Hochschule für Politik München
an der Technischen Universität München

Hochschule für Politik München | Richard-Wagner-Str. 1 | 80333 München

An den Ausschuss Digitale Agenda
des Deutschen Bundestags

- per Email -

Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)049

Prof. Dr. Simon Hegelich
Political Data Science
Technische Universität München
Hochschule für Politik
Richard-Wagner-Str. 1
80333 München

Email: simon.hegelich@hfp.tum.de
Blog:
https://politicaldatascience.blogspot.de
Twitter: @SimonHegelich

München, 09.04.2019

Fragenkatalog für das Fachgespräch zum Thema „Resilienz von Demokratien im digitalen Zeitalter im Kontext der Europawahl“ im Ausschuss Digitale Agenda am 10. April 2019

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?

Die derzeitigen sozialen Netzwerke (insbesondere Facebook) sind nicht für den politischen Diskurs entwickelt. Viele im Design verankerte Aspekte funktionieren gut in privaten Freundesnetzwerken, sind aber für die politische Kommunikation problematisch. Ein privater Beitrag, der extrem häufig „geliked“ wird, ist meistens tatsächlich relevant. Ein politischer Beitrag wird eventuell sehr häufig geteilt, weil es eine Vielzahl von politischen Aktivist*innen gibt, die ein Interesse an der Verbreitung haben. Viele sehr wirksame Schritte lassen sich nur in Kooperation mit den Plattformbetreibern entwickeln: Der Schritt, die Monetarisierung von Falschnachrichten zu erschweren, hat zum Beispiel sehr viel Bewirkt. Bei Facebook wäre es denkbar, politische Inhalte mit angepassten Algorithmen zu verbreiten. Derzeit optimiert die Plattform „time well spent“, d. h. so genannte „meaningfull interaction“ (und dazu zählen Likes, Shares, Comments) führen dazu, dass ein Beitrag auch vielen anderen Nutzern angezeigt wird. Alternativ könnten zum Beispiel Interaktionen, die über politische Lager hinweg gehen, oder Beiträge, die gründlich gelesen werden stärker gewichtet werden. Eine gesetzliche Regelung auf dieser Ebene ist aber nicht denkbar, weil damit unmittelbar in das Produkt eingegriffen würde. Gesetzliche Regelungen können aber ein höheres Maß an Transparenz erreichen, zum Beispiel durch umfangreiche Berichtpflichten und einen Datenzugang, der es ermöglicht, komplexe Effekte in der politischen Kommunikation auch zu untersuchen. Wobei angemerkt sei, dass „die Wissenschaft“ zwar gerne Datenzugang verlangt, aber es derzeit nicht annähernd genügend Ressourcen gibt, dass Wissenschaftler*innen die Daten, die bereits zur Verfügung

stehen, umfassend analysieren könnten. Im Bereich der Medienkompetenz ist daher auch an die Forschung zu denken, die bei der digitalen politischen Kommunikation noch vor vielen ungelösten Fragen der Grundlagenforschung steht.
Interessant sind auch Überlegungen, eine öffentlich-rechtliche Struktur für die digitale politische Kommunikation zu schaffen. Wenn man nicht will, dass diese Sphäre nach rein privatwirtschaftlichen Regeln funktioniert, wäre dies eine logische Schlussfolgerung. Wie ein „öffentlich-rechtliches Facebook“, das dann auch bei den Nutzer*innen ankommt, aussehen könnte, ist allerdings völlig offen.

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?

In einem Forschungsprojekt das über Social Science One läuft, wollen wir an der TU München mit Hilfe von Daten von Facebook zu geteilten URLs untersuchen, ob sich ein Effekt einer größeren Desinformationskampagne auf die Umfrageergebnisse der Parteien im Bundestagswahlkampf 2017 zeigen lässt. Mir ist nicht bekannt, dass es bereits Studien gibt, die den Effekt solcher Kampagnen belegen oder falsifizieren konnten.
Generell spricht viel in der Forschung dafür, dass eine Beeinflussung, wenn sie denn überhaupt stattfindet, sehr indirekt ist. Am ehesten würde man solche Effekte bei kulturellen Themen wie Migration, Anti-Political-Correctness, Religion und Homophobie erwarten.

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?

Bislang ist wissenschaftlich völlig unklar, ob eine digitale Wahlbeeinflussung möglich ist.
Dennoch haben die Plattformbetreiber diverse Schritte unternommen, dieses Risiko zu verringern. Hierzu zählen der Aufbau von Teams, die sich mit dem Thema beschäftigen, das Vorgehen gegen gefälschte Accounts und die Erhöhung der Registrierungsanforderungen bei politischer Werbung. Wichtig ist, dass Desinformationskampagnen nicht über den Inhalt definiert werden können. Völlig harmlose Posts, wie zum Beispiel Nachrichten über Dynamo Dresden, können Teil einer Kampagne sein, mit dem Ziel, höhere Reichweiten aufzubauen. Daher lässt sich die Identifikation nur über das Verhalten im ganzen (also weder über Inhalte, Nutzer oder Infrastruktur für sich) erzielen. Alle unsere Untersuchungen an der TU München zeigen, dass unauthentisches Verhalten, Strategien zur Manipulation von Algorithmen und Desinformation in

aller erster Linie ein Phänomen von rechts ist. Ein Grund dafür ist sicher auch, dass rechtsorientierte Menschen auf kulturelle Themen wie Migration, Religion, Homophobie und Anti-Political-Correctness stärker anspringen und sich diese Themen besonders gut für eine Beeinflussung eigenen. Hinzu kommt die politische Situation in Deutschland, in der eine rechte Partei stark als Anti-Establishment-Bewegung wahrgenommen wird. Selbst wenn die Urheber einer Desinformationskampagne völlig andere Interessen verfolgen und zum Beispiel aus dem Ausland kommen, und zur Destabilisierung der politischen Verhältnisse in Deutschland beitragen wollen, wären die Anhänger*innen der AfD ein naheliegendes Publikum für eine solche Kampagne.

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?

Zur Europawahl sind mir keine Anhaltspunkte bekannt, aber wir untersuchen diese Frage an der TU München. Wir können aber zeigen, dass dieselbe Kampagne, die im US-Wahlkampf aktiv war und die in der Öffentlichkeit – ob zu recht oder nicht – mit Russland in Verbindung gebracht wird, auch in Deutschland aktiv war. Wir können zeigen, dass es eine hohe Wahrscheinlichkeit gibt, dass diese Kampagne auf Twitter und Facebook agierte und dass es ihr gelungen ist, traditionelle Medien dazu zu bewegen, Nachrichten und Accounts auf ihren Internetseiten zu zitieren. Daher gehen wir davon aus, dass die Reichweite dieser Kampagne über die unterschiedlichen Plattformen und Medien hinweg wesentlich größer war, als bislang angenommen. Ob sich daraus ein Effekt ergeben hat, ist Gegenstand der aktuellen Forschung.

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?

Siehe Antwort zu Frage 4. Auf Initiative von Facebook gibt es jetzt eine Arbeitsgruppe, die am BSI angesiedelt ist. Mein Eindruck ist allerdings, dass Facebook wesentlich besser vorbereitet ist und auch mehr Ressourcen zur Verfügung stellt als das BSI, welches das Thema zunächst als Teilproblem der technischen Infrastruktur und weniger als gesellschaftspolitische Herausforderung zu verstehen scheint. Meines Wissens gibt es bislang auch kein explizites Bedrohungsszenario, was aber der Ausgangspunkt einer Sicherheitsstrategie sein sollte. Ein solches Bedrohungsszenario hätte sich mit den vielen Hinweisen auseinanderzusetzen, dass Desinformation ein Phänomen ist, welches häufig von rechts ausgeht und auf das rechte Spektrum der Wahlbevölkerung zielt.

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?

Welche Akteure mit digitalen Manipulationsversuchen in Verbindung gebracht werden können, liegt auch sehr stark an der zugrundeliegenden Definition von Manipulation. Ich bevorzuge inzwischen das Wort „Hacking“, in dem Sinne, dass versucht wird, Regeln strategisch auszunutzen, um zum Beispiel einen Einfluss auf die Algorithmen zu bekommen. Dieses Hacking ist in den meisten Fällen nicht rechtlich zu beanstanden. Bei dieser weiten Definition ist auch das Feld von Akteuren sehr groß und reicht von „unintendierten Akteuren“, wie zum Beispiel SPAM-Bots, die zufällig politische Inhalte verbreiten, über politische Aktivist*innen im In- und Ausland bis hin zu Politiker*innen selbst, die sich mit fragwürdigen Mitteln eine höhere Reichweite verschaffen. Bei großangelegten Kampagnen scheint das Ziel in erster Linie Verunsicherung zu sein. Insofern kann eine Kampagne auch deshalb erfolgreich sein, weil viel über Manipulation geredet wird und in der Bevölkerung der Eindruck entsteht, die Wahlen seien manipuliert, auch wenn das gar nicht der Fall ist.

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?

Bislang ist es keiner Studie gelungen, einen Effekt von Desinformationskampagnen nachzuweisen. Es ist aber zum Beispiel auch nach wie vor umstritten, welchen Effekt normale Wahlwerbung hat. Dass kein Effekt bewiesen ist, heißt daher nicht, dass er widerlegt wäre. Dennoch ist eine große Gefahr, dass Desinformationskampagnen genau deshalb ihr Ziel (Vertrauensverlust in demokratische Institutionen) erreichen, weil die Gefahr in der öffentlichen Debatte überschätzt wird. Durch moderne Datenanalysen ist es möglich, sehr viel über laufende Kampagnen zu erfahren. Der Aufwand ist allerdings sehr groß und wird m. W. derzeit nur von Facebook und Google systematisch betrieben. In der Wissenschaft in Deutschland gibt es weder die Daten, noch genügend Leute, die sich mit diesen Themen beschäftigen. Im Verhältnis zu den großen Plattformunternehmen herrscht hier längst ein struktureller Nachteil, der sich auch darin zeigt, dass maßgebliche Forschungsergebnisse immer häufiger in den Unternehmen entwickelt werden. Mein Eindruck ist, dass bei den deutschen Behörden die Situation eher noch schlechter aussieht als an den Universitäten.
Die Gefahr einer substantiellen Wahlbeeinflussung erscheint im Lichte aller bisher bekannter Forschungsergebnisse eher gering zu sein. Problematischer erscheinen langfristige Tendenzen eines Vertrauensverlusts und einer Polarisierung. Aber auch solche Phänomene sind weder eindeutig belegt noch eindeutig mit der digitalen Kommunikation verknüpft.

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?

Geht man davon aus, dass wir einen Strukturwandel der Öffentlichkeit erleben, dann sind gesetzgeberische Maßnahmen absolut notwendig, weil der Wandel gestaltet werden muss. Derzeit wird man aber keine wirksamen Maßnahmen ohne die Unterstützung der Plattformen hinbekommen, weil einfach die Kompetenzen fehlen und viele entscheidende Aspekte in die geschäftliche Freiheit fallen. Der Gesetzgeber kann aber einen Rahmen schaffen, in dem die Kooperationsbereitschaft steigt und mehr Transparenz herrscht.
Künstliche Intelligenz (im Sinne von maschinellem Lernen) ist ein sehr mächtiges Werkzeug, um verborgene Strukturen aufzufinden. Daher können solche Systeme einen wichtigen Beitrag leisten, um gegen Desinformationskampagnen vorgehen zu können. Aber: Maschinelles Lernen ist erstens nicht einfach. Die Entwicklung eines erstklassigen Systems kostet Millionen. Schlechte Systeme sind Fehleranfällig und häufig unzureichend getestet. Leider sind die meisten Systeme, die derzeit zum Beispiel zur Erkennung von Social Bots eingesetzt werden, schlecht. Der Stand der Technik entspricht fast nie dem Stand der Forschung. Hinzu kommt zweitens, dass Mustererkennung zwar hilfreich ist, aber nicht wirklich „intelligent“. Bei den bekannten Desinformationskampagnen ist ein deutlicher Lerneffekt zu beobachten. Die Durchführung variiert und die Muster verändern sich. Ein technisches System kann daher immer nur ein unterstützendes Werkzeug sein, was gerade bei der Auffindung neuer, bislang unbekannter Muster, versagen wird.

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?

Siehe die vorherigen Antworten.

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?

Der Unterschied ist, dass die Verbreitung digital völlig anders funktioniert. Es gibt weniger Gatekeeper, heterogene Akteure und die Verbreitung von Informationen ist schneller, durch mobile Technologie unabhängig von Ort und Setting und folgt anderen Gesetzmäßigkeiten als bisherige Kommunikation. Zur Frage nach den Effekten siehe die vorherigen Antworten.

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?

Ein Ansatz für die Politik kann sein, mehr „Stellschrauben“ einzubauen, um gradueller regulieren zu können. Zum Beispiel lässt sich schlecht argumentieren, warum ein Beitrag, der nicht rechtswidrig ist, entfernt werden sollte. Dennoch gibt es aber auch kein Recht darauf, dass jeder Beitrag gleichermaßen verbreitet wird. Hier könnten die Plattformbetreiber als Distributoren und eben nicht als Urheber oder als Zensurinstanz in die Pflicht genommen werden. In der Theorie könnten die Plattformen verpflichtet werden, für eine „ausgewogene“ Verbreitung der Inhalte zu sorgen und ihre Medienmacht nicht zu missbrauchen. Wie solche Regelungen aber aussehen könnten und welche Instanz überhaupt in der Lage wäre, so etwas zu kontrollieren, muss letztenendes die Politik beantworten.

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?

Zum jetzigen Zeitpunkt scheint eine Kennzeichnungspflicht von Social Bots nicht sinnvoll. Denn in die Definition (Fake-Accounts, die ihre Identität verschleiern) geht eine Intention ein, die sich nur selten eindeutig nachweisen lässt. Automatisierung lässt sich generell sehr einfach kennzeichnen. Twitter hat diesen Schritt aber bereits umgesetzt, in dem die Information, von welchem System aus der Tweet gesendet wurde, angezeigt wird.
Es gibt Forscher*innen, die sich auch mit Social Bots beschäftigen. Es gibt aber keine einheitliche Forschung zu dem Thema. Manche Erkenntnisse sind sehr gut belegt, andere sind eher auf der Ebene von Vermutungen. Es gibt bislang – wie auch bei

Desinformationskampagnen – keine Beweise für Effekte aber genügend Ergebnisse, die eine Beeinflussung theoretisch möglich erscheinen lassen. In Zukunft werden automatisierte Inhalte nicht mehr von menschlich generierten Inhalten zu unterscheiden sein. Gerade durch so genannte Generative Adversarial Networks (GAN) wurden in den letzten Jahren hier immense Fortschritte erzielt. Die Politik sollte sich daher schon heute dringend fragen, wie generell damit umgegangen werden kann, dass manche Inhalte zukünftig nur noch einer Maschine zuzuordnen sind und Authentizität nahezu nicht mehr überprüfbar ist.

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?

Transparenz bei politischer Werbung ist sehr wichtig. Die Plattformbetreiber haben sich verpflichtet, hier für mehr Transparenz zu sorgen. Facebook stellt alle politischen Werbeanzeigen in einem Archiv zur Verfügung. Die Umsetzung ist m. W. noch nicht abgeschlossen. Für u. a. die USA und Großbritannien existiert dies Ad-Archive bereits und lässt relativ wenig Wünsche offen: Man sieht, wer wie viel für welche Werbung bezahlt hat und wie viele Nutzer*innen (aufgegliedert nach demographischen Faktoren) erreicht wurden. Nicht inbegriffen sind allerdings politische Posts, für die kein Geld bezahlt wurde. Außerdem ist anzumerken, dass die Einordnung, was politisch ist, nicht trivial ist und es dementsprechend auch Fehler geben wird. Wie genau die Plattformen diese Einordnung vornehmen, sollte daher transparent gemacht werden.

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?

Siehe vorherige Antwort. Auch die Parteien selbst sollten transparenter mit Online-Werbung umgehen und in einem Report veröffentlichen, wann welche Werbung für welche Gruppe ausgespielt wurde.

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?

Die Forschung zu Desinformation und Meinungsbildung in den sozialen Netzen ist naturgemäß noch ganz am Anfang. Die Entwicklungen sind sehr neu und die Plattformen verändern sich sehr dynamisch. Es fehlt auch an Grundlagenforschung. Dass die Wissenschaft keinen wirklichen Zugang zu den Daten hat, ist ein Problem. Allerdings nicht das einzige. Es fehlt auch ganz massiv an Förderung, damit überhaupt die vorhandenen Daten systematisch ausgewertet

werden können. Derzeit gibt es nur meine Professur in Deutschland zu Political Data Science. In den Bereichen Computational Social Science und teilweise auch in der traditionellen Politikwissenschaft entstehen viele spannende Arbeiten zu den Themen. Es bleibt aber für Wissenschaftler*innen ein großes Risiko, die Schnittstelle zwischen Politikwissenschaft und Informatik zu erforschen, weil es nach wie vor keinen wirklichen Stellenmarkt für transdisziplinäre Forschung gibt.

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?

Auch hier ist über die wirklichen Effekte nicht viel bekannt. Es ist auch beinahe unmöglich, eine Kampagne einem bestimmten Akteur zuzuordnen. Aber wenn es ein koordiniertes Vorgehen in den sozialen Netzen gibt, dann lässt sich dies auch theoretisch mit Datenanalysen erkennen. Entscheidend ist hier allerdings das Verhalten der Accounts und nicht bloß der Inhalt, der Absender oder die Infrastruktur.

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

Bislang war es aufgrund fehlender Daten (zumindest uns) nicht wirklich möglich, hierzu Untersuchungen anzustellen. Der Begriff „Dark Ads“ ist aber irreführend, da es sich dabei um ganz normale Werbung in den sozialen Netzwerken handelt, die auf bestimmte Personengruppen zugeschnitten ist. Durch die höhere Transparenz bei Wahlwerbung werden hier neue Erkenntnisse möglich werden.

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?

Konkreter Handlungsbedarf besteht auf jeden Fall bei der Sicherung von Social Media Accounts. Alle Personen, die mittelbar im politischen Bereich tätig sind, sollten höhere Sicherheitsstandard benutzen, insbesondere Zwei-Wege-Authentifizierung. Die Fälle, in denen Daten geleakt wurden, legen m. M. nach nahe, dass der Schaden weniger durch die Leaks selbst als durch einen fahrlässigen Umgang damit entstanden ist. Im Falle von Macron wurden falsche Informationen zum Beispiel innerhalb von wenigen Stunden identifiziert und dadurch die Wirkung der Aktion sehr stark beschränkt. Bei den Podesta-Leaks wurde hingegen übersehen, dass sich Verschwörungstheorien, die auf den Leaks aufbauten, verselbstständigt hatten. Generell ist also zwischen den Rollen zu unterscheiden: Wer verschafft sich Daten? Wer veröffentlicht diese? Wer benutzt diese Informationen wofür? In einer Demokratie ist auch der Schutz von Whistleblowern ein wichtiges Instrument, damit mögliche Missstände aufgezeigt werden können.