

Kapitel 6: Handlungsempfehlungen

Autoren:

Dr. Carolin Jansen
Paul Christopher Johannes
Prof. Dr. Nicole Krämer
Dr. Michael Kreuzer
Lena Isabell Löber
Prof. Dr. Lars Rinsdorf
Prof. Dr. Alexander Roßnagel
Dr. Leonie Schaewitz

Wie im Fazit des vorangegangenen Kapitels dargelegt, handelt es sich bei digitaler Desinformation um ein Problem, das unter Einbeziehung einer Vielzahl von Akteuren auf verschiedenen gesellschaftlichen Ebenen angegangen werden muss. Die Handlungsempfehlungen dieses Kapitels sind dementsprechend nach den Adressatengruppen strukturiert.¹

A. *Empfehlungen für Bürgerinnen und Bürger*

I. Merkmale von Desinformation (wiederer)kennen und Plausibilitätschecks vornehmen

Bürgerinnen und Bürger, die sich in politische Diskurse einbringen möchten, sind auf richtige und vielfältige Informationen angewiesen. Insbesondere technikaffinen Bürgerinnen und Bürgern stehen bereits jetzt eine Reihe hilfreicher Instrumente zur Verfügung, mit deren Hilfe sie (Des-)Informationen überprüfen können.

1 Die nachfolgenden Empfehlungen korrespondieren zu den im Policy Paper „Desinformation aufdecken und bekämpfen“ (Bader et al., 2018) gegebenen. Sie erweitern das Policy Paper in zweierlei Hinsicht. Auf Basis der zwischenzeitlich erlangten Forschungsergebnisse werden neue Empfehlungen ergänzt. Zudem enthält die nachfolgende Darstellung die wissenschaftlichen Belege, auf denen sie fußen.

1. Webseiten

Bezogen auf Webseiten lässt sich prüfen, ob die Website über ein Impressum verfügt und dies ausreichende Informationen über die presserechtlich verantwortlichen Betreiber enthält. Falls die Webseite in verschiedenen Fact-Checking-Initiativen mehrfach erwähnt wird, dann handelt es sich um erhebliche Verdachtsmomente. In Internet-Archiven lässt sich zudem recherchieren, welche Inhalte auf jenen Webseiten in der Vergangenheit publiziert wurden (s. Kapitel 4, A.I.).

2. Bilder und Videos

Auch für Bilder und Videos gibt es erste Plausibilitätschecks, die auch Laien durchführen können: Eine Rückwärtsbildersuche liefert etwa sehr schnell Hinweise darauf, in welchem Umfeld identische oder sehr ähnliche Bilder bereits veröffentlicht wurden (s. Kapitel 4, B.III.1.). Auch Metadaten, die über Exif-Viewer erfasst werden können, lassen Rückschlüsse auf die Authentizität des Bildmaterials zu.

3. Posts

Posts auf Online-Plattformen wiederum können mit Hilfe von Graph-Suchmaschinen daraufhin untersucht werden, wie die Autorinnen und Autoren von Posts, die den Verdacht erregen, Desinformation zu enthalten, miteinander vernetzt sind. Zudem liefern häufig auch Recherchen auf Online-Plattformen Hinweise auf den politischen Hintergrund von Personen, die Desinformationen teilen (s. Kapitel 4, B.I.).

4. Darstellungsmuster

Gerade technisch weniger versierten Bürgerinnen und Bürgern hilft bei der Entlarvung von Desinformationen ein konzentrierter Blick darauf, wie manipulativ intendierte (Falsch-)Meldungen geschrieben worden sind. Diese Meldungen zeigen in der Textgestaltung typische Muster in Bezug auf die (Nicht-)Einhaltung professioneller journalistischer Standards und die Instru-

mente, die eingesetzt werden, um die Aufmerksamkeit der Nutzerinnen und Nutzer zu maximieren (s. Kapitel 2, F.II.):

Vorsicht ist etwa geboten, wenn Meldungen besonders reißerisch dargestellt werden: Im Vergleich zu Meldungen, die von professionellen journalistischen Nachrichtenmedien verbreitet werden, weisen Desinformationen auf deutschsprachigen Portalen im Durchschnitt deutlich höhere Anteile nutzermaximierender Merkmale auf – wie etwa Sensationalismus oder die Skandalisierung von Ereignissen.

Der Grad der Nutzermaximierung hängt auch von dem behandelten Thema ab (s. Kapitel 2, F.III.). Hierzu beispielhaft ein wiederholt angetroffenes Muster: Eine umfassende Maximierung war zum Zeitpunkt der Erhebung von DORIAN häufiger anzutreffen, wenn gleichzeitig über Migration *und* innere Sicherheit berichtet wird, als wenn nur isoliert über eines der beiden Themen berichtet wird.

Weitere Beispiele (s. Kapitel 2, F.II.) sind unpräzise Überschriften, ein fehlender nachrichtlicher Einstieg in das Thema oder eine mangelhafte Gliederung entlang der Relevanz einzelner Informationen. Schließlich ist die Prüfung der Plattform, von der eine Meldung stammt, wichtig.

II. Die eigene Filterblase verlassen

1. Unterschiedliche Quellen nutzen

Eine zentrale Strategie für Bürgerinnen und Bürger, die sich nicht von Desinformation täuschen lassen möchten, ist ein vielfältiges Medienrepertoire, das sich aus unterschiedlichen Quellen zusammensetzt. Insbesondere durch das Lesen von verschiedenartigen Posts aus unterschiedlichen Quellen auf Online-Plattformen können Nutzende Informationen außerhalb ihrer Filterblase erhalten, ohne dass ihre Weltanschauung dabei notwendigerweise konkret angegriffen wird. Zusätzlich führt eine vielfältige Nutzung von Onlinemedien dazu, dass die Fehlwahrnehmung eines Sachverhalts durch Personen, die Desinformation gelesen haben, reduziert werden kann. Darüber hinaus könnte das Bewusstmachen des Bestätigungsfehlers helfen, Desinformation – auch wenn sie die eigene Einstellung bestätigen würde – eher zu erkennen.

Diese Empfehlung setzt bei den typischen Vorgehensweisen an, die Individuen bei der Nutzung von Nachrichten anwenden: Sie verarbeiten und bewerten neue Informationen basierend auf ihren vorherigen Einstellungen.

Dabei wenden sie sich in ihrer Auswahl eher den Nachrichten zu, die ihren Ansichten und politischen Einstellungen entsprechen. Da sie motiviert sind, ihre Ansichten zu verteidigen, neigen sie zudem dazu, Informationen zu akzeptieren, die mit ihrer Einstellung übereinstimmen und davon abweichende zu vermeiden oder anzuzweifeln.

Es ist daher anzunehmen, dass Desinformation eher von Personen mit einer deckungsgleichen Einstellung zum Thema der Nachricht geglaubt wird. Empirische Untersuchungen konnten einen signifikanten positiven Zusammenhang zwischen der wahrgenommenen Glaubwürdigkeit einer fabrizierten Falschmeldung und der Einstellung zum Thema der Nachricht feststellen (s. Kapitel 3, B.I.1.). Eine zusätzliche Gefahr geht von einseitigem Nachrichtenkonsum zu einem Thema aus (wenn man durch den Bestätigungsfehler bestimmte Nachrichtenkanäle/Sender bevorzugt). Das wiederholte Lesen und Wahrnehmen von einer Falschinformation führt dazu, dass diese für glaubwürdiger gehalten wird.

III. Desinformation melden und Freunde ansprechen

1. Verbreitung eindämmen

Um Falschinformationen zu bekämpfen, scheint es wirkungsvoller zu sein, die Verbreitung von vorneherein einzudämmen, anstatt im Nachhinein zu versuchen, diese zu korrigieren (s. Kapitel 3, B.II.1.). Hinsichtlich der Verbreitung hat sich gezeigt, dass vor allem Menschen und nicht Social Bots zur Weiterleitung von Desinformation beitragen (Vosoughi et al., 2018). Dies wird insbesondere darauf zurückgeführt, dass Menschen oft Nachrichten weiterleiten, ohne sich intensiv mit deren Inhalt auseinanderzusetzen. Die Entscheidung, eine Nachricht zu teilen, fällt vielmehr in der Regel auf Basis des Informationsgehalts und der sprachlichen Gestaltung von Überschrift und Teasern (Gabelkov et al., 2016; Vosoughi et al., 2018).

2. Desinformation nicht weiterleiten, bei Verdacht auf strafbare Inhalte der jeweiligen Distributionsplattform melden

Ein wichtiger Weg, Desinformation einzudämmen, besteht somit darin, dafür zu sorgen, dass Desinformationen nicht weitergeleitet werden. Personen, die Desinformation auf Online-Plattformen entdecken oder den Verdacht haben,

dass es sich um Desinformation handelt, sollten die Meldung daher nicht an ihr Umfeld weiterleiten, sondern der jeweiligen Distributionsplattform melden, sofern eine solche Funktionalität – wie etwa bei Facebook – angeboten wird.

Mit der Meldefunktion können sie auch (strafbare) Inhalte melden, die sie nicht selbst betreffen. Die Online-Plattformen müssen nach den Regelungen der begrenzten Hostproviderhaftung nicht proaktiv nach Gesetzesverstößen suchen. Erst wenn sie Kenntnis von den rechtswidrigen Inhalten erlangen, zu meist durch Meldungen von Nutzenden, werden die Prüf- und Löschpflichten aktiviert (s. Kapitel 5, C.II.).

3. Keine Desinformation wiederholen

Eine Weiterleitung mit gleichzeitigem Warnhinweis empfiehlt sich nicht, da noch unklar ist, inwieweit die Falschnachricht trotz vorhandener Kennzeichnung nicht als falsch abgespeichert wird (s. Kapitel 3, B.II.2.). Ferner können Weiterleitung und Kommentierung dazu beitragen, dass die Nachricht über Auswahl- und Verbreitungs-Algorithmen erfolgreicher wird. Bürgerinnen und Bürger, die die Qualität politischer und gesellschaftlicher Diskurse auf Online-Plattformen steigern wollen, indem sie Falschmeldungen sorgfältig recherchierte Fakten entgegenstellen, sollten darauf achten, dass in ihren Posts die ursprüngliche, falsche Nachricht nicht als Link enthalten ist.

4. Hinweis auf Desinformation

Außerdem kann es hilfreich sein, Freunde und Bekannte, die Desinformation geteilt haben, direkt darauf hinzuweisen. Ein Vertrauensverhältnis zwischen den Nutzenden kann bei der Akzeptanz von Korrekturdarstellungen von Vorteil sein: Korrekturen auf Twitter sind bedeutend häufiger erfolgreich, wenn die beteiligten Personen miteinander vernetzt waren (Margolin et al. 2018). Demnach ist es empfehlenswert, innerhalb seines persönlichen digitalen Netzwerks proaktiv darauf hinzuweisen, wenn eine vertraute Person einer Falschinformation aufsitzt und sie verbreitet. Damit dies gelingen kann, sollte man darauf achten, auch die Informationen besonders zu prüfen, die von Freunden kommen, denn prinzipiell kann man davon ausgehen, dass auf Basis des Vertrauens, das man in Freunde hat, im persönlichen Umfeld eher seltener Fact-Checking betrieben wird (s. Kapitel 3, D.).

B. *Empfehlungen an Medienunternehmen, die sich zum Pressekodex bekennen*

I. Sorgfalt vor Schnelligkeit, Sachlichkeit vor Leseanreiz

1. Professionelle Standards wahren

Um bei den Nutzenden glaubwürdiger zu wirken, übernehmen die Autorinnen und Autoren von Desinformation häufig professionelle Regeln für das Schreiben von Nachrichten. Allerdings hat die Forschung (s. Kapitel 2, C.) gezeigt, dass diese Mimikry nur teilweise gelingt: Gerade komplexere journalistische Regeln, die die Argumentationsstruktur betreffen, werden von den meisten Verfassern von Fake News nicht eingehalten. Nachrichtenmedien sollten professionelle Standards der Nachrichtenerstellung noch konsequenter einhalten – dies wird sie noch klarer von Desinformationsangeboten abgrenzen.

2. Angaben zu Fakten prüfen

Hierzu gehört zum einen, der sorgfältigen Prüfung von Fakten im Zweifel den Vorzug zu geben vor einer möglichst schnellen Veröffentlichung einer Nachricht – auch im gerade in dieser Hinsicht harten Wettbewerbsumfeld auf Online-Märkten. Dies zahlt sich mittelfristig in einer höheren Glaubwürdigkeit aus. Jede fehlerhafte Meldung schwächt die Glaubwürdigkeit von seriösen Medien bei Nutzenden, faktenbasierte Berichterstattung stärkt sie (s. Kapitel 2, F.II.).

3. Sachliche Meldungen

Auch bei professionellen journalistischen Meldungen ist es legitim und richtig, mit sprachlichen Mitteln Aufmerksamkeit für relevante Inhalte zu generieren – gerade auch in Teasern, die auf Kommunikationsplattformen verbreitet werden. Angesichts des massiven Einsatzes dieser Instrumente auf Desinformationsplattformen empfiehlt sich im Sinne einer Abgrenzungsstrategie auch hier Zurückhaltung – im Zweifel sollten sich Redaktionen für die sachlichere Variante entscheiden (s. Kapitel 2, C.).

4. Offene Fehlerkultur

Bei aller journalistischen Sorgfalt lassen sich Fehler nicht vermeiden. Ein offener Umgang mit Fehlern und eine grundsätzlich hohe Transparenz hinsichtlich der redaktionellen Abläufe und den Qualitätssicherungsmechanismen sind daher mehr denn je geboten, um die nach wie vor hohe Glaubwürdigkeit, die etablierte Nachrichtenmedien in Deutschland genießen, auf diesem Niveau zu halten (Sängerlaub et al., 2018: 12).

Gerade eine offene Fehlerkultur findet sich auf Desinformationsportalen nicht. Und so gut es diesen Portalen gelingt, offensichtliche Fehler oder Mängel zu vermeiden, ist es für sie schwierig, professionelle journalistische Standards in einer Vielzahl von Dimensionen zu erfüllen, von geeigneten Schlagzeilen bis hin zur Konsistenz der präsentierten Fakten. Einige von ihnen versuchen, diese Defizite durch den Verweis auf glaubwürdigere Quellen auszugleichen.

II. Technische Unterstützung zur Aufdeckung von Desinformation nutzen und vorantreiben

Redakteurinnen, die den Wahrheitsgehalt einer Meldung untersuchen, können inzwischen auf eine Vielzahl von technischen Werkzeugen und Dienstleistungen zurückgreifen, die sie hierbei unterstützen (s. Kapitel 4, C.). Um mittels maschinellen Lernens in der Zukunft immer bessere Ergebnisse zu erzielen, ist das Schaffen einer Trainingsgrundlage durch Medienunternehmen von großer Bedeutung. Werden große Mengen von Texten und auch anderen Medien, die als Desinformation erkannt wurden, in Datenbanken abgelegt und entsprechend kommentiert, dann wird die Erkennung immer präziser (s. Kapitel 4, B.).

III. Entlarvung und Korrektur ansprechend gestalten

Die Entlarvung von Desinformation ist eine wichtige gesellschaftliche Aufgabe, der sich zivilgesellschaftliche Akteure ebenso annehmen wie Redaktionen etablierter journalistischer Medien. Dabei ist es eine Herausforderung für Fakt-Checking-Organisationen und journalistische Aufklärungsarbeit, ansprechende Narrative zu finden, damit sich korrekte Informationen schnell und breit verteilen. Eine ansprechende Geschichte erfüllt dabei zwei Zwecke:

Zum einen kann sie dazu beitragen, dass das Interesse der Leserinnen und Leser geweckt und die korrekte Information mit höherer Wahrscheinlichkeit gelesen und weitergeleitet wird. Zum anderen kann die Verpackung in eine Geschichte (inklusive korrekter, alternativer Erklärungen und Hintergrundinformationen) dazu beitragen, dass die richtige Information fester in den Wissensbestand aufgenommen wird.

1. Ansprechende Narrative

Ansprechende Narrative sind ein zentraler Erfolgsfaktor für Fact-Checking-Aktivitäten, denn eine Korrekturmeldung muss eine vergleichbar hohe Reichweite erzielen, wie die Falschmeldung selbst, um eine vergleichbare Wirkung erzielen zu können (s. Kapitel 3, B.II.). Schlichte Gegendarstellungen verbreiten sich im Allgemeinen in Online-Netzwerken deutlich weniger als Desinformation.

2. Regeln des Widerlegens

Bei der Widerlegung von Falschinformationen sollten grundsätzliche Regeln des Widerlegens beachtet werden, wie zum Beispiel Fakten in den Vordergrund zu stellen, komplizierte Korrekturen zu vermeiden und alternative Erklärungen anzubieten. Die Herausforderung besteht darin, einfache und kurze Korrekturen zu produzieren, die in der Wahrnehmung attraktiver sind als die entsprechende Desinformation (s. Kapitel 3, B.II.).

Darüber hinaus kann die Darstellungsform einer Widerlegung dazu beitragen, dass die relevanten Informationen von der Zielgruppe aufgenommen und erinnert werden. Sowohl Texte als auch grafische Wahrheitsskalen sind in der Lage, eine Korrektur effektiv zu vermitteln. Auch kann es hilfreich sein, die korrigierenden Informationen in Form eines Videos darzustellen, da hierdurch die Aufmerksamkeit gesteigert und gleichzeitig eine mögliche Verwirrung reduziert werden kann (Young, Jamieson, Poulsen & Goldring, 2017).

C. *Empfehlungen an Online-Plattformen und Betreiber von Systemen mit Nutzer-generierten Inhalten*

I. Overblocking und Underblocking vermeiden und freiwillige Selbstkontrolle einführen

1. Verantwortung von Online-Plattformen

Wirtschaftlich wie publizistisch einflussreiche Online-Plattformen haben sich zu relevanten Foren der öffentlichen Kommunikation entwickelt, in denen Einfluss auf den öffentlichen Meinungsaustausch und die Meinungsbildung genommen wird. Hieraus resultieren eine besondere gesellschaftliche Verantwortung sowie rechtliche Pflichten, denen sie verstärkt nachkommen müssen – auch im Umgang mit Desinformation.

Die Kommunikationsplattformen sollten ihrem selbst auferlegten Anspruch der Verteidigung der Meinungsfreiheit gerecht werden, indem sie sowohl „Over-“ als auch „Underblocking“ möglichst effizient vermeiden. Eine Sperrung oder Löschung von Inhalten und Nutzerkonten muss sachlich gerechtfertigt und darf nicht willkürlich sein. Bei nicht offensichtlich rechts- und regelwidrigen Inhalten ist nach den Umständen des Einzelfalls dem Ersteller von Inhalten Gelegenheit zur Stellungnahme zu geben, bevor eine Maßnahme ergriffen wird. Im Umgang mit Nutzerbeschwerden wegen (unrechtmäßig) gelöschter und gesperrter Inhalte und Nutzerkonten müssen klare Regeln und Verfahren etabliert werden, welche den Erstellern von Inhalten die Möglichkeit einräumen, einen Antrag auf (erneute) Überprüfung des Inhalts zu stellen. Die Regeln und Verfahren zur Wiederherstellung von unrechtmäßig entfernten Inhalten müssen verbessert und transparenter werden (s. Kapitel 5, C.II. und D.II.). Beim Umgang mit strafbaren Inhalten auf ihren Plattformen sollten sie die Kooperation mit den Strafverfolgungsbehörden verbessern und diese Aufgabe mit systematischen Strukturen und Prozessen angehen.

2. Meinungsfreiheit beachten

Als private Unternehmen sind Kommunikationsplattformen nicht unmittelbar an Grundrechte gebunden. Daher haben sie etwas weitere Spielräume für ihre eigenen Plattformregeln. Als wirkmächtige Anbieter öffentlicher Kommunikationsräume unterliegen sie jedoch einer intensivierten mittel-

baren Drittwirkung in Bezug auf die Kommunikationsfreiheiten und den Persönlichkeitsschutz der Nutzenden.

Wegweisend dürfte die Rechtsprechung zur Reichweite der Befugnisse der Kommunikationsplattformen bei der Formulierung und Anwendung von AGB im Zusammenhang mit Hassrede sein. Da auch die Grundrechte, insbesondere die Berufsfreiheit, der Anbieter zu berücksichtigen sind, ist zu befürworten, dass für die Anbieter die Wertentscheidungen für die Meinungsfreiheit des Grundgesetzes bei der privaten Rechtssetzung richtungsweisend sind. Dies bedeutet vor allem, dass die eigenen Regeln derart ausgestaltet sein dürfen, dass sie sich im Großen und Ganzen auf einer Linie mit den Grundsätzen zur Gewährleistung der Meinungsfreiheit bewegen. Die Unternehmen dürfen folglich im Kontext von Hassrede strengere Regeln aufstellen, sodass im Einzelfall auch Äußerungen erfasst sein können, die grundsätzlich noch von der Meinungsfreiheit erfasst sind. Hierfür spricht auch, dass durch Hassrede eine Diskussion nachhaltig negativ beeinflusst werden kann, sodass andere Nutzende eingeschüchtert werden und von einer (weiteren) Beteiligung absehen. Bei „abstrakt“ politischer, öffentlichkeitsbedeutsamer Rede sind strengere Regeln hingegen nicht zulässig (s. Kapitel 5, C.III.).

Desinformation darf bei Zugrundelegung der Wertentscheidung für die Meinungsfreiheit auch unter Heranziehung etwaiger AGB in der Regel nicht entfernt werden, wenn die unwahren Tatsachenbehauptungen einen starken Meinungsbezug durch die Verbindung mit Werturteilen aufweisen, Rechte Dritter nicht verletzt sind und der Inhalt nicht strafbar ist. Ein größerer Handlungsspielraum besteht hingegen bei (offensichtlich) bewusst unwahren Tatsachenbehauptungen, die nicht in Zusammenhang mit einem Werturteil verbreitet werden. Denn bewusst unwahre Tatsachenbehauptungen fallen schon gar nicht in den Schutzbereich der Meinungsfreiheit, wenn sie unter keinem denkbaren Gesichtspunkt zum grundrechtlich geschützten Prozess der Meinungsbildung beitragen können (s. Kapitel 5, A.II.).

3. Selbstregulierung

Des Weiteren ist die Einrichtung einer Selbstregulierungsstelle „Desinformation“ für die großen Online-Plattformen empfehlenswert. In regelmäßigen Berichten über den Umgang mit Desinformation und die Lösch- und Sperrpraxis können die Unternehmen zeigen, dass sie sich in der gesellschaftlichen Verantwortung sehen und sich dieser stellen. Zudem könnte so eine vertiefte, faktenbasierte Diskussion über die private Regulierung, Wirkung und Be-

deutung der Online-Plattformen aus Makroperspektive geführt und zu einem besseren Verständnis der Verfahrensweise der Online-Plattformen auch aus Sicht der Nutzenden beigetragen werden. Die im „EU-Praxiskodex Desinformation“ vorgesehene Selbstverpflichtung zur jährlichen Berichterstattung ist ein wichtiger Schritt hin zu mehr Transparenz. Die im Vorfeld der Europawahl 2019 durch die Unterzeichner zu veröffentlichenden Berichte wurden seitens der EU-Kommission bereits positiv aufgenommen, die Notwendigkeit anhaltenden und verstärkten Engagements der Unterzeichner jedoch betont. Weitere Berichte sowie die erste umfassende und konkrete Würdigung der in den ersten zwölf Monaten erfolgten Maßnahmen der Unterzeichner durch die EU-Kommission Ende des Jahres 2019 bleiben abzuwarten. Die Transparenzberichte im Rahmen des Netzwerkdurchsetzungsgesetzes (NetzDG) betreffen nur bestimmte strafbare Inhalte auf den Plattformen. Die Online-Plattformen sollten sich einer freiwilligen Selbstkontrolle unterwerfen, wie sie z. B. mit Erfolg auch im Bereich des Jugendmedienschutzes etabliert ist. Hier ist es aber auch Aufgabe der Politik, auf die Einrichtung und den Ausbau entsprechender Institutionen im Bereich der Online-Plattformen hinzuwirken (s. Kapitel 5, C.V.).

II. Social Bots aufspüren und Malicious Social Bots systematisch eliminieren

Die Betreiber von Plattformen haben die beste Ausgangssituation, um Social Bots aufzuspüren (s. Kapitel 4, B.V.). Dieses Privileg sollten sie – auch im Eigeninteresse – nutzen: Bei Kenntnis können sie die Profile von Social Bots kennzeichnen (s. Kapitel 6, D.II.4.).

Die Betreiber sind bei Kenntnis der Social-Bot-Profile zudem gut vorbereitet, wenn sie wirksame Gegenmaßnahmen bei massenhafter Verbreitung von Desinformation und auch weiterer unerwünschter Inhalte (die beispielsweise gegen ihre Community-Richtlinien verstoßen) durch Malicious Bots einleiten möchten.

Darüber hinaus ist es für die Wahrung ihrer eigenen Interessen bezüglich Cybersicherheit und Privatsphärenschutz essenziell diese Profile aufzuspüren, denn die Kenntnis der Bots einer Plattform stellt ein notwendiges Element im Angreifermodell der Cybersicherheitsbetrachtung der Betreiber der Plattformen dar: Mit Hilfe dieser Bots könnten ggf. skalierbare Angriffe auf die Verfügbarkeit, Integrität und Vertraulichkeit der Betreiberinfrastruktur und der gesamten Plattform lanciert werden.

Sobald Malicious Social Bots als solche überführt wurden und ihre Aktionen nachweislich gegen Richtlinien des Plattformbetreibers verstoßen, können (und sollten) sie unmittelbar gelöscht oder gesperrt werden (s. Kapitel 5, C.I.). Für diese Aufgabe sollten die Betreiber Strukturen und systematische Prozesse vorsehen.

D. Empfehlungen für Politik und Gesetzgebung

I. Zivilgesellschaftliche Akteure (Medienbildung, Faktenchecker) unterstützen

1. Bildungsaufgaben

Die Motivation und Fähigkeit von Online-Nutzenden zum elaborierten Umgang mit (Des-)Informationen im Internet sind zentrale „Stellschrauben“, die Einfluss auf die Wirksamkeit der Desinformation haben können. Durch gezielte Bildungsarbeit könnten diese bereits frühzeitig in den Blick genommen werden, um sowohl das Interesse an Politik und komplexen Zusammenhängen sowie Kompetenzen im Umgang mit Informationsmedien zu schulen (s. Kapitel 4, B.II.).

Besondere Aufmerksamkeit sollte auf die Ausbildung eines analytischen Denkvermögens gelegt werden, da Personen mit einer stärkeren Neigung zum analytischen Denken Falschinformationen besser erkennen können. Ein hohes Bedürfnis nach kognitiver Betätigung hängt positiv mit dem Erkennen von korrekten oder inkorrekten Informationen zusammen. Dies spricht ebenfalls dafür, die Neigung, sich mit komplexen Inhalten auseinanderzusetzen, bereits in der Schule zu fördern (s. Kapitel 4, A.III.).

2. Medienkompetenz

Medienkompetenzschulungen sind jedoch nicht nur für Kinder und Jugendliche, sondern auch für Erwachsene sinnvoll, die möglicherweise nicht so gut mit den digitalen Möglichkeiten der Informationserstellung vertraut sind. Zwischen dem Alter der Versuchsteilnehmenden und der Glaubwürdigkeitsbewertung von Falschinformationen besteht ein positiver Zusammenhang, der zeigt, dass die Desinformation von älteren Personen glaubwürdiger wahrgenommen wurde (s. Kapitel 4, A.III.).

3. Sensibilisierung

Weitere Schwerpunkte der Medienbildung im Hinblick auf Desinformation sollten eine grundlegende Kenntnis professioneller journalistischer Kriterien zur Auswahl und sprachlichen Aufbereitung von Nachrichten, die Entwicklung von Fähigkeiten zum Gebrauch einfacher Instrumente zur Überprüfung von Desinformation sowie eine Sensibilisierung für die Kommunikationsdynamiken beim Teilen von Informationen auf Online-Plattformen sein (s. Kapitel 2, F.II.).

II. Gesetzliche Feinjustierungen

1. Ausgeglichene Regelungen

Ein größerer Korrekturbedarf hinsichtlich der materiellen Rechtslage besteht nicht. Eine neue, pauschale rechtliche Regelung zu Desinformation neben den bereits vorhandenen Straftatbeständen erscheint ebenso wenig erforderlich wie praktisch realisierbar. Ein neuer Straftatbestand würde vor allem symbolische Bedeutung haben und in der Praxis wenig wirksam sein. Eine solche Vorschrift könnte sich sogar nachteilig auf die Motivation von Betreibern und Nutzenden von Online-Plattformen auswirken, selbstverantwortlich und freiwillig Maßnahmen zum Kampf gegen Desinformation zu ergreifen. Hierzu zählen auch ihre technischen Strukturen, die stetig fortentwickelt werden. Sie werden auch im Hinblick auf die Ermittlung und das Ranking anhand der Faktentreue von Websites Fortschritte erzielen. Soweit die Desinformation ehrverletzende, unwahre Tatsachenbehauptungen über Personen enthält, stehen bereits die Straftatbestände der Verleumdung und der üblen Nachrede zur Verfügung (s. Kapitel 5, A.).

2. Schutz der Meinungsfreiheit

Im Übrigen setzt die Meinungsfreiheit dem Handlungsspielraum des Gesetzgebers enge Grenzen. Nicht in den Schutzbereich der Meinungsfreiheit fallen lediglich solche Äußerungen, die reine Tatsachenbehauptungen darstellen, also dem Beweis zugänglich sind. Sie können einfacher gelöscht werden. Soweit die Äußerung jedoch „Elemente des Dafürhaltens“ aufweist, liegt eine Meinungsäußerung vor, die auch dann insgesamt als Meinungsäußerung

zu qualifizieren ist, wenn sie meinungsbezogene Tatsachenbehauptungen enthält. Im Zweifel ist von einer Meinungsäußerung auszugehen. Diese darf nur reguliert werden, wenn die Vorschriften dem Schutz der Jugend und dem Recht der persönlichen Ehre dienen oder wenn sie Themen betreffen, die nichts mit einer spezifischen Meinung zu tun haben. Es verbleibt ein weiter Bereich der Desinformation, der rechtlich nicht verboten ist. Eine freie Demokratie muss sie aushalten und sich ihr immer wieder im öffentlichen Meinungskampf stellen (s. Kapitel 5, A.II.).

3. Nachbesserungen des NetzDG

Im Rahmen des NetzDG sind Nachbesserungen notwendig, um den Schutz von Autoren zu erhöhen, deren Beiträge zu Unrecht gesperrt oder gelöscht worden sind. Bislang schreibt das NetzDG den Kommunikationsplattformen kein Verfahren vor, blockierte Nutzerinhalte erneut zu prüfen und unrechtmäßig entfernte Inhalte wiederherzustellen (s. Kapitel 5, D.II.).

4. Transparenz von Social Bots

Im Hinblick auf die Regulierung von Social Bots sollten zuvörderst die Online-Plattformen durch Selbstverpflichtungen, klare Allgemeine Geschäftsbedingungen und ihre Durchsetzung den Einsatz von Social Bots regulieren. Auch wenn die Verbreitung von Desinformation bisher (noch) nicht überwiegend durch Malicious Social Bots erfolgt, so bewirken sie doch Verstärkereffekte der Desinformation, die vermeintliche Mehrheitsverhältnisse vortäuschen und die Reichweite der Desinformation erheblich erweitern können. Ihr Einsatz ist häufig für die Rezipienten nicht erkennbar. Ob Selbstverpflichtungen der Online-Plattformen, insbesondere die im „EU-Praxiskodex Desinformation“ vorgesehenen, eher vage formulierten Maßnahmen zum Umgang mit Fake-Accounts und Online-Bots, künftig genügen werden, muss vor einem gesetzgeberischen Tätigwerden überprüft werden. Ein pauschales Verbot von Social Bots wäre unverhältnismäßig. Eine Kennzeichnungspflicht und Transparenzvorgaben für Social Bots – wie auch der Entwurf für einen neuen Medienstaatsvertrag vorschlägt – sind jedoch möglich und mit der Meinungsfreiheit vereinbar (s. Kapitel 5, C.V.).

III. Rechtsdurchsetzung verbessern

1. Strafverfolgung verbessern

Soweit Desinformation strafbar ist, sollte die Strafbarkeit der Äußerungen eine größere abschreckende Wirkung entfalten, als es bislang der Fall ist. Eine bessere Rechtsdurchsetzung bei strafbaren Äußerungen im Internet sowie die schnelle Klärung von Fällen und die Zuführung der Täter zu Strafverfahren ist erforderlich, um (potenzielle) Täter von strafbarer Desinformation und Hetze im Internet künftig abzuhalten und die Zahl dieser Straftaten nachhaltig zu reduzieren. Das NetzDG ist ein wichtiger Baustein zur Durchsetzung des geltenden Rechts. Auch wenn es nur bestimmte Formen strafbarer Beiträge erfasst, hilft es, die Zahl strafbarer Inhalte auf den Seiten der Online-Plattformen zu reduzieren. Außerdem hat es eine öffentliche, kontroverse Diskussion über den richtigen Umgang mit rechtswidrigen und gesellschaftlich schädlichen Inhalten auf Kommunikationsplattformen in Gang gebracht. Für besonders wichtig erachten wir zudem die Kooperation von Strafverfolgungsbehörden und Online-Plattformen. So müssen strafbare Beiträge nicht nur nicht mehr sichtbar sein, sondern die Inhaltersteller und -verbreiter auch konsequent der Strafverfolgung zugeführt werden. Dazu beitragen könnte die Einführung einer Pflicht der Anbieter bei Löschung oder Sperrung wegen Officialdelikten diese an Strafverfolgungsbehörden zu melden. Daneben sind jedoch auch weitere Maßnahmen, die die faktischen Voraussetzungen der Strafverfolgung betreffen, erforderlich (s. Kapitel 5, C.II.).

2. Sorgfaltspflicht durchsetzen

Hinsichtlich der Regulierung von Telemedienanbietern mit journalistisch-redaktioneller Prägung sind schärfere Sanktions- und Aufsichtsmöglichkeiten bei Verstößen gegen die Wahrheits- und Sorgfaltspflichten empfehlenswert. Die Telemedien mit journalistisch-redaktionell gestalteten Angeboten (weite Auslegung) sind nach den Regelungen des Rundfunkstaatsvertrags zur Einhaltung der anerkannten journalistischen Grundsätze und zur Prüfung von Nachrichten mit der nach den Umständen gebotenen Sorgfalt auf Inhalt, Herkunft und Wahrheit verpflichtet (s. Kapitel 5, A.I.).

Soweit jedoch keine Rechte Dritter betroffen sind, ist die Anwendung des Telemedienrechts auf Anbieter von Websites, die bewusst oder grob fahrlässig Falschmeldungen verbreiten, kaum wirkungsvoll. Im Rundfunk-

staatsvertrag sind keine Aufsichtsmaßnahmen vorgesehen. Da die bewusste Verbreitung von Desinformationen (z. B. zur Erzielung von Klicks für höhere Werbeeinnahmen oder zur Unterstützung einer bestimmten politischen oder verschwörerischen Ausrichtung) einen besonders schweren Verstoß gegen die journalistischen Wahrheits- und Sorgfaltspflichten darstellt und die öffentliche Meinungsbildung beeinflussen kann, sollte es möglich sein, entsprechende Richtigstellungen, Entfernungen oder andere Maßnahmen zu erwirken. Entsprechend könnten die Befugnisse der Landesmedienanstalten erweitert werden (s. Kapitel 5, A.IV. und D.III.).

3. Freiwillige Selbstkontrolle

Mit dem Deutschen Presserat existiert zudem ein Organ der freiwilligen Selbstkontrolle. Auch wenn Politik und Gesetzgebung hier aus gutem Grunde keinen direkten Einfluss haben, könnte eine Diskussion mit den beteiligten Akteuren angestoßen werden, ob bezogen auf Desinformation Sanktionsmöglichkeiten entwickelt werden können, die über eine öffentliche Rüge hinausgehen, was jedoch einen Bruch des auf Freiwilligkeit beruhenden Selbstregulierungskonzeptes bedeuten würde (s. Kapitel 5, A.IV.).

E. Empfehlungen für Einrichtungen der Forschungsförderung in der EU und in Deutschland

I. Anwendungsorientierte, interdisziplinäre Forschung stärken

1. Interdisziplinäre Forschung

Die anwendungsorientierte Forschung zu Desinformationen muss intensiviert werden, um verantwortliche Akteure in die Lage zu versetzen, Gesellschaft und Wirtschaft vor der Zunahme schädlicher Desinformation wirksam zu schützen. Bezüglich Einzelaspekten von Desinformation liegen zwar Ergebnisse vor, allerdings sind diese durch disziplinäre Sichtweisen eingeschränkt und auch innerhalb von Disziplinen fragmentiert (s. Kapitel 2, F.IV.).

Ein Beispiel für die Notwendigkeit der Zusammenführung von Forschungsansätzen selbst innerhalb einer Disziplin ist die Erkennung von („böartigen“) Social Bots, die Desinformation vollautomatisch verteilen und verstärken. Hier gibt es eine Reihe von Mechanismen, die jeweils eine einzige statische

Eigenschaft oder ein Spezifikum des Verhaltens dieser Bots erkennen. Gebraucht werden aber Kombinationsansätze, die die Erkennungsrate messbar steigern und sogar Social Bots erkennen können, deren Existenz zum Beispiel mit adversarial machine learning verschleiert werden soll (s. Kapitel 4, B.V.).

Anwendungsorientierte Forschung kann beispielsweise Wege aufzeigen, wie mittels Technikeinsatz faktenbasierter Journalismus gestärkt werden kann. Exemplarisch hierfür steht ein Mechanismus zur nachprüfbaren Zitierweise: Durch kryptographische Mechanismen lassen sich die Unverändertheit (Integrität) und die Echtheit der angegebenen Quelle (Authentizität) eines Zitats in einem Text überprüfen (Kreutzer, Niederhagen, Shrishak & Fhom, 2019). Weitere Forschung ist notwendig, um verstehen zu können, ob dieses und andere Ergebnisse tatsächlich transferierbar sind.

Die Themenfelder für Angstnarrative von Desinformationskampagnen entwickeln sich im Laufe der Zeit sicherlich weiter bzw. verschieben sich. Um darüber gesicherte Aussagen machen zu können, ist ebenfalls interdisziplinäre Forschung notwendig. In den ersten drei Quartalen von 2019 zeigten beispielsweise Umfragen auf, dass das Themenfeld Ausländer/Migration/Flüchtlinge von wesentlich weniger Menschen in Deutschland als „wichtiges Problem“ wahrgenommen wird, als in dem Zeitraum, der im Rahmen der DORIAN-Samples untersucht wurde (Forschungsgruppe Wahlen, 2019). Dem Themenfeld Umwelt und Energiewende wird in der Bevölkerung seit Anfang 2019 eine wachsende Bedeutung zugeschrieben (Forschungsgruppe Wahlen, 2019). In weitergehenden Forschungsaktivitäten könnte untersucht werden, ob ähnliche Angstnarrative wie zum Thema Migration und innere Sicherheit auch zu anderen Themen aufgebaut werden, beispielsweise in Bezug auf Dieselfahrverbote oder in Bezug auf eine angeblich drohende „Ökodiktatur“. Ein Vergleich der Argumentationsstruktur in Fake News zu unterschiedlichen Themen könnte hier interessante und aktuelle Erkenntnisse für alle beteiligten Disziplinen liefern. So könnten diese helfen den Einsatz von maschinellem Lernen zur Erkennung von Desinformation weiterzuentwickeln.

2. Maschinelles Lernen stärken

In DORIAN wurde damit begonnen, maschinelles Lernen für die Erkennung von Desinformation zu erforschen. Die Zwischenergebnisse dieses Ansatzes sind sehr vielversprechend. Allerdings besteht noch erheblicher Forschungsbedarf, um dieses Werkzeug effizient und effektiv einsetzen zu können. Auch in anderen Bereichen der Technikforschung und in den anderen Disziplinen

von DORIAN werden die gewählten Forschungsansätze durch den Erfolg bestätigt. Die dort umgesetzten Pionierarbeiten müssen fortgesetzt werden, um ihr Nutzenpotenzial entfalten zu können (s. Kapitel 4, C.).

3. Gesamthafte Sicht ermöglichen

Ein technischer Ansatz allein würde aber keine empirisch fundierten Maßnahmvorschläge liefern, wie gesellschaftliche Akteure Desinformation begegnen können. Die Sicht der Technik muss mindestens ergänzt werden durch die Beiträge der Journalistik, der Psychologie, des Rechts, der Sozialwissenschaften und der Politikwissenschaft. Für die nächsten fünf Jahre werden mindestens die beiden nachfolgenden Zielstellungen der Forschungsförderung zu Desinformation empfohlen:

II. Verbreitungswege und Verbreitungsgrad von Desinformation erforschen

Um das Phänomen Desinformation in Deutschland erfassen zu können, braucht es belastbare Informationen über die tatsächlichen Verbreitungswege auf Websites und Online-Plattformen (Social Networks). Hierzu müssen technische Mechanismen entwickelt werden, die dies quantitativ und qualitativ auf den verschiedenen Desinformationskanälen ermitteln können.

III. Wirkungsweise und Wirkmächtigkeit von Desinformation erforschen

Um Desinformation effektiv bekämpfen zu können, sind die Erforschung der Wirkungsweise, Wirkmächtigkeit und Wirkmaximierung notwendig – sowohl von Desinformation und in Kontrast dazu von faktenbasierten Informationen ohne Manipulationsabsicht.

Literaturverzeichnis zu Kapitel 6

- Bader, K., Jansen, C., Johannes, P. C., Krämer, N., Kreutzer, M., Löber, L. I., Rinsdorf, L., Röser, L. & Roßnagel, A. (2018). Desinformationen aufdecken und bekämpfen: Handlungsempfehlungen. Policy-Paper. Hrsg.: Fraunhofer-Institut für System- und Innovationsforschung ISI. Verfügbar unter <https://www.forum-privatheit.de/wp-content/uploads/Policy-Paper-DORIAN-Desinformation-aufdecken-und-bekaempfen-1.pdf>
- Forschungsgruppe Wahlen (2019). Abruf am 23.9.2019 Verfügbar unter: http://www.forschungsgruppe.de/Umfragen/Politbarometer/Langzeitentwicklung_-_Themen_im_Ueberblick/Politik_II/
- Gabielkov, M., Ramachandran, A., Chaintreau, A., & Legout, A. (2016). Social clicks: What and who gets read on Twitter?. *ACM SIGMETRICS Performance Evaluation Review*, 44(1), 179-192.
- Kreutzer, M., Niederhagen, R., Shrishak, C. & Fhom, H. (2019). Quotable Signatures using Merkle Trees. *INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik–Informatik für Gesellschaft*.
- Margolin, D. B., Hannak, A., & Weber, I. (2018). Political fact-checking on Twitter: When do corrections have an effect?. *Political Communication*, 35(2), 196-219.
- Sängerlaub, A., Meier, M., & Rühl, W.-D. (2018). Fakten statt Fakes: Das Phänomen »Fake News«. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017 (Abschlussbericht Projekt »Measuring Fake News«). Berlin. Verfügbar unter: https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151.
- Young, D. G., Jamieson, K. H., Poulsen, S., & Goldring, A. (2018). Fact-checking effectiveness as a function of format and tone: Evaluating FactCheck. org and FlackCheck. org. *Journalism & Mass Communication Quarterly*, 95(1), 49-75.

