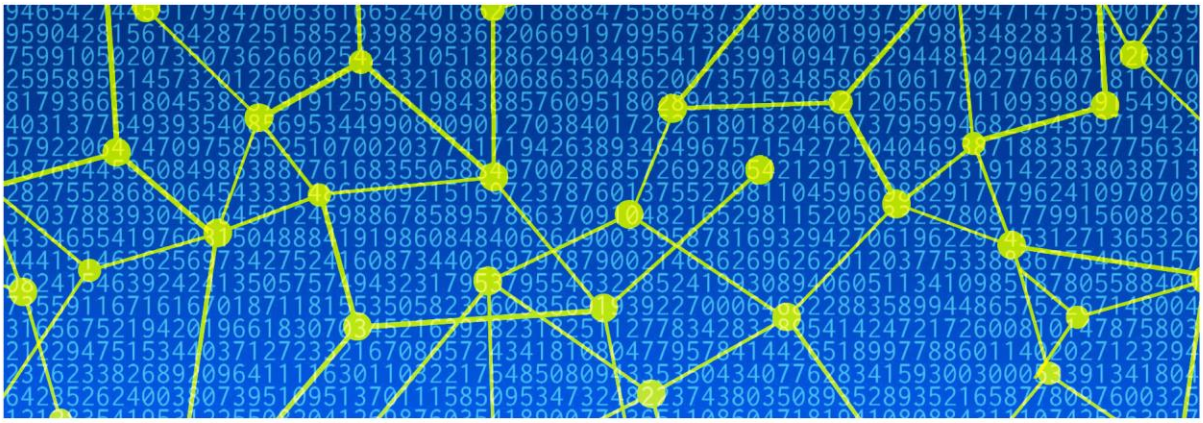

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 3/2018

Stellungnahme des EDSB zu Online-Manipulation und personenbezogenen Daten

EDPS

19. März 2018

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und speziell mit einem konstruktiven und proaktiven Vorgehen beauftragt. In seiner im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

Zusammenfassung

Die Digitalisierung von Gesellschaft und Wirtschaft hat uneinheitliche Auswirkungen auf das bürgerschaftliche Engagement bei der Entscheidungsfindung und auf die Hindernisse für die Beteiligung der Öffentlichkeit an demokratischen Prozessen.

Dank Big-Data-Analysen und Systemen der künstlichen Intelligenz ist es nun möglich, große Datenmengen zu sammeln, zu kombinieren, zu analysieren und unbegrenzt zu speichern. In den letzten zwei Jahrzehnten hat sich für die meisten webbasierten Dienste ein vorherrschendes Geschäftsmodell herausgebildet, das darauf beruht, Menschen online nachzuverfolgen und Daten über ihren Charakter, ihre Gesundheit, ihre Beziehungen und Gedanken und Meinungen zu sammeln, um digitale Werbeeinnahmen zu generieren. Diese digitalen Märkte haben sich um einige wenige Unternehmen gruppiert, die als effektive „Türöffner" zum Internet fungieren und über höhere inflationsbereinigte Marktkapitalisierungswerte verfügen als alle anderen Unternehmen seit Beginn der Aufzeichnungen.

Dieses digitale Ökosystem hat 50 % der Weltbevölkerung im Internet verbunden, wenngleich dies in Bezug auf Geografie, Vermögen und Geschlecht sehr ungleichmäßig geschah. Der anfängliche Optimismus hinsichtlich des Potenzials von Internet-Tools und sozialen Medien für das bürgerschaftliche Engagement ist der Sorge gewichen, dass Menschen manipuliert werden – erstens, indem kontinuierlich oftmals sehr vertrauliche Informationen über sie gesammelt werden, und zweitens, indem die Informationen, die sie online sehen, je nach der Kategorie, in der sie sich befinden, kontrolliert werden. Für viele algorithmengetriebene Dienste ist virale Empörung ein wichtiger Werttreiber geworden, mit Produkten und Anwendungen, die darauf ausgelegt sind, die Aufmerksamkeit und das Suchtverhalten zu maximieren. Die Vernetztheit hat – zumindest im Rahmen des aktuellen Modells – zu Spaltung geführt.

Die anschließende Debatte drehte sich um die irreführenden, falschen oder verunglimpfenden Informationen („Inhalte"), die den Menschen mit der Absicht zugeleitet wurden, den politischen Diskurs und die Wahlen zu beeinflussen – ein Phänomen, das als „Fake News" oder „online verbreitete Desinformation" bezeichnet wird. Die Lösungsansätze konzentrierten sich auf Transparenzmaßnahmen, bei denen die Informationsquelle aufgedeckt wurde, während gleichzeitig die Rechenschaftspflicht der Akteure im Ökosystem, die von schädlichem Verhalten profitieren, vernachlässigt wurde. Mittlerweile stellen Marktkonzentration und die zunehmende Plattformdominanz eine neue Bedrohung für den Medienpluralismus dar. Für den EDSB veranschaulicht diese Vertrauenskrise in das digitale Ökosystem die gegenseitige Abhängigkeit von Privatsphäre und Meinungsfreiheit. Die Einschränkung der Intimsphäre der Menschen infolge der unvermeidlichen Überwachung durch Unternehmen und Staaten hat eine abschreckende Wirkung auf die Fähigkeit und Bereitschaft der Menschen, frei ihre Meinung zu sagen und Beziehungen zu knüpfen, auch in dem für die Gesundheit der Demokratie so wichtigen Bereich des bürgerschaftlichen Engagements. Diese Stellungnahme befasst sich daher mit der Art und Weise, wie personenbezogene Daten verwendet werden, um Einzelpersonen und Gruppen mit spezifischen Inhalten zu erreichen, mit den auf dem Spiel stehenden Grundrechten und Werten und mit den einschlägigen Gesetzen zur Eindämmung der Bedrohungen.

Der EDSB setzt sich seit mehreren Jahren für eine stärkere Zusammenarbeit zwischen den Datenschutzbehörden und anderen Regulierungsbehörden ein, um die Rechte und Interessen des Einzelnen in der digitalen Gesellschaft zu schützen, weshalb im Jahr 2017 das Digital Clearinghouse ins Leben gerufen wurde. Angesichts der Befürchtung, dass politische

Kampagnen den digitalen Raum nutzen könnten, um bestehende Gesetze zu umgehen[1], halten wir es für an der Zeit, diese Zusammenarbeit auf die Wahlaufsichtsbehörden und Regulierungsbehörden für audiovisuelle Medien auszudehnen.

INHALT

1. Warum wir diese Stellungnahme veröffentlichen

i. Intensive öffentliche Debatte

Derzeit gibt es eine intensive öffentliche Debatte darüber, wie sich das umfassende und komplexe Ökosystem digitaler Informationen sowohl auf die Marktwirtschaft als auch auf die politische Ökonomie auswirkt, und wie das politische Umfeld mit der Wirtschaft interagiert. Die großen Plattformen stehen im Zentrum dieses Ökosystems. Sie profitieren in überproportionaler Weise vom Wachstum der digitalen Werbung und steigern ihre relative Macht im Laufe der Zeit. Personenbezogene Daten werden benötigt, um Nachrichten an Einzelpersonen in Segmente zu unterteilen, zu fokussieren und zu personalisieren, doch die meisten Werbekunden wissen nicht, wie derartige Entscheidungen getroffen werden, und die meisten Einzelpersonen wissen nicht, wie diese Daten verwendet werden. Das System belohnt spektakuläre und virale Inhalte und unterscheidet im Allgemeinen nicht zwischen kommerziellen und politischen Werbekunden. Enthüllungen darüber, wie gezielte Desinformation („Fake News“) über dieses System verbreitet wurde, haben zu Befürchtungen geführt, dass die Integrität von Demokratien bedroht sein könnte. Systeme der künstlichen Intelligenz, deren Markt ebenfalls durch Konzentration gekennzeichnet ist, sind selbst datengetrieben und werden – sofern sie keiner Kontrolle unterworfen sind – die Praxisferne und mangelnde Rechenschaftspflicht bei der Entscheidungsfindung in diesem Umfeld noch verstärken.

ii. Bedeutung des Datenschutzrechts und politischer Kampagnen

Die Grundrechte auf Schutz der Privatsphäre und Datenschutz sind eindeutig ein entscheidender Faktor, um dieser Situation abzuhelfen, weshalb dieses Thema für alle unabhängigen Datenschutzbehörden eine strategische Priorität darstellt. In ihrer *Resolution zur Verwendung von Personendaten für die politische Kommunikation* von 2005 haben die Datenschutzbeauftragten wichtige weltweite Datenschutzfragen im Zusammenhang mit der zunehmenden Verarbeitung personenbezogener Daten durch nichtkommerzielle Akteure formuliert. Darin bezog sie sich insbesondere auf die Verarbeitung sensibler Daten „wie Informationen über – tatsächliche oder bloß vermutete – ethische oder politische Überzeugungen oder Aktivitäten oder über das Wahlverhalten“ und die Erstellung invasiver Profile von verschiedenen Personen, die derzeit „klassifiziert werden – manchmal unzutreffenderweise oder auf der Grundlage eines flüchtigen Kontakts – als solche, die mit einer bestimmten politischen Strömung sympathisieren, sie unterstützen, ihr angehören oder gar Parteimitglieder sind“.[2] In der internationalen Resolution wird eine strengere Durchsetzung der Datenschutzbestimmungen in Bezug auf Datenminimierung, rechtmäßige Verarbeitung, Einwilligung, Transparenz, Rechte der betroffenen Personen, Zweckbindung und Datensicherheit gefordert. Möglicherweise ist nun die Zeit gekommen, um diese Forderung zu erneuern.

Die EU-Rechtsvorschriften über den Datenschutz und die Vertraulichkeit der elektronischen Kommunikation gelten für die Datenerhebung, die Profilerstellung und das Mikrotargeting und sollten bei ordnungsgemäßer Durchsetzung dazu beitragen, den Schaden durch Versuche, Einzelpersonen und Gruppen zu manipulieren, zu minimieren. Politische Parteien, die in der EU Wählerdaten verarbeiten, fallen in den Anwendungsbereich der DSGVO. In der DSGVO sind personenbezogene Daten, die politische Meinungen offenbaren, als besondere Datenkategorien definiert. Die Verarbeitung dieser Daten ist grundsätzlich untersagt, es sei

denn, es gilt eine der aufgeführten Ausnahmen. Im Zusammenhang mit politischen Kampagnen sind die beiden folgenden Ausnahmen besonders relevant und verdienen es, vollständig zitiert zu werden:

> *(d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,*
>
> *(e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat, [...]*
>
> *(g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich.*

Erwägungsgrund 56 erläutert Absatz 9 Nummer 2 Buchstabe g: „Wenn es in einem Mitgliedstaat das Funktionieren des demokratischen Systems erfordert, dass die politischen Parteien im Zusammenhang mit Wahlen personenbezogene Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen des öffentlichen Interesses zugelassen werden, sofern geeignete Garantien vorgesehen werden."

Mehrere Datenschutzbehörden haben Vorschriften oder Leitlinien zur Datenverarbeitung für politische Zwecke entwickelt:

- Im März 2014 verabschiedete die italienische Datenschutzbehörde Vorschriften für die Verarbeitung personenbezogener Daten durch politische Parteien. In den Vorschriften wird auf das allgemeine Verbot hingewiesen, personenbezogene Daten, die im Internet veröffentlicht wurden, wie z. B. in sozialen Netzwerken oder Foren, zu Zwecken der politischen Kommunikation zu nutzen, wenn diese Daten für andere Zwecke erhoben wurden.[3]

- Im November 2016 legte die französische nationale Datenschutzkommission (CNIL) ergänzende Leitlinien zu ihren Empfehlungen für die politische Kommunikation von 2012 vor, in denen die Vorschriften für die Verarbeitung personenbezogener Daten in sozialen Netzwerken festgelegt sind. Insbesondere betonte die CNIL, dass die Zusammenführung personenbezogener Daten von Wählern zwecks Erfassung und Nutzung ihrer Profile in sozialen Netzwerken nur dann rechtmäßig sein kann, wenn sie sich auf die Einwilligung als Grundlage für die Datenverarbeitung stützt.[4]

- Im April 2017 veröffentlichte die britische Datenschutzbehörde Information Commissioner's Office (ICO) aktualisierte Leitlinien für politische Kampagnenführung (*Guidance on political campaigning*), die auch Leitlinien für den Einsatz von Datenanalysen im Rahmen politischer Kampagnen umfasst. Die ICO erklärte, dass, wenn eine politische Organisation ein Drittunternehmen mit der

> Durchführung von Analysen beauftragt, es sich bei diesem Unternehmen wahrscheinlich um einen Auftragsverarbeiter handele, während die Organisation ein für die Verarbeitung Verantwortlicher sei. Um die Rechtmäßigkeit der Verarbeitung sicherzustellen, sind besondere datenschutzrechtliche Bestimmungen, die das Verhältnis zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter regeln, zu berücksichtigen.[5]

Die Leitlinien der nationalen Datenschutzbehörden können eine zusätzliche verbindliche Auslegung der datenschutzrechtlichen Bestimmungen ermöglichen, die den Unterschieden in der Organisation der nationalen politischen Systeme Rechnung trägt.[6]

iii. Zweck dieser Stellungnahme des EDSB

Das Leitbild des Europäischen Datenschutzbeauftragten besteht darin, der EU zu helfen, im globalen Dialog über Datenschutz und Privatsphäre im digitalen Zeitalter mit gutem Beispiel voranzugehen, indem interdisziplinäre politische Lösungen für die Herausforderungen im Zusammenhang mit Big Data ermittelt werden und eine ethische Dimension für die Verarbeitung personenbezogener Daten entwickelt wird.[7] Wir haben gefordert, die betroffene Person „als Individuum und nicht nur als Verbraucher oder Nutzer“ zu behandeln, und haben ethische Fragen im Zusammenhang mit den Auswirkungen von prediktiver Profilerstellung und durch Algorithmen bestimmter Personalisierung aufgeworfen.[8] Wir haben eine verantwortungsvolle und nachhaltige Entwicklung der digitalen Gesellschaft gefordert, die auf individueller Kontrolle der sie betreffenden personenbezogenen Daten, datenschutzbewusster Technik, Rechenschaftspflicht und kohärenter Durchsetzung beruht.[9] Die Ethik-Beratergruppe des EDSB stellte in ihrem Bericht vom Januar 2018 fest, dass das Mikrotargeting der Wahlwerbung die Regeln der öffentlichen Rede verändere und den Raum für Diskussionen und den Austausch von Ideen verringere, weshalb eine demokratische Debatte über die Nutzung und Verwertung von Daten für politischen Wahlkampf und die politische Entscheidungsfindung dringend erforderlich sei.[10]

Diese Frage der Nutzung von Informationen und personenbezogener Daten zur Manipulation von Menschen und Politik geht natürlich weit über das Recht auf Datenschutz hinaus. Durch eine personalisierte, mikrozentrierte Online-Umgebung entstehen „Filterblasen“, in denen Menschen mit den „immergleichen“ Informationen konfrontiert werden und weniger Meinungen begegnen, was eine stärkere politische und ideologische Polarisierung zur Folge hat.[11] Dies führt zu einer stärkeren Verbreitung und Überzeugungskraft von Falschmeldungen und Verschwörungstheorien.[12] Untersuchungen deuten darauf hin, dass die Manipulation von Newsfeeds oder Suchergebnissen ihr Wahlverhalten beeinflussen könnte.[13]

Der EDSB möchte dazu beitragen, dass die Verarbeitung personenbezogener Daten – um es in den Worten der DSGVO zu sagen – im Dienste der Menschheit steht und nicht umgekehrt.[14] Der technologische Fortschritt soll nicht behindert, sondern gemäß unseren Werten gesteuert werden. Die Achtung der Grundrechte, einschließlich des Rechts auf Datenschutz, ist von entscheidender Bedeutung, um den fairen Charakter der Wahlen zu gewährleisten, und dies insbesondere mit Blick auf die Wahlen zum Europäischen Parlament im Jahr 2019.[15] Diese Stellungnahme ist die jüngste in einer Reihe von breit angelegten Arbeiten des EDSB zur Frage, wie der Datenschutz angewandt werden sollte, um den drängendsten Anliegen der öffentlichen Ordnung Rechnung zu tragen. Er baut auf den bisherigen Arbeiten des EDSB zu Big Data, digitaler Ethik und der Notwendigkeit der Koordinierung der Regulierung wettbewerbsfähiger und fairer Märkte auf.[16] Am Anfang der Stellungnahme steht eine Zusammenfassung des Prozesses, bei dem personenbezogene Daten den vorherrschenden

Zyklus von digitaler Nachverfolgung, Mikrotargeting und Manipulation antreiben und bestimmen. Anschließend wird auf die Rolle der verschiedenen Akteure im Ökosystem der digitalen Informationen eingegangen. Gegenstand der Stellungnahme sind ferner die auf dem Spiel stehenden Grundrechte, die einschlägigen Datenschutzgrundsätze und andere einschlägige rechtliche Verpflichtungen. Abschließend wird das Fazit gezogen, dass sich das Problem der Online-Manipulation nur noch verschärfen wird und dass einzelne Regulierungsansätze nicht ausreichen werden; daher wird dringend eine Zusammenarbeit der Regulierungsbehörden empfohlen, um nicht nur lokalen Missbrauch, sondern auch strukturelle Verzerrungen durch übermäßige Marktkonzentration zu bekämpfen.

2. Wie werden personenbezogene Daten genutzt, um das Online-Erlebnis zu bestimmen?

„Infonomics“ ist der Begriff, der Ende der 1990er Jahre geprägt wurde, als sich Unternehmen für den Wert und die Monetarisierbarkeit von Daten interessierten.[17] Der Besuch einer einzelnen Website führt heute typischerweise zur Offenlegung des Browserverhaltens gegenüber mehr als 100 Dritten, die ihre eigene rechtliche Haftung durch umfangreiche „Datenschutzrichtlinien“ einschränken wollen, die sich auf Hunderte von Seiten erstrecken können. Das dezentrale Internet der Vergangenheit wurde durch geschlossene „Communities“ ersetzt; diese werden von einigen wenigen großen Technologieunternehmen bewacht, die von den Nutzern ihrer Dienste die Preisgabe ihrer Identität und persönlichen Daten verlangen. Mitglieder dieser Communities sind dazu angehalten, innerhalb der Mauern zu bleiben, und auf verlinkte Inhalte Dritter kann nur innerhalb der Mauern zugegriffen werden.[18] Die Datenanalyse dient zur Interpretation großer Datenmengen, um Unternehmen und Staaten in die Lage zu versetzen, das Verhalten des Einzelnen beim Kauf und der Nutzung öffentlicher Dienstleistungen besser zu verstehen und zu beeinflussen. Wenngleich Techniken zur Aggregation und Anonymisierung eingesetzt werden, ist die Datenanalyse auf die Verarbeitung personenbezogener Daten angewiesen.[19]

Online-Manipulation kann als Höhepunkt eines dreistufigen Zyklus von der Datenerhebung (eine Form der Datenverarbeitung nach EU-Recht) über die Profilerstellung bis hin zu Mikrotargeting oder Personalisierung als Form der Manipulation angesehen werden, die in ihrem Ausmaß von harmlos bis sehr schädlich variieren kann.[20] Diese Phasen werden im Folgenden kurz beschrieben.

i. Datenerhebung

Datenerhebung ist eine Form der Datenverarbeitung nach EU-Recht.[21] Personenbezogene Daten werden aus einer Vielzahl von Quellen unter Verwendung verschiedener Techniken zur Zusammenführung von Datensätzen erhoben. Einige Daten werden von den betroffenen Personen bewusst zur Verfügung gestellt, z. B. durch das Ausfüllen eines Online-Formulars. Die meisten Daten werden jedoch automatisch erfasst oder aufgezeichnet; sie lassen sich als eine Art „digitaler Brotkrümel“ beschreiben, der als Ergebnis der Online- und Offline-Aktivitäten von Einzelpersonen unwissentlich hinterlegt wurde.[22] Zu den erfassten Daten gehören die Zeiten und Orte, an denen sich Mobilgeräte mit Mobilfunktürmen oder GPS-Satelliten verbinden, IP-Adressen der Endgeräte, WiFi-Zugriffspunkte, Browser-Verlauf, „Likes“ und „Shares“, von digitalen Videoüberwachungssystemen gesammelte Bilder, Kaufhistorie, Nutzung sozialer Medien und geräteübergreifendes Browsing-Verhalten.[23] Laut einer aktuellen Studie ist die Wahrscheinlichkeit der Verbreitung von Informationen, die als „falsch“ eingestuft werden, viel größer als die der Verbreitung verifizierter Informationen. Bots und Trolle, einschließlich derer, die im Namen feindlicher Drittstaaten handeln, tragen zu

dieser weiteren Verbreitung bei.[24] Eine wichtige Kategorie sind die Daten von Menschen, die an psychologischen Online-Frage-und-Antwort-Spielen teilnehmen, die oft virale Popularität erreichen, wenn sie über soziale Medien aufgerufen und geteilt werden. Die Ergebnisse eines Teilnehmers in Kombination mit den in sozialen Medien verfügbaren personenbezogenen Daten ermöglichen eine komplexe Persönlichkeitsprognose.[25]

Unternehmen nutzen Tracking-Technologien, um beobachtete Daten zu erfassen; dabei handelt es sich in der Regel um Cookies sowie um Flash-Cookies, Web-Beacons und Device Fingerprinting, die über verschiedene Geräte hinweg verfolgt werden können.[26] Mittlerweile bietet die Verbreitung vernetzter Dinge und im Haus installierter Abhörgeräte, wie z. B. intelligente Lautsprecher (der Markt ist bereits durch Konzentration gekennzeichnet), neue Möglichkeiten zur Beobachtung des privaten Verhaltens von Menschen in Echtzeit.[27] Wenn Nachrichten und Inhalte, die auf der Grundlage der Profilerstellung an eine Person gerichtet sind, eine Reaktion von dieser Person auslösen, wird wiederum diese Reaktion überwacht, wodurch zusätzliche Daten für die Erfassung und Verwendung zur Verfeinerung des Profils und der zukünftigen Zielgruppenansprache generiert werden.

ii. Profilerstellung

Erfasste personenbezogene Daten werden zur Segmentierung von Personen nach genauen Profilen ausgewertet. Es gibt eine Vielzahl von Merkmalen, die gemessen werden können und mit denen sich aus einem Nutzerprofil Präferenzen ableiten lassen, wie z. B. Alter, Geschlecht, Ort usw.[28] Schätzungen zufolge hat der größte Social-Media-Anbieter über 52 000 persönliche Merkmale verwendet, um die Interessen und Merkmale der Menschen zu klassifizieren. Anschließend werden statistische Methoden verwendet, um analytische Informationen zu generieren oder um zukünftige Verhaltensweisen oder Entwicklungen vorherzusagen.[29] Durch die automatisierte Profilerstellung werden Muster identifiziert, die für das menschliche Auge unsichtbar sind.[30] Je mehr Nutzerdaten über eine Person verfügbar sind und je länger ein Nutzer in einem Profil erfasst werden kann, desto umfangreicher sind die Rückschlüsse, die sich aus dem Profil der Person ziehen lassen.[31] Fortgeschrittenere Methoden der Profilerstellung erlauben es, Personen anhand von Referenzwerten vordefinierter Verhaltensmuster zu erfassen oder zu bewerten. Ein Beispiel für solche Anwendungen ist eine Recruiting-Software, die die Stimme eines Bewerbers analysiert, um Sprachkenntnisse, Redegewandtheit, kritisches Denken und aktives Zuhören zu bewerten.[32] Ein weiteres Beispiel ist, wie Vertrauen, Nervosität, Traurigkeit und Müdigkeit einer Person anhand ihrer Tippmuster auf der Computertastatur vorhergesagt werden können. Ein besonderes Merkmal solcher Rückschlüsse ist, dass hochsensible Daten wie der emotionale Zustand einer Person aus scheinbar unsensiblen Informationen, wie z. B. der Dynamik ihres Tastenanschlags vorhergesagt werden können.[33]

In Kombination mit der Verhaltensforschung ermöglichen Big Data Rückschlüsse auf noch detailliertere Persönlichkeitsportraits. Einige Datenanalyse-Unternehmen sind darauf spezialisiert, Personen anhand von fünf Persönlichkeitsmerkmalen zu bewerten, die als „Big Five“ bzw. OCEAN bekannt sind. Dabei werden Daten aus Online-Persönlichkeitstests (siehe oben) verwendet – eine Methode, die im US-Präsidentschaftswahlkampf von 2016 und im Vorfeld des britischen Brexit-Referendums verwendet worden sein soll.[34] Diese Bewertungen werden dann durch weitere Merkmale ergänzt, darunter Werte, Bedürfnisse, Likes und Shares.[35] Die Profilerstellung dient außerdem zur Identifizierung anderer Personen, die an einem Produkt und einer Dienstleistung interessiert sein könnten, nämlich „Lookalike Audiences“ und Kunden der großen Social-Media-Plattformen.[36]

Die Qualität des neuen Wissens, das als Ergebnis der Profilerstellung entsteht, ist Gegenstand von Diskussionen. Bestimmte Studien zeigen, dass Data-Mining-Techniken die Persönlichkeit eines Menschen genauer vorhersagen können als die meisten seiner Freunde und Familienangehörigen.[37] Andere betrachten die Profilerstellung als situativ und von Natur aus probabilistisch.[38] In jedem Fall ist der Einfluss der Profilerstellung auf das Leben einer Person nicht vernachlässigbar, da das erzeugte Wissen weiter genutzt wird, um Entscheidungen (automatisiert oder nicht) über eine Person oder eine Gruppe von Personen zu treffen.

iii. Mikrotargeting und Manipulation

Entscheidungen, die auf Profilerstellung basieren, personalisieren das Informationsumfeld einer Person mit einem hohen Grad an Personalisierung, einer Praxis, die als Mikrotargeting bezeichnet wird.[39] Sie kann in einer persönlicheren Botschaft an ein Personensegment bestehen, das bestimmte Eigenschaften teilt, oder sogar potenziell die Preise für Produkte oder Dienstleistungen bestimmen. Sie kann in einer Methodik bestehen, nach der Social-Media-Plattformen bestimmen, welche Inhalte in welcher Reihenfolge in den einzelnen Newsfeeds erscheinen.

Unternehmen, die digitale Werbeflächen verkaufen, profitieren von der Platzierung gezielter Inhalte unabhängig von ethischen Überlegungen: Es wird nicht zwischen einem guten und einem schlechten Klick von einer Zielgruppe unterschieden.[40] Diese Mikrotargeting-Aktivitäten mögen bei manchen Menschen zwar wenig Wirkung zeigen, doch die Komplexität der Technologie, das geringe Maß an Vertrauen und die erklärten Absichten einiger wichtiger Tech-Player deuten auf eine Kultur der Manipulation in der Online-Umgebung hin.[41] Diese Manipulation kann durch die von den Marktteilnehmern selbst gewählten Geschäftsstrategien oder durch die Handlungen von Einzelpersonen und Staaten erfolgen, die versuchen, Plattformen zu nutzen, um Märkte und den öffentlichen Diskurs zu stören oder zu untergraben.

Darüber hinaus war die Absicht hinter dem Design von Geräten und Software, süchtig machendes Verhalten zu induzieren. Funktionen wie Auto-Play, endlose Newsfeeds, Benachrichtigungen und „Streaks“ (ununterbrochener Austausch von Nachrichten oder Bildern) sind nach Ansicht einiger ehemaliger Mitarbeiter in der Technologiebranche bewusste Versuche, die Aufmerksamkeit durch Mikrotargeting in Bezug auf Nutzer, insbesondere Kinder, zu maximieren, ähnlich den von der Glücksspielindustrie verwendeten Techniken.[42] Webbasierte Dienste, die Netzwerkeffekte erzielt haben, appellieren explizit an die „Angst vor dem Verpassen“, wenn die App nicht regelmäßig überprüft wird.[43]

Die Manipulation erfolgt auch in Form einer auf Mikrozielgruppen zugeschnittenen, gemanagten Darstellung von Inhalten, die für den Einzelnen als „relevant“ dargestellt werden, aber zur Umsatzmaximierung für die Plattform bestimmt ist. Dies ist vergleichbar mit den „geheimen Menüs“, die zur Steuerung der Nutzer von E-Commerce-Websites verwendet werden, und den „dunklen Mustern“, die dazu dienen, Entscheidungen, die aus Sicht der Plattform weniger wünschenswert sind (wie z. B. es abzulehnen, zusätzliche Artikel, wie Versicherungen, in einen Einkaufswagen zu legen), abzuwenden.

Die wichtigsten Plattformen gaben 2017 zu, dass über 125 Millionen Menschen in den Vereinigten Staaten durch „polarisierende“ Inhalte – Werbeanzeigen und Nachrichten von gefälschten Konten – erreicht wurden. In weiteren Berichten, die kurz vor Veröffentlichung dieser Stellungnahme herausgegeben wurden, wurde ein weitaus größeres Ausmaß an Einmischung behauptet, wenngleich die genauen Auswirkungen auf das tatsächliche Abstimmungsverhalten noch nicht bekannt sind.[44] Eine bedeutendere und chronischere Form

der Manipulation kann jedoch in der abschreckenden Wirkung auf die Meinungsfreiheit bestehen, die aus der ständigen Überwachung resultiert, die für das digitale Ökosystem kennzeichnend ist.[45]

3. Das digitale (Fehl-)Informations-Ökosystem

Manipulationen und Fehlinformationen sind so alt wie die Menschheit, aber mit der rasanten Digitalisierung sind sie zu Fragen von drängender gesellschaftlicher, rechtlicher und ethischer Bedeutung geworden. Man hatte gehofft und erwartet, dass neue Formen des bürgerschaftlichen Engagements gedeihen würden, da mehr Menschen mit dem Internet verbunden sind – durch Online-Kampagnen, Crowdsourcing und verursachergerechte Communities in sozialen Medien.[46] Die Nachhaltigkeit des Mikrotargeting ist derzeit jedoch Gegenstand hitziger Diskussionen.[47]

Die Manipulation mittels Mikrotargeting setzt die Existenz und den Zugriff auf die Datenbanken mit einer Vielzahl von Datenpunkten über Personen und Lösungen für geistiges Eigentum in Form von analytischen Algorithmen voraus, die Rückschlüsse und Vorhersagen über Personen ermöglichen können, die diese Daten verwenden. Hierbei handelt es sich um einen vielschichtigen Prozess, in dem zwei Gruppen von Akteuren interagieren:

- das Werbe-Ökosystem, das sich auf die Erhebung und Analyse persönlicher Daten als vorherrschendes Geschäftsmodell stützt,
- nichtkommerzielle Werbekunden.

Im Rahmen der künstlichen Intelligenz entsteht gerade ein dritter großer Akteur, der die Grenzen der Verantwortlichkeit weiter verwischt. Die Komplexität dieses umfassenden digitalen Ökosystems, das sich aus Unternehmen und Organisationen zusammensetzt, die in der Vergangenheit durch verschiedene Rechtsgebiete (Verbraucherrecht, Wahlrecht, Medienrecht, Wettbewerbsrecht usw.) reguliert wurden, macht es schwieriger, jedem von ihnen die rechtliche Verantwortung zu übertragen, die bestehenden Regeln durchzusetzen und sicherzustellen, dass dem Einzelnen im Falle eines Missbrauchs ein wirksamer Rechtsbehelf zur Verfügung steht.

i. Plattformvermittler im Zentrum der digitalen Werbung

Eine sehr kleine Anzahl von Branchenriesen hat sich zu einem effektiven Gatekeeper der digitalen Inhalte, die die meisten Menschen konsumieren, entwickelt. Diese Unternehmen nehmen unter einer Vielzahl anderer Akteure, darunter Werbeunternehmen, Datenbroker und Datenanalysefirmen, eine dominierende Position ein. In der EU-Bürgerbefragung 2015 gaben mehr als sieben von zehn Befragten (72 %) an, Internetplattformen als Informationsquelle zu nutzen. In Europa wird derzeit mehr als ein Drittel der Werbeausgaben für digitale Kanäle ausgegeben, das ist mehr, als für Fernsehwerbung ausgegeben wird (wenngleich es erhebliche regionale Unterschiede gibt). Im Vereinigten Königreich, einem der fortschrittlichsten digitalen Märkte, gehen mehr als 50 % aller Werbeausgaben an Online-Kanäle[48], wobei Zeitungen (63 %) und Fernsehen (62 %) die zweit- und drittbeliebtesten Informationsquellen zu EU-Angelegenheiten waren.[49] Ein Großteil des Suchverkehrs ist auf Smartphones migriert, wo das größte Unternehmen über einen Marktanteil von 97 % verfügt. Werbekunden, die eine der beiden großen Plattformen nutzen, die als „Duopol“ bezeichnet werden, weil sie zwischen 80 % und 99 % des gesamten Umsatzwachstums im Bereich der digitalen Werbung ausmachen, können nicht kontrollieren, wo ihre Werbung platziert wird. Mittels undurchsichtiger Algorithmen wurden solche Anzeigen auf Websites mit rassistischen,

hetzerischen oder anstößigen Inhalten platziert, was dazu führte, dass sich eine Reihe großer Werbekunden von programmgesteuerten Anzeigenmärkten zurückgezogen haben, auf denen Software zum Kauf und Verkauf von Werbung eingesetzt wird.[50] In vielen Ländern ist eines der beiden größten Technologieunternehmen zum einzigen Tor zum Internet geworden.[51] Es gibt einen Rückgang der Kapitalinvestitionen in Start-Ups (minus 40 % seit 2015), was darauf hindeutet, dass Investoren weniger Spielraum für Störungen im konzentrierten Markt sehen.[52]

Die Datenanalyse könnte dem Einzelnen helfen, sich in der immer lauter werdenden Informationsumgebung zurechtzufinden. Tatsächlich hat sich das Nutzen-Gleichgewicht von der individuellen, vertiefenden Informationsasymmetrie zu den Eigentümern proprietärer Algorithmen verschoben. Indem die Exposition gegenüber bestimmten Informationen, beispielsweise in Stellenanzeigen, auf der Grundlage des Geschlechts oder des abgeleiteten Gesundheitsstatus eingeschränkt wird, können sich diskriminierende Einstellungen und Praktiken weiter festigen.[53] Das Forum des öffentlichen Diskurses und der zur Verfügung stehende Raum für Meinungsfreiheit wird nun durch die Profitmotive mächtiger Privatunternehmen begrenzt, die aufgrund der technischen Komplexität oder aus Gründen des Geschäftsgeheimnisses nicht erklären wollen, wie Entscheidungen getroffen werden. Die wenigen großen Plattformen mit ihrer außergewöhnlichen Reichweite bieten daher für Menschen, die das System für böswillige Zwecke nutzen wollen, ein einfaches Ziel.

ii. Nichtkommerzielle Werbekunden

Werbekunden sind nicht auf wirtschaftliche Akteure beschränkt, die Kundenwissen erschließen möchten.[54] Staaten, politische und ideologische Bewegungen, politische Parteien, Kampagnen, Bewerber für ein politisches Amt und andere ursachenorientierte Organisationen haben immer versucht, ihre Botschaft zu verbreiten, Freiwillige zu rekrutieren, Spender anzuwerben und auf andere Weise die öffentliche Meinung zu beeinflussen und sowohl online als auch offline Communities aufzubauen. Sie werden als „nichtkommerzielle Werbekunden“ bezeichnet, da ihr Ziel nicht darin besteht, ein kommerzielles Produkt oder eine Dienstleistung zu verkaufen oder zu bewerben, sondern ihre Botschaft zu vermitteln, um politische, soziale oder andere Ansichten von Einzelpersonen zu beeinflussen und für oder gegen die Unterstützung einer Sache oder die Teilnahme an einer Wahl Stimmung zu machen.[5556]

Bis vor kurzem hatten nichtkommerzielle Werbekunden nur begrenzten Zugang zu Daten über ihren Wahlkreis. Inzwischen haben sie begonnen, das gleiche zielgerichtete Internet-Werbesystem zu nutzen, das von kommerziellen Unternehmen verwendet wird, indem sie die Reaktionen und Diskussionen in sozialen Medien in Echtzeit analysieren und Daten aggregieren und aus diesen Daten einen „Wert“ extrahieren, wie etwa Rückschlüsse auf Persönlichkeitsmerkmale und wahrscheinliches Wahlverhalten der Wähler. Viele staatliche Institutionen, politische und andere Interessengruppen verfügen über eigene Websites, die in größerem oder geringerem Umfang Tracking-Technologien verwenden. Sie sind auch aktiv in den sozialen Medien präsent und nutzen die Zielgruppenansprache-Tools der Online-Unternehmen.[57] Nichtkommerzielle Werbekunden interagieren mit den Social-Media-Plattformen, wie z. B. „Fanpages“ oder „Gruppen“ in sozialen Medien, die integrierte Werbe- und Publikationswerkzeuge anbieten. Administratoren von Fanseiten können Statistiken abrufen und unter den Followern von Fanseiten und unter allen Plattformnutzern auf der Grundlage von Demografie, Interesse, Verhalten oder anderen Kriterien Zielgruppen auswählen, um die Plattform-Nachrichten besser zu personalisieren. Anschließend können sie die Nachrichten, die an die Zielgruppe zurückgesendet werden, je nach Profil und Standort anpassen.[58] Wie diese Werkzeuge eingesetzt werden, ist von Land zu Land und je nach Art der Organisation unterschiedlich.[59] In jedem Fall verschwimmen die Grenzen zwischen

„kommerziellen“ und „politischen“ Daten: Während in der traditionellen politischen Forschung die Wählerregistrierung und die Parteizugehörigkeit betrachtet wurde, verarbeiten Datenanalysten nun alle Informationen, die Persönlichkeitsmerkmale offenbaren.

Politische Kampagnen verlassen sich zunehmend auf Big Data-Analyse, um durch gezielte Botschaften oder Online-Werbung Meinungen und Abstimmungsverhalten zu beeinflussen. In vielen Fällen geht es darum, Menschen mit irreführenden Informationen anzusprechen.[60] Ob KI und Big Data in der Lage sind, signifikante demokratische Prozesse, insbesondere außerhalb der Vereinigten Staaten, zu beeinflussen, ist umstritten. Verfügbare empirische Belege aus Praktiken des politischen Wahlkampfs in den Niederlanden und Deutschland zeigen ein nur geringes Interesse an Mikrotargeting-Praktiken, was auf praktische Einschränkungen zurückzuführen ist, zu denen mangelndes Fachwissen, fehlende Mittel, Besonderheiten der lokalen Rechtsprechung oder der rechtliche Rahmen selbst gehören.[61] In der laufenden Untersuchung der britischen Datenschutzbeauftragten und einer parallelen Untersuchung der Wahlkommission zu angeblichen Fällen von Datenschutzmissbrauch bei Kampagnen während des Brexit-Referendums werden dagegen die Aktivitäten von 30 Organisationen untersucht, darunter politische Parteien und Kampagnen, Datenunternehmen und Social-Media-Plattformen.[62] Unabhängig von ihrer Wirksamkeit gibt es ein deutliches Interesse seitens nichtkommerzieller Werbekunden, die ursprünglich für den kommerziellen Bereich entwickelten Zielgruppenansprache-Techniken zu erforschen.[63]

iii. Künstliche Intelligenz

In diesem digitalen Ökosystem werden durch automatisierte Systeme in zunehmendem Maße die Kommunikation zwischen Einzelpersonen, Unternehmen und Staaten vermittelt und neue maschinengenerierte Inhalte produziert. Künstliche Intelligenz wird zur präzisen Beobachtung, Überwachung, Filterung und Zensur von Nachrichten zwischen Nutzern von Nachrichtenübermittlungsanwendungen eingesetzt.[64] Algorithmen für maschinelles Lernen sollen ein Maximum an Aufmerksamkeit und Likes erzeugen, was Medien manipulationsanfällig macht.[65] Social-Media-Bots, die Nachrichten verzerren oder Wut oder Dissens schüren, können autonom oder von Menschen gesteuert sein.[66] Anspruchsvollere Anwendungen der künstlichen Intelligenz, wie Deepfakes, Sprachsimulation und automatisierte Nachrichtenberichterstattung, dürften in diesem Ökosystem an Bedeutung gewinnen, da ihr Einsatz immer kostengünstiger wird, sofern keine erfolgreichen Gegenmaßnahmen ergriffen werden. Die automatische Nachrichtenanpassung, die bereits im kommerziellen Bereich verbreitet ist, könnte, wenn sie auf die politische Sphäre angewendet wird, theoretisch dazu führen, dass die Webseite eines Bewerbers für ein politisches Amt oder einer Partei ihren Inhalt an die bekannten politischen Präferenzen des Besuchers anpasst. Außerdem könnten Hindernisse für qualitativ hochwertige Forschungs- und Rechenschaftsinitiativen geschaffen werden, deren Ziel es ist zu verfolgen, inwieweit politische Kandidaten ihre Versprechen einhalten, nachdem sie ein politisches Amt übernommen haben.[67]

Künstliche Intelligenz ist skalierbar und somit sind diesen Trends keine Grenzen gesetzt. Das Verhältnis zwischen Technologie und Politik ist symbiotisch, wobei der Zugang zu und die Kompetenz im Umgang mit Technologie das Machtgleichgewicht zwischen Staaten und zwischen Regimes und Protestbewegungen bestimmen.[68]

4. Die Grundrechte und Werte, um die es geht

Mikrotargeting und Online-Manipulation beeinträchtigen offenbar in erheblichem Maße eine Reihe von Rechten und Freiheiten, die in der EU-Grundrechtecharta verankert sind.

i. Datenschutz und andere Freiheiten

Privatsphäre und der Schutz personenbezogener Daten sind Grundrechte gemäß Artikel 7 und 8 der EU-Grundrechtecharta. Artikel 7 schützt das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, während Artikel 8 ein eigenes Recht auf den Schutz personenbezogener Daten vorsieht. Die Unentbehrlichkeit persönlicher Informationen für das digitale Informationsökosystem setzt diese beiden Rechte offensichtlich unter Druck.

Die Privatsphäre und der Schutz personenbezogener Daten gehören zu den „Freiheiten" der EU, zu denen die Gedanken-, Gewissens- und Religionsfreiheit, die Meinungs- und Informationsfreiheit sowie die Versammlungs- und Vereinigungsfreiheit gehören (Artikel 10, 11 und 12). Diese stehen ebenfalls eindeutig auf dem Spiel, da die wichtigsten Plattformvermittler die Verbreitung von Informationen entweder erleichtern oder behindern können. Zum Beispiel werden Inhalte, die nicht von einer Internet-Suchmaschine gelistet oder hoch eingestuft werden, mit geringerer Wahrscheinlichkeit ein großes Publikum erreichen oder überhaupt gesehen werden. Alternativ kann ein Suchalgorithmus auch auf bestimmte Arten von Inhalten oder Anbieter von Inhalten ausgerichtet sein, wodurch die Gefahr besteht, dass damit verbundene Werte wie Medienpluralismus und Vielfalt beeinträchtigt werden. Dies gilt insbesondere im Zusammenhang mit angeblich dominanten Online-Suchmaschinen.[69]

ii. Medienpluralismus

Gemäß Artikel 11 der Charta sind die Freiheit der Medien und ihre Pluralität zu achten. In einer Entschließung des Europäischen Parlaments vom Dezember 2017 wurde auf die „Konzentration der Macht von Medienkonglomeraten, Plattformbetreibern und Internet-Mittlern" hingewiesen, die „möglicherweise schädlich für den Pluralismus der öffentlichen Debatte und den Zugang zu Informationen sind". Der Sachverständigenausschuss des Europarates erarbeitet auch eine Empfehlung zum Medienpluralismus und zur Transparenz des Medienbesitzes.

Es gibt Hinweise darauf, dass diese Konzentration und Verdrängung des Lokaljournalismus die Verbreitung von Desinformation erleichtert.[70] Soziale Medien wurden genutzt, um Menschen zu ermutigen, zu wählen, für einen bestimmten Kandidaten zu stimmen oder sie von der Stimmabgabe abzuhalten („digitale Wahlkreisschiebungen"). Der wichtigste Social-Media-Anbieter selbst hat die Wähler ermutigt, ihr Stimmrecht auszuüben, und es gibt nichts, das sie daran hindert, das Gegenteil zu tun. Im Vergleich zu den Massenmedien, die über eine Nachricht berichten, gibt es keine Spur oder Aufzeichnung einer redaktionellen Entscheidung, sondern nur die Ergebnisse der Filterung durch einen Algorithmus. Online-Vermittler könnten es einer politischen Partei, mit der ihre geschäftlichen oder ideologischen Interessen übereinstimmen, theoretisch erleichtern, ihre Anhänger zu erreichen oder umgekehrt, wobei ehemalige Social-Media-Mitarbeiter jüngst behaupteten, daran beteiligt gewesen zu sein, zu verhindern, dass konservative Themen auf der Website zu einem Trendthema würden.[71] Ob vermeintlich dominante Online-Plattformen (bewusst oder unbewusst) ihre Macht zur Beeinflussung des Wahlverhaltens nutzen können oder nicht, ist weniger wichtig als die

Tatsache, dass sie – grundsätzlich – die Möglichkeit haben, auf politische Entscheidungsprozesse Einfluss zu nehmen.[72]

Die EU-Wettbewerbsregeln gestatten es den Mitgliedstaaten, gemäß Artikel 21 Absatz 4 der Fusionskontrollverordnung zum Schutz der Medienvielfalt einzugreifen. Es wurden Forderungen nach einer Neudefinition dieser Regeln im Hinblick auf die durch Plattformvermittler und die Konzentration auf dem Markt verursachten Störungen laut.

iii. Freie Wahlen

Darüber hinaus garantiert Artikel 3 des Protokolls I zur Europäischen Menschenrechtskonvention jedem Bürger das Recht auf freie Wahlen. Freiheit, Fairness und Transparenz werden als Schlüsselprinzipien demokratischer Wahlen anerkannt.[73] Im Rahmen der EU garantiert Artikel 39 der Charta das Wahlrecht bei den Wahlen zum Europäischen Parlament. Im Allgemeinen sind Wahlen frei, wenn die Kandidaten sich zur Wahl stellen können, ohne dass Behörden ihnen Hindernisse in den Weg legen, bei denen die Wähler über echte Wahlmöglichkeiten und einen freien Zugang zu Informationen über diese Wahlmöglichkeiten verfügen. Die Fairness der Wahlen kann beeinträchtigt sein, wenn eine staatliche Einmischung vorliegt, die zu einer Chancenungleichheit für die Wahlkandidaten führt. Der Grundsatz der Wahltransparenz wird nicht eingehalten, wenn die Wähler nicht über die Freiheit verfügen, Informationen über das Verfahren und die Kandidaten zu suchen, zu empfangen und weiterzugeben, einschließlich der Herkunft und Verwendung der finanziellen Unterstützung, die ein Kandidat oder eine Partei erhält.[74] Diese Rechte sind folglich ebenfalls durch Online-Manipulation bedroht.

5. Maßgebliche Rechtsrahmen

Die Komplexität des digitalen Informationsökosystems bedingt eine Reihe von Regulierungsbereichen, bei denen bisher wenig Anlass zur Interaktion bestand. In diesem Abschnitt wird zunächst die Bedeutung der Grundrechte skizziert. Anschließend werden die maßgeblichen Bereiche der EU-Rechtsvorschriften umrissen, nämlich der Datenschutz, der Grundsatz des Medienpluralismus und der audiovisuelle Bereich.

i. Datenschutzbestimmungen und -grundsätze

In der EU wurden die Datenschutzvorschriften so konzipiert, dass sie zur Achtung aller Grundrechte und -freiheiten beitragen, nicht nur zur Achtung des Datenschutzes.[75] Besondere Vorschriften für die Verarbeitung personenbezogener Daten sind in der Verordnung (EU) 2016/679 („DSGVO“) festgelegt, die ab dem 25. Mai 2018 Richtlinie 95/46/EG ersetzt.[76] Die DSGVO sieht vor, dass bei der Verarbeitung personenbezogener Daten – alle Informationen über eine identifizierte oder identifizierbare natürliche Person – die Grundsätze der Datenverarbeitung beachtet werden, einschließlich Rechtmäßigkeit, Fairness und Transparenz, Zweckbindung, Datenminimierung u. a. Personenbezogene Daten, die politische Meinungen preisgeben, gelten als „besondere Kategorie von personenbezogenen Daten“, die ein höheres Schutzniveau verdienen. Die Verarbeitung dieser Daten ist grundsätzlich untersagt, es sei denn, es gilt eine der aufgeführten Ausnahmen.[77] Eine juristische Person, einschließlich politischer Parteien und zivilgesellschaftlicher Organisationen, oder eine natürliche Person, wie ein unabhängiger politischer Kandidat, die personenbezogene Daten im Rahmen ihrer beruflichen Tätigkeit verarbeitet, ist zur Einhaltung der DSGVO verpflichtet.

Die DSGVO wird durch die derzeit überarbeitete Richtlinie 2002/58/EG („Datenschutzrichtlinie für elektronische Kommunikation“) konkretisiert und ergänzt. Die

Richtlinie enthält spezifische Vorschriften zum Schutz der Vertraulichkeit und Sicherheit der elektronischen Kommunikation, einschließlich Vorkehrungen gegen die Verletzung der Privatsphäre durch unerwünschte Nachrichten für Zwecke der Direktwerbung. Der Begriff „Direktwerbung“ ist in der Richtlinie nicht definiert; gleichwohl wird von einigen die Ansicht vertreten, dass er sich auf den Aufruf zur Bereitstellung von Mitteln oder zur Unterstützung einer politischen Sache erstrecke, indem Einzelpersonen durch Spendenaufrufe über E-Mails, soziale Netzwerke und andere elektronische Kommunikationsmittel ermutigt würden, für oder gegen eine politische Partei oder einen Kandidaten zu stimmen.[78] Seit 2009 enthält die Datenschutzrichtlinie für elektronische Kommunikation das Erfordernis, dass jede Partei, die Informationen wie ein Tracking-Cookie auf dem Gerät einer Person speichert oder darauf zugreift, die Zustimmung dieser Person einholt, es sei denn, es gilt eine Ausnahmeregelung.[79]

Anwendungsbereich

Die DSGVO findet in erster Linie auf in der EU niedergelassene Verantwortliche und Auftragsverarbeiter[80] sowie auf außerhalb der EU niedergelassene Verantwortliche und Auftragsverarbeiter Anwendung, wenn sie Personen in der EU Waren und Dienstleistungen anbieten oder deren Verhalten innerhalb der EU überwachen.[81] Während staatliche Institutionen, politische oder ursachenorientierte Bewegungen, die in den EU-Mitgliedsstaaten tätig sind, üblicherweise in ihrem Hoheitsgebiet ansässig sind, kann ihr digitales Geschäft entweder im Hoheitsgebiet der EU-Mitgliedstaaten oder in den Drittstaaten ansässig sein. Einige Unternehmen hätten Niederlassungen und Tochtergesellschaften in der EU, andere hätten möglicherweise keine stabilen Strukturen in der Union. Beispielsweise gibt es Berichte über EU-basierte Kampagnen, die sich auf die Erkenntnisse von Datenanalysefirmen stützen, die sich auf die Erstellung von Profilen von Personen zur Vorhersage ihrer persönlichen Präferenzen und politischen Einstellungen spezialisiert haben.[82] Eine solche Tätigkeit würde als Beobachtung des Verhaltens von Personen im Sinne der DSGVO angesehen werden. Dies bedeutet, dass außerhalb der Union ansässige Datenanalysefirmen, die sich mit der Erstellung von Profilen von Personen in der EU befassen, der DSGVO unterliegen und zur Einhaltung der Vorschriften in Bezug auf Fairness (einschließlich einer angemessenen Rechtsgrundlage für die Verarbeitung), Transparenz der Verarbeitung, Profilerstellung und andere Anforderungen verpflichtet sind. Die DSGVO würde zudem häufig auf Unternehmen Anwendung finden, die sich mit der Erstellung von Profilen von natürlichen Personen mit Wohnsitz außerhalb der Union befassen, wenn sie über Niederlassungen, Tochtergesellschaften oder andere Einrichtungen im Gebiet der EU verfügen. Dabei spielt die Staatsangehörigkeit oder der Wohnsitz der Personen, die Gegenstand der Profilerstellung sind, keine Rolle. Damit hat die DSGVO das Potenzial, den Rechtsschutz wie das Recht auf Information, den Zugang zu personenbezogenen Daten und Berichtigung auf Personen in Nicht-EU-Ländern auszudehnen.[83]

Verantwortliche und Rechenschaftspflicht

In Anbetracht der Vielzahl von Akteuren und Aktivitäten im digitalen Informationsökosystem kann es schwierig sein, alle Verantwortlichen und Auftragsverarbeiter zu identifizieren und eine angemessene Verteilung der Verantwortung im Rahmen der DSGVO sicherzustellen.[84] Wenn ein nichtkommerzieller Werbekunde Big-Data-Analysen an andere Unternehmen auslagert, sollte daher sorgfältig geprüft werden, wo die Verantwortung für die Verarbeitung personenbezogener Daten tatsächlich liegt, denn dies hat Auswirkungen auf die Einhaltung der Vorschriften und die Haftung nach der DSGVO. Wenn die Big-Data-Auslagerung im Rahmen einer Verantwortlicher-Auftragsverarbeiter-Beziehung erfolgt, in der der nichtkommerzielle Werbekunde die Zwecke und Mittel der Verarbeitung bestimmt und das

Datenanalyseunternehmen die Daten ausschließlich in seinem Auftrag verarbeitet, dann müssen die Beteiligten gemäß DSGVO einen Vertrag oder einen anderen Rechtsakt schließen, in dem ihre Beziehung geregelt wird.[85] Das Bestehen eines solchen Vertrages würde jedoch nicht automatisch bedeuten, dass das Unternehmen, das die Datenanalyse durchführt, wirklich ein Auftragsverarbeiter ist. Ein Unternehmen ist z. B. insofern wahrscheinlich ein Auftragsverarbeiter, als es im Auftrag einer politischen Partei Datenanalysen für die Zwecke einer bestimmten Wahl durchführt, während die politische Partei, die den Zweck der Verarbeitung bestimmt, wahrscheinlich der für die Verarbeitung Verantwortliche ist. Je mehr Freiheiten das Unternehmen hat bei der Entscheidung, welche Daten es erheben und wie es seine Analyseverfahren anwenden will, desto mehr wird das Unternehmen als gemeinsamer Verantwortlicher betrachtet.[86]

Die Beziehung zwischen der Plattform und den Organisationen, die ihre Dienste in Anspruch nehmen, ist Gegenstand einer Anfechtungsklage, die derzeit vor dem EuGH anhängig ist.[87] Nach Ansicht des Generalanwalts sind sowohl die Plattform als auch der Betreiber einer Fanpage als für die Verarbeitung Verantwortliche zu betrachten.[88] Die Stellungnahme berücksichtigt alle politischen Parteien, Kandidaten oder ideologische Bewegungen, die über eine Fanpage eine Präsenz im sozialen Netzwerk haben und somit in der Lage sind, „die konkrete Umsetzung dieses [Werbe-]Tools zu beeinflussen", indem sie Filter verwenden, um ein personalisiertes Zielpublikum festzulegen und die Kategorien von Personen zu bestimmen, deren personenbezogene Daten von dem Social-Media-Unternehmen erhoben werden. Ein solches Unternehmen hätte alle Pflichten des für die Verarbeitung Verantwortlichen gemäß der DSGVO, einschließlich der Verpflichtung, eine Rechtsgrundlage für die Verarbeitung zu ermitteln, Einzelpersonen über die Verarbeitung ihrer Daten zu informieren und die Einhaltung der DSGVO nachzuweisen.[89]

Zweckbindung

Der Grundsatz der Zweckbindung setzt voraus, dass der Zweck der Erhebung personenbezogener Daten zum Zeitpunkt der Erhebung festgelegt wird. Die Informationen dürfen nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist. Bei jeder Änderung des Verarbeitungszwecks ist dies anzugeben.[90]

Bei der Datenanalyse handelt es sich um Methoden und Nutzungsmuster, die weder die erhebende Stelle noch die betroffene Person zum Zeitpunkt der Datenerhebung berücksichtigt hat oder sich vorstellen konnte. Die algorithmische Verarbeitung personenbezogener Daten eröffnet Möglichkeiten zur Generierung neuer Daten. Wenn eine betroffene Person einige vertrauliche Daten teilt, ist es oft möglich, dass diese Daten zusammengeführt werden, wodurch eine zweite und sogar dritte Generation von Daten über die Person entsteht.[91]

Beispielsweise könnten begrenzte Informationen über Anhänger einer politischen Partei, die in ihren Datenbanken gespeichert sind, oder grundlegende Informationen über Mitglieder einer Organisation, die von ihnen direkt zur Verfügung gestellt werden, mit Daten über das Kaufverhalten von Einzelpersonen zusammengeführt werden, die von Datenbrokern stammen.[92] Durch den Einsatz von Tools der Social-Media-Plattformen können diese Daten mit demografische Informationen (z. B. Daten zum Familienstand) und Informationen zu individuellem Verhalten und Interessen kombiniert werden. Durch die Anwendung der oben beschriebenen Methoden der Datenanalyse können interessierte Wahlkämpfer oder mitgliedschaftsbasierte Organisationen aus scheinbar unverbundenen und unsensiblen Datensätzen auf psychologische Profile und detaillierte politische Präferenzen einzelner Personen schließen.

Das Problem bei der Verwendung von Daten aus Profilen für verschiedene Zwecke durch Algorithmen besteht darin, dass die Daten aus ihrem ursprünglichen Kontext herausgerissen werden. Die Umnutzung von Daten kann die informationelle Selbstbestimmung einer Person gefährden, die Kontrolle der Betroffenen über ihre Daten weiter einschränken und damit das Vertrauen in digitale Umgebungen und Dienste beeinträchtigen.[9394] Daher kommt der Zweckbindung als Grundsatz des Datenschutzrechts eine so entscheidende Bedeutung zu.

Eine rechtmäßige Verarbeitung durch nichtkommerzielle Werbekunden sowie die Parteien des Werbeökosystems würde daher in erster Linie eine Rechtsgrundlage für die Verarbeitung erforderlich machen, wie etwa Einwilligung der betroffenen Personen. Eine ausdrückliche Einwilligung wäre für die Verarbeitung sensibler Informationen, die politische oder religiöse Ansichten preisgeben, unerlässlich, und die Einwilligung ist nicht gültig, wenn sie zur Bedingung für die Nutzung des Dienstes gemacht wird.

Sie müssten die betroffenen Personen über die künftigen Formen der Verarbeitung informieren und ihre Praktiken genau überwachen, um sicherzustellen, dass sie die zulässigen Grenzen der Verarbeitung innerhalb der angegebenen Zwecke nicht überschreiten.[95]

ii. Vorschriften für audiovisuelle Medien

Die EU-Richtlinie über audiovisuelle Mediendienste wird derzeit überarbeitet. Sie umfasst die EU-weite Koordinierung der nationalen Rechtsvorschriften für alle audiovisuellen Medien, d. h. sowohl für traditionelle Fernsehsendungen als auch für Abrufdienste. Zu den Zielen der Überarbeitung gehört die Bekämpfung von „Hetze“ und sicherer Medienpluralismus. Inzwischen ist politische Werbung im Fernsehen in der Regel in der EU reguliert, und es bestehen Unparteilichkeitsanforderungen an die öffentlich-rechtlichen Rundfunkanstalten. Für die Nutzung algorithmischer Vorhersagen von Präferenzen und Wählerverhalten, die eine ebenso starke, wenn nicht sogar stärkere Wirkung haben können, existiert jedoch keine gleichwertige Regelung.[96] Aus diesem Grund wurde erneut die Forderung geäußert, traditionelle Standards der Medienverantwortung auf Social-Media-Plattformen anzuwenden. Aufgrund ihrer Entscheidungen darüber, welche Nachrichten wem angezeigt werden sollen, agieren diese Plattformen als Nachrichtenredakteure mit Verantwortung für ihre Trendthemen. Es stellt sich die Frage, ob Social-Media-Plattformen durch ihre Algorithmen, die Beiträge Dritter klassifizieren und kuratieren, eine Form der redaktionellen Kontrolle ausüben, die traditionell von Medienprofis ausgeübt wird, und somit spezifische Medienverantwortung übernehmen.[97]

Lange Zeit mussten die Sender bei der Veröffentlichung von Meinungsumfragen Zurückhaltung üben und zudem vor dem Wahltag Ruhezeiten durchsetzen („Blackout“). In einigen Fällen erstreckte sich die Regulierung der politischen Werbung auch auf die Begrenzung der Zeit für die Parteien der öffentlich-rechtlichen Rundfunkanstalten, um gleiche politische Rahmenbedingungen für größere und kleinere politische Parteien und Kandidaten sicherzustellen.[98] Allerdings wirft der Übergang zum „Digital Narrowcasting“, bei dem politische Kampagnen zunehmend online durchgeführt werden, mit der Nutzung der oben erläuterten Analyse- und Mikrotargeting-Tools Fragen nach der Anwendung der Rundfunkvorschriften auf die wichtigsten Plattformen auf und stellt die für Audiovisuelles und Medien zuständigen Behörden vor die Herausforderung, ihre Funktionsweise zu verstehen.

iii. Wahlordnung

In den nationalen Wahlkampfvorschriften der EU-Mitgliedstaaten sind Anforderungen an die Offenlegung von Wahlkampfspenden und/oder Ausgaben der Kandidaten niedergelegt.[99] Selbst wenn diese Vorschriften gleichermaßen für Online- und Offline-Kampagnen gelten, erschwert die Abhängigkeit der Parteien von digitalen Werbedienstleistungen und Social-Media-Tools von Drittanbietern die Anwendung dieser Vorschriften. Beispielsweise kann es sein, dass die gemeldeten Ausgaben für Kampagnenmaterial keine ausreichenden Angaben über die Ausgaben für digitale Werbung und damit verbundene Dienstleistungen enthalten, z. B. gezielte Anzeigen in sozialen Medien, Analysedienste, Erstellung von Wählerdatenbanken oder die Zusammenarbeit mit Datenbrokern. Die Botschaften, die online, auch über soziale Medien, verbreitet werden, enthalten selten ein Impressum, in dem angegeben ist, wer sie veröffentlicht hat; dadurch wird den Wählern die Möglichkeit genommen herauszufinden, wer Geld ausgibt, um sie bei den Wahlen zu beeinflussen.[100] Ein Mangel an Transparenz in Bezug auf diese Praktiken kann negative Auswirkungen auf Fairness und Entscheidungsfreiheit haben.

iv. Verbraucherschutz

Nach der EU-Grundrechtecharta haben die Verbraucher Anspruch auf ein hohes Verbraucherschutzniveau. Insofern liegen dem europäischen Verbraucherrecht zwei unterschiedliche Grundprinzipien zugrunde: Die Verbraucher sollen als souveräner Marktakteur gestärkt werden, indem ihnen die Rechte und Informationen zur Verfügung gestellt werden, die sie benötigen, um in dieser Rolle zu handeln, und die Verbraucher sollen in Situationen Schutz erhalten, in denen sie die schwächere Partei im Geschäftsverkehr sind und es ihnen nicht möglich ist, den Schutz ihrer Rechte, (wirtschaftlichen) Interessen und Sicherheit in die eigenen Hände zu nehmen.[101]

Die EU hat verschiedene Maßnahmen zum Schutz der Nutzer von Produkten und Dienstleistungen ergriffen, unabhängig davon, wo sie im Binnenmarkt angeboten oder verbraucht werden.[102] Eines dieser Instrumente, die Richtlinie über unlautere Geschäftspraktiken, verbietet irreführende, aggressive und anderweitig unlautere Geschäftspraktiken.[103][104][105] Solche Praktiken sind im Rahmen von Geschäftspraktiken zwischen Unternehmen und Verbrauchern verboten. Politische und ideologische Zielgruppenansprache und Werbung fallen nicht unter das Verbraucherrecht. Aktivitäten, die darauf hinauslaufen, Personen mittels Fehlinformationen zu manipulieren und politische Argumente anhand aufdringlicher persönlicher Profile zu personalisieren, weisen jedoch offensichtliche Ähnlichkeiten mit den Arten des Missbrauchs auf, die im Verbraucherrecht angegangen werden.[106] Internationale Menschenrechtsnormen unterscheiden tendenziell zwischen Empfängern von politischer und Empfängern von kommerzieller Zielgruppenansprache.[107] Wie in der oben genannten Resolution zur Verwendung von Personendaten für die politische Kommunikation erwähnt, hat „die politische Kommunikation, auch wenn sie gelegentlich Elemente typischer Werbetätigkeiten aufweist, doch Eigenheiten [...], die sie vom kommerziellem Marketing unterscheiden“.[108]

v. Wettbewerbsrecht

In unserer vorläufigen Stellungnahme von 2014 zum Thema Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von Big Data und später in unserer Stellungnahme von 2016 zur kohärenten Durchsetzung von Grundrechten im Zeitalter von Big Data haben wir argumentiert, dass das Wettbewerbsrecht eine entscheidende Rolle bei der Gewährleistung der

Rechenschaftspflicht marktbeherrschender Akteure und beim Schutz der Demokratie vor übermäßiger Marktmacht spielt. Es gibt Anzeichen dafür, dass Konzentration für böswillige Betreiber innerhalb des „Ökosystems“ ein leichtes Ziel darstellt, das das Mikrotargeting unterstützt. Die Interessen von Einzelpersonen sollten bei der Bewertung des möglichen Missbrauchs einer marktbeherrschenden Stellung oder von Unternehmenszusammenschlüssen, die eine beträchtliche Informationsmacht angesammelt haben könnten, besser berücksichtigt werden.[109] So hat die deutsche Wettbewerbsbehörde im Dezember 2017 eine vorläufige rechtliche Bewertung im Verfahren über den Missbrauch einer marktbeherrschenden Stellung gegen Facebook abgegeben. Sie stellte fest, dass Facebook diese marktbeherrschende Stellung missbraucht, indem es die Nutzung seines sozialen Netzwerks davon abhängig macht, dass es jede Art von Daten, die durch die Nutzung von Websites Dritter generiert werden, unbegrenzt sammeln und mit dem Facebook-Konto des Nutzers zusammenführen darf.[110] Da das Mikrotargeting auf die von diesem Social-Media-Netzwerk erhobenen personenbezogenen Daten angewiesen sein kann, sind die Ergebnisse des Bundeskartellamtes auch im Rahmen dieser Stellungnahme relevant.

Auf der zweiten Sitzung des Digital Clearinghouse wurden die Gründe für Interventionen im Rahmen des Datenschutz-, Verbraucherschutz- und Wettbewerbsrechts erörtert, um mögliche negative Auswirkungen des Mikrotargeting auf die Grundrechte von Einzelpersonen anzugehen.[111] Es wurde beschlossen, diese Angelegenheit weiterhin als einen Bereich der möglichen Zusammenarbeit zwischen den Regulierungsbehörden, einschließlich der Wahl- und Medienbehörden, zu betrachten. Der EDSB wird mit der Koordinierung dieser Bemühungen fortfahren und dabei auch die laufenden Arbeiten der Europäischen Kommission und der nationalen Regulierungsbehörden berücksichtigen.[112][113]

6. Empfehlungen

Online-Manipulation ist ein komplexes Problem, für das es keine einfache Lösung gibt. Durch einen einzigen Regulierungszweig ist dies nicht zu bewältigen. In dieser Stellungnahme wird jedoch argumentiert, dass der Datenschutz ein großer Teil der Lösung sein muss. Im Folgenden geben wir fünf Empfehlungen für Maßnahmen, die sich aus dem Datenschutzrecht ergeben und bei denen unabhängige Datenschutzbehörden einen wertvollen Beitrag leisten können, beginnend mit dem Abschluss der Reform des Datenschutzrahmens und dessen konsequenter Durchsetzung, wobei die Regulierungsbehörden versuchen, auf der Grundlage bestehender Maßnahmen auf nationaler und EU-Ebene für die Zusammenarbeit mit anderen Regulierungsbehörden, die Selbstregulierung und die Stärkung der Eigenverantwortung des Einzelnen zu einem besseren Verständnis des Themas zu gelangen.

I. Vervollständigung und Durchsetzung der Datenschutzbestimmungen

Es ist von entscheidender Bedeutung, den Schutz spezieller Datenkategorien, die Grundsätze der Transparenz, der Zweckbindung und der Datenminimierung sowie den Schutz vor unrechtmäßiger Profilerstellung und automatisierter Entscheidungsfindung zu verstärken.

Ohne ein Rechtsinstrument zum Schutz des Rechts auf Privatleben, das durch Artikel 7 der EU-Grundrechtecharta garantiert wird, wäre der EU-Rahmen für den Schutz der Privatsphäre und des Datenschutzes unvollständig. Die vorgeschlagene E-Privacy-VO hat das Potenzial, Negativanreize für die kontinuierliche Verfolgung und Manipulation von Personen zu schaffen.

Zu diesem Zweck haben wir dem Gesetzgeber bereits empfohlen, folgende Ergänzungen in den Verordnungsvorschlag aufzunehmen[114]:

- ein vollständiges und ausdrückliches Verbot so genannter „Tracking-Walls“;
- ein ausdrückliches Verbot der Praxis, Nutzern den Zugriff zu verwehren, die zum Schutz ihrer Informationen und Endgeräte Anti-Werbungssoftware oder andere Anwendungen und Erweiterungen installiert haben;
- eine Bestätigung, dass die Verarbeitung von Daten zum Zweck der Bereitstellung zielgerichteter Werbung nicht als für die Erbringung einer Dienstleistung notwendig erachtet werden kann;
- das Erfordernis, dass Browser und andere Programme oder Betriebssysteme in ihren Voreinstellungen Zugriff auf Kontrollmechanismen bieten, über die der Nutzer einem Tracking auf einfache Weise zustimmen oder widersprechen kann.

Der EDSB wird das Europäische Parlament und den Rat weiterhin unterstützen, um eine rasche Fertigstellung der neuen Rechtsvorschriften zu gewährleisten und Anreize für eine nachhaltige Grundlage für die Achtung der Privatsphäre und des Datenschutzes zu schaffen.[115] Nach unserer Überzeugung wird die EU damit Chancen für neue Geschäftsmodelle und datenschutzfreundlichere Technologien und Unternehmen eröffnen, die dazu beitragen würden, die Risiken zu umgehen, die das zugrunde liegende Ökosystem für Mikrotargeting birgt.

II. Die Regulierungsbehörden sollten eine gemeinsame Diagnose des Problems anstreben.

Die Datenanalyse bietet beispiellose Möglichkeiten, von Personen Profile zu erstellen, um ihr Verhalten zu messen, einzuordnen, zu bewerten und auf ihrer Grundlage fundierte Entscheidungen zu treffen. Sie personalisiert die Erfahrungen und Informationen der Menschen, um ihr Verhalten und ihre Entscheidungen zu beeinflussen, sei es im Hinblick auf ihre Kaufentscheidungen als Verbraucher oder ihre Entscheidungen als Bürger, die sich zivilgesellschaftlich engagieren.[116] Die Herausforderung besteht darin, die Technologie so zu nutzen, dass die Menschen sich freier und wirksamer in den zivilgesellschaftlichen Entscheidungsprozess einbringen können. Es geht darum, die Risiken einer unzulässigen Manipulation zu steuern und die Idee eines Individuums als quantifiziertes Selbst in Frage zu stellen.[117]

Die Datenschutzbehörden und alle betroffenen Regulierungsbehörden müssen die lokalen Mikrotargeting-Praktiken kennen, einschließlich der Frage, inwieweit sich politische und ideologische Bewegungen mit der Profilerstellung und Zielgruppenansprache von Einzelpersonen befassen; außerdem müssen sie wissen, auf welche Quellen personenbezogener Daten sie angewiesen sind und welche Tools sie verwenden, um von ihnen ein Profil zu erstellen und sie gezielt anzusprechen. Obwohl einige globale und regionale Trends erkennbar sind, machen die unterschiedlichen institutionellen, sozialen und rechtlichen Rahmenbedingungen es erforderlich, dass die Behörden länderspezifische Untersuchungen durchführen.[118] Auf nationaler Ebene sind bereits große Anstrengungen unternommen worden, und die Kommission ist bei der Suche nach Lösungen federführend.[119] Die Regulierungsbehörden können bestehende Richtlinien der Datenschutzbehörden zu politischen Kampagnen und die Möglichkeit, diese auch auf andere soziale und ideologische Bewegungen anzuwenden, die sich mit der Profilerstellung und Zielgruppenansprache von Personen mit

nichtkommerziellen Botschaften befassen, berücksichtigen. Insbesondere der datenschutzrechtliche Begriff des öffentlichen Interesses und seine Abgrenzung zu den privaten Interessen von Unternehmen oder politischen Bewegungen ist der Schlüssel zur Bekämpfung von Missbrauch und Manipulation im politischen Online-Raum. Die Regulierungsbehörden sollten zusammenarbeiten, um darauf aufzubauen.

III. Regulierungsbehörden sollten sektorübergreifend zusammenarbeiten

Die gegenwärtigen Reaktionen auf „Fake News" müssen durch eine verstärkte Zusammenarbeit zwischen den Behörden unterstützt werden.[120]

Erstens besteht eine Konvergenz zwischen Kartellrecht und Datenschutz, da die Behörden erkennen, dass ein großer Teil des strukturellen Missbrauchs das Ergebnis von Verzerrungen in einem zu stark konzentrierten digitalen Markt ist. Das Kartellrecht spielt eine entscheidende Rolle bei der Überwachung des Verhaltens marktbeherrschender Unternehmen und bei der Anwendung der Fusionskontrolle, um schädliche längerfristige Auswirkungen von Fusionen zu vermeiden.

Zweitens könnte durch die Zusammenarbeit zwischen den für Datenschutz und Verbraucherschutz zuständigen Regulierungsbehörden das zugrunde liegende Ökosystem untersucht werden, das politisches Mikrotargeting erleichtert, d. h. Online-Dienste, die von der Werbewirtschaft, Datenbrokern, Datenanalyse-Unternehmen und Social-Media-Plattformen angeboten werden.[121] Nach dem Verbraucherschutzrecht können sie sich sowohl als „Unternehmer"[122] als auch als Dienstleistungserbringer für Dritte qualifizieren. So ist es den Datenschutz- und Verbraucherschutzbehörden möglich, Normen für die Transparenz und Verständlichkeit von Vertragsbedingungen und Online-Diensten zu berücksichtigen, die insbesondere von den Unternehmen mehr Transparenz bei der Entscheidungsfindung in der Datenverarbeitung verlangen.[123]

Die Synergien könnten auch die potenzielle Überzeugungskraft des Behavioral Targeting (verhaltensorientierte Zielgruppenansprache) erhöhen, indem sie die „Fairness" bestimmter Merkmale dieser Online-Dienste untersuchen[124], die in erster Linie darauf abzielen, Kunden dazu zu bewegen, mehr persönliche Informationen zur Verfügung zu stellen, um detailliertere Profildaten zu erhalten, und ausgeklügeltere Möglichkeiten der Zielgruppenansprache anzubieten, wodurch der Wert des Dienstes für Werbekunden (aus Wirtschaft und Politik) erhöht wird.

Drittens ist die Abstimmung mit der Wahlordnung unerlässlich geworden. In den Datenschutz- und E-Privacy-Vorschriften gibt es Ausnahmen, die sich auf politische Aktivitäten und das öffentliche Interesse beziehen, und die Regulierungsbehörden müssen zusammenarbeiten, um sicherzustellen, dass Manipulationen der Regulierung nicht entgehen können. Wie in der Resolution zur Verwendung von Personendaten für die politische Kommunikation ausgeführt, könnten „die Datenschutzbeauftragten künftig eine stärkere Rolle in der Planung koordinierter Aktionen spielen [...], auch in Zusammenarbeit mit anderen Aufsichtsbehörden in den Bereichen Telekommunikation, Information, Meinungsumfragen oder Wahlverfahren".[125] Das Datenschutzrecht, das Wahlrecht und das audiovisuelle Recht haben gemeinsame Grundsätze, wie Transparenz und Fairness, und die Zusammenarbeit zwischen den jeweiligen Regulierungsbehörden, insbesondere während der Wahlperiode, könnte zur Verbesserung ihrer kohärenten Anwendung führen und den Schutz des Einzelnen vor potenziell unlauteren Mikrotargeting-Praktiken erhöhen.

Im Rahmen eines im Jahr 2013 durchgeführten EU-Forschungsprojekts wurde eine mangelnde Koordination in der Frage der Datenverarbeitung für politische Kampagnen zwischen den Datenschutzbeauftragten festgestellt.[126] Abgesehen von einer bemerkenswerten Ausnahme bei der Anwendung des Datenschutzes und des audiovisuellen Rechts bei politischen Kampagnen gibt es offenbar auch keine aktive Zusammenarbeit zwischen Datenschutz-, Wahl- und Medienbehörden auf nationaler oder EU-Ebene.[127] Im Rahmen politischer Kampagnen scheinen die Regulierungsbehörden jedoch in allen drei Rechtsbereichen – Datenschutz, Wahlen und Medien – vor Herausforderungen zu stehen, wenn es um die Anwendung der gemeinsamen Grundsätze der Transparenz und Fairness auf die neuen Realitäten politischer Kampagnen geht, was die Verfolgung, Profilerstellung und Zielgruppenansprache von Personen im Internet beinhaltet. Berichte politischer Parteien über ihre Wahlkampfausgaben und Untersuchungen durch die Wahlbehörden können den Datenschutzbehörden wertvolle Informationen über die Datenerhebungs- und -verarbeitungspraktiken liefern, die im Rahmen von politischen Kampagnen (mit oder ohne Unterstützung Dritter) angewandt werden. Diese können in die Bewertung ihrer Einhaltung der Anforderungen der DSGVO, einschließlich Rechenschaftspflicht, Rechtmäßigkeit, Transparenz und Fairness der Datenverarbeitung, einfließen. Die Datenschutzbehörden verfügen über umfassende Kenntnisse über die Funktionsweise des Ökosystems der digitalen Werbung, die sie den für Audiovisuelles zuständigen Behörden zur Verfügung stellen könnten, um sie bei der Anwendung der Vorschriften für politische Werbung auf die Online-Umgebung zu unterstützen. Dies sind nur einige Beispiele für die potenziellen Vorteile, die eine aktivere Zusammenarbeit zwischen den Regulierungsbehörden mit sich bringen könnte.

Wie wir in unserer vorherigen Stellungnahme dargelegt haben, verfügen die Regulierungsbehörden in jedem Rechtsbereich über begrenzte Befugnisse und damit sind den Instrumenten, die ihnen zur Verfügung stehen, ebenfalls Grenzen gesetzt. So wachen die Datenschutzbehörden allein über die Rechtmäßigkeit, Transparenz und Fairness von Profilerstellung und Zielgruppenansprache in Bezug auf die Verarbeitung personenbezogener Daten, während die Fairness und Wahrhaftigkeit der personalisierten Nachrichten nicht durch das Datenschutzgesetz geregelt werden.[128] In Anbetracht der potenziellen Risiken, die sich durch Mikrotargeting, das über das Recht auf Datenschutz hinaus auf die Bereiche Meinungs- und Informationsfreiheit, Gleichberechtigung und freie Wahlen ausgedehnt wird, ergeben können, müssen daher die Aussichten für eine Zusammenarbeit zwischen Datenschutz- und anderen Regulierungsbehörden geprüft werden.

IV. Selbstregulierung und Verhaltensregeln sollten gefördert werden

Online-Manipulation ist zu systemisch, zu existentiell in ihrer Bedrohung der Grundrechte und -werte, um ihre Bekämpfung der Industrie zu überlassen. Gleichwohl spielt Selbstregulierung eine wichtige Rolle.

Im Rahmen der DSGVO sind die nationalen Aufsichtsbehörden, der Europäische Datenschutzausschuss, die EU-Mitgliedstaaten und die Kommission verpflichtet, die Ausarbeitung von Verhaltensregeln zu fördern, „die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen“[129]: Wie von der Artikel 29-Datenschutzgruppe angegeben, kann die Einhaltung eines Verhaltenskodex zum Nachweis von Transparenz beitragen. Es könnten Regeln aufgestellt werden, um die Anwendung der DSGVO u. a. im Hinblick auf eine faire und transparente Verarbeitung, die Bereitstellung von Information für die Öffentlichkeit und betroffene Personen und den Schutz von Kindern zu präzisieren.[130] Darüber hinaus kann die

Ausarbeitung eines Verhaltenskodex politische Parteien, Wahlkampfteams und andere soziale und politische Vereinigungen dazu anregen, über die ethische Dimension der Datenverarbeitung zu diskutieren, wie z. B. über Entscheidungen bestimmter für die Verarbeitung Verantwortlicher, sich nicht an bestimmten Datenverarbeitungsvorgängen zu beteiligen.[131]

V. Ermächtigung des Einzelnen zur Ausübung seiner Rechte, einschließlich Sammelklagen

Verschlüsselung, Apps und Browser-Erweiterungen, die Zielgruppenansprache aufdecken sollen, sowie weitere Sicherheitsmaßnahmen zum Schutz persönlicher Daten bilden eine Barriere gegen Manipulationen.

Informationsbroker, Werbenetzwerke, Anbieter von sozialen Netzwerken und andere Akteure im digitalen Geschäft verfügen mehr denn je über vollständige Dossiers über Menschen, die an der heutigen digitalen Gesellschaft teilnehmen, und die Menschen verlieren die Kontrolle über den digitalen Fußabdruck, den sie hinterlassen. Menschen, die von Akteuren, über die sie keine Kontrolle haben oder von denen sie meist gar nichts wissen, gezielt beobachtet werden, Gegenstand einer Profilerstellung und Bewertung durch sie sind, fühlen sich hilflos und müssen in die Lage versetzt werden, Kontrolle über ihre Identität zu gewinnen. Auch wenn die Menschen formal eine Art „Hinweis“ oder die Möglichkeit erhalten haben, ihre „Einwilligung“ zu allgemeinen Geschäftsbedingungen zu geben, finden sie sich häufig in einem System wieder, das darauf angelegt ist, aus personenbezogenen Daten möglichst großen Profit zu schlagen, womit den Menschen keine echte Wahl oder Kontrolle bleibt.[132]

Transparenz ist nur ein Teil der Lösung – die Argumentation hinter dem überparteilichen Honest Ads Act, der Käufer von politischer Online-Werbung lediglich zur Offenlegung ihrer Identität verpflichten würde.

Verschiedene Umfragen zeigen, dass rund 75 % der Verbraucher kein Vertrauen in den Umgang mit ihren Daten durch Social-Media-Marken und Marketingunternehmen haben.[133] Weniger als 20 % der Europäer haben das Gefühl, die volle Kontrolle über die Informationen, die sie online zur Verfügung stellen, zu haben, während jeder dritte Europäer das Gefühl hat, überhaupt keine Kontrolle darüber zu haben.[134]

Wir haben bereits die digitale Wirtschaft, die viel Zeit und Mühe in die Suche nach neuen Möglichkeiten für die Nutzung personenbezogener Daten investiert, aufgefordert, dasselbe innovative Denken auch bei der Umsetzung des Datenschutzrechts an den Tag zu legen.[135] Unsere *Stellungnahme zu Systemen für das Personal Information Management* von 2016 untersucht das Konzept, das hinter Technologien und Ökosystemen steht, mit denen Menschen in die Lage versetzt werden sollen, die Weitergabe ihrer personenbezogenen Daten zu kontrollieren („Personal Information Management-Systeme“ oder kurz „PIMS“). Wir haben das Potenzial von PIMS analysiert, die Nutzer in die Lage zu versetzen, ihre personenbezogenen Daten zu kontrollieren, und der Kommission und den Mitgliedstaaten vorgeschlagen, Maßnahmen zur Förderung von Forschung und Entwicklung und Markteinführung im Bereich PIMS zu ergreifen.

Um die Grundrechte praxistauglich und wirksam zu machen, müssen alle von den Verantwortlichen und Auftragsverarbeitern geschaffenen rechtlichen, politischen und technologischen Ex-Ante-Schutzvorkehrungen mit dem Ex-Post-Recht auf wirksame Rechtsbehelfe für diejenigen einhergehen, deren Rechte und Freiheiten verletzt wurden.[136] Da Mikrotargeting weitgehend von automatisierten Entscheidungsfindungsprozessen abhängt,

stellt sie Personen, die wirksame Rechtsbehelfe benötigen, vor besondere Herausforderungen.[137] Dazu gehören die Intransparenz der Entscheidung selbst, ihre Grundlage, die Frage, ob der Einzelne der Verwendung seiner Daten bei dieser Entscheidung zugestimmt hat, sowie die Frage, ob er von der ihn betreffenden Entscheidung überhaupt Kenntnis erlangt hat.[138] Aufgrund verfahrenstechnischer Hindernisse[139] beim Zugriff auf seine personenbezogenen Daten oder aufgrund der Informationsasymmetrie zwischen Verantwortlichen und Auftragsverarbeitern kann der Einzelne mit Schwierigkeiten konfrontiert sein, wenn es darum geht, die Vollständigkeit der Informationen, die er als Antwort auf die Zugriffsanfragen erhält, zu prüfen. Aufgrund der Schwierigkeit, die Verantwortung für die Entscheidung zuzuordnen, ist es auch für den Einzelnen schwierig zu wissen, an wen er sich mit seiner Beschwerde wenden kann.[140] Darüber hinaus existieren für Einzelpersonen, die einen Rechtsbehelf einlegen wollen, eine Reihe von Hindernissen.[141]

In Anbetracht dieser und anderer Hindernisse für die wirksame Ausübung der Rechte gemäß der DSGVO sind in der Verordnung im Vergleich zur Datenschutzrichtlinie zusätzliche Möglichkeiten zur Ausübung dieses Rechts vorgesehen. Insbesondere Artikel 80 der DSGVO gibt betroffenen Personen das Recht, „eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht [...] zu beauftragen“, unter bestimmten Voraussetzungen in ihrem Namen bestimmte Rechte wahrzunehmen, und räumt den Mitgliedstaaten die Möglichkeit ein, vorzusehen, dass diese Organisationen ähnliche Funktionen unabhängig von einem Auftrag der betroffenen Person selbstständig ausüben können. Wenngleich die Einführung dieses Rechts als große Errungenschaft anerkannt werden sollte[142], empfiehlt der EDSB Folgendes, um dem Recht auf einen wirksamen Rechtsbehelf volle Wirkung zu verleihen:

- Für die EU-Legislative: Es sollten eine ausdrückliche Bestimmung für die kollektive Rechtsdurchsetzung und wirksame Rechtsbehelfe hinzugefügt werden oder andernfalls sollte der Text näher erläutert werden (z. B. durch eine ausdrückliche Bestätigung der Anwendbarkeit von Artikel 80 DSGVO), um zu gewährleisten, dass die nach der DSGVO verfügbaren kollektiven Rechtsdurchsetzungsinstrumente voll und ganz zur Verfügung stehen.[143]

- Für die Mitgliedstaaten bei der Ausübung ihres Ermessens in Bezug auf die Umsetzung von Artikel 80 Absatz 2 DSGVO: In ihren nationalen Rechtsvorschriften sollte für die im Bereich des Schutzes der Rechte und Freiheiten der betroffenen Personen tätigen gemeinnützigen Einrichtungen, Organisationen oder Vereinigungen des öffentlichen Interesses eine rechtliche Befugnis vorgesehen sein, Beschwerden bei der Aufsichtsbehörde einzureichen und weitere in diesem Artikel niedergelegte Rechte der betroffenen Personen unabhängig vom Mandat der betroffenen Person auszuüben.

Der EDSB ist der Ansicht, dass ein solcher Ansatz zu einer kohärenteren und gleichberechtigten Durchsetzung der Rechte der betroffenen Personen in der Praxis in den verschiedenen EU-Ländern beitragen würde. Besonders wichtig ist dies im Zusammenhang mit Praktiken der Verarbeitung sensibler personenbezogener Daten, wie der Erstellung von Profilen und der automatisierten Entscheidungsfindung von Einzelpersonen, die, wenn sie rechtswidrig, intransparent oder ungerecht sind, die Ausübung der Rechte von Millionen von Bürgern beeinträchtigen können. Beispielsweise kann eine Datenschutzverletzung in einer Wählerdatenbank, die dazu führt, dass die Profile der Wähler mit Einblicken in ihre Persönlichkeit, ihren Lebensstil und ihr psychologisches Profil offengelegt werden, als besonders schwerwiegende Verletzung des Rechts auf Achtung des Privatlebens angesehen werden. Die Verfügbarkeit eines Opt-out-Mechanismus für kollektive Rechtsbehelfe[144] kann es Organisationen des öffentlichen Interesses ermöglichen, diese Verletzung zu beheben, selbst

wenn Einzelpersonen aus den oben beschriebenen Gründen möglicherweise nicht in der Lage sind, rechtliche Schritte gegen den für die Verarbeitung Verantwortlichen und/oder den Auftragsverarbeiter einzuleiten.[145]

7. Schlussfolgerung

Online-Manipulationen stellen eine Bedrohung für die Gesellschaft dar, da Filterblasen und geschlossene Communities es den Menschen erschweren, sich gegenseitig zu verstehen und Erfahrungen auszutauschen. Die Schwächung dieses „sozialen Kitts" kann die Demokratie sowie einige andere Grundrechte und -freiheiten untergraben. Online-Manipulation ist außerdem ein Symptom der Intransparenz und mangelnden Rechenschaftspflicht im digitalen Ökosystem. Das Problem ist real und dringlich und wird sich wahrscheinlich noch verschlimmern, da immer mehr Menschen und Dinge mit dem Internet verbunden sind und die Rolle der Systeme der künstlichen Intelligenz an Bedeutung gewinnt. Die Wurzel des Problems liegt zum Teil in der unverantwortlichen, illegalen oder unethischen Verwendung personenbezogener Daten. Transparenz ist notwendig, aber nicht ausreichend. Content Management kann eine Notwendigkeit sein, darf aber nicht die Grundrechte beeinträchtigen. Ein Teil der Lösung besteht daher darin, die bestehenden Vorschriften, insbesondere die DSGVO, konsequent und parallel zu anderen Normen für Wahlen und Medienpluralismus durchzusetzen.

Als debattenfördernden Beitrag wird der EDSB im Frühjahr 2019 einen Workshop veranstalten, bei dem die nationalen Regulierungsbehörden im Bereich des Datenschutzes, des Wahlrechts und des audiovisuellen Rechts diese Wechselwirkungen weiter untersuchen, die Herausforderungen, vor denen sie stehen, erörtern und Möglichkeiten für gemeinsame Aktionen auch unter Berücksichtigung der bevorstehenden Wahlen zum Europäischen Parlament prüfen können.

In dieser Stellungnahme wird dargelegt, dass Technologie und Marktverhalten durch strukturelle Ungleichgewichte und Verzerrungen Schaden anrichten. Wir haben eine Anpassung der Innovationsanreize gefordert. Die Technologieriesen und -vorreiter haben bisher davon profitiert, in einem relativ ungeregelten Umfeld zu arbeiten. Betroffen sind traditionelle Branchen und Grundkonzepte der territorialen Gerichtsbarkeit, Souveränität und auch soziale Normen, einschließlich der Demokratie. Diese Werte hängen von einer Meinungspluralität und dem Gleichgewicht zwischen den Parteien ab. Kein einzelner Akteur oder Sektor kann dieses Problem allein bewältigen. Der Schutz der Daten ist Teil der Lösung, möglicherweise ein größerer Teil als erwartet. Es reicht nicht aus, sich auf den guten Willen der letztlich nicht rechenschaftspflichtigen Wirtschaftsakteure zu verlassen. Wir müssen jetzt etwas tun, damit alle in den Genuss der Vorteile der Digitalisierung kommen.

Brüssel, 19. März 2018

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

ANMERKUNGEN

[1] Siehe z. B. http://www.independent.co.uk/news/uk/politics/election-2017-facebook-ads-marginal-seats-tories-labour-outdated-election-spending-rules-a7733131.html [Zugriff am 18.3.2018].

[2] Die Resolution ist hier einsehbar: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf [Zugriff am 18.3.2018].

[3] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267„Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale", veröffentlicht am 26.03.2014 im Amtsblatt Nr. 71 der italienischen Datenschutzbehörde [doc. web n. 3013267].

[4] https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux „Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?", veröffentlicht am 08.11.2016 von der französischen Datenschutzbehörde Commission Nationale de l'informatique et des libertés.

[5] https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Leitlinien für politische Kampagnenführung der britischen Datenschutzbehörde [20170426].

[6] Gemäß Artikel 57 Absatz 1 Buchstabe d der DSGVO muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet [...] die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren.

[7] Siehe Mit gutem Beispiel vorangehen: Strategie des EDSB für 2015-2019, S. 17. Unserer Ansicht nach bezieht sich der Begriff „Big Data" auf die Praxis des Kombinierens immenser Mengen von Informationen aus verschiedenen Quellen und ihre Analyse; dabei kommen komplexere Algorithmen als Grundlage der Entscheidungsfindung zur Anwendung. Einer der größten Vorteile von Big Data für Unternehmen und Behörden leitet sich jedoch aus der gruppen- und personenbezogenen Überwachung von menschlichem Verhalten her und beruht auf ihrem Prognosepotenzial; Stellungnahme 4/2015 des EDSB, Der Weg zu einem neuen digitalen Ethos: Daten, Würde und Technologie, 11.9.2015, S. 6.

[8] Bei Profilen, die zur Vorhersage von menschlichen Verhaltensweisen dienen, besteht die Gefahr der Stigmatisierung: bestehende Stereotypen, soziale und kulturelle Segregation und Ausgrenzung werden verstärkt, da eine derartige „kollektive Intelligenz" die Wahlmöglichkeiten des Einzelnen und die Gleichberechtigung zunichte macht. Es könnte sich herausstellen, dass derartige „Filterblasen" oder „persönliche Hallräume" gerade die Kreativität, die Innovation und die Möglichkeiten der freien Meinungsäußerung und der Versammlungsfreiheit ersticken, dank derer digitale Technologien sich überhaupt entwickeln konnten; Stellungnahme 4/2015 des EDSB, S. 13 (Textstellen ausgelassen).

[9] Stellungnahme 7/2015 des EDSB, Bewältigung der Herausforderungen in Verbindung mit Big Data, S. 9.

[10] Bericht der Ethik-Beratergruppe des EDSB vom Januar 2018, S. 28.

[11] Siehe z. B. The Economist, How the World Was Trolled (4.-10. November 2017), Bd. 425, Nr. 9065, S. 21-24.

[12] Allcott, H. und Gentzkow, M., Social Media and Fake News in the 2016 Election (Spring 2017). Stanford University, Journal of Economic Perspectives, Bd. 31, Nr. 2, S. 211-236. https://web.stanford.edu/~gentzkow/research/fakenews.pdf, S. 219.

[13] In einem der Experimente wurde Nutzern der sozialen Plattform erzählt, wie ihre Freunde nach eigener Aussage gewählt hätten, was zu einem statistisch signifikanten Anstieg des Bevölkerungssegments (0,14 % der Bevölkerung im wahlfähigen Alter bzw. etwa 340 000 Wähler) führte, das bei den Kongresswahlen 2010 seine Stimme abgab; Allcott, H. und Gentzkow, M., Social Media and Fake News in the 2016 Election (Spring 2017), Stanford University, Journal of Economic Perspectives, Bd. 31, Nr. 2, S. 211-236., S. 219). In einer anderen Studie behaupteten die Forscher, dass Unterschiede bei den Google-Suchergebnissen die Wahlpräferenzen der unentschiedenen Wähler um 20 % verschieben könnten; Zuiderveen Borgesius, F. & Trilling, D. & Möller, J. & Bodó, B. & de Vreese, C. & Helberger, N. (2016). Should we worry about filter bubbles?. Internet Policy Review, 5(1). DOI: 10.14763/2016.1.401, S. 9.

[14] Erwägungsgrund 4 der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, im Folgenden „DSGVO".

[15] Wie der Europäische Gerichtshof für Menschenrechte im Fall Orlowskaja Iskra gegen Russland feststellte, bilden freie Wahlen und Meinungsfreiheit, insbesondere die Freiheit der politischen Debatte, zusammen das Fundament eines jeden demokratischen Systems. Die beiden Rechte sind miteinander verbunden und verstärken sich gegenseitig: So ist beispielsweise die Meinungsfreiheit eine der Voraussetzungen, um die freie Meinungsäußerung des Volkes bei der Wahl der Legislative zu gewährleisten. Darum ist es im Vorfeld einer Wahl besonders wichtig, dass Meinungen und Informationen aller Art frei zirkulieren können. Im Rahmen der

Wahldebatten kommt der ungehinderten Ausübung der Redefreiheit durch die Kandidaten eine besondere Bedeutung zu (Textstellen ausgelassen), Abs. 110. http://hudoc.echr.coe.int/eng?i=001-171525.

[16] 2014 - Vorläufige Stellungnahme zum Thema „Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von Big Data"; 2015 - Stellungnahme 4/2015, Der Weg zu einem neuen digitalen Ethos: Daten, Würde und Technologie; 2015 - Stellungnahme 7/2015, Bewältigung der Herausforderungen in Verbindung mit Big Data. Ein Ruf nach Transparenz, Nutzerkontrolle, Datenschutz durch Technik und Rechenschaftspflicht; 2016 - Stellungnahme 8/2016 des EDSB zur kohärenten Durchsetzung von Grundrechten im Zeitalter von Big Data.

[17] http://docs.house.gov/meetings/IF/IF17/20171129/106659/HHRG-115-IF17-20171129-SD002.pdf, Anhörung des Ausschusses für Energie und Handel des US-Repräsentantenhauses mit dem Titel „Algorithms: How Companies' Decisions About Data and Content Impact Consumers" (Algorithmen: Wie Entscheidungen von Unternehmen über Daten und Inhalte die Verbraucher beeinflussen), 27.11.2017, S. 2.

[18] https://www.wsj.com/articles/its-time-to-bust-the-online-trusts-1509487518 (CF NYC-Artikel, Yelp-Artikel WSJ) The Wall Street Journal 'It's Time to Bust the Online Trusts' (Es ist an der Zeit, die Online-Trusts zu zerschlagen), 31.10.2017.

[19] Einige der erstellten Daten sind nicht personenbezogen. Dabei handelt es sich um Daten, die aus Aktivitäten wie der Analyse von Wettermustern, der Erforschung des Weltraums, wissenschaftlichen Material- oder Designtests oder den Risiken im Zusammenhang mit dem Wertpapierhandel an den Finanzmärkten stammen. Ein großer Teil davon sind jedoch Daten, die wir selbst erstellen oder die über uns erstellt werden (The Information Accountability Foundation, Origins of Personal Data and its Implications for Governance (Die Information Accountability Foundation, Herkunft personenbezogener Daten und ihre Auswirkungen auf die Governance), siehe http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf).

[20] Basierend auf dem Rahmen von https://biblio.ugent.be/publication/8541057. Für nähere Informationen siehe auch:
https://www.maastrichtuniversity.nl/sites/default/files/mcel_master_working_paper_20172_mondschein_2.pdf.

[21] Artikel 4 Absatz 2 DSGVO.

[22] Schwartz, E., Finding our way with digital bread crumbs, MIT Technology Review, 18. August 2010; Artikel 29-Datenschutzgruppe - Leitlinien zum Recht auf Datenübertragbarkeit, WP 242.

[23] Bericht des Sonderberichterstatters für das Recht auf Privatheit, 19.10.2017, Abs. 31-32; Stellungnahme der Artikel 29-Datenschutzgruppe zur verhaltensorientierten Werbung, S. 7, 10-11.

[24] Facebook enthüllte kürzlich, dass während der Präsidentschaftswahlen 2016 mehr als 62 000 Nutzer ihre Teilnahme an 129 Veranstaltungen zugesagt hatten, die von russischen Trollen organisiert wurden, z. B. an Kundgebungen der verfeindeten Gruppen Heart of Texas und United Muslims of America, deren unterschiedliches Publikum sich zur selben Zeit am selben Ort versammelte; Quelle. Als sich am Wahltag eine Falschmeldung über mögliche Manipulationen in Sizilien im Internet verbreitete, retweeteten Twitter-Nutzer die Falschinformationen laut einer Analyse von EU DisinfoLab etwa 1000 Mal. Auf Facebook wurde dieselbe Geschichte gar mehr als 18 000 Mal geteilt – und das nur auf öffentlichen Facebook-Seiten. Wie sich diese Falschinformationen auf den privaten Seiten der Facebook-Nutzer verbreiteten (und vor allem, wer dabei geholfen hat, sie zu verbreiten), ist nicht bekannt; **Quelle.**

[25] The Atlantic, The Dark Side of That Personality Quiz You Just Took, 13.7.2017. https://www.theatlantic.com/technology/archive/2017/07/the-internet-is-one-big-personality-test/531861/.

[26] Stellungnahme der Artikel 29-Datenschutzgruppe zum Device Fingerprinting. Für einen Überblick über die verschiedenen Tracking-Technologien siehe Mondschein, C., The Regulation of Targeted Behavioural Advertising in the European Union, MCEL Master Working Paper 2017/2. Im Jahr 2017 wurde eine Methode eingeführt, die es erlaubt, eine Person über mehrere Browser auf demselben Gerät zu verfolgen; Browser Fingerprinting Tech Works Across Different Browsers for the First Time, 24.2.2017, https://spectrum.ieee.org/tech-talk/telecom/internet/new-online-fingerprinting-technique-works-across-browsers [Zugriff am 18.3.2018].

[27] Helberger, N., Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law, 6.2. 2016, S. 3.

[28] Mondschein, S. 9.

[29] Vermeulen, G., Lievens, E. (eds.), Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data, 2017, S. 316.

[30] Kaltheuner, F. und Bietti, E., Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR, IRP&P, S. 3.

[31] Mondschein, S. 11.

[32] Kaltheuner, F. und Bietti, S. 5.

[33] Kaltheuner, F. und Bietti, S. 4.

[34] OCEAN ist ein Akronym für openness (Offenheit), conscientiousness (Gewissenhaftigkeit), extroversion (Extraversion), agreeableness (Verträglichkeit), neuroticism (Neurotizismus). Siehe z. B. Grassegger, H. und Krogerus, M., The Data That Turned the World Upside Down, Stanford

Public Policy Program, 28.1.2017; Polonski, P., How artificial intelligence conquered democracy, 8.8.2017, http://theconversation.com/how-artificial-intelligence-conquered-democracy-77675 [Zugriff am 18.3.2018].

[35] z. B.: IBM Watson 'Leveraging cognitive computing and social media data to generate deep constituent insights' https://www01.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/Jalal%20Mahmud%27s%20Presentation/$file/Jalal%20Mahmud%27s%20Presentation.pdf.

[36] Siehe den Bericht des Ausschusses für Energie und Handel des US-Repräsentantenhauses, Unterausschuss für Kommunikation und Technologie und Unterausschuss für digitalen Handel und Verbraucherschutz, 27.11.2017, Anhörung mit dem Titel „Algorithms: How Companies' Decisions About Data and Content Impact Consumers" (Algorithmen: Wie Entscheidungen von Unternehmen über Daten und Inhalte die Verbraucher beeinflussen). Mindestens eine Datenschutzbehörde hat die Rechtmäßigkeit der Verwendung von „Custom Audiences" aus Kundenlisten zur Erstellung von „Lookalike Audiences" ohne Zustimmung der betroffenen Personen in Frage gestellt; Pressemitteilung des Bayerischen Landesamtes für Datenschutzaufsicht, Facebook Custom Audience bei bayerischen Unternehmen, 4.10.2017.

[37] Die Wirksamkeit dieser Vorhersagen wurde in einem der von den Wissenschaftlern der Stanford University durchgeführten Experimente geprüft. Sie fanden heraus, dass ein Computer die Persönlichkeit einer Person durch die Auswertung ihrer „Likes" auf Facebook besser vorhersagen konnte als die meisten ihrer Freunde und Familienangehörigen. Nur der Ehepartner einer Person sei den Ergebnissen des Computers nahegekommen. Die Computer-Vorhersagen basierten darauf, welche Artikel, Videos, Künstler und andere Gegenstände die Person auf Facebook gelikt hatte. https://news.stanford.edu/2015/01/12/personality-computer-knows-011215/.

[38] *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, Journal of Information Rights, Policy, and Practice 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR' S. 9 Bd. 2, Nr. 2 (2017).

[39] Mikrozielgruppenansprache bzw. Mikrotargeting ist ein aktueller Begriff, der zunehmend verwendet wird, wenn ein Stichprobenverfahren auf einer detaillierten Segmentierung der Zielgruppe basiert, meist in Online-Werbespots, um personalisierte Botschaften oder Angebote zu erstellen und deren Wirkung richtig einzuschätzen. Im politischen Kontext wurde der Begriff zunächst im Rahmen der Lobbyarbeit im US-amerikanischen Wahlkampf verwendet; Barbu, O., Microtargeting in social media: definitions and ethical issues, Studia Universitatis Babes Bolyai Ephemerides, 58, 2013, S. 83-90. Um ihn von zu kommerziellen Zwecken eingesetztem Mikrotargeting abzugrenzen, wurde der Begriff „politisches Mikrotargeting" definiert als Nutzung verschiedener Kommunikationsmittel (Post, Telefon, Werbung, Direktwerbung, Werbung in sozialen Medien usw.) zur Kommunikation mit und zum Aufbau einer Beziehung zu potenziellen Wählern; Bodó, B. & Helberger, N. & de Vreese, C. (2017), Political microtargeting: a Manchurian candidate or just a dark horse?, Internet Policy Review, 6(4). DOI: 10.14763/2017.4.776. Siehe auch Colin J. Bennett; Voter databases, microtargeting, and data protection law: can political parties campaign in Europe as they do in North America?, International Data Privacy Law, Band 6, Ausgabe 4, 1. November 2016, S. 261-275.

[40] Damian Tambini, zitiert in Pennycook und Rand, The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Stories Increases Perceived Accuracy of Stories Without Warnings, 2017.

[41] Ein erfolgreicher Tech-Unternehmer und Dozent schrieb 2012 in einem Artikel mit dem Titel „The art of manipulation" (Die Kunst der Manipulation): 'We build products meant to persuade people to do what we want them to do. We call these people "users" and even if we don't say it aloud, we secretly wish every one of them would become fiendishly addicted' (Wir entwickeln Produkte, die Menschen dazu bewegen sollen, das zu tun, was wir wollen. Wir nennen diese Leute „Nutzer", und selbst wenn wir es nicht laut sagen, so wünschen wir uns insgeheim, dass jeder von ihnen unheimlich süchtig wird.); https://techcrunch.com/2012/07/01/the-art-of-manipulation/ [Zugriff am 18.3.2017].

[42] Siehe z. B. Tim Wu, The Attention Merchants, 2017; Roger McNamee, Why not regulate social media like tobacco or alcohol?, https://www.theguardian.com/media/2018/jan/29/social-media-tobacco-facebook-google [Zugriff am 18.3.2017]; https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them/ [Zugriff am 18.3.2017].

[43] Siehe z. B. https://www.psychologytoday.com/blog/in-one-lifespan/201510/facebook-and-the-fear-missing-out-fomo [Zugriff am 18.3.2017].

[44] Am 17.3.2018 erschienen Artikel, in denen es um den mutmaßlichen Missbrauch der Daten von 50 Millionen Facebook-Profilen ging; New York Times, How Trump Consultants Exploited the Facebook Data of Millions; Guardian, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.

[45] Siehe z. B. den Bericht der nationalen Telekommunikations- und Informationsverwaltung des US-Handelsministeriums, „Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities" (Mangelndes Vertrauen in die Privatsphäre und Sicherheit im Internet kann wirtschaftliche und andere Online-Aktivitäten beeinträchtigen), 13.5.2016.

[46] http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52016DC0288 Europäische Kommission „Online-Plattformen im digitalen Binnenmarkt - Chancen und Herausforderungen für Europa“ [SWD82016) 172 final] 25.5.2016.

[47] Beispiele für Engagement sind die Organisation oder Teilnahme an sozialen Online-Kampagnen oder Petitionen, der Aufbau von verursachergerechten Communities in sozialen Medien, die Beteiligung der Bürger an der Online-Zuweisung lokaler Mittel, die Erarbeitung und Überprüfung von Rechtsvorschriften oder Ideen zur Crowdsourcing-Politik. Weitere Beispiele finden sich unter: https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE253/RAND_PE253.pdf, https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF373/RAND_CF373.pdf.

[48] Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED), Feasibility Study on the Use of Internet in Elections, MSI-MED (2016)10rev (9. März 2017), https://rm.coe.int/16806fd666, S. 8.

[49] http://ec.europa.eu/justice/citizen/document/files/2015_public_consultation_booklet_en.pdf, S. 11.

[50] Siehe z. B. Digiday UK Interview mit Guardian Media CEO 19.12.2017; FT, Advertisers’ challenge to Facebook and Google (Werbekunden fordern Facebook und Google heraus) https://www.ft.com/content/d43fd706-0fec-11e8-8cb6-b9ccc4c4dbbb 12.02.2018.

[51] Eine kritische Studie zu dieser Initiative ist Global Voices AdVox, Global Free Basics in Real Life: Six case studies on Facebook's internet “On Ramp” initiative from Africa, Asia and Latin America, 27.7.2017.

[52] CNBC, Seed funding slows in Silicon Valley, 1.8.2017; https://www.cnbc.com/2017/08/01/seed-funding-slows-in-silicon-valley.html [Zugriff am 18.3.2018].

.[53] *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, S. 9. Manche Wissenschaftler sind weniger optimistisch, was das Potenzial der personalisierten Kommunikation angeht. Sie weisen darauf hin, dass gezielte Online-Werbung noch keine Klickrate von mehr als 0,5 Prozent erreicht habe und es daher den Anschein habe, dass die Technologie noch nicht in der Lage sei, das Verhalten einer Person wesentlich zu beeinflussen. https://policyreview.info/articles/analysis/should-we-worry-about-filter-bubbles, S. 10.

[54] Die aus Big Data-Analysen gewonnenen Erkenntnisse können für eine Vielzahl von Zwecken genutzt werden, u. a. für Einstellungsentscheidungen, Kreditwürdigkeitsprüfungen, die Bewertung von Asylanträgen oder die Identifizierung und Sperrung gefälschter Social-Media-Konten. Für eine Übersicht siehe *https://journals.winchesteruniversitypress.org/index.php/jirpp/article/view/45*, S. 4-6.

[55] https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00035/544506-00035.pdf, The Progress & Freedom Foundation ‘Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech’ S. 18, 07.12.2009.

[56] Ebenda, siehe auch https://policyreview.info/articles/analysis/political-microtargeting-manchurian-candidate-or-just-dark-horse, S. 3 und 5. Siehe auch Ideen für die gemeinfreie praktische Anwendung von Datenanalyse und KI: https://medium.com/@drpolonski/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first-7b1257cb4285.

[57] Siehe z. B. S. 29, http://webbut.unitbv.ro/Bulletin/Series%20V/BULETIN%20I/03_Biea.pdf; S. 12, http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20%20The%20new%20political%20campaigning_final.pdf.

[58] https://medium.com/tow-center/cambridge-analytica-the-geotargeting-and-emotional-data-mining-scripts-bcc3c428d77f Medium, ‘Cambridge Analytica: the Geotargeting and Emotional Data Mining Scripts’ 13.10.2017.

[59] https://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting Internet Policy Review ‘Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques.’ 31.12.2017.

[60] P 3, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

[61] https://policyreview.info/articles/analysis/political-microtargeting-manchurian-candidate-or-just-dark-horse, Computational Propaganda Research Project, Working Paper No. 2017.11, Computational Propaganda Worldwide: Executive Summary, S. 8. Samuel C. Woodley und Philip N. Howard, University of Oxford.

[62] https://iconewsblog.org.uk/2017/05/17/information-commissioner-elizabeth-denham-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/, https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/ Information Commissioner’s Office, ‘The Information Commissioner opens a formal investigation into the use of data analytics for political purposes’ (Britische Datenschutzbehörde, Die britische Datenschutzbeauftragte leitet eine förmliche Untersuchung in Bezug auf die Verwendung von Datenanalyse für politische Zwecke ein), 17.05.2017, und ‘Update on ICO investigation into data analytics for political purposes’ (Aktuelle Informationen

zur Untersuchung der britischen Datenschutzbehörde in Bezug auf Datenanalyse für politische Zwecke), 13.12.2017, Elizabeth Denham, britische Datenschutzbeauftragte.

[63] Forscher im Bereich des Wähler-Mikrotargeting gehen davon aus, dass datengesteuerte Kampagnen und damit verbundene Mikrotargeting-Techniken zunehmend in die europäische politische Landschaft Einzug erhalten werden. Siehe z. B. https://academic.oup.com/idpl/article-abstract/6/4/261/2567747?redirectedFrom=fulltext, S. 262.

[64] Jason Ng, 2015 https://citizenlab.ca/2015/07/tracking-censorship-on-wechat-public-accounts-platform/

[65] Marwick und Lewis 2017.

[66] Brundage, M., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation; S. 45.

[67] Siehe O'Neil, C., Weapons of Math Destruction, 2016, S. 195.

[68] Brundage, S. 44.

[69] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6. Oktober 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, S. 36.

[70] Siehe z. B. Moore, M., Tech Giants and civic power, Centre for the Study of Media, Communication and Power, April 2016.

[71] Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED), Feasibility Study on the Use of Internet in Elections, MSI-MED (2016)10rev (9. März 2017), https://rm.coe.int/16806fd666, S. 13.

[72] Ebenda.

[73] http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2010)037-e Europäische Kommission für Demokratie durch Recht (Venedig-Kommission), 'Report on the timeline and inventory of political criteria for assessing an election' (Bericht über den Zeitplan und das Inventar der politischen Kriterien für die Bewertung einer Wahl), S. 4, Studie Nr. 558/2009, Straßburg, 21.10.2010.

[74]http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20%20The%20new%20political%20campaigning_final.pdf London School of Economics, Media Policy Brief 19 'The New Political Campaigning' S. 6. März 2017

[75] Erwägungsgrund 2 DSGVO.

[76] Die in dieser Stellungnahme dargestellte Analyse stützt sich auf die DSGVO.

[77] Artikel 9 DSGVO.

[78] Der Vorschlag der Kommission für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (E-Privacy-VO) sieht vor, dass „Nachrichten von politischen Parteien, die sich über elektronische Kommunikationsdienste an natürliche Personen wenden, um für ihre Parteien zu werben" sowie „Nachrichten [...], die von anderen Organisationen ohne Erwerbszweck übermittelt werden, um die Zwecke ihrer Organisation zu fördern" in den Anwendungsbereich von „Direktwerbung" fallen: Erwägungsgrund 32, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), 10.1.2017 COM(2017) 10 final. In den Leitlinien für politische Kampagnenführung der britischen Datenschutzbehörde wird die Definition von Direktwerbung auf Aktivitäten im Zusammenhang mit politischen Kampagnen ausgedehnt.

[79] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:de:PDF. Amtsblatt der Europäischen Union L 337/11, Richtlinie 2009/136/EG vom 25. November 2009. Weitere Informationen über die unterschiedlichen Auswirkungen dieser Bestimmung finden Sie unter https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

[80] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241, Erwägungsgrund 22, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG. 2017/0003 (COD).

[81] Artikel 3 Absatz 2.

[82] Siehe z. B. http://www.telegraph.co.uk/news/2017/02/24/exclusive-tiny-canadian-company-helped-swing-brexit-vote-leave/; https://www.theguardian.com/technology/2017/may/14/robert-mercer-cambridge-analytica-leave-eu-referendum-brexit-campaigns.

[83] Für das Beispiel einer solchen Anwendung siehe https://medium.com/personaldata-io/quick-guide-to-asking-cambridge-analytica-for-your-data-52f9e74bd059;
https://www.theguardian.com/technology/2017/oct/01/cambridge-analytica-big-data-facebook-trump-voters.
Auf die Frage, ob Cambridge Analytica den amerikanischen Wählern alle 5000 Datenpunkte in ihrem Profil zur Verfügung stellen würde, wenn sie einen Antrag nach britischem Datenschutzrecht stellten, erklärte ihr CEO Alexander Nix fälschlicherweise, das Gesetz gelte nicht für Amerikaner.

[84] Siehe ein ähnliches Problem im Zusammenhang mit mHealth: https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf.
[85] Artikel 28 Absatz 3 DSGVO.
[86] Big-Data-Leitlinien der britischen Datenschutzbehörde, S. 5.
[87] Vorabentscheidungsersuchen an den EuGH in der Rechtssache C-210/16, http://curia.europa.eu/juris/document/document.jsf?text=&docid=181773&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1.
[88] Siehe die Stellungnahme des Generalanwalts in der Rechtssache C-210/16, http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=DE.
[89] Siehe die Stellungnahme des Generalanwalts in der Rechtssache C-210/16, Absatz 57 http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=DE.
[90] Artikel 5 Absatz 1 Buchstabe b.
[91] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6. Oktober 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, S. 32-33.
[92] Hier erfahren Sie, welche Informationen politische Parteien in Deutschland über die Wähler besitzen: https://policyreview.info/articles/analysis/restrictions-data-driven-political-microtargeting-germany.
[93] 'Incompatible: The GDPR in the Age of Big Data' Tal Z. Zarsky, S. 1006-1007, http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr.
[94] Ebenda, S. 34.
[95] 'Incompatible: The GDPR in the Age of Big Data' Tal Z. Zarsky, S. 1008-1009, http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr.
[96] Ebenda, S. 47-48.
[97] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6. Oktober 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, S. 40.
[98] Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED), Feasibility Study on the Use of Internet in Elections, MSI-MED (2016)10rev (9. März 2017), https://rm.coe.int/16806fd666, S. 6.
[99] London School of Economics 'Media Policy Brief 19: The New Political Campaigning' S. 9, http://eprints.lse.ac.uk/71945/7/LSE%20MPP%20Policy%20Brief%2019%20%20The%20new%20political%20campaigning_final.pdf.
[100] Political finance regulation at the June 2017 UK general election 'Report on the UK Parliamentary General Election held on 8 June 2017' November 2017 S. 12-15, https://www.electoralcommission.org.uk/__data/assets/pdf_file/0004/237550/Political-finance-regulation-at-the-June-2017-UK-general-election-PDF.pdf.
[101] Common Market Law Review, Bd. 54 (2017), Ausgabe 5. The perfect match? A closer look at the relationship between EU consumer law and data protection law, S. 7, https://www.ivir.nl/publicaties/download/CMLR_2017.pdf.
[102] Vorläufige Stellungnahme des EDSB, S. 23.
[103] Artikel 6 Absatz 1.
[104] Dies könnte gegen Artikel 6 Absatz 1 Buchstabe a und Anhang I Nr. 7 der Richtlinie über unlautere Geschäftspraktiken, S. 149 der Verbraucherschutzpolitik, -strategien und -statistiken verstoßen http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf.
[105] Indem ein Unternehmer Verbrauchern gefälschte „Likes" präsentiert, kann er sie über seinen eigenen Ruf oder den Ruf seiner Produkte oder Dienstleistungen in die Irre führen, was möglicherweise dazu führt, dass die Verbraucher Transaktionsentscheidungen treffen, die sie sonst nicht getroffen hätten. Artikel 6 der Richtlinie, http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf, S. 144.
[106] Neuere Forschungen deuten beispielsweise darauf hin, dass Erfolg in sozialen Medien eine selbstverstärkende Wirkung haben kann. Jedes Facebook-Profil und jeder Beitrag enthalten viele „soziale Informationen": Jeder Nutzer kann sofort den augenscheinlichen Erfolg oder Misserfolg bestimmter Beiträge und Profile sehen, indem er sich die Anzahl der Shares, Likes und Follower anschaut, die Facebook stets zur Verfügung stellt. Eine hohe Anzahl von Interaktionen kann somit die große Bedeutung und Gültigkeit bestimmter Botschaften signalisieren. Viele Persönlichkeiten des öffentlichen Lebens, insbesondere Politiker, verfügen über Hunderttausende gefälschter Follower auf Twitter. Facebook hingegen hat weniger automatisierte Profile, obwohl ihre Zahl immer noch auf rund 65 Millionen geschätzt wird (Facebook hatte bis März 2017 fast zwei Milliarden Profile), http://www.delorsinstitut.de/2015/wpcontent/uploads/2017/04/20170419_SocialNetworksandPopulismDittrich.pdf.

[107] Der Europäische Gerichtshof für Menschenrechte hat erkannt, dass die nationalen Behörden einen größeren Ermessensspielraum haben, wenn es darum geht, die Notwendigkeit und Verhältnismäßigkeit einer Beeinträchtigung der kommerziellen Meinungsäußerung festzustellen (siehe z. B. Markt intern Verlag GmbH und Klaus Beermann gegen Deutschland, 20. November 1989; Krone Verlag GmbH & Co. KG gegen Österreich (Nr. 3), 11. Dezember 2003, Randnr. 31), wobei die Freiheit der politischen Rede ein höheres Schutzniveau verdient und ein diesbezüglicher Eingriff nur aus gewichtigen Gründen gerechtfertigt sein kann (siehe z. B. Lingens gegen Österreich, 8. Juli 1986).

[108] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/print/1170616, Garante per la Protezione dei Dati Personali, Resolution zur Verwendung von Personendaten für die politische Kommunikation, siehe Präambel. [doc. web n.1170616].

[109] Stellungnahme des EDSB zur kohärenten Durchsetzung von Grundrechten im Zeitalter von Big Data, S. 14.

[110] Aus der Pressemitteilung der Wettbewerbsbehörde: „Wir sehen vor allem die Datensammlung außerhalb des sozialen Netzwerks von Facebook und ihre Zusammenführung mit dem Facebook-Konto als problematisch an. Mithilfe von Schnittstellen fließen auch dann Daten an Facebook und werden dort gesammelt und verwertet, wenn man andere Internetseiten besucht. Dies geschieht sogar schon, wenn man z. B. einen „Gefällt-mir-Button" gar nicht nutzt, aber eine entsprechende Seite aufgerufen hat, in die ein solcher Button eingebettet ist. Dies ist den Nutzern nicht bewusst. Wir sehen nach dem jetzigen Stand der Dinge auch nicht, dass zu diesem Verhalten von Facebook, dem Daten-Tracking und der Zusammenführung mit dem Facebook-Konto, eine wirksame Einwilligung der Nutzer vorliegt. Das Ausmaß und die Ausgestaltung der Datensammlung verstößt gegen zwingende europäische Datenschutzwertungen." https://webgate.ec.europa.eu/multisite/ecn-brief/en/content/germany-bundeskartellamt.

[111] https://edps.europa.eu/sites/edp/files/publication/17-11-30_statement_2nd_meeting_dch_en.pdf Zweite Sitzung des Digital Clearinghouse, Brüssel 27.11.2017.

[112] https://ec.europa.eu/info/consultations/public-consultation-fake-news-and-online-disinformation_de Europäische Kommission „Öffentliche Konsultation zu Fake News und online verbreiteter Desinformation" 13.11.2017-23.02.2018.

[113] z. B. https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/.

[114] https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_de.pdf, Stellungnahme 6/2017, Stellungnahme des EDSB zu dem Vorschlag für eine Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-VO) S. 16-17.

[115] https://edps.europa.eu/press-publications/press-news/blog/crucial-moment-communications-privacy_en European Data Protection Supervisor, A crucial moment for communications privacy (Europäischer Datenschutzbeauftragter, Ein entscheidender Moment für den Datenschutz bei der Kommunikation). 27.09.2017.

[116] Weitere Informationen zu den verschiedenen Verfahren der Profilerstellung: Privacy International Submission, S. 4-6.

[117] https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_de.pdf, Europäischer Datenschutzbeauftragter, Stellungnahme 1/2015, Mobile-Health-Dienste *Wie lassen sich technologische Innovation und Datenschutz miteinander vereinbaren?* Absatz 32.

[118] https://policyreview.info/articles/analysis/restrictions-data-driven-political-microtargeting-germany, Internet Policy Review 'Restrictions on data-driven political micro-targeting in Germany' S. 2. 31.12.2017.

[119] Verweis auf den Bericht der Sachverständigengruppe.

[120] Siehe z. B. Bericht der Sachverständigengruppe; für einen Überblick über die Strategien: Dead Reckoning: Navigating Content Moderation after „Fake News", Februar 2018; Gesetzentwurf von Macron, der von Online-Plattformen verlangt offenzulegen, wenn als Information gekennzeichnete Artikel gesponsert werden; Vereinigtes Königreich **; Deutschland**.

[121] https://www.ivir.nl/publicaties/download/CMLR_2017.pdf, Common Market Law Review, Bd. 54 (2017), Ausgabe 5. The perfect match? A closer look at the relationship between EU consumer law and data protection law, S. 28.

[122] http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf, S. 143. Ebenso können sie sich nach dem Datenschutzgesetz, je nach Art der Datenverarbeitung, sowohl als für die Verarbeitung Verantwortliche als auch als Auftragsverarbeiter qualifizieren.

[123] Vorläufige Stellungnahme des EDSB, S. 35.

[124] https://www.ivir.nl/publicaties/download/CMLR_2017.pdf, Common Market Law Review, Bd. 54 (2017), Ausgabe 5. The perfect match? A closer look at the relationship between EU consumer law and data protection law, S. 20-22.

[125] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/print/1170616, Garante per la Protezione dei Dati Personali, Resolution zur Verwendung von Personendaten für die politische Kommunikation, siehe Präambel. [doc. web n. 1170546].

[126] http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-II-Repository_CNIL_UJI_October-2016.pdf, Phaedra II 'Guidance on political campaigning' S. 2. Oktober 2016.
[127] https://www.cnil.fr/sites/default/files/atoms/files/guide_cnil_et_csa.pdf. CNIL 'Pluralisme dans les médias audiovisuels. Règles informatique et Libertés'. Außerdem hat die britische Datenschutzbehörde kürzlich erklärt, dass sie mit der Wahlkommission bei der Untersuchung von Datenanalysen für politische Zwecke zusammenarbeite, https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/.

[128] Stellungnahme des EDSB zur kohärenten Durchsetzung von Grundrechten im Zeitalter von Big Data, S. 11.
[129] Diese Befugnis ist nicht auf die Aufsichtsbehörden beschränkt, sondern erstreckt sich auch auf die Mitgliedstaaten, die Aufsichtsbehörden, den Ausschuss und die Kommission.
[130] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Artikel 29-Datenschutzgruppe, Leitlinien zur Transparenz gemäß Verordnung (EU) 2016/679, S. 19.
[131] Aus der empirischen Forschung über den Einsatz von Techniken des politischen Mikrotargeting durch die politischen Parteien der Niederlande: „Stellungnahme 7/2015 Bewältigung der Herausforderungen in Verbindung mit Big Data", Vor allem D66 und die Seniorenpartei 50PLUS lehnen die Datenerhebung und den Einsatz von PBT grundsätzlich ab. Während D66 sich als Datenschutz-Vorkämpfer präsentiert und daher niemals Informationen über (Gruppen von) Wählern sammeln und nutzen werde, warnt 50PLUS-Wahlkampfleiter 6 vor der Gefahr eines unverantwortlichen Umgangs mit den Daten, die durch das von ihm als „moralisch unverantwortlich" bezeichnete „quasi Stalken von Menschen" gesammelt würden. (https://policyreview.info/articles/analysis/two-crates-beer-and-40-pizzas-adoption-innovative-political-behavioural-targeting).
[132] https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf Stellungnahme 9/2016 Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), Hin zu einer intensiveren Einbindung der Nutzer in das Management und die Verarbeitung personenbezogener Daten, Absatz 1.

[133] Pressemitteilung: Verbraucher in Europa und im Nahen und Mittleren Osten stehen Prioritäten in den Bereichen Piraterie und Sicherheit zwiespältig gegenüber, 17.05.2017. https://f5.com/about-us/news/press-releases/european-and-middle-eastern-consumers-deeply-conflicted-over-privacy-and-security-priorities-19968.
[134] Europäische Kommission, Datenschutz Vorschriften für den Schutz personenbezogener Daten innerhalb und außerhalb der EU. http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf.
[135] Stellungnahme „Bewältigung der Herausforderungen in Verbindung mit Big Data", S. 29; siehe auch https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf, S. 14.
[136] Zum Grundsatz der Praxistauglichkeit und Wirksamkeit siehe https://academic.oup.com/hrlr/article-abstract/5/1/57/606751 *Human Rights Law Review*, Bd. 5, Ausgabe 1 'The Creativity of the European Court of Human Rights', 01.01.2015.

[137] Artikel 47 Absatz 1 der EU-Grundrechtecharta. In seinem Urteil vom 15. Mai 1986 hat der Gerichtshof das Recht auf einen wirksamen Rechtsbehelf als allgemeinen Grundsatz des Unionsrechts verankert (Rechtssache 222/84, Johnston [1986]. Slg. 1651; siehe auch Urteil vom 15. Oktober 1987, Rechtssache 222/86, Heylens [1987]. Slg. 4097 und Urteil vom 3. Dezember 1992, Rechtssache C-97/91, Borelli [1992]. Slg. I-6313).
[138] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6. Oktober 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, S. 41-42. Siehe auch die Stellungnahme der Artikel 29-Datenschutzgruppe zu Profilerstellung und automatisierter Entscheidungsfindung, S. 5.
[139] z. B. MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6. Oktober 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing

techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, S. 41-42.

[140] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6. Oktober 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", https://rm.coe.int/msi-net-4th-meeting-18-19-september-2017/168075f8e9, S. 41-42.

[141] Generaldirektion Interne Politikbereiche, 'Overview of existing collective redress schemes in EU Member States' (Überblick über die bestehenden kollektiven Rechtsbehelfe in den EU-Mitgliedstaaten). Siehe z. B. S. 9, http://www.europarl.europa.eu/document/activities/cont/201107/20110715ATT24242/20110715ATT24242EN.pdf.

[142] Während des Prozesses der Ausarbeitung der DSGVO empfahl der EDSB dem Gesetzgeber, dass Einzelpersonen angesichts der deutlichen Hindernisse, in der Praxis einen Ausgleich für Schäden zu erlangen, die Möglichkeit erhalten sollten, sich bei Gerichtsverfahren von Einrichtungen, Organisationen und Verbänden vertreten zu lassen. Siehe Stellungnahme 3/2015 des EDSB „Eine große Chance für Europa – Empfehlungen des EDSB zu den Optionen der EU für die Datenschutzreform", S. 6. https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_de.pdf.

[143] Stellungnahme des EDSB zum Vorschlag für eine E-Privacy-VO.

[144] Die Möglichkeit für ein Vertretungsorgan, eine Sammelklage im Namen nicht identifizierbarer Opfer einzuleiten (Opt-out).

[145] In Bezug auf kollektive Opt-out-Rechtsbehelfe erklärte BEUC, dass sich in verschiedenen Fällen gezeigt habe, dass das Opt-out-Verfahren viel wirksamer sei als das Opt-in-Verfahren (im Durchschnitt wenden nur etwa 1 % aller geschädigten Verbraucher das Opt-in-Verfahren an). Es sei schwierig, die Verbraucher zur Unterzeichnung einer Opt-in-Maßnahme zu bewegen, da sie dies bereits zu Beginn des Verfahrens tun müssten, noch bevor sie überhaupt wissen, ob es erfolgreich sein wird. In Portugal, den Niederlanden und teilweise in Spanien werde der kollektive Opt-out-Rechtsbehelf erfolgreich angewandt. In Belgien und im Vereinigten Königreich sei er erlaubt (im letzteren Fall seien private Schadenersatzklagen wegen Wettbewerbsverzerrung zulässig; dies sei jedoch erst vor kurzem eingeführt worden, weshalb es für eine Bewertung noch zu früh sei), http://www.beuc.eu/publications/beuc-x-2017-086_ama_european_collective_redress.pdf. Für einen europaweiten Überblick über die Mechanismen für kollektive Rechtsbehelfe siehe https://www.opensocietyfoundations.org/sites/default/files/litigation-kosa-hungary-thirdparty-20170201.pdf. Insbesondere in der Empfehlung „Gemeinsame Grundsätze für kollektive Unterlassungs- und Schadensersatzverfahren in den Mitgliedstaaten bei Verletzung von durch Unionsrecht garantierten Rechten" bestimmte die Kommission, dass der Rückgriff auf kollektive Rechtsschutzverfahren nach dem „Opt-out"-Prinzip mit Gründen der ordnungsgemäßen Rechtspflege gerechtfertigt werden könnte, siehe Artikel 21, Empfehlung der Kommission vom 11. Juni 2013 „Gemeinsame Grundsätze für kollektive Unterlassungs- und Schadensersatzverfahren in den Mitgliedstaaten bei Verletzung von durch Unionsrecht garantierten Rechten" (2013/396/EU) http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:JOL_2013_201_R_NS0013.