antonio Stiftung zeigen, wie Hassrede oft mit rechtsterroristischen Inhalten überlappt.[13] Das Institute for Strategic Dialogue (ISD) hat in zahlreichen Publikationen[14] aufgezeigt, dass extremistische Bewegungen, vor allem Rechtsextremist*innen und dschihadistische Bewegungen, ausgefeilte Kommunikationsstrategien umsetzen, in denen gewalttätige Rhetorik ein wichtiges Element ist, um Anhänger*innen zu radikalisieren und zu mobilisieren. Das ISD hat auch aufgezeigt, dass ein Großteil der Hassreden oft von einem sehr kleinen Teil von Nutzer*innen ausgeht oder verbreitet wird.[15]

Zu den Risiken vor den Bundestagswahlen gehören:

- Systematische Hasskampagnen, um Menschen mit anderen Meinungen einzuschüchtern oder sie zum Schweigen zu bringen. Diese richten sich oft gegen Frauen, Minderheiten oder Menschen, die im politischen Betrieb eine herausgehobene Rolle spielen (Politiker*innen, Journalist*innen usw.). Durch derart belastete Debatten werden Menschen darüber hinaus davon abgehalten, an politischen Prozessen teilzunehmen, vom Wählen bis zur Kandidatur für ein Amt.

- Eingriff in den Wahlprozess durch Hassrede gegen Menschen, die mit der Wahlorganisation befasst sind (Wahlhelfer*innen, Offizielle).

- Kampagnen zur Mobilisierung zu gewalttätigen Aktionen, um Aufmerksamkeit zu erzielen. Der versuchte Sturm in das Reichstagsgebäude gehört in dieses Bild.

13. Manemann, „Rechtsterroristische Online-Subkulturen: Analysen und Handlungsempfehlungen“, Amadeu Antonio Stiftung, 2020, https://www.amadeu-antonio-stiftung.de/wp-content/uploads/2021/02/Broschu%CC%88re-Rechtsterroristische-Online-Subkulturen_pdf.pdf
14. Baldauf, Ebner und Guhl (Eds.), „Hate Speech and Radicalisation Online: The OCCI Research Report”, Institute for Strategic Dialogue, 2019, https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf
15. Kreißel, Ebner, Urban und Guhl, „Hass auf Knopfdruck: Rechtsextreme Trollfabriken und das Ökosystem koordinierter Hasskampagnen im Netz“, Institute for Strategic Dialogue, 2018, https://www.isdglobal.org/wp-content/uploads/2018/07/ISD_Ich_Bin_Hier_2.pdf

- Die Zunahme von Hassrede besonders in Kanälen und auf Plattformen, die nicht unter das NetzDG fallen. Der Telegram-Dienst enthält viele Konten, die offensichtlich antisemitische, rassistische oder gewalttätige Inhalte teilen und denen zehntausende von Nutzer*innen folgen. Trotzdem unterliegt der Dienst in Deutschland fast keiner Regulierung. Es ist nicht einmal erkennbar, von wo er betrieben wird oder wie man die Betreiber*innen erreichen kann.

Das Netzwerkdurchsetzungsgesetz (NetzDG) verpflichtet große Plattformen, offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden zu löschen, z. B. in Fällen von Volksverhetzung. In welchem Umfang die verpflichteten Plattformen dem Gesetz Genüge tragen, ist schwer zu beurteilen. In der gegenwärtigen Auslegung des Gesetzes werden Messenger-Dienste durch das Gesetz nicht erfasst.

Desinformation

Desinformation ist in den letzten Jahren subtiler geworden, indem sie Wahrheit und Unwahrheit mischt, Kontexte ignoriert oder ausblendet oder den Eindruck, es handele sich um große öffentliche Debatten, künstlich erzeugt. Gerade die systematische Verbreitung falscher oder irreführender Angaben zu politischen Sachverhalten oder Verfahren gefährdet den Meinungs- und Willensbildungsprozess in demokratischen Gesellschaften. Davon ist nicht nur die Darstellung einzelner Politikinhalte und politischer Akteur*innen betroffen. Besonders die Diskreditierung von Journalist*innen und redaktionellen Medien führt zu einem Vertrauensverlust und stellt die Verständigung über nachprüfbare Fakten generell in Frage. Insofern kann Desinformation die Einschätzung der Qualität demokratischer Wahlen („Integrität der Wahlen“) durch die Bevölkerung kompromittieren. Desinformation geht dabei vielfach von einheimischen Akteur*innen aus, die aber regelmäßig Kampagnen aus anderen Ländern, vor allem den USA, kopieren.[16]

Zu den konkreten Risiken vor der Bundestagswahl gehören:

- Kontroverse Themen, zu denen es eine gesellschaftliche Polarisierung gibt, die in Demokratien normal ist, werden ins Extreme gezogen. Das Muster gibt es in allen großen Debatten. Eine legitime Diskussion zur Einwanderung wird durch eine behauptete globale Verschwörung ins Extreme verzerrt. Eine Auseinandersetzung über die richtige Vorgehensweise gegen die Corona-Pandemie wird mit den abwegigen Behauptungen ad absurdum geführt, dass es keine Pandemie gebe oder Impfungen wiederum eine globale Verschwörung seien.

- Es existieren Versuche, die Wahrnehmung dessen, was politisch wichtig ist, zu manipulieren: Sei es durch automatisierte Konten, die einem Thema oder einer Behauptung künstliche Reichweite verschaffen, oder durch koordinierte Aktionen von echten Nutzer*innen, die eine spontane öffentliche Erregung suggerieren wollen.

- Desinformation kann sich auch direkt auf Fragen der Wahl konzentrieren, um ihre Glaubwürdigkeit zu untergraben. Die AfD importiert die Strategie eines großen Teils der amerikanischen Republikanischen Partei, indem sie suggeriert, die Briefwahl würde zum systematischen Betrug missbraucht.[17]

- Wie bei der Hassrede ist auch hier ein Ausweichen auf andere Plattformen oder Dienste (Messenger-Dienste, Newsletter) zu registrieren, die weniger beobachtet werden und weniger reguliert sind. Ebenso besteht auch hier die Gefahr, dass Online-Desinformation Auswirkungen außerhalb der Online-Sphäre hat (in Deutschland seit dem „Fall Lisa“ wohlbekannt[18]).

16. Huesmann, „Europawahl: AfD und rechte Aktivisten wollen das Vertrauen in die Demokratie untergraben“, Watson, 23. Mai 2019, https://www.watson.de/deutschland/politik/503310736-afd-und-ein-prozent-rechtsextreme-untergraben-vertrauen-in-die-demokratie
17. Pohl und Humbs, „Die Mär von der gestohlenen Wahl“, Tagesschau Investigativ, 14. Januar 2021, https://www.tagesschau.de/investigativ/kontraste/usa-afd-wahlbetrug-101.html
18. z. B. DFRLab, „Lisa 2.0: How pro-Kremlin media in Germany have been using a new fake to justify an old one”, 11. März 2017, https://medium.com/@DFRLab/lisa-2-0-133d44e8acc7

- Ungeschickte behördliche oder journalistische Kommunikation. Eine Studie der SNV hat im Zusammenhang mit der letzten Bundestagswahl herausgefunden, dass erfolgreiche Desinformation sich oft schlechte Kommunikation zunutze machte.[19]

- Desinformationskampagnen, die schnell auf unerwartete plötzliche Ereignisse reagieren (Beispiel: Brand der Notre-Dame-Kathedrale in Paris).

- Cyber-Angriffe gegen Behörden oder gegen (Online-)Versammlungen (Beispiel: CDU-Parteitag im Januar) haben auch einen Aspekt der Desinformation: Sie verbreiten ein Gefühl der Bedrohung und des Durcheinanders, um das Vertrauen in demokratische Prozesse zu schwächen.

Ausländische Einflussnahme

Russland wird regelmäßig als wichtigster ausländischer Akteur der Desinformation in Deutschland genannt. Nach Erkenntnissen des Europäischen Auswärtigen Dienstes ist Deutschland die wichtigste Zielscheibe russischer Desinformationskampagnen in Europa.[20] Demnach wurden seit Ende 2015 mehr als 700 Fälle registriert, in denen russische Medien Falschinformationen über Deutschland verbreitet haben, vielfach allerdings eher für die russische Öffentlichkeit, während auf russischen Kanälen in Deutschland, wie RT, offenkundige Erfindungen eher vermieden werden.

In diesem Zusammenhang wird auch China zunehmend erwähnt. Grundsätzlich ist aber davon auszugehen, dass Akteure in Deutschland bei der Desinformation eine größere Wucht entfalten. Die Zuordnung von Desinformationskampagnen zu ausländischen Akteuren sollte vorsichtig erfolgen, um diese Akteure nicht als wichtiger oder mächtiger darzustellen, als sie sind.

Vor der Bundestagswahl bestehen diese Risiken:

- Grundsätzlich gibt es ein gesteigertes geopolitisches Interesse an der Ausrichtung Deutschlands nach dem Ende der Ära Merkel. Dies kann sich auch im Interesse an einer Schwächung zentraler politischer Akteur*innen oder Institutionen manifestieren.

- Erkenntnisse aus vergangenen und zukünftigen Hackerangriffen (oder auch Phishing-Angriffen) auf den Bundestag und Behörden können taktisch zu bestimmten Zeitpunkten (z. B. kurz vor der Wahl) veröffentlicht werden, um den Wahlkampf und die öffentliche Meinungsbildung zu beeinflussen.

- Solche Erkenntnisse können auch dazu genutzt werden, private Daten zu veröffentlichen oder zur Einflussnahme zu nutzen (Doxing). Dies führt unter anderem zu einer Verunsicherung davon betroffener Kandidierender, die sich gefährdet fühlen und gegebenenfalls ihr Verhalten verändern. Auch die öffentliche Wahrnehmung von Betroffenen kann auf diesem Weg beschädigt werden.

- Desinformation für bestimmte Zielgruppen mit Migrationshintergrund. Hier wird etwa in einem Antrag der FDP-Bundestagsfraktion zum Schutz der Bundestagswahl 2021[21] vor allem auf das Zusammenspiel von Auslandssendern wie RT Deutsch mit Online-Desinformation hingewiesen oder die Rolle des türkischen Auslandssenders TRT 4 angesprochen.

19. Sängerlaub, Meier und Rühl, „Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017“, Stiftung Neue Verantwortung, 26. März 2018, https://www.stiftung-nv.de/de/publikation/fakten-statt-fakes-verursacher-verbreitungswege-und-wirkungen-von-fake-news-im
20. EuvsDisinfo, „Vilifying Germany; wooing Germany“, 9. März 2021, https://euvsdisinfo.eu/villifying-germany-wooing-germany/
21. Deutscher Bundestag, „Antrag der Abgeordneten und der Fraktion der FDP“, Drucksache 19/28743, 20. April 2021, https://dip21.bundestag.de/dip21/btd/19/287/1928743.pdf

4. Handlungsempfehlungen zur Risikominimierung bei der Bundestagswahl 2021

Politische Onlinewerbung

- Grundsätzlich muss die DSGVO umfassend umgesetzt werden, da sie auch politisch Werbetreibenden besonders problematische Praktiken des Targeting mittels personenbezogener Daten untersagt.

- Online-Plattformen, die politische Werbung verkaufen, müssen sorgfältig die Einhaltung ihrer eigenen Standards und der Gesetze prüfen.

- Bei der Definition und Kennzeichnung politischer Werbung sind nicht nur von den Anbietern etablierte Formate zu berücksichtigen, sondern alle Inhalte, die gegen Bezahlung erstellt werden. Dies betrifft auch Influencer.

- Online-Plattformen, die politische Werbung anbieten, müssen umfassende, detaillierte Archive vorhalten, in denen diese sofort öffentlich einsehbar ist. Diese Archive müssen einfach durchsuchbar sein und auch Schnittstellen für systematische Forschungen zur Verfügung stellen, inklusive erweiterter, detaillierter Informationen zu den Targeting- und Ausspielungskriterien (detaillierte Empfehlungen dazu hat SNV vorgelegt[22]).

- Medien und zivilgesellschaftliche Organisationen können Nutzer*innen Browser-Erweiterungen zur Verfügung stellen, mit denen politische Werbung gesammelt werden kann, um sie mit Informationen aus Archiven abzugleichen (für die Bundestagswahl 2021 kooperiert dazu beispielsweise das ZDF Magazin Royale mit der Initiative „Who Targets Me“[23]).

- Die politischen Parteien können sich selbst in einem Verhaltenskodex dazu verpflichten, beim Kauf von Online-Werbung verantwortungsvoll und transparent vorzugehen. In den Niederlanden haben zahlreiche Parteien und Plattformen im Vorfeld der Parlamentswahl vom 17.3.2021 einen Verhaltenskodex für mehr Transparenz bei der politischen Onlinewerbung unterzeichnet.[24]

22. Jaursch, „Regeln für faire digitale Wahlkämpfe”, Stiftung Neue Verantwortung, 8. Juni 2020, https://www.stiftung-nv.de/sites/default/files/regeln_fur_faire_digitale_wahlkampfe.pdf
23. https://whotargets.me/de/
24. International IDEA, „First national Code of Conduct on online political advertising in the European Union signed by Dutch political parties and global online platforms“, 9. Februar 2021, https://www.idea.int/news-media/news/first-national-code-conduct-online-political-advertising-european-union-signed-dutch

Online-Hassrede und gesetzeswidrige Inhalte

- Die Anbieter von Online-Plattformen müssen ihre eigenen Standards sorgfältig und umfassend umsetzen. Wo anwendbar, gilt das Gleiche für ihre Verpflichtungen aus dem NetzDG, auch hinsichtlich der im Mai 2021 beschlossenen Verbesserung der Nutzerfreundlichkeit der Meldewege beim Übermitteln von Beschwerden über rechtswidrige Inhalte.[25] Über Löschungen hinaus sollten Ranking-Fragen im Vordergrund stehen: Hassrede ist hochemotional, führt daher in der Regel schnell zu vielen Reaktionen, die wiederum Algorithmen dazu bringen können, entsprechende Inhalte in Timelines von Nutzer*innen oder in Empfehlungen höher einzustufen.

- Das Bundesamt für Justiz sollte § 1 des NetzDG gemäß Wortlaut sowie Sinn und Zweck des Gesetzes auslegen und es auch auf Dienste anwenden, die sich der Form nach als private Messenger-Dienste präsentieren, aber zum Teil auch soziale Netzwerke sind. Das wäre zum Beispiel für den Dienst Telegram zu prüfen, auf dem sich Gruppen mit bis zu 200.000 Teilnehmer*innen bilden können, die öffentlich zugänglich sind.[26]

- Politisch Verantwortliche und Behörden sind stärker für die destruktiven Auswirkungen von Hassrede auf die politische Partizipation zu sensibilisieren.

Desinformation

Desinformation kann illegal sein (wenn sie zum Beispiel verleumderisch ist), aber es gibt kein allgemeines Verbot zu lügen. Eine kurzfristige Minimierung von Risiken in diesem Handlungsfeld muss sich daher vor allem auf Transparenz-Gesichtspunkte konzentrieren und auf Faktenchecks, die allerdings oft wesentlich weniger sichtbar sind als die Desinformationen, mit denen sie sich beschäftigen. Wesentlich ist vor allem ein Fokus auf die automatisierte Verbreitung von Nachrichten durch Plattformen, deren Algorithmen oft anfängliches Interesse (Desinformation ist oft aufregend) als Signal interpretieren, sie prominent zu verbreiten (Ranking). Es ergeben sich folgende Handlungsmöglichkeiten:

- Systematische Bemühungen der Plattformen, Desinformationen zu identifizieren und sicherzustellen, dass Verteilungsalgorithmen Desinformationen ein niedriges Ranking geben. Dazu gehört auch die proaktive Kooperation mit zivilgesellschaftlichen Organisationen und anderen Expert*innen, die sich mit entsprechenden Herausforderungen beschäftigen. Wünschenswert ist die Etablierung direkter Kontakte auf Arbeitsebene, um aktuelle Entwicklungen kurzfristig zu kommunizieren.

- Standards der Selbstregulierung sind konsequent anzuwenden, was in besonderen Fällen auch zum Löschen von Konten führen könnte. Solche Schritte müssen transparent erfolgen, damit Betroffene den Beschwerde- oder Rechtsweg einschlagen können (siehe NetzDG).

- Plattformen können ihr Design anpassen, indem Desinformation gekennzeichnet wird oder virale Verbreitung verhindert oder verlangsamt wird.

- Schließlich sind die beispielsweise bei der US-Präsidentschaftswahl 2020 zum Teil ad hoc spezifizierten Regeln der Plattformen bezüglich wahlbezogener Inhalte eindeutig zu formulieren und für Nutzer*innen nachvollziehbar zu publizieren.

25. Die Bundesregierung, „Änderung des Netzwerkdurchsetzungsgesetzes: Gezielte Bekämpfung von Hasskriminalität“, 6. Mai 2021, https://www.bundesregierung.de/breg-de/suche/bekaempfung-hasskriminalitaet-1738150
26. Laufer, „Fällt Telegram wirklich nicht unter das NetzDG?“, Netzpolitik.org, 4. Februar 2021, https://netzpolitik.org/2021/hasskriminalitaet-faellt-telegram-wirklich-nicht-unter-das-netzdg/

- Behörden und Medien müssen insbesondere im Wahlkampfjahr ihre öffentliche Kommunikation überprüfen, um sicherzustellen, dass Verlautbarungen oder Artikel nicht leicht fehlinterpretiert werden können. Unter anderem sollten Medien das Alter von Online-Artikeln deutlich kennzeichnen (z. B. „Artikel mehr als sechs Monate alt“), um zu verhindern, dass alte Angaben als neue Nachrichten bzw. „Skandale“ verbreitet werden (vorbildlich verfährt diesbezüglich theguardian.com).

- Behörden, gerade wenn sie an der Organisation der Wahlen beteiligt sind, müssen umfassend und proaktiv kommunizieren, vor allem auch auf sozialen Medien. Hier gibt es noch viel zu tun.[27] Zwar werden Plattformen Nutzer*innen offizielle Informationen zur Bundestagswahl präsentieren, doch auch generell sollte die Sichtbarkeit von vertrauenswürdigen Quellen dort verstärkt werden.

Ausländische Einflussnahme

Eine kurzfristige Minimierung von Risiken in diesem Handlungsfeld scheint schwierig, aber möglich:

- Die bereits begonnene Sensibilisierung potenziell davon betroffener Funktionsträger*innen sowie für die Wahl relevanter Institutionen und Organisationen etwa durch das Bundesamt für Sicherheit in der Informationstechnik ist zu intensivieren. Vor allem die Parteien sind dazu aufgerufen, ihre Vorkehrungen auch bei der Beteiligung von ehrenamtlich im Wahlkampf Engagierten auszuweiten.

- Die Parteien verpflichten sich zum Verzicht auf die systematische Nutzung von aus Doxing und Leaks hervorgehenden personenbezogenen Angaben im Wahlkampf.

- Redaktionelle Medien genießen weiterhin ein großes Vertrauen in der deutschen Bevölkerung. Bei der Berichterstattung über Desinformationskampagnen sollte eine breite Aufklärung beabsichtigt werden.

27. Der Bundeswahlleiter betreibt beispielsweise Profile in den sozialen Medien, die allerdings noch über eine geringe Reichweite verfügen dürften (Mitte Mai 2021 werden bei Twitter für @Wahlleiter_Bund über 9.000 Follower ausgewiesen und bei Instagram knapp 200 Abonnenten).

5. Längerfristige Handlungsempfehlungen und Herausforderungen

Viele der thematisierten Problemstellungen erfordern mittel- und langfristige Lösungsstrategien: entweder, um Regelungen herbeizuführen, umzusetzen und deren Wirkung zu evaluieren, oder, um gesellschaftliche Resilienz etwa durch politische Bildung und digitale Medienkompetenz zu stärken. Ansatzpunkte sind:

- In der nächsten Legislaturperiode sollte der rechtliche Rahmen für die Parteien- respektive die Wahlkampffinanzierung den Realitäten der Zeit systematisch angepasst werden. Eine Kommission zur Zukunft digitaler Wahlen könnte Anstöße zur Erarbeitung von Regelungen geben und die Sensibilisierung für bereits bestehende Gesetze steigern.

- Für langfristige Lösungen hat die Europäische Kommission verschiedene Regelungswerke vorgeschlagen, die Desinformationen im Netz verringern oder verhindern sollen. Die beteiligten Organisationen haben dazu Stellungnahmen vorgelegt.

- Einige Formate und Plattformen sind bislang noch nicht ausreichend in den Fokus der Wahrnehmung durch die politisch Verantwortlichen gerückt. So können Live-Videos bereits zum Ausstrahlungszeitpunkt ein erhebliches Publikum erreichen. Hier greifen viele der vorgeschlagenen Maßnahmen dann nicht mehr effektiv. Insofern ist gerade die inzwischen gewachsene und wachsende mediale Infrastruktur einer mobilisierten Gegenöffentlichkeit inklusive Echtzeitkommunikation zu beobachten, die zuletzt durch das Phänomen der „Querdenker“ befördert wurde. In diesem Kontext ist etwa bei YouTube auch die Möglichkeit der Monetarisierung von absichtlich irreführenden Inhalten zu problematisieren. Diese sollte nach einer entsprechenden Einstufung ausgeschlossen werden. Werbetreibende sind dazu aufgerufen, einzufordern, dass ihre Werbung nicht vor desinformierenden Videos gezeigt wird. Auch TikTok gilt es gerade im Hinblick auf steigende Nutzungszahlen hier stärker in den Blick zu nehmen.

Gerade weil es sich bei Online-Kommunikation und ihren Risiken für die demokratische Meinungs- und Willensbildung um ein ausgesprochen dynamisches Geschehen handelt, bedarf es einer beständigen Auseinandersetzung mit problematischen Phänomenen. Democracy Reporting International verfolgt dabei den Ansatz eines Austausches zwischen Aufsichtsbehörden und Wissenschaft, zivilgesellschaftlichen Initiativen und den privatwirtschaftlichen Plattformen, um Gefahren frühzeitig zu erkennen und ihnen in kooperativer Weise zu begegnen. Die Runden Tische und die vorliegende Bewertung bilden die Basis für einen fortlaufenden Prozess bei der Bundestagswahl 2021 und darüber hinaus.