GEFÄHRDUNG DEMOKRATISCHER WILLENSBILDUNG DURCH DESINFORMATION

Impulspapier | Dezember 2019

Zusammenfassung

Gezielte Desinformation gefährdet zunehmend die demokratische Willensbildung und bedarf daher gesteigerter Aufmerksamkeit und gezielter Gegenmaßnahmen.

Desinformation wird vor allem über das Internet und insbesondere Social Networks als Text- oder Bildnachricht verbreitet. Künftig ist verstärkt mit manipulierten Bild- und Tonaufnahmen („Deep Fakes“) zu rechnen, die durch ihre sinnliche Nachvollziehbarkeit besonders glaubwürdig wirken. Desinformation verfolgt das **Ziel**, politische Gegner in der öffentlichen Wahrnehmung zu diskreditieren, Stimmung für oder gegen bestimmte Gruppen zu erzeugen und so die öffentliche Meinungsbildung zu beeinflussen. Entscheidend für digitale Desinformation ist, dass jeder sie erzeugen und einfach, kostengünstig und anonym verbreiten kann. Oft findet die **Verbreitung** auch durch professionelle „Trolle“ oder gar „Trollarmeen“ sowie Social Bots statt, die als Computerprogramme in Social Networks menschliche Nutzer imitieren.

In ihrer **Wirkung** untergräbt Desinformation das Vertrauen in Institutionen oder Personen, unterstützt Verschwörungstheorien und fördert eine grundsätzliche politische Lagerbildung. Sie erzeugt Unsicherheit darüber, auf welche Wahrheit man sich in der politischen Kommunikation vernünftigerweise einigen kann. Individuell bleibt die falsche Information besser im Gedächtnis als eine nachträglich korrigierte. Social Bots können vermeintliche Mehrheitsverhältnisse vortäuschen und so durch die „Schweigespirale“ das öffentliche Meinungsklima beeinflussen.

Gegenmaßnahmen können auf **technischer** Ebene wirksam nur die Betreiber von Social Networks ergreifen. Sie können auf Beschwerden schnell reagieren und Inhalte oder Accounts sperren oder löschen. Automatisierte Verfahren werden immer besser, werden aber nie vollständig zuverlässig sein. Auf **rechtlicher** Ebene sind bei Straftaten Gegenmaßnahmen möglich. Die Betreiber sind hierzu durch das Netzwerkdurchsetzungsgesetz auch verpflichtet. Jenseits des Strafrechts sind alle Regulierungsmaßnahmen aber an der von Artikel 5 Absatz 1 des Grundgesetzes geschützten Meinungsfreiheit zu messen, die nur inhaltsneutrale Maßnahmen erlaubt.

Politische Gegenmaßnahmen helfen, den notwendigen Meinungskampf zu unterstützen:

Bezogen auf **Social Networks** ist der geltende zivil- und strafrechtliche Rechtsrahmen besser durchzusetzen. Sie sollten auch anders formulierte, aber inhaltsgleiche Inhalte entfernen müssen. Soweit sie automatisierte Verfahren einsetzen, sollten sie ihre Eingreifkriterien veröffentlichen. Strafbare Inhalte sollten sie anzeigen und ihre Autoren aufdecken müssen. Für Social Bots sind Kennzeichnungspflichten vorzusehen. Zum Schutz der Meinungsfreiheit sollten sie ein wirksames und schnelles Beschwerdeverfahren für zu Unrecht gesperrte oder gelöschte Inhalte vorsehen.

Es sind technische und interdisziplinäre **Forschungsprojekte** zu fördern, die die Erkenntnisse verschiedener Disziplinen (wie Technik, Journalistik, Psychologie, Recht) zusammenbringen, um gesamthaft wirksame und umsetzbare Lösungen zu entwickeln. Zu erforschen ist, wie – auch mit Künstlicher Intelligenz – Desinformation, Deep Fakes, Malicious Social Bots und ihre Verbreitungswege erkannt, gekennzeichnet, gesperrt und gelöscht werden können. Zu untersuchen sind Charakteristika von Desinformation und ihre Wirkungen auf Einzelne und die Gesellschaft sowie politische und rechtliche Gegenmaßnahmen, die eine wirksame Bekämpfung bewirken, ohne Meinungsfreiheit zu behindern. Für diese Forschung sollten Social Networks (zu diesem Zweck geschützt) ausreichende Mengen an – anonymisierten oder pseudonymisierten – Kommunikationsdaten zur Verfügung stellen (müssen).

Urheber und Ziele von Desinformation

Unter Desinformation sollen hier falsche Informationen verstanden werden, die in Täuschungsabsicht und mit dem Ziel, die öffentliche Meinungsbildung zu beeinflussen, über das Internet und insbesondere Social Networks verbreitet werden. Sie können sowohl Texte als auch manipulierte Bilder, Filme oder Tondokumente nutzen und alle denkbaren Inhalte haben. Durch Deep-Fake-Programme sind Manipulationen von Bild- und Tonaufnahmen möglich, die bestimmten Personen alle denkbaren Aussagen „in den Mund legen" und sie alle möglichen ehrenrührigen oder strafbaren Handlungen ausführen lassen. Da diese Personen mit ihren Gesichtern, ihrer Stimme und ihrem spezifischen Sprachduktus auftreten, sind diese Manipulationen durch ihre sinnliche Nachvollziehbarkeit besonders glaubwürdig. Im politischen Kontext werden sie eingesetzt, um Botschaften zu transportieren, politische Gegner in der öffentlichen Wahrnehmung zu diskreditieren und Stimmung für oder gegen bestimmte Gruppen zu erzeugen.

Desinformation aus dem Ausland wird in Deutschland verbreitet, um Einfluss auf die demokratische Willensbildung zu nehmen. Am stärksten erfolgt dies aus Russland. Aber auch innerhalb Deutschlands wird Desinformation durch einzelne politische Parteien und andere politisch orientierte Organisationen verbreitet – weit überwiegend mit rechtsradikalem Hintergrund.

Verbreitung digitaler Desinformation

Weite Verbreitung findet Desinformation vor allem in Social Networks wie Twitter oder Facebook, in Internetblogs, Videoplattformen, Onlineforen und in den Kommentarspalten unterschiedlichster Webseiten. Sie werden ab einer gewissen Verbreitung oder bei ausreichendem Neuigkeitswert mitunter von klassischen Medien aufgegriffen und durch diese weiterverbreitet. Besonders bei emotionalen Reizthemen wie Gewalttaten, Flüchtlingskrise, Missbrauch oder gar Krieg ist eine reflexartige Empörung oft nicht weit. Solche Inhalte haben ein hohes Potenzial, dass Nutzer sie sehr schnell viral weiterverbreiten und sie dadurch ein globales Publikum erreichen.

Entscheidend für digitale Desinformation ist, dass jeder sie erzeugen und einfach und kostengünstig verbreiten kann. Social Networks sind für jedermann zugänglich und ohne größeren Verschleierungsaufwand anonym nutzbar. Die Urheberschaft einer Desinformation kann oftmals nur schwer aufgedeckt werden. Auch daher ist online verbreitete Desinformation nur schwer wieder einzufangen. Darüber hinaus bleibt digitale Desinformation aufgrund der Dynamik, Heterogenität und Komplexität des digitalen Raums oftmals einige Zeit unbemerkt.

Desinformation wird vielfach von professionell arbeitenden Aktivisten verbreitet, die öffentliche Diskussionen gezielt stören, insbesondere indem sie provokative Beiträge veröffentlichen („Trolle"). „Trolling" wird von Einzelnen, Organisationen, aber auch von staatlichen Organisationen („Trollarmeen") genutzt.

Ein anderes Mittel, die Verbreitung von Desinformation erheblich zu erweitern und beschleunigen, sind Social Bots. Dies sind Computerprogramme, die in Social Networks menschliche Nutzer imitieren. Massenhaft eingesetzt können sie automatisiert das Mehrheitsbild zu bestimmten Themen und Trends in der öffentlichen Meinung verändern und um andere Meinungen zu marginalisieren oder deren Träger einzuschüchtern.

Desinformation kann mit Hilfe von Microtargeting die jeweils gewünschten Zielgruppen personengenau erreichen und so automatisiert und individualisiert beeinflussen.

Wirkung von Desinformationen

Durch Desinformation können ihre Urheber Empörung verursachen, das Vertrauen in bestimmte Institutionen oder Personen untergraben, Verschwörungstheorien unterstützen, bestimmte Gruppierungen aktivieren und den Zusammenhalt ihrer Anhänger stärken. Sie können aber auch Verwirrung stiften, Gruppen und Einzelne einschüchtern und destabilisierend auf die Gesellschaft wirken. Sie können – insbesondere über mobile Endgeräte – Krisensituationen auslösen und in solchen viele Menschen im betroffenen Gebiet beeinflussen und so die Krise verstärken.

Desinformation ist weniger geeignet, Personen mit diametral entgegenstehenden Ansichten zu überzeugen. Schon eher beeinflussen sie in ihrer Meinungsbildung offene Personen sowie Nichtwähler und unentschlossene Wähler. Jedenfalls aber wirken sie auf die jeweilige politische Anhängerschaft bestätigend und auch radikalisierend. Diese Wirkung steht der gesamtgesellschaftlichen Inklusion entgegen und fördert eine grundsätzliche politische und gesellschaftliche Lagerbildung. Auf diese Weise entsteht eine Dynamik, die eine Fragmentierung von Öffentlichkeit begünstigt: Zum einen verliert die gruppenübergreifende Auseinandersetzung dadurch an Reichweite, dass gesellschaftliche Gruppen sich in Informationsblasen einkapseln, in denen sie immer weniger mit den Wissensformen, Argumenten und Sichtweisen der anderen Seite konfrontiert werden. Zum anderen wird die Verpflichtung geschwächt, die eigene Position auf gesamtgesellschaftlich gültige Verfahren und Mechanismen der Wahrheitsproduktion zu stützen. Desinformation erzeugt Unsicherheit darüber, auf welche Wahrheit man sich innerhalb von Gemeinschaften von Kommunikationspartnern

vernünftigerweise einigen kann. So entsteht aus der Gesamtperspektive betrachtet eine Art Beliebigkeit verschiedener Wahrheiten.

Desinformationen sind auch deshalb besonders gefährlich, weil – empirisch nachgewiesen – selbst bei Personen, die motiviert sind, die korrekten Informationen zu kennen und zu verarbeiten, eine spätere Korrektur der Information nicht erfolgreich ist. Die falsche Information bleibt im Gedächtnis bestehen und bleibt nachhaltig besser abrufbar als die korrigierte.

Indem Social Bots vermeintliche Mehrheitsverhältnisse vortäuschen, können sie das öffentliche Meinungsklima erheblich beeinflussen. Nach der Theorie der „Schweigespirale" orientieren sich Menschen am Handeln anderer und tendieren dazu, sich der Mehrheitsmeinung anzuschließen. Die von Social Bots manipulierten Stimmungsbilder können in „etablierte" Medienöffentlichkeiten eingehen oder Grundlage von Big-Data-Analysen werden. Sie können insbesondere in Bezug auf singuläre Ereignisse, wie Wahlen oder Krisensituationen, zu erheblichen Verwerfungen führen.

Technische Gegenmaßnahmen

Technisch können wirksam nur die Betreiber von Social Networks Desinformation erkennen und bekämpfen, indem sie Inhalte und Accounts löschen. Sie könnten auf Beschwerden schnell reagieren, als Desinformation detektierte Inhalte auch in anderen Kommunikationen erkennen, ihre Herkunft feststellen und Accounts, von denen aus sie verbreitet werden, sperren oder löschen. Sie könnten auch – nach dem jeweiligen Stand der Technik – automatisierte Social Bots aufgrund spezifischer Verhaltensmuster automatisiert erkennen und nur zulassen, wenn diese gekennzeichnet sind, sodass Nutzer verstehen können, dass sie nicht mit einem Menschen, sondern mit einem Algorithmus kommunizieren. Die technischen Möglichkeiten, Desinformation und Verbreitungsformen automatisiert zu erkennen, werden immer besser, werden aber nie vollständig zuverlässig sein, weil auch die Gegenseite auf diese Möglichkeiten immer wieder reagiert. Sie können aber die Verbreitung von Desinformationen erheblich erschweren und helfen, in unklaren Fällen durch einen Entscheidungsvorschlag schnell zu reagieren.

Rechtliche Gegenmaßnahmen

Die Rechtsordnung enthält zwar geeignete Strafnormen, um gemeinschaftsschädliche und persönlichkeitsverletzende Aussagen zu bestrafen. Die Erzeuger von Desinformation können jedoch nur selten rechtlich zur Rechenschaft gezogen werden, weil sie unbekannt bleiben oder in einem sie schützenden Ausland agieren. Für die Strafverfolgung und für wirksame Gegenmaßnahmen sind die Betreiber von Social Networks diejenigen, die ausreichende Informationen und Handlungsmöglichkeiten haben, Desinformationen wirksam zu bekämpfen. Sie sind nach § 10 TMG auch verpflichtet, ihnen angezeigte Inhalte, die Strafnormen erfüllen, zu beseitigen. Diese Pflicht mit einem Beschwerdemanagementsystem auch tatsächlich umzusetzen und hierüber halbjährlich zu berichten, fordert seit 2018 das Netzwerkdurchsetzungsgesetz. Social Networks haben sich zu relevanten Foren der öffentlichen Kommunikation entwickelt, in denen Einfluss auf die öffentliche Meinungsbildung genommen wird. Hieraus resultieren eine besondere gesellschaftliche Verantwortung sowie rechtliche Pflichten, denen sie verstärkt nachkommen müssen – auch im Umgang mit Desinformation.

Jenseits des Strafrechts wird es schwieriger, Desinformationen rechtlich zu bekämpfen. Es gibt kein allgemeines Verbot zu lügen. Auch falsche Behauptungen können unter das Grundrecht der Meinungsfreiheit fallen. Maßnahmen gegen Desinformation müssen dieses Grundrecht beachten. Daher können nur begrenzt Systeme, die automatisiert über die Grundrechtsausübung entscheiden, eingesetzt werden. Sämtliche Regulierungsüberlegungen sind am von Artikel 5 Absatz 1 des Grundgesetzes angestrebten Ziel der Gewährleistung freier individueller und öffentlicher Meinungsbildung zu messen.

Soweit Desinformationen nicht extrem diskriminieren, muss eine rechtsstaatliche Demokratie sich mit ihnen im öffentlichen Meinungskampf auseinandersetzen.

Politische Gegenmaßnahmen

Neben den bisher schon ergriffenen Maßnahmen (z. B. Netzwerkdurchsetzungsgesetz) erfordert eine Verbesserung der Bekämpfung von Desinformation ein Bündel politischer Maßnahmen, zu denen die folgenden gehören können:

- Um eine Übernahme von Desinformation in etablierte Medien zu verhindern, ist die strikte Einhaltung der publizistischen Grundsätze gemäß Pressekodex zu fordern, die für die Rezipienten den Unterschied zu Desinformation deutlich macht.
- Die Landesmedienanstalten müssen gegenüber Telemedienanbietern mit journalistisch-redaktionellen Angeboten bei Verstößen gegen die Wahrheitspflichten Anordnungen treffen können. Ihre Aufsichtsbefugnisse sollten dahingehend erweitert werden.
- Bezogen auf Social Networks ist der geltende zivil- und strafrechtliche Rechtsrahmen besser durchzusetzen. Vor allem sollten sie neben den gemeldeten, rechtswidrigen Inhalten auch anders formulierte, aber inhaltsgleiche Inhalte entfernen müssen. Soweit sie automatisierte Verfahren zur Erkennung und Verhinderung von rechts- und

vertragsverletzenden Inhalten einsetzen, sollten sie ihre Standards und Kriterien transparent machen müssen. Außerdem sind ihre Betreiber zur besseren Zusammenarbeit mit den Strafverfolgungsbehörden zu verpflichten. Für bestimmte strafbare Inhalte sind Anzeigepflichten und die Aufdeckung der Akteure vorzusehen.

- Für Social Bots (wie im Entwurf des Medienstaatsvertrags) und Microtargeting sind – im Rahmen des Möglichen – Kennzeichnungspflichten vorzusehen.
- Zum Schutz der Meinungsfreiheit sollten die Betreiber von Social Networks ein wirksames und schnelles Beschwerdeverfahren für zu Unrecht gesperrte oder gelöschte Inhalte vorsehen. Außerdem sollten sie eine Selbstregulierungsstelle „Desinformation" einrichten müssen, die Anbieter in der Bewertung von Informationen unterstützen und Kampagnen gegen Desinformation durchführen.
- Notwendig ist eine Steigerung von Medienkompetenz, zu der auch die Sensibilisierung gegenüber Desinformation und eine Vermittlung der Charakteristik journalistischer Qualitätsstandards gehören.
- Öffentliche Stellen sollten Hinweise für Bürger anbieten, wie Desinformationen erkannt werden können und wie mit Desinformationen umzugehen ist: nicht weiterverbreiten, Freunde warnen, dem Betreiber des Social Networks melden, Anzeige erstatten.
- Öffentliche Stellen sollten zivilgesellschaftliches Engagement unterstützen – insbesondere Initiativen zum Fact-Checking und zum Betrieb von Empfehlungssystemen für geprüfte Nachrichten.
- Es sind technische und interdisziplinäre Forschungsprojekte zu fördern, die die Erkenntnisse verschiedener Disziplinen wie Technik, Journalistik, Psychologie, Recht zusammenbringen, um gesamthaft wirksame und umsetzbare Lösungen zu entwickeln. Es ist zu erforschen, wie technisch – auch mit Künstlicher Intelligenz – Desinformationen, Manipulationen, Deep Fakes, Trolle und Malicious Social Bots und ihre Verbreitungswege erkannt, gekennzeichnet, gesperrt und gelöscht werden können. Forschungsprojekte sollten sozialwissenschaftlich Charakteristika von Desinformationen und ihre Wirkungen auf Einzelne und die Gesellschaft untersuchen sowie politische und rechtliche Gegenmaßnahmen erforschen, die eine wirksame Bekämpfung von Desinformationen bewirken, ohne Meinungsfreiheit und legitime demokratische Auseinandersetzungen zu behindern. Für diese Forschung sollten die Betreiber von Social Networks (zu diesem Zweck geschützt) ausreichende Mengen an – anonymisierten oder pseudonymisierten – Kommunikationsdaten aus ihren Netzwerken zur Verfügung stellen (müssen).

Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat

Seit Oktober 2018 unterstützt die Wissenschaftliche Arbeitsgruppe den Nationalen Cyber-Sicherheitsrat. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Mitglieder der Wissenschaftlichen Arbeitsgruppe sind: Prof. Dr. Alexander Roßnagel (Hauptautor dieses Impulspapiers), Prof. Dr. Claudia Eckert, Dr. Timo Hauschild, Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Michael Waidner