

upgrade
democracy

Impuls Serie #5

August 2023

EU-Wahlen 2024: Wie wir resilienter gegen Desinformationskampagnen auf sozialen Plattformen werden

Cathleen Berger, Charlotte Freihse, Vincent Hofmann,
Matthias C. Kettemann, Katharina Mosene



ALEXANDER VON HUMBOLDT
INSTITUT FÜR INTERNET
UND GESELLSCHAFT

| BertelsmannStiftung

Über die Impulsserie und diese Veröffentlichung

In einer Kooperation zwischen dem Upgrade Democracy Team der Bertelsmann Stiftung und dem Humboldt Institut für Internet und Gesellschaft organisieren wir von April bis September 2023 eine fünfteilige Impulsserie zum Thema „**Digitale Plattformen: Gestaltungsvorschläge und Alternativen**“. Mittelpunkt der Serie ist eine intensive Auseinandersetzung mit aktuellen Herausforderungen und Problemen auf bestehenden sozialen Plattformen und der Vorstellung und Diskussion von Alternativen. Die Themen Beteiligung und robuste Governance in Hinblick auf die demokratische Ausgestaltung der dominanten sozialen Plattformen stehen ebenso im Fokus wie Fragen nach gemeinwohlorientierten Entscheidungsprozessen. Die einzelnen Impulse greifen thematisch ineinander und zielen darauf ab, Ideen, Handlungs- und Policy-Empfehlungen für eine zukunftsfähige Plattform und Content Governance in digitalen Räumen zu entwickeln.

Alle Impulse greifen Ideen aus Expert:innen-Workshops auf, in denen in kleiner, vertrauter Runde und unter Chatham-House-Regeln jeweils provokante Hypothesen und zentrale Fragestellungen diskutiert werden. Im Anschluss jeder Veranstaltung wird ein Impulspapier veröffentlicht, das die wichtigsten Aspekte der Diskussion zusammenfasst.

Die Serie wurde von Cathleen Berger, Charlotte Freihse, Matthias C. Kettemann, Katharina Mosene und Vincent Hofmann konzipiert.

Teilnehmer:innen der Diskussion am 22. August 2023

Impulsgebende:

- Dr. Clara Iglesias Keller, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut
- Sabine Frank, YouTube

Expert:innen:

- Josephine Ballon, HateAid
- Cathleen Berger, Bertelsmann Stiftung
- Irene Broer, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut
- Stephan Dreyer, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut
- Charlotte Freihse, Bertelsmann Stiftung
- Dominik Hierlemann, Bertelsmann Stiftung
- Carla Hustedt, Stiftung Mercator
- Richard Kuchta, Democracy Reporting International
- Sami Nenno, Humboldt Institut für Internet und Gesellschaft
- Jan Rau, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut

Moderation:

- Georgia Langton, Bertelsmann Stiftung

Übersetzung aus dem Englischen von Lara Wagner.

1 Wahlprozesse und Desinformation: Stärkung des digitalen Diskurses im Vorfeld von 2024

Die bevorstehenden EU-Wahlen 2024 sind ein wichtiger Moment für den digitalen Wahlkampf, die Steuerung von Online-Diskursen – und die Zukunft Europas insgesamt. Desinformationskampagnen, Hassrede und Versuche, öffentliche Debatten zu manipulieren, werden eine zentrale Herausforderung darstellen. Es besteht die Gefahr, dass die Bürger:innen demokratischen Prozessen, öffentlichen Diskursen und den politischen Institutionen Europas skeptisch und misstrauisch gegenüberstehen. Und dieses Risiko ist real: Aktuelle, von der Landesanstalt für Medien Nordrhein-Westfalen in Auftrag gegebene *forsa*-Umfragen haben den Einfluss digitaler Desinformation, insbesondere im Kontext von Wahlen, untersucht. Sie ergaben, dass 54 % der Internetnutzer:innen zumindest gelegentlich mit politisch motivierter Desinformation in Berührung kommen. Ganze 85% glauben, dass Desinformation demokratische Prozesse gefährden kann. Es gibt jedoch auch eine gute Nachricht: Studien belegen, dass Desinformationen nicht in großem Umfang die Meinungen beeinflussen und dass die Nutzer:innen immer besser in der Lage sind, solche irreführenden oder falschen Inhalte zu erkennen, auch wenn sie ermutigt werden könnten, diese regelmäßiger und aktiver zu melden.

Bemühungen und Initiativen zum Schutz demokratischer Wahlen – einschließlich der EU-Wahlen – vor Informationsmanipulation und ausländischer Einmischung haben in den letzten Jahren erheblich an Bedeutung gewonnen. Beispiele aus jüngsten Wahlen in anderen Ländern werfen die Frage auf, ob wir (ausreichend) vorbereitet sind: Desinformationskampagnen, die auf den Wahlprozess und seine Legitimität abzielen, spielten eine wichtige Rolle bei den brasilianischen Unruhen im Januar 2022 und dem Sturm auf das US-Kapitol in Washington D.C. im Januar 2021. In beiden Fällen lassen die Gegenmaßnahmen der sozialen Netzwerke, die mit Behauptungen und Anschuldigungen des Wahlbetrugs oder der Wahlverweigerung überschwemmt wurden, lange bevor die eigentlichen Unruhen begannen, viel zu wünschen übrig. Hier ist Vorsicht geboten, da die Plattformen weiterhin zu langsam und ohne angemessene Vorbereitung handeln. Dies wird dadurch verschärft, dass in jüngster Zeit fast alle Plattformen Entlassungen oder Personalabbau vorgenommen haben, insbesondere in den Teams, die für die Überwachung und den Umgang mit Desinformationen zuständig sind (oft als „Trust & Safety“-Teams bezeichnet).

Hinzu kommt die besorgniserregende Tendenz, dass politische Akteur:innen polarisierende Themen ausnutzen, um Wähler:innen zu mobilisieren und den sozialen Zusammenhalt zu untergraben. Themen, die regelmäßig für Desinformationen genutzt werden, sind z. B. Maßnahmen während der COVID-19-Pandemie, Russlands Angriff auf die Ukraine, Gender- und Klimathemen (die wir in [unserem letzten Impuls](#) besprochen haben), Migration, Energiepreise oder Mobilität in Städten – sie alle werden instrumentalisiert, um emotionale Reaktionen auszulösen und einen konstruktiven, öffentlichen Diskurs mit differenzierten Argumenten zu verhindern. Auf diese Weise werden politische Debatten verzerrt und das Vertrauen in politische Prozesse und Institutionen zunehmend untergraben. Solche Desinformationskampagnen können von ausländischen Akteur:innen lanciert oder von inländischen Akteur:innen aus kurzsichtigen Motiven gezielt verbreitet werden. Geeignete Gegenmaßnahmen zu finden, ist daher noch komplexer.

Die Europäische Union hat bereits verschiedene Maßnahmen zur Bekämpfung von Desinformation ergriffen. So wird das sogenannte Europäische Schnellwarnsystem für Desinformation rechtzeitig zu den EU-Wahlen 2024 voll einsatzfähig sein. Darüber hinaus wird das Gesetz über digitale Dienste

(DSA) auf den Prüfstand gestellt, ob es die Verbreitung von Desinformationen auf digitalen Plattformen wirksam regelt. Anbieter digitaler Plattformen wie Meta, X (früher Twitter) und Google haben Richtlinien zur Wahlintegrität entwickelt, die darauf abzielen, gefälschte Konten und illegale Inhalte zu identifizieren und zu entfernen. Angesichts der Volatilität der öffentlichen Debatten und der Bedeutung von Wahlprozessen könnte es jedoch sein, dass noch viel mehr getan werden muss.

2 Zusammenführung von Erfahrungswerten und neuen Ideen zur Gestaltung einer widerstandsfähigen Zukunft

Ein Blick auf vergangene Wahlen und andere politische Prozesse zeigt, dass soziale Medien und Messaging-Dienste eine zunehmend einflussreiche Rolle spielen:

- Bei den **Präsidentswahlen in den USA 2016** beispielsweise wurde über die sozialen Medien erheblicher Einfluss ausgeübt. Es wurde festgestellt, dass russische Akteur:innen Plattformen wie Facebook, Twitter und Instagram nutzen, um Desinformationen zu verbreiten, Kontroversen zu schüren und die öffentliche Meinung zu polarisieren. Die berühmte Internet Research Agency (IRA) orchestrierte erfolgreich koordinierte Kampagnen, die Millionen von Amerikaner:innen erreichten. Die **Wahlergebnisse von 2020** führten schließlich zu einem Sturm auf das US-Kapitol im Januar 2021.
- Das **Brexit-Referendum** im Vereinigten Königreich im Jahr **2016** war von einer umfangreichen Nutzung von Kampagnen in den sozialen Medien geprägt. Sowohl das „Leave“ (Aussteigen) – als auch das „Remain“ (Bleiben) -Lager setzten gezielte Werbung auf Plattformen wie Facebook ein, um bestimmte Wählergruppen mit maßgeschneiderten Botschaften zu erreichen.
- Der **Cambridge-Analytica-Skandal**, der 2018 ans Licht kam, deckte außerdem auf, wie personenbezogene Daten von Millionen von Facebook-Nutzer:innen ohne Zustimmung gesammelt und für gezielte politische Werbung und unzulässige Einflussnahme verwendet wurden.
- Bei den **brasilianischen Präsidentswahlen 2018** spielten die sozialen Medien eine prägende Rolle bei der Ausgestaltung des Diskurses. Der rechtsextreme Kandidat und letztliche Sieger Jair Bolsonaro nutzte Plattformen wie WhatsApp, um ungeprüfte Informationen und Verschwörungserzählungen zu verbreiten. Die Verwendung von verschlüsselten Messaging-Apps machte die Herausforderungen bei der Überwachung und Bekämpfung von Fehlinformationen deutlich. Die **Wahlen im Jahr 2021** wurden zu einem Brennpunkt für Betrugsvorwürfe und Ergebnisanfechtungen, die über soziale Medien verbreitet wurden und im Januar 2022 in Gewalt ausarteten.
- Bei den **Parlamentswahlen 2019 in Indien** gab es einen starken Anstieg der Aktivitäten in den sozialen Medien. Die politischen Parteien setzten gezielte Werbung und Kampagnen in den sozialen Netzwerken ein, um verschiedene Wählergruppen zu erreichen. Die Wahlen 2024 werden sicherlich nach einem ähnlichen Muster ablaufen.

All dies sind Beispiele für potenziell schädliche und schwerwiegende Auswirkungen. Die meisten Plattformen haben inzwischen Transparenzmaßnahmen für politische und themenbezogene Werbung eingeführt. Auf dieser Grundlage müssen die Werbetreibenden Informationen darüber bereitstellen, wer die Werbung finanziert und wer die Zielgruppe ist. Viele Plattformen arbeiten auch mit Fact-Checking-Organisationen zusammen, um falsche oder irreführende Inhalte zu erkennen und zu kennzeichnen.

Darüber hinaus werden den Nutzer:innen bei der Interaktion mit solchen Inhalten zusätzliche Kontextinformationen oder Warnhinweise angezeigt, wie dies während der Covid-19-Pandemie weithin zu beobachten war. Außerdem wurden neue Regeln zur Gewährleistung der Integrität von Wahlen eingeführt, die eine beschleunigte Kennzeichnung, Entfernung von Inhalten, oder ähnliche Maßnahmen ermöglichen.

Auf regulatorischer Ebene hat die EU das Gesetz über digitale Dienste (DSA) verabschiedet, das auf mehrere Probleme digitaler Plattformen abzielt, die demokratischen Wahlen schaden können, wie z. B. die Verbreitung illegaler Inhalte oder gezielter Werbung. Zu den Gegenmaßnahmen gehören unter anderem der Einsatz von vertrauenswürdigen Kennzeichnern, Faktenüberprüfung, Risikobewertungen, Datenzugang für Forschende und Transparenzanforderungen. Die EU hat auch ein Schnellwarnsystem entwickelt, um den Informationsaustausch und koordinierte Reaktionen auf Desinformationsbedrohungen zwischen den Mitgliedstaaten und Plattformen zu erleichtern. Darüber hinaus hat die EU die Europäische Beobachtungsstelle für digitale Medien (EDMO) eingerichtet, um Desinformationskampagnen zu überwachen und zu bekämpfen und eine verstärkte Zusammenarbeit zwischen Forscher:innen, Faktenprüfer:innen und Online-Plattformen zu fördern.

Vor diesem vielschichtigen und hochpolitischen Hintergrund haben wir zwei Hypothesen aufgestellt, um den Dialog anzustoßen:

1. Die von den großen sozialen Plattformen ergriffenen Maßnahmen zum Schutz von Wahlprozessen und den mehrsprachigen EU-Wahlen gehen nicht weit genug und bieten keine Anreize, um koordinierte Desinformationskampagnen zu verhindern.
2. Die Ressourcen für die unabhängige Überwachung von Desinformationskampagnen und der jeweiligen (kontextspezifischen) Narrative, die zur Beeinflussung und Manipulation von EU-Wahlen instrumentalisiert werden, müssen erheblich aufgestockt werden. Ohne Allianzen zwischen zivilgesellschaftlichen Überwachungsorganisationen und der Forschung wird eine datenbasierte Analyse der Resilienz von EU-Wahlen nicht möglich sein.

Auf dieser Grundlage haben wir in unserem Austausch mit Expert:innen **drei Fragen** aufgeworfen und reflektiert:

1. Welche konkreten Maßnahmen sollten die EU und die Anbieter großer sozialer Plattformen wie Meta, Google & Co ergreifen, um die Resilienz gegen Desinformation während der Wahlen 2024 zu stärken? Und wie können europäische Regelungen wie der DSA solche Bemühungen unterstützen – und wo liegen ihre Grenzen?
2. Was wären mögliche Anreize, um Partnerschaften zwischen den EU-Mitgliedstaaten und der Zivilgesellschaft zu fördern, transparente und rechenschaftspflichtige politische Debatten zu unterstützen, und das Vertrauen der Bürger:innen in die europäischen politischen Institutionen zu stärken, auch um ausländische Einmischung zu verhindern?
3. Welche anderen Maßnahmen und innovativen Konzepte können wir vorschlagen, um die Resilienz der europäischen Demokratien zu erhöhen und wie können wir die Dringlichkeit unterstreichen, umgehend mit der Vorbereitung zu beginnen?

2.1 Wirksamkeit und Grenzen von Maßnahmen seitens der Plattformen und von Regulierungsansätzen zum Schutz von Wahlen

Um wirksam gegen Desinformation vorgehen zu können, ist es von entscheidender Bedeutung zu verstehen, wie Einflussnahme und Desinformationskampagnen funktionieren und/oder welche Aspekte sozialer Plattformen sie zu ihrem Vorteil ausnutzen können. Es gibt drei übergreifende Aspekte, die instrumentalisiert werden können, um die Verbreitung von digitaler Desinformation zu fördern:

1. **Amplifikation und Viralität:**

Soziale Medienplattformen sind so konzipiert, dass sie die schnelle Verbreitung von Informationen erleichtern. Die Teilbarkeit und Sichtbarkeit von Beiträgen in Verbindung mit Interaktionsmechanismen wie „Likes“, „Shares“ und „Kommentieren“ tragen dazu bei, dass bestimmte Narrative, Botschaften oder (die sie vertretenden) Kandidat:innen verstärkt werden.

2. **Micro-Targeting und bezahlte Inhalte:**

Soziale Plattformen bauen ihr Geschäft auf der Fähigkeit auf, bestimmte Demografien und Einzelpersonen anzusprechen. Kampagnen können ihre Botschaften so anpassen, dass sie bei bestimmten Wähler:innensegmenten Anklang finden, was die Wahrscheinlichkeit eines Engagements erhöht. Fortgeschrittene Datenanalysen und Nutzer:innenprofile ermöglichen es den politischen Akteur:innen außerdem, Inhalte auf der Grundlage der Vorlieben, des Verhaltens und sogar der psychologischen Eigenschaften der Nutzer:innen anzupassen und so einen personalisierten und überzeugenden Kommunikationsansatz zu schaffen. Gesponserte Inhalte, die im Umfeld von organischen Beiträgen präsentiert werden, lassen die Grenze zwischen informativen Inhalten und bezahlter Werbung verschwimmen und beeinflussen die Wahrnehmung der Nutzer:innen zusätzlich.

3. **Nutzergenerierte Inhalte und „Grassroots“-Mobilisierung:**

Soziale Medien ermöglichen es normalen Nutzer:innen, zu politischen Aktivist:innen und Einflussnehmer:innen zu werden oder diese zumindest zu imitieren. Von Nutzer:innen erstellte Inhalte wie Videos, Memes und Beiträge können „viral“ gehen (sich erheblich verbreiten) und so den öffentlichen Diskurs beeinflussen. Graswurzelbewegungen können schnell an Schwung gewinnen, Anhänger:innen mobilisieren und etablierte politische Narrative in Frage stellen.

Leider können alle drei Aspekte missbraucht werden, um die Reichweite von Desinformationskampagnen zu erhöhen, insbesondere bei Wahlen. Falsche Narrative, fabrizierte und manipulierte Inhalte oder Bilder können sich damit schnell verbreiten, oft angeheizt durch koordinierte (und automatisierte) Bemühungen, die öffentliche Meinung zu täuschen und zu manipulieren.

Die Vielschichtigkeit der Bedrohungen, die demokratische Wahlprozesse gefährden, erfordert die Einbeziehung verschiedener Akteur:innen und eine effizientere Zusammenarbeit zwischen ihnen. Die Tatsache, dass EU-Wahlen über Landesgrenzen hinweg stattfinden, macht die Umsetzung von Maßnahmen noch komplexer. Im Folgenden wird ein breiter Überblick über die bestehenden Maßnahmen auf Plattform- und Regulierungsebene gegeben und aufgezeigt, wo und wie diese verstärkt oder ausgeweitet werden könnten und sollten:

Soziale Plattformen:

- Um die steigende Flut digitaler Desinformationen zu bekämpfen, müssen die Plattformbetreiber:innen proaktive Maßnahmen ergreifen und sicherstellen, dass ihre Nutzer:innen über die Mittel und das Wissen verfügen, um Fakten von Unwahrheiten zu unterscheiden. Dazu gehört auch die Stärkung von Mechanismen zur Überprüfung von Inhalten, mit denen falsche oder

irreführende Informationen identifiziert, gekennzeichnet, gemeldet und blockiert werden können, sowie die Bereitstellung von Warnhinweisen und/oder eindeutigen Informationen über die Quelle von Inhalten und deren Richtigkeit. Auf der Grundlage spezifischer Strategien zur Bekämpfung wahlbezogener Desinformation können solche Inhalte mit größerer Sensibilität für die Angreifbarkeit der demokratischen Prozesse entfernt werden.

- Die Plattformen haben und sollten weiterhin spezielle Schnellreaktionsteams einrichten, die in kritischen Zeiten wie bei Wahlen Desinformationskampagnen schnell erkennen, bewerten und bekämpfen können. Diese Teams sollten daran arbeiten, falsche Narrative zu entlarven und die Öffentlichkeit in Echtzeit mit korrekten Informationen zu versorgen. Zur Unterstützung dieser Teams ist es wichtig, unabhängigen Forscher:innen den Zugang zu Daten zu ermöglichen, damit sie die Aktivitäten auf den Plattformen kontinuierlich überwachen können, um Desinformationskampagnen zu erkennen, zu verstehen, zu analysieren und ihnen entgegenzuwirken. Eine solche Forschung ist auch für die Durchführung von Systemrisikobewertungen von zentraler Bedeutung.
- Darüber hinaus müssen die Überwachung und die Transparenz von Empfehlungsalgorithmen („recommendation algorithms“) verbessert werden. Regelmäßige Überprüfungen und Transparenzberichte können Aufschluss darüber geben, wie Algorithmen Inhalte priorisieren und anzeigen, um Fairness und Genauigkeit zu gewährleisten.
- „Prebunking“-Methoden, bei denen einfache Aufklärungstexte über Desinformationstaktiken und -techniken (und nicht über einzelne Inhalte) verwendet werden, haben sich als wirksam erwiesen und sollten in großem Umfang eingeführt werden.
- Um Desinformationen zu erkennen, kann eine enge Zusammenarbeit zwischen Plattformen und unabhängigen Fact-Checking-Organisationen die Identifizierung und Korrektur von Falschinformationen beschleunigen. Solche Partnerschaften können auch dabei helfen, die Notwendigkeit der raschen Entfernung schädlicher Inhalte mit der Wahrung des Rechts auf Meinungsfreiheit in Einklang zu bringen.

Die gute Nachricht ist: Die genaue Identifizierung schädlicher und irreführender Inhalte ist sehr wohl möglich – wenn eine kontinuierliche Überwachung und der Zugang zu Studien gewährleistet sind, wenn zuverlässige journalistische Quellen zur Verfügung stehen, wenn technische und gestalterische Merkmale die Kennzeichnung, Markierung und Berichterstattung unterstützen, wenn die Nutzer:innen über die notwendigen Fähigkeiten verfügen, um Quellen und Inhalte zu bewerten, und wenn Zusammenarbeit und Partnerschaften eine weitere Kontextualisierung ermöglichen.

Doch nicht nur die Plattformen tragen hier Verantwortung.

Regulatorische und gesetzliche Maßnahmen:

- Das Gesetz über digitale Dienste (DSA) stellt den wichtigsten Regulierungsansatz zur Bekämpfung illegaler Inhalte im digitalen Raum dar. Wenn es jedoch um die Bekämpfung digitaler Desinformation geht, enthält der DSA verschiedene Einschränkungen, vor allem weil Desinformation oft nicht unter den Tatbestand der illegalen Inhalte fällt – dennoch bleiben ihre Auswirkungen schädlich, auch im Kontext von Wahlen. Dies erfordert kontextspezifische Bewertungen, Nuancierung und Zusammenarbeit, insbesondere mit der Zivilgesellschaft.
- Da der DSA eine stärkere Beziehung zwischen den sehr großen Online-Plattformen (Very Large Online Platforms – VLOPs) und der EU-Kommission schafft, ist es von entscheidender Bedeutung, dass bei der Umsetzung und Durchführung konstante Multi-Stakeholder-Prozesse gewährleistet werden – auch wenn alle beteiligten Akteur:innen unterschiedliche Unterstützungshebel benötigen, um ihre jeweiligen Aufgaben zu erfüllen, sind sie doch stark voneinander abhängig.

- Darüber hinaus sind digitale Plattformen weltweit tätig, was die Durchsetzung von EU-Vorschriften über die Grenzen hinaus erschwert – auch in Bezug auf Desinformationskampagnen, die von außerhalb der EU ausgehen. Auch Desinformationstaktiken entwickeln sich ständig weiter, weshalb die Regulierungsbehörden beweglich bleiben und sich schnell an neue Herausforderungen anpassen müssen. Es muss ein Gleichgewicht zwischen einer weit gefassten Formulierung, die offen für neue technologische Entwicklungen ist, und einer klaren und präzisen Auslegung der rechtlichen Definitionen bestehen – sowie ein Gleichgewicht zwischen neuen rechtlichen Anforderungen und einer ergebnisorientierten Auslegung bestehender Gesetze.
- Ein weiterer Regulierungsansatz neben dem DSA ist die Verordnung zu politischer Werbung. Die Tatsache, dass diese Verordnung möglicherweise nicht rechtzeitig für die Wahlen 2024 fertig ist, ist alarmierend, da sie einen wichtigen Schritt zur (Wieder-)Herstellung von Transparenz der politischen Parteien und ihrer Kandidat:innen darstellt.
- Alle Regulierungsansätze für digitale Inhalte stützen sich zu einem gewissen Grad auf daten- und evidenzbasiertes Wissen, das in erster Linie von Forscher:innen generiert wird. Legislative Maßnahmen, z. B. Vereinbarungen zur gemeinsamen Nutzung von Daten, könnten daher dazu beitragen, das Monitoring sozialer Medien zu erleichtern und zu verstärken. Darüber hinaus muss die Europäische Union ihre Zusammenarbeit mit internationalen Partner:innen, darunter Technologieunternehmen, die außereuropäische Zivilgesellschaft und Regierungen, verstärken, um eine koordinierte und breit angelegte Reaktion auf Desinformationskampagnen zu entwickeln, die sich gegen mehrere Regionen richten.

Auch hier ist die gute Nachricht: Regulierungsmechanismen wie der DSA sind entscheidend. Ihr Einfluss auf die EU-Wahlen im nächsten Jahr wird jedoch von ihrer Durchsetzung abhängen. Außerdem können und sollten die Mitgliedstaaten auf bereits bestehenden Strukturen aufbauen, zum Beispiel wenn es um Frühwarnsysteme und gemeinsame Krisenreaktionsmechanismen geht.

2.2 Überwachung und Bekämpfung von Desinformation bei Wahlen erfordert Zusammenarbeit und Partnerschaften

Es ist von entscheidender Bedeutung, kontinuierlich in das unabhängige Monitoring sozialer Medien zu investieren, um Desinformation als systemisches Risiko zu erkennen, zu verstehen und zu analysieren. Nur dann werden wir in der Lage sein, wirksame Gegenmaßnahmen zu entwickeln. So oder so werden Desinformationskampagnen nicht einfach verschwinden – um ihre Verbreitung und Wirkung zu begrenzen, müssen alle Akteur:innen einen Beitrag leisten. Wir brauchen zuverlässige und vertrauensvolle Partnerschaften zwischen der EU, den Mitgliedstaaten, der Zivilgesellschaft und Plattformen.

Hier sind nur fünf Anreize, die diese Zusammenarbeit fördern könnten:

- **Gemeinsame Ziele der Demokratie:** Akteur:innen identifizieren, die ein gemeinsames Interesse an der Aufrechterhaltung demokratischer Werte und der Gewährleistung fairer Wahlen haben. Gemeinsame Anstrengungen können zur Aufrechterhaltung der Integrität demokratischer Prozesse beitragen, insbesondere wenn dies eindeutig als gemeinsames Ziel festgelegt wird – was die öffentliche Unterstützung, die Glaubwürdigkeit und die Vertrauenswürdigkeit aller Beteiligten fördern kann.
- **Verbesserte Wirksamkeit:** Mitgliedstaaten können von dem Fachwissen und der Erfahrung profitieren, die zivilgesellschaftliche Organisationen bei der Überwachung und Bekämpfung von

Desinformation zur Verfügung stellen können, was zu wirksameren Strategien führt. Auf diese Weise kann die Zivilgesellschaft einen wertvollen Beitrag zu den politischen Diskussionen leisten und somit eine fundiertere und wirksamere Politik zur Bekämpfung von Desinformation erwirken.

- **Zugang zu Informationen und Ressourcen:** Die Zivilgesellschaft hat oft Zugang zu Informationen und Erkenntnissen, über die die Mitgliedstaaten nicht verfügen. Die Zusammenarbeit kann den Mitgliedstaaten ein tieferes Verständnis für Desinformationsfragen vermitteln. Durch die Bündelung von Ressourcen können beide Seiten auf ein breiteres Spektrum von Datenquellen zugreifen, was zu genaueren Analysen von Desinformationskampagnen führt.
- **Breitere Wirkung:** Eine wirksame Zusammenarbeit kann zu einer breiteren Wirkung bei der Bekämpfung von Desinformation führen und dazu beitragen, dass die Gesellschaft widerstandsfähiger gegen Manipulation und Fehlinformation wird.
- **Rechenschaftspflicht und Transparenz:** Zusammenarbeit fördert Transparenz und Verantwortlichkeit und verringert so die Wahrscheinlichkeit von Fehlinformationen innerhalb der Bekämpfung von Desinformation.

2.3 Empfehlungen: Die Zeit für die Vorbereitung auf 2024 ist jetzt

Die Herausforderung, Desinformation zu bekämpfen, kann nicht von einer einzelnen Einrichtung effektiv bewältigt werden. Wie bei den Diskursen selbst gibt es viele Akteur:innen, normative Ebenen und Einflussvektoren: soziale, rechtliche, politische, wirtschaftliche und technische. Deshalb ist ein kooperativer Ansatz erforderlich, bei dem jede:r Akteur:in ihre Rolle und seine Verpflichtungen wahrnimmt.

Was Regierungen tun können:

- **Sicherstellen, dass Regulierungsmaßnahmen wie der DSA durchgesetzt werden:** Das Gesetz über digitale Dienste bietet einen notwendigen Rechtsrahmen für die Beseitigung illegaler Inhalte, doch seine Auswirkungen auf die Wahlen 2024 könnten zu kurz kommen, wenn es nicht rasch umgesetzt und zuverlässig durchgesetzt wird. Dazu gehört auch, dass angemessene Mittel für die Zivilgesellschaft und die Forschung zur Verfügung stehen, damit sie die mit dem Datenzugang verbundenen Rechte nutzen können.
- **Förderung der Zusammenarbeit, um die Reichweite zuverlässiger Quellen zu erhöhen:** Staatliche Stellen sollten das Potenzial von Partnerschaften mit digitalen Plattformen ausloten, um verifizierte Quellen zu ermitteln und aufzuwerten. Je nach Kontext und politischem System kann dies die Unterstützung öffentlich-rechtlicher Rundfunkanstalten, die Identifizierung und Verstärkung der Stimmen unabhängiger Organisationen für Faktenprüfung, Überwachung, Bildung und Demokratieförderung oder institutionelle Unterstützung für systemische Risikobewertungen hinsichtlich der Auswirkungen digitaler Desinformation umfassen.
- **Bereitstellung von mehr Ressourcen und Finanzmitteln für Bemühungen und Akteur:innen zur Stärkung der Demokratie – online und offline:** Bemühungen, die darauf abzielen, demokratische Gesellschaften online und offline zu stärken, sollten in ein nachhaltiges System eingebettet sein, das es der Forschung und der Zivilgesellschaft ermöglicht, effizient zu arbeiten. Dies erfordert eine ausreichende Finanzierung, die verlässlich und flexibel ist und mit einem geringen Verwaltungsaufwand einhergeht. Darüber hinaus wurde in unseren Gesprächen deutlich, dass die Verantwortung und die Rolle der Medien bei der Bekämpfung jeglicher Art von Desinformation nicht hoch genug eingeschätzt werden kann – dies setzt voraus, dass Qualitätsjournalismus mit den notwendigen Ressourcen ausgestattet ist und dass Journalisten bei ihrer Arbeit geschützt und sicher sind.

Was Plattformanbieter:innen tun können:

- **Vertrauenswürdige Quellen hervorheben:** Um der Verbreitung von Desinformationen entgegenzuwirken, müssen glaubwürdige und vertrauenswürdige Quellen hervorgehoben werden. Durch die Hervorhebung gut recherchierter und zuverlässiger Informationen können Einzelpersonen in die Lage versetzt werden, fundierte Entscheidungen zu treffen und sich dem Einfluss irreführender Narrative zu widersetzen. Die Anbieter digitaler Plattformen können dazu beitragen, vertrauenswürdige Quellen, glaubwürdige Informationen über Wahlprozesse usw. zu verbreiten. Um politische Zensur zu vermeiden, müssen die Plattformen Multi-Stakeholder-Prozesse einführen und einen transparenten Rahmen schaffen, der angibt, wie glaubwürdige und vertrauenswürdige Informationsquellen identifiziert und gekennzeichnet werden.
- **Transparenz, Datenzugang und Zusammenarbeit mit der Forschung:** Die Verfügbarkeit von APIs von Plattformen wie YouTube sowie von Berichten über Anzeigen sind wichtig und sollten von allen Social-Media-Plattformen umgesetzt werden. Der Zugang muss einfach, zuverlässig und erschwinglich sein, was die Datenverarbeitung, -speicherung und -analyse angeht. Darüber hinaus ist ein klarer Überblick darüber, welche Daten den Plattformen zur Verfügung stehen, entscheidend, damit Forscher:innen ihre Fragen und Methoden entsprechend gestalten können.
- **Umfassender Ansatz zur Wahlintegrität:** Eine Synergie aus menschlicher Intelligenz und maschinellen Eingriffen erweist sich als wesentlich. Vierteljährlich erscheinende Transparenz-Blogs, eine Bibliothek politischer Werbung oder spezielle Richtlinien zur Wahlintegrität, in denen Prozesse, verfügbare Ressourcen und Berichtsmechanismen beschrieben werden, gehen zwar über rechtliche Anforderungen hinaus, können sich aber für die Effizienz des digitalen Diskurses nur als nützlich erweisen. Die Zusammenarbeit mit der Zivilgesellschaft bietet darüber hinaus die Möglichkeit, fundierte Maßnahmen zu ergreifen und Erkenntnisse zu gewinnen, die einen wichtigen Beitrag zum Gesamtbild leisten.

Was die Zivilgesellschaft tun kann:

- **Aufmerksamkeit erregen und Sensibilisierungskampagnen durchführen:** In der EU gibt es kein einheitliches Medienumfeld. Dadurch ist es schwerer, grenzüberschreitend Wähler:innen zu mobilisieren, die Bürger:innen zu überwachen und über mögliche Desinformationskampagnen zu informieren und vertrauenswürdige Quellen in allen EU-Sprachen bereitzustellen. Umso wichtiger ist es, dass zivilgesellschaftliche Organisationen aus allen EU-Mitgliedstaaten ihre Sensibilisierungskampagnen koordinieren, zusammenarbeiten und sich gegenseitig verstärken, um eine starke, gut informierte und widerstandsfähige Wähler:innenbasis zu schaffen.
- **Vermittlung von Medien- und Digitalkompetenz:** Die Umsetzung von Programmen zur Vermittlung digitaler Kompetenzen, die den Bürger:innen kritisches Denken, Medienkompetenz und verantwortungsbewusstes Online-Verhalten beibringen, ist ein wesentlicher Faktor zur langfristigen Bewältigung von Herausforderungen im Zusammenhang mit Desinformation.
- **Unterstützung von Konfliktlösung und Content Governance durch strategische Prozessführung:** Dort, wo die Gesetze für Inhalte von Land zu Land unterschiedlich sind, entscheiden die Plattformen oft darüber, was wo, für wen und wie sichtbar ist. Solche Entscheidungen über die Steuerung von Inhalten sollten in breit angelegte Input-Mechanismen und/oder Konsultationen mit der Zivilgesellschaft eingebettet sein. In Fällen, in denen Streitigkeiten Schaden anrichten, können kann die strategische Prozessführung ein wirksames Instrument sein, um Widersprüche zwischen den Gesetzen aufzuzeigen und grenzüberschreitend zu lösen.

Was politische Kandidat:innen und Einrichtungen tun können:

- **Gehen Sie mit gutem Beispiel voran und verbessern Sie Ihre digitale Sicherheit:** Social-Media-Kampagnen sind zu einem integralen Bestandteil von Wahlprozessen geworden. Es ist nicht nur wichtig, die digitale Sicherheit von Konten und Personen zu gewährleisten, sondern technische Maßnahmen können auch die Glaubwürdigkeit politischer Kampagnen unterstützen. Deep Fakes und andere Formen manipulierter Inhalte sind auf dem Vormarsch: Parteien und Kandidat:innen sollten den effektiven Einsatz von Tools wie Wasserzeichen auf Bild- oder Tonmaterial demonstrieren, um das Vertrauen in die Inhalte zu stärken. Darüber hinaus könnte die Einführung solcher Techniken einen Dominoeffekt auslösen, der andere Akteur:innen dazu veranlasst, sie ebenfalls zu nutzen.

In Bezug auf Wahlen zeigen unsere Beobachtungen eine Tendenz zu kurzfristigen Maßnahmen. Auch wenn diese Beobachtung die Bedeutung verstärkter Maßnahmen in Wahlkampfzeiten nicht in Abrede stellt, empfehlen wir nachdrücklich, sich auf langfristige, nachhaltige Strategien und Maßnahmen zu konzentrieren. Die Strategien müssen über Wahlzyklen hinausgehen und einen umfassenderen Ansatz zur Bekämpfung von Desinformation bieten.

Wenn Sie nur eines aus dieser Lektüre mitnehmen: Wir dürfen nicht passiv abwarten, wir müssen jetzt handeln. Die Wirksamkeit der Desinformationsbekämpfung hängt sehr stark davon ab, wie gut die Akteur:innen vorbereitet sind und welche Präventivmaßnahmen ergriffen worden sind. Da die EU-Wahlen näher rücken, fordern wir alle Akteur:innen auf, jetzt zu handeln – schließlich ist eine widerstandsfähige europäische Gesellschaft der wirksamste Schutz gegen digitale Desinformation bei den Wahlen im Jahr 2024.



3 Vertiefung der Themen Wahlen, digitale Desinformation und Demokratie:

- Das Projekt Upgrade Democracy der Bertelsmann Stiftung hat in einer aktuellen Studie untersucht, wie Bürger:innen der Europäischen Union Desinformation wahrnehmen und welche Erfahrungen sie bisher damit gemacht haben. Die Studie und eine Zusammenfassung der Ergebnisse finden Sie hier: [Neue Studie: Einstellungen und Wahrnehmungen zu Desinformation in Europa – Upgrade Democracy](#)
- Eine aktuelle forsa-Studie im Auftrag der Landesanstalt für Medien Nordrhein-Westfalen zeigt, wie Menschen Desinformation wahrnehmen, wie wir unsere Demokratien davor schützen können und welche Instrumente am Beispiel von Wahlen funktionieren. Die vollständige Studie finden Sie hier: [Forsa-Umfrage_zum_Informationsverhalten_bei_Wahlen_2023 \(medienanstalt-nrw.de\)](#)
- In einem Papier für die Konrad-Adenauer-Stiftung befassen sich Clara Iglesias Keller, Laura Schertel Mendes und Victor Fernandes mit dem brasilianischen Rechtsrahmen für die Regulierung von Online-Inhalten in den ersten hundert Tagen der dritten Lula-Regierung (Januar bis April 2022) auf deskriptive und präskriptive Weise. Lesen Sie das vollständige Papier hier (auf Portugiesisch und Englisch): [efdd5b2d-e5c5-6c5c-8a0c-315cef9cb65b \(kas.de\)](#)
- In diesem Artikel veranschaulicht Charlotte Freihse das Verhalten verschiedener Social-Media-Plattformen während der letzten Wahlen in den USA und Brasilien und kommt zu dem Schluss, dass es ihnen immer noch an Strategien fehlt, um auf Desinformationskampagnen, angefochtene Wahlergebnisse und die damit verbundene Aufstachelung zur Gewalt reagieren zu können. Lesen Sie die Analyse hier (auf Englisch): [Riots Reloaded: Große soziale Plattformen sind immer noch schlecht gerüstet, um Desinformationskampagnen im Vorfeld von Wahlen zu begegnen – Upgrade Democracy](#)
- Das von führenden Journalisten der BBC, Storyful, ABC, Digital First Media und anderen Verifizierungsexperten verfasste „Verification Handbook“ bietet Werkzeuge, Techniken und schrittweise Richtlinien für den Umgang mit nutzergenerierten Inhalten (UGC) in Notfällen. Sie können das Handbuch hier finden: [Verification Handbook: Homepage](#)
- Die Regulierung von Desinformation ist keine leichte Aufgabe. Das Recht auf freie Meinungsäußerung setzt dem Staat klare Grenzen. Werfen Sie einen Blick auf diesen umfangreichen Überblick über normative Vektoren zur Regulierung sozialer Praktiken im Zusammenhang mit Desinformationsverhalten durch ein Team des Leibniz-Instituts für Medienforschung: [HBI_Desinformation_07112021.indd \(medienanstalt-nrw.de\)](#)
- Prebunking ist ein Ansatz zur Bekämpfung von Desinformation. Die Google-Tochter Jigsaw, das Sozialunternehmen Moonshot und sechs deutsche Nichtregierungsorganisationen haben in enger Zusammenarbeit mit lokalen Experte:innen eine Videokampagne gestartet, die die „Prebunking“-Methode anwendet. Erfahren Sie hier mehr über das Projekt: [Falschinformationen bekämpfen, bevor sie verbreitet werden \(blog.google\)](#)
- Das National Democratic Institute (NDI) hat Ansätze zum Umgang mit der Bedrohung durch Desinformation im Wahlkontext skizziert, insbesondere die Maßnahmen, die bürgerliche Wahlbeobachter:innen und internationale Beobachter:innen ergreifen können, um Desinformation zu entschärfen, aufzudecken und zu bekämpfen. Lesen Sie den vollständigen Bericht hier (auf Englisch): [Disinformation and Electoral Integrity: A Guidance Document for NDI Elections Programs | National Democratic Institute \(Desinformation und Integrität von Wahlen: Ein Leitfaden für NDI-Wahlprogramme | National Democratic Institute\)](#)

- In diesem Essay argumentieren Erik C. Nisbet, Chloe Mortenson und Quin Li, dass der mutmaßliche Einfluss von Fehlinformationen (PIM) ebenso schädlich und weit verbreitet sein kann wie der direkte Einfluss politischer Fehlinformationen auf die Wähler:innen. Lesen Sie ihr Essay und ihre Umfrage hier (auf Englisch): [The presumed influence of election misinformation on others reduces our own satisfaction with democracy | HKS Misinformation Review \(harvard.edu\)](#) (Der vermutete Einfluss von Wahlfehlinformationen auf andere verringert unsere eigene Zufriedenheit mit der Demokratie | HKS Misinformation Review (harvard.edu))
- In ihrem Artikel geben Dr. Julie Posetti, Felix Simon und Nabeelah Shabbir Einblicke in die nationalen Wahlen in Südafrika, auf den Philippinen und in Indien, wo die Desinformationsbekämpfungsstrategien von drei digital arbeitenden Nachrichtenredaktionen getestet wurden. Lesen Sie ihre Ergebnisse hier (auf Englisch): [Reporting elections on the frontline of the disinformation war | Reuters Institute for the Study of Journalism \(ox.ac.uk\)](#) (Wahlberichterstattung an der Frontlinie des Desinformationskriegs | Reuters Institute for the Study of Journalism (ox.ac.uk))
- Das Zentrum für Innovation und Technologie hat Schulungen zur Verbesserung der Medien- und Nachrichtenkompetenz angeboten, damit möglichst viele Wähler:innen in der Lage sind, zwischen zuverlässigen Nachrichten und Desinformation zu unterscheiden. Sie finden es hier (auf Englisch): [FEATURE-Zimbabwe fights fake news with lessons in spotting disinformation | Reuters \(FEA-TURE-Simbabwe bekämpft Fake News mit Lektionen zum Erkennen von Desinformation | Reuters\)](#)
- Inwieweit verändert künstliche Intelligenz die Desinformationslandschaft, und müssen wir unsere Wahlen gegen Deepfakes und andere gefälschte Inhalte schützen? Das Brennan Center for Justice schlägt einige Schutzmaßnahmen vor (auf Englisch und Spanisch): [How AI Puts Elections at Risk – And the Needed Safeguards | Brennan Center for Justice \(Wie KI Wahlen gefährdet – und die notwendigen Sicherheitsvorkehrungen | Brennan Center for Justice\)](#)
- Das EU Disinfo Lab hat eine Übersicht über die bestehenden Maßnahmen der Plattformen zur Bekämpfung von Wahlfälschungen erstellt, die für Vergleiche sehr hilfreich ist (auf Englisch): [20230621_ElectionsFS.pdf \(disinfo.eu\)](#)
- Dieses von den Vereinten Nationen in Auftrag gegebene Gedankenpapier ermutigt Staaten und Plattformen, ihre Kräfte in Bezug auf die Informationsintegrität zu bündeln. Eine vorgeschlagene gemeinsame Agenda befasst sich auch mit der Anfälligkeit von Wahlen (auf Englisch): [our-common-agenda-policy-brief-information-integrity-de.pdf \(un.org\)](#)