Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)050

Fragenkatalog zur Anhörung

„Resilienz von Demokratien im digitalen Zeitalter im Kontext der Europawahl" im Ausschuss Digitale Agenda

10. April 2019

Karolin Schwarz, freie Journalistin

1. **Uns ist es wichtig, den demokratischen Diskurs in den sozialen Netzwerken zu stärken. Welche Maßnahmen - auch neben gegebenenfalls gesetzgeberischen - können hier sinnvoll sein? Wie wichtig werden in diesem Zusammenhang die Themen Medien- und Digitalkompetenz bewertet? Würde eine bessere Medienkompetenz der Bürgerinnen und Bürgern den Einfluss solcher Kampagnen verhindern? Welche Maßnahmen sollten hier von politischer Seite unternommen werden?**

   Grundsätzlich sollte eine Umsetzung bereits bestehender Gesetze im Vordergrund stehen. Neue Gesetzesinitiativen laufen einerseits Gefahr, der hohen Dynamik von Spielarten und Akteuren im Feld digitaler Manipulation nicht gerecht zu werden. Zum anderen könnten Gesetzesinitiativen immer auch zu unerwünschten Effekten, wie der Einschränkung der Meinungsfreiheit oder der Verdrängung marginalisierter Gruppen aus digitalen Räumen, etwa durch Identifikationspflichten, führen.

   Denkbar wären beispielsweise Schulungsmaßnahmen und die Einführung von Handlungsleitfäden für Akteure, die mit Falschmeldungen konfrontiert werden. Dazu gehören neben Politikern auch die Polizei, Gerichte und verschiedene Ämter.

   Eine Stärkung der Medien- und Informationskompetenz der Bevölkerung sollte immer auch Ziel politischer Maßnahmen in diesem Bereich sein. Hierbei sind vor allem auch diejenigen einzubeziehen, die nicht über die Schulen erreichbar sind. Ein Aufbau entsprechender Angebote für Internetnutzende muss der demographischen Entwicklung Deutschlands gerecht werden und alle Altersstufen, vor allem aber derjenigen, die nicht zu den sogenannten Digital Natives gehören, einbeziehen.

2. **Inwiefern sind Desinformationskampagnen und andere Mittel zur Beeinflussung des öffentlichen Diskurses im Status Quo bereits rechtlich erfasst? Welche Mittel im Bereich der Desinformation und Wahlbeeinflussung sind bekannt? Gibt es Kennzahlen bzw. Kriterien, um den Erfolg (versuchter) Wahlbeeinflussung zu messen? Welche Forschungsstellen und NGOs beschäftigen sich mit der Analyse von**

Desinformationskampagnen und Wahlbeeinflussung?

Mehrere Urteile aus den vergangenen 3 Jahren zeigen, dass verschiedene Falschbehauptungen gegen bestehende Gesetze verstoßen. Auch auf dem zivilrechtlichen Weg wurden in jüngerer Vergangenheit einige Urteile erwirkt. Einen Anlass zur Einführung neuer Straftatbestände gibt das nicht.

Die Bandbreite an Tools und Maßnahmen zur Beeinflussung der politischen Debatte oder Einschüchterung politisch aktiver Personen oder Journalisten ist groß. Zunehmend setzen entsprechende Akteure beispielsweise auf das sogenannte Doxing, also die Veröffentlichung von Sammlungen privater Daten von Journalisten, Politikern und Aktivisten mit dem Ziel der Einschüchterung oder des Verfügbarmachens für böswillige Akteure.

Verschwörungstheorien und Falschmeldungen werden zahlreich verbreitet und häufig zudem auf unterschiedliche Zielgruppen angepasst aufbereitet. Ein großer Teil dieser Botschaften wird als Memes, sowie über entkontextualisierte Bilder und Videos verbreitet.

Eine ganze Reihe von Forschungsstellen und NGOs beschäftigt sich weltweit mit diesen Phänomenen. Anzuregen wäre hier eine weitere, interdisziplinäre Vernetzung zum Austausch von Wissen und best practices. In diesem Bereich sind beispielsweise Poynter und First Draft aktiv.

Die Erfahrung der vergangenen Jahre zeigt, dass böswillige Akteure über länderübergreifende Strukturen verfügen und in mal mehr, mal weniger festen Netzwerken organisiert sind.

3. **In diesem Jahr stehen die Europawahl und vier Landtagswahlen in Deutschland an. Die Sorge vor möglicher digitaler Wahlbeeinflussung treibt nicht nur die Europäische Kommission, sondern auch die deutsche Politik um: Wie sicher sind die Wahlen vor dem Hintergrund bisheriger Erkenntnisse zur Wahlbeeinflussung? Welche Maßnahmen haben die sozialen Netzwerke ergriffen, um eine mögliche digitale Wahlbeeinflussung zu verhindern? Welche Maßnahmen zur Vermeidung von und Reaktion auf Versuche der digitalen Manipulation/Wahlmanipulation sind für die jeweiligen Stakeholder anzuraten? Wer hätte ein Interesse an einer Manipulation und wie könnte diese nachgewiesen werden? Welche Motivationen lassen sich für Desinformationskampagnen und (versuchte) Wahlbeeinflussung unterscheiden?**

Die Social-Media-Plattformen haben eine Reihe von Maßnahmen eingeführt, die

Wahlbeeinflussungen und digitale Manipulation im Allgemeinen verhindern oder beschränken sollen. Alle Plattformen haben beispielsweise in der Vergangenheit massenhaft angelegte Fake-Accounts blockiert und das entsprechend auch bekannt gegeben. Facebook und Twitter haben Archive für in Deutschland geschaltete politische Werbung eingerichtet, Google bereitet die Veröffentlichung einer solchen Plattform für April 2019 vor.

Facebook arbeitet mit Deutschland inzwischen mit zwei Kooperationspartnern (Correctiv, dpa) zusammen, um Falschmeldungen, die auf der Plattform in Form von externen Artikeln, aber auf Bildern und Videos verbreitet werden, um Faktenchecks zu ergänzen.

Google hat das Plug-In ClaimReview implementiert. Über ein entsprechendes Plug-In in den Content-Management-Systemen von Medien können Faktenchecks hierüber mit Metadaten zur bearbeiteten Behauptung, deren Urheber und dem Fazit der Faktenchecker versehen werden. Faktenchecks sollen auf diese Weise über die Google-Suche prominenter angezeigt werden. In Deutschland wurde ClaimReview bislang nur von Correctiv implementiert. Die US-Fact-Checking-Organisation Snopes hat die Arbeit mit dem Plug-In kürzlich aufgegeben und unter anderem eine Lizenzierung der Inhalte sowie Transparenz hinsichtlich der Wirkung von ClaimReview eingefordert.

Insgesamt ist festzuhalten, dass mehr Transparenz seitens der Plattformbetreiber wünschenswert wäre. Zum Einen in Bezug auf Netzwerke politischer Akteure, die sich durch Fake Accounts und andere Mittel in der Beeinflussung politischer Prozesse versuchen. Zum Anderen in Bezug auf Gegenmaßnahmen, etwa die Wirkung der Fact-Checking-Kooperationen bei Facebook.

4. **Gibt es bereits Anhaltspunkte - und wenn ja welche -, ob die EU-Wahlen eventuell manipuliert werden? Und wenn ja, auf welche Art und Weise? Hat es solche Manipulationen - bewiesen - bei vergangenen Wahlen gegeben?**
5. **Vor der Bundestagswahl 2017 gab es Befürchtungen, dass es zu Wahlbeeinflussung, speziell im digitalen Raum, kommen könnte: Gab es hier Erkenntnisse, die diese Befürchtungen bestätigen? Welche Maßnahmen wurden und werden von den Plattformen ergriffen, etwa, um mögliche, auf Algorithmen basierende Wahlbeeinflussung zu verhindern? Mit wem arbeiten die Plattformen in Deutschland zusammen?**

(Die Fragen 4 und 5 werden nachfolgend wegen ihrer inhaltlichen Überschneidung gebündelt beantwortet)

Für den Bundestagswahlkampf 2017 wurden eine Reihe von Manipulationsversuchen nachgewiesen. Über die Chat-Plattform Discord wurden in mindestens zwei Kanälen verschiedene Akteure versammelt, die versuchen wollten, Einfluss auf die Bundestagswahl zu nehmen. Dort wurden beispielsweise Anleitungen zum anlegen von Fake-Accounts verbreitet, politische Memes erstellt und zeitlich koordinierte Aktionen durchgeführt. Dazu gehörte beispielsweise das massenhafte Kommentieren auf Youtube oder die Generierung von Tweets unter bestimmten Hashtags, ebenso wie Angriffe auf Personen, die zuvor zu Feinden erklärt wurden.

Unmittelbar vor der Wahl verbreiteten Fake-Konten auf Twitter die Meldung, sie hätten sich als linke Aktivisten unter die Wahlhelfenden gemischt, um das Wahlergebnis zu manipulieren. Zudem wurden unter dem Hashtag #Wahlbetrug zahlreiche Falschmeldungen verbreitet. Bemerkenswert war in diesem Zusammenhang die antizipierende Arbeit des Teams des Bundeswahlleiters, das entsprechende Tweets ausfindig machte und Falschmeldungen richtig stellte.

In Deutschland arbeitet Facebook zur Widerlegung von Falschmeldungen seit 2017 mit Correctiv als Fact-Checking-Partner zusammen. Im März 2019 übernahm auf die dpa eine solche Kooperation.

6. **Welche Folgen könnten digitale Manipulationsversuche haben? Welche Akteure sind an der Verbreitung von Desinformation und Durchführung von Manipulationsversuchen beteiligt? Gibt es Bezüge dieser Akteure untereinander und wenn ja, welche? Welche Methoden spielen in Sachen Desinformation in Deutschland und Europa eine Rolle? Welche Motive sind im Bereich der digitalen Manipulation und Einflussnahme auf demokratische Prozesse auszumachen?**
7. **Unter anderem bei der US-amerikanischen Präsidentenwahl sowie bei dem Brexit-Referendum soll es digitale Wahlbeeinflussung und damit Meinungsbeeinflussung gegeben haben: Welche Bedeutung messen Sie solchen Meldungen bei? Welche Gefahren sehen Sie durch Desinformationskampagnen in sozialen Netzwerken? Gibt es Möglichkeiten, diese Kampagnen zu analysieren und gegen sie vorzugehen? Wo liegen eventuelle Problematiken (z. B. Datenzugang für die Analyse, etc.)? Wie schätzen Sie die Gefahr für die Europawahl und anstehende Wahlen in Deutschland ein?**

(Die Fragen 6 und 7 werden nachfolgend wegen ihrer inhaltlichen Überschneidung gebündelt beantwortet)

Die Ziele und Folgen digitaler politischer Manipulationsversuche sind vielfältig. Dazu

gehören die Mobilisierung und Demobilisierung von Wählenden sowie eine Polarisierung der Gesellschaft. Desinformation als politisches Werkzeug von in Deutschland ansässigen Akteuren ist hierbei sowohl als Symptom einer gesellschaftlichen Polarisierung, aber auch als Instrument weiterer Polarisierung zu verstehen. Zudem sind Manipulationsversuche Teil einer Strategie, den politischen Diskurs zu lenken und andere Diskurse zu verdrängen.

Aus Indien und Nigeria wissen wir, dass Falschmeldungen zum Anlass für Gewalttaten werden können. Das jüngste Beispiel antiziganistischer Gewalt in Frankreich nach Falschmeldungen über angebliche Kindesentführungen und Organhandel, die in dieser und abgewandelter Form seit unzähligen Jahren kursieren, weisen auf mögliche Folgen hin. Auch in Deutschland wurden in der Vergangenheit falsche Fahndungsaufrufe veröffentlicht, die vielfach von gewaltverherrlichenden Kommentaren begleitet wurden.

Eine Vielzahl von Akteuren unternimmt Versuche der digitalen Beeinflussung und Manipulation im Netz. Sie sind zum Teil in mehr oder weniger losen Netzwerken organisiert, zudem kopieren sie Strategien und Meldungen und passen sie für ihre Zwecke an. Direkte Kontakte sind in diesem Zusammenhang nicht mehr nötig.

Auch die Motive sind vielfältig und können sich untereinander überschneiden. Politisch motivierte Manipulationsversuche sind beispielsweise häufig auszumachen. Etwa, um dem eigenen politischen Lager einen Vorteil zu verschaffen oder dem politischen Gegner zu schaden oder um zu polarisieren.

Auch finanzielle Motive sind in diesem Zusammenhang ersichtlich. Etwa werden besonders emotionalisierende Nachrichten erfunden und verbreitet, um so Anzeigeneinnahmen zu erzielen. Auch der illegale Verkauf von Waffen über den sogenannten „Migrantenschreck"-Shop unter der Konstruktion einer dauerhaften Bedrohung der inneren Sicherheit ist unter diesem Aspekt zu betrachten. Ebenso wie Blogs und sogenannte „Alternativmedien", die zusätzlich beispielsweise politisch gefärbtes Merchandise, Bücher und Prepper-Ausrüstung in ihren jeweiligen Shops verkaufen.

Letztlich ist auch Trolling und das Erzwingen einer irgendwie gearteten Reaktion eine Motivation für digitale Manipulationsversuche. So werden seit Jahren auf Twitter im Falle von Terroranschlägen oder Amokläufen die immer gleichen Fotos falscher Verdächtiger sowie Fotos von angeblichen Vermissten verbreitet. Das gleiche gilt auch im Fall von Naturkatastrophen. Im weniger schlimmen Fall beispielsweise mit dem Foto eines Hais, der angeblich schon seit 2012 nach jedem Hurricane durch die Highways der USA schwimmt.

Zur Analyse von Kampagnen ist vermehrte Transparenz seitens der Plattformen unerlässlich. Dabei ist jedoch zu beachten, dass private Konversationen als solche erhalten bleiben. Forschende und Journalisten fordern lediglich Zugriff auf ohnehin öffentliche Daten, um sie maschinell zu analysieren. Der entsprechende Zugriff auf Programmierschnittstellen wurde nach dem Skandal um Cambridge Analytica seitens der Plattformen zunächst erheblich eingeschränkt. Zu den ebenfalls von Forschung und Presse eingeforderten Daten gehören außerdem solche, die bislang nicht öffentlich sind: Gemeint ist der Zugriff auf Daten zu politischer Werbung, ihren Kosten und der jeweils ausgewählten Zielgruppe.

8. **Welche Schritte müssten von politischer Seite eingeleitet werden, um digitale Wahlbeeinflussung sinnvoll zu verhindern? Bedarf es gesetzgeberischer Maßnahmen? In welchem Rahmen wären diese sinnvoll? Wie soll das Frühwarnsystem der EU denn aussehen – bzw. wie müsste es aussehen, um wirksam zu sein? Bietet der Einsatz von künstlicher Intelligenz oder anderer technischer Mittel die Möglichkeit, Desinformation und Wahlbeeinflussung vorherzusehen, zu erkennen und einzudämmen? Ist es Aufgabe des Gesetzgebers, darüber zu entscheiden, ab wann eine unzureichende oder tendenziell gefasste Information wahlbeeinflussend wirkt?**

Neben Maßnahmen zur Sensibilisieren und Schulung verschiedener Akteure und der Investition in die Förderung der Medien- und Informationskompetenz der Bevölkerung sind weitere Maßnahmen denkbar.

Während Modellprojekte und Innovationsförderung wichtig und richtig sind, sollten langfristige Förderungen im Bereich Bildung, Journalismus und Technologie verstärkt werden. Nachhaltiger Journalismus, beispielsweise in gemeinnützigen Modellen, sowie technologische Innovationen im Bereich Fact-Checking und Verifikation können langfristig dazu beitragen, die Wirkung digitaler Manipulationsversuche einzuschränken.

Zudem sollten Informationen, etwa auf Seiten der Ministerien, besser auffindbar und nachvollziehbar aufbereitet werden. Das bloße Verlinken von PDF-Dokumenten kann demnach nicht länger als Standard gelten. Solche Maßnahmen sollten auch antizipierend erdacht werden. Etwa hätte die Kampagne gegen den „Globalen Pakt für sichere, geordnete und geregelte Migration" antizipiert werden und entsprechende Informationsangebote aufbereitet werden können. Durch den Mangel an entsprechend aufbereiteten, auffindbaren Informationen ergab sich in Bezug auf die Diskussion um den Migrationspakt eine Datenlücke (data void), die von rechtspopulistischen Akteuren

genutzt wurde. Folglich waren vor allem ihre Inhalte aus Blogs und Videoplattformen während der ersten Zeit der Kampagne gegen den Pakt über Suchmaschinen auffindbar, nicht aber umfassende Informationen von Seiten des Außenministeriums oder anderen Akteuren.

9. **Fake News, Fake Accounts, Desinformationskampagnen, Trolle, Social Bots, … der Werkzeugkasten für politische Manipulationsversuche scheint groß. Welche Möglichkeiten werden tatsächlich mit welcher Wirkung genutzt? Wie wichtig sind in diesem Zusammenhang unabhängige Fakten-Checker? Wie stark wirken sich nachgelagerte Effekte, z. B. Berichterstattung in Zeitungen, aus? Welche weiteren Faktoren können manipulativ wirken? Öffentlich-rechtliche Medien produzieren hochwertige Inhalte in Bild, Ton und Text, insbesondere auch auf dem Gebiet der politischen Berichterstattung. Ein Teil dieser Inhalte wird jedoch durch Depublikationspflichten nicht dauerhaft im Internet verfügbar gemacht. Gibt es über die Depublikation hinaus weitere gesetzliche Vorgaben, die aus Ihrer Ansicht die Verbreitung von Desinformation begünstigt und welche rechtlichen Änderungen könnten hier helfen?**

Fact-Checking oder Debunking hat sich, anders als in anderen Ländern, in Deutschland noch nicht als journalistisches Tätigkeitsfeld etabliert. Dabei ist Fact-Checking hier als Überprüfung von Statements von politischen Akteuren oder viralen Behauptungen auf ihren Faktengehalt zu verstehen. Obwohl bereits vor der Bundestagswahl 2017 zahlreiche Falschmeldungen, insbesondere im Themenfeld Asyl ab Sommer 2015, in sozialen Medien verbreitet wurden, gab es zu diesem Zeitpunkt kaum entsprechende Fact-Checking-Projekte. Auch im politischen Diskurs wurde das Thema Desinformation erst nach der Wahl Donald Trumps aufgegriffen.

Nach der Bundestagswahl wurden einige Projekte zudem eingestellt, in anderen wurde die Zahl der Mitarbeitenden verringert. Spätestens seit den Falschmeldungen im Zusammenhang mit dem tödlichen Messerangriff in Chemnitz und den Kampagnen gegen den EU-Migrationspakt sollte jedoch klar sein, dass die massenhafte Verbreitung von Falschinformationen oder gar Desinformationskampagnen nicht nur im Wahlkampf eine Rolle spielen, sondern auch anlassbezogen zum Einsatz kommen.

Auch die Depublikationspflichten führen in diesem Zusammenhang zu Problemen. Seit geraumer Zeit werden Falschmeldungen mehr und mehr recycelt, also einfach neu gepostet oder anderweitig wiederverwendet. Die Depublikation von entsprechenden Faktenchecks, referenzierten Interviews oder Berichten ist in diesem Zusammenhang nicht zeitgemäß.

10. **Falsche, unzureichende oder tendenziell gefasste Informationen sind auch in der analogen Kommunikation und Berichterstattung bekannt. Was macht die Besonderheit von Falschinformationen - von Fake News - im digitalen Kontext aus? Welche Rolle spielen Fake News bei der Wahlbeeinflussung? Haben Falschinformationen im Netz einen (messbar) größeren Einfluss auf die Wahlentscheidungen der Bürgerinnen und Bürger, als die Berichterstattung in den klassischen Medien? Wie ließe sich effektiv gegen Fake News vorgehen?**

    Gewissermaßen handelt es sich bei der Verbreitung von Desinformation über soziale Medien um eine Art Demokratisierung der Propaganda. Jeder Mensch mit Zugriff auf ein Social-Media-Konto verfügt grundsätzlich über die Möglichkeit, eine Falschmeldung zu erstellen und einer großen Anzahl Internetnutzender zugänglich zu machen.

    Ähnlich wie sich andere Interessengruppen im Netz zusammen finden, finden sich auch demokratiefeindliche oder opportunistische Akteure mit Gewinnabsichten im Netz zusammen und können sich über Landesgrenzen hinweg koordinieren.

    Hinsichtlich der Wirkung von Desinformation auf die Wahlentscheidungen von Bürgerinnen und Bürgern sind weitere Studien nötig. Untersucht werden sollte außerdem, inwiefern digitale Propaganda zur Mobilisierung oder Demobilisierung von Wählenden beiträgt.

11. **Ergeben sich Handlungsempfehlungen für die Politik? Wäre ein möglicher Ansatzpunkt, dass beispielsweise alle Nutzer, die mit Fake News konfrontiert worden sind, über deren Identifizierung als solche sowie, gegebenenfalls, deren Richtigstellung obligatorisch informiert werden müssen? Wäre das angemessen? Wäre ein möglicher Ansatzpunkt zur Bekämpfung von Falschinformation, das journalistische Konzept der „Trust Chain" auf dem technischen Konzept der „Chain of Trust" abzubilden? Wie können technische Innovationen in diesem Bereich politisch gefördert werden, insbesondere vor dem Hintergrund, dass die Entscheidung darüber, was journalistisch integer ist und was nicht, frei von dem Vorwurf staatlicher Einflussnahme bleiben muss? Wie gehen Plattformen mit Werbung im Umfeld von Fake News um?**

    Grundsätzlich wäre es möglich und sinnvoll, Nutzern, die auf ihren Social-Media-Kanälen mit einer Falschmeldung konfrontiert waren, die entsprechende Richtigstellung auszuspielen. Insgesamt ist die Zahl derer, die in Deutschland in entsprechenden Fact-Checking-Teams arbeiten, allerdings sehr überschaubar. Besteht man auf einer

unabhängigen Überprüfung vermeintlich falscher Fakten, muss also berücksichtig werden, dass nur ein Teil der verbreiteten Behauptungen widerlegt werden kann und wird. Auch eine zivilrechtlich zu erwirkende Gegendarstellung wäre denkbar, liegt jedoch nicht innerhalb des Handlungsspielraumes eventuell betroffener Personen.

Zudem sollte auch im politischen Kontext von der Verbreitung von Falschbehauptungen oder pauschalen Angriffen auf Journalisten abgesehen werden.

12. **Wie sinnvoll ist eine Kennzeichnung von Social Bots? Können Social Bots überhaupt eindeutig identifiziert werden? Welche Definition von „Social Bot" legen Sie Ihrer Einschätzung dabei zugrunde? Wie ist die bisherige Forschung zu Social Bots zu bewerten? Welche Rolle spielen Social Bots – sind sie eine echte Gefahr oder herrscht eine eher übertriebene Furcht? Ist Deutschland - vor dem Hintergrund zu erwartender erheblicher Entwicklungssprünge im Bereich der Bot-Technologie und immer schwieriger zu enttarnender Social Bots - auf Neues vorbereitet?**

Grundsätzlich ist gegen eine Kennzeichnung automatisierter Accounts nichts einzuwenden. Fraglich ist allerdings, ob eine Kennzeichnung allein die anvisierte Wirkung erzielt. Aktuell werden Bots, die vorgeben, echte Personen zu sein, nicht massenhaft eingesetzt, um eigene politische Botschaften zu streuen. Vielmehr werden sie zur Verbreitung und Amplifizierung von bestimmten Inhalten genutzt, sie retweeten und liken beispielsweise Inhalte auf Twitter. Eine Kennzeichnung allein würde entsprechend nur dann helfen, wenn zusätzlich erkennbar wäre, wie hoch der Anteil automatisierter Accounts bei Retweets und Likes eines jeden Tweets ist.

Im Hinblick auf technologische Entwicklungen im Bereich der Desinformation und digitaler politischer Manipulation sollte antizipierend gearbeitet und vor allem geforscht werden. Das gilt insbesondere auch für die Zukunft von Deep-Fake-Videos und anderen maschinell generierten Inhalten. Gleichzeitig sollten diese Debatten allerdings nicht dringend notwendige Debatten über aktuell bestehende Probleme, wie etwa der massenhaften Verbreitung entkontextualisierter Fotos und Videos, verdrängen oder gänzlich ersetzen.

13. **Eine Studie der Europäischen Kommission aus dem letzten Jahr hat unter anderem gezeigt, dass 81 Prozent der Bürger sich mehr Transparenz bei der Werbung in sozialen Netzwerken wünschen. Wie könnten Plattformen diese gewünschte Transparenz konkret herstellen? Inwieweit könnte ein Mehr an Transparenz durch die Plattformen sinnvoll sein? Sind Ihnen Planungen der Anbieter bekannt?**
14. :: **Wie bewerten Sie digitale Wahlwerbekampagnen? Gibt es Probleme, z.B. in**

Bezug auf Transparenz, und wie könnten diese gelöst werden? Können Wahlwerberegister, wie sie Facebook und Twitter bereits in den USA, Brasilien und Großbritannien anbieten, Abhilfe schaffen? Könnte man Plattformen dazu verpflichten, solche Daten zur Verfügung zu stellen?::

(Die Fragen 13 und 14 werden nachfolgend wegen ihrer inhaltlichen Überschneidung gebündelt beantwortet)

Einige Plattformen haben entsprechende Datenbanken bereits veröffentlicht. Insgesamt ist zu sagen, dass diese Datenbanken nicht einheitlich sind und unterschiedlich aufbereitet sind.

Facebook und Twitter haben bereits vor einer Weile ein entsprechendes Angebot eingeführt, über das User sich über alle geschalteten Werbeanzeigen einer Facebook-Seite oder eines Twitter-Kontos informieren können.

Facebook hat zudem vor kurzem eine Datenbank für politische Werbeanzeigen in EU-Ländern eingeführt. Zuvor waren entsprechende Daten nur für die USA, Brasilien und wenige andere Länder einsehbar. Hierüber können einzelne Akteure sowie Stichworte gesucht werden. Die angezeigten Werbeinhalte können eingesehen werden und enthalten außerdem Informationen über die Regionen, das Geschlecht und das Alter der Nutzenden, denen die Anzeigen ausgespielt wurden. Außerdem werden ungefähre Angaben zu den Kosten der jeweiligen Anzeigen gemacht.

Google bereitet eine entsprechende Datenbank für politische Werbung aktuell vor. Diese soll noch im April veröffentlicht werden. Solche Angebote gibt es bereits für die USA und Indien. Enthalten sind hier auch Werbeanzeigen, die auf Youtube geschaltet werden.

Google und Facebook stellen zudem Überblicksberichte über geschaltete politische Werbung bereit, über die sich politisch werbende Akteure identifizieren lassen.

Nach aktuellem Stand lassen sich zwei Schwachpunkte aus den jeweils angebotenen Datenbanken ausmachen. Zum Einen müssen Nutzer der Datenbanken bei Twitter, zum Teil aber auch bei Facebook wissen, welchen politischen Akteur oder welches Stichwort sie einsehen wollen. Zum Anderen könnten einzelne politische Akteure, etwa weil sie unbekannt sind oder bestimmte Stichworte, die politischer Werbung zugeordnet werden, nicht aufgreifen, nicht in den Datenbanken enthalten sein, weil sie nicht als politisch Werbende identifiziert wurden.

Aus dem Bundestagswahlkampf 2017 wissen wir, dass politische Werbung nicht zwingend über die Social-Media-Konten von Parteien oder zur Wahl stehenden Kandidierenden geschaltet wird. So betrieb der sogenannte „Greenwatchblog" negative Kampagnen gegenüber den Grünen und schaltete Werbung auf Twitter und Facebook. Das Blog verschwand mit dem Wahlsonntag. Für die AfD warb auf Twitter Wirtschaftsexperte Max Otte.

Im Zusammenhang mit dem tödlichen Messerangriff in Chemnitz und der darauf folgenden Kontroverse um den damaligen Verfassungsschutzchef Hans-Georg Maaßen schaltete die Facebook-Seite „Solidarität mit Hans-Georg Maaßen" Werbeanzeigen auf Facebook und Instagram. Hier ist nicht bekannt, wer hinter der Facebook-Seite steckt und wieviele Anzeigen geschaltet wurden. Der Fall zeigt jedoch, dass ein Zugriff auf die entsprechenden Werbedatenbanken der Plattformen auch abseits von Wahlkampfzeiten wichtig sind.

Wünschenswert ist zudem die Bereitstellung von sinnvoll nutzbaren Programmierschnittstellen, über die Forschende Zugriff auf den Datensatz und einzelne Funktionen der Datenbanken erhalten. So können automatisierte Abrufe größerer Datensätze zu Forschungszwecken gewährleistet werden.

Nicht nur die Plattformen sollten in die Pflicht genommen werden, einen transparenten Umgang mit digitaler Wahlwerbung zu finden. Generell sollten politische Parteien und Akteure allgemein, besonders aber im Wahlkampf, Informationen über die von ihnen geschalteten Anzeigen zu veröffentlichen. Das schließt neben dem Inhalt der Anzeigen auch die Kosten sowie Informationen zur Zielgruppe ein.

15. **Was ist der Forschungsstand zu Desinformation und Meinungsbildung in sozialen Netzwerken und wo sind die Forschungsbedarfe besonders hoch? Wie kommen Forscherinnen und Forscher derzeit an die benötigten Daten, um diese Phänomene zu erforschen und wie kann der Zugang zu diesen Daten verbessert werden? Welche Möglichkeiten für den Zugang zu Social-Media-Daten sollten für wissenschaftliche Zwecke geschaffen werden?**

Sowohl zur Wirkung von Desinformation als auch zur Wirkung von Fact-Checking gibt es noch hohen Forschungsbedarf. Der absolut größte Anteil verfügbarer Studien betrachtet beides im Kontext der USA. In Bezug auf das politische sowie das Mediensystem sind viele Erkenntnisse jedoch nicht übertragbar.

Anzumerken ist zudem, dass viele Studien nur kleine Teilbereiche des Themenbereichs

abdecken und dass Studien zur Wirkung sowohl von Desinformation als auch Fact-Checking sich zum Teil auch widersprechen.

Zum Ausmaß und der Wirkung von Bildern und Videos, die zur Verbreitung von Falschmeldungen genutzt werden, gibt es auf Deutschland bezogen keine Studien. Obwohl vor allem entkontextualisierte Bilder und Videos zu den erfolgreichsten Methoden der Verbreitung von Desinformation in Deutschland gehören, wissen wir bislang wenig über Verbreitungswege und Wirkung.

Das liegt unter anderem auch daran, dass sich die Verbreitung von Artikeln sogenannter „Alternativmedien" aktuell leichter nachverfolgen lässt. Ähnlich lässt sich auch der große Anteil an Studien zu Desinformation auf Twitter erklären: Dort lassen sich Verbreitungswege und Netzwerke leichter untersuchen, als beispielsweise auf Facebook und Youtube.

Auch die Rolle der sogenannten Alt-Tech-Plattformen und anderer Ausweichplattformen als Mittel der Vernetzung antidemokratischer Akteure ist in Bezug auf Deutschland bislang weitestgehend unerforscht. Eine Ausnahme bilden Untersuchungen zu zwei Discord-Kanälen, die vor der Bundestagswahl 2017 zum Zwecke der politischen Beeinflussung eingerichtet wurden.

16. **Welche Rolle spielen digitale Astroturfing-Kampagnen, die Graswurzel-Engagement vortäuschen, aber in Wahrheit von externen Akteuren gesteuert werden? Wie kann man solchen Kampagnen begegnen?**

Bisher ist bekannt, dass unter anderem in Vorbereitung der Versuche zur Beeinflussung der Bundestagswahl 2017 auch Strategiepapiere zur Erstellung von Fake Accounts kursierten. In einem entsprechenden Discord-Channel (einer Chat-Plattform, die für Gamer entwickelt wurde und für vielfältige Zwecke benutzt wird) wurden solche Anleitungen verbreitet, die unter anderem die Anweisung enthielten, Twitter-Konten durch unpolitische Inhalte, etwa zum Thema Autos oder Fußball, anzureichern. So sollte die Identifikation dieser Sockenpuppen-Accounts, also manuell gesteuerter Fake-Accounts, erschwert werden. Wie viele dieser Accounts vor der Bundestagswahl angelegt wurden oder aktuell für politische Zwecke eingesetzt werden, ist jedoch schwer abzuschätzen.

Mögliche Gegenmaßnahmen betreffen beispielsweise das gezielte Monitoring politischer Kampagnen auf Plattformen wie Youtube, Facebook und Twitter. Gleichzeitig ist von einer pauschalen Verächtlichmachung politischer Protestformen im Internet abzusehen.

Im Zusammenhang von möglichen staatlichen oder nicht-staatlichen Akteuren, die solche Kampagnen steuern oder zu beeinflussen versuchen, ist entsprechende Transparenz von Seiten der Plattformen einzufordern. Werden Netzwerke dieser Art identifiziert, sollten Nutzer, die mit diesen interagiert haben, entsprechend informiert werden.

Von einer Klarnamenpflicht oder ähnlichen Maßnahmen ist vor dem Hintergrund, dass gerade Angehörige diskriminierter Minderheiten aus verschiedenen Gründen anonym im Internet agieren, abzusehen. Zudem werden zahlreiche Falschmeldungen ebenso wie Drohungen und hasserfüllte Nachrichten auch unter Angabe von Klarnamen verbreitet. Ein Abschreckungseffekt in diesem Sinne ist nicht zu beobachten.

17. **Inwieweit ist die Wirkung von „Dark Ads" im Kontext von Wahlen untersucht worden?**

Der Forschungsstand in diesem Bereich ist insgesamt sehr gering, im Bezug auf Wahlen in Europa im Allgemeinen und Deutschland im Speziellen sind noch weniger Studien zu verzeichnen. Das liegt unter anderem auch an einem Mangel an verfügbaren Daten, sowohl seitens politischer Parteien und Akteure, als auch der Plattformen, auf denen Werbung geschaltet wird.

Abzuwarten bleibt, ob die neu aufgesetzten Datenbanken für politische Werbung, etwa von Facebook und Google, künftig entsprechende Studien ermöglichen. Voraussetzungen wären dafür auch entsprechende Programmierschnittstellen, die automatisierte Abrufe, etwa zu bestimmten Stichworten, ermöglichen.

18. **Veröffentlichungen von geleakten oder erbeuteten Daten können durch falsche Daten angereichert worden sein. Ist der Umgang und die mögliche Veröffentlichung dieser Daten ausreichend geregelt oder besteht hier noch Handlungsbedarf?**

Die Veröffentlichung falscher oder manipulierter Datensätze kann sowohl Taktik des veröffentlichenden Akteurs als auch der anvisierten Akteure sein. Wie uns die Erfahrung aus dem französischen Wahlkampf 2017 gelehrt hat, können Datensätze auch in Antizipation eines Hacks oder Datenklaus und deren entsprechender Veröffentlichung mit falschen Daten angereichert werden.

Grundsätzlich sollten jedoch alle von einem Datenleak betroffenen Personen schnellstmöglich von den Behörden informiert werden, da in der Regel nicht nur Personen, deren Konten gehackt oder Daten erbeutet wurden, betroffen sind, sondern auch deren Kontakte.

Zur Vorbeugung künftiger Angriffe dieser Art sollten Abgeordnete und ihre Mitarbeitenden zudem stärker sensibilisiert werden. Auch entsprechende Beratungsangebote für andere potentiell betroffene Akteure wären wünschenswert. Der umfangreiche Doxing-Fall vom Januar 2019 zeigt, dass neben Politikern auch deren Familien, sowie außerdem politisch aktive Prominente, Journalisten und andere zu Zielen solcher Angriffe werden.

Politisch motivierte Phishing-Angriffe sind heutzutage oft gründlich und gut vorbereitet. Zudem besteht die Gefahr, dass Social Engineering zum Einsatz kommt. Böswillige Angreifer könnten sich beispielsweise als Journalisten oder Mitarbeitende ausgeben und auf diese Weise versuchen, private Daten zu erbeuten.