KONRAD ADENAUER STIFTUNG

Das Hacken der Wählerschaft

Die Nutzung personenbezogener Daten in politischen Kampagnen

www.kas.de

Impressum

Herausgeberin:
Konrad-Adenauer-Stiftung e. V., 2020, Berlin

Umschlagfoto: © iStock/Orbon Alija
Kapiteltrenner: S. 10 © Adobe Stock/Gorodenkoff;
S. 30 © Adobe Stock/Alexander; S. 42 © Shutterstock/mrmohock
Gestaltung und Satz: yellow too, Pasiek Horntrich GbR
Die Printausgabe wurde bei copy print Kopie & Druck GmbH, Berlin gedruckt.
Printed in Germany.

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

Der Text dieser Publikation ist lizenziert unter den Bedingungen von „Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 4.0 international", CC BY-SA 4.0 (abrufbar unter: https://creativecommons.org/licenses/by-sa/4.0/legalcode.de).

ISBN 978-3-95721-757-8

Das Hacken der Wählerschaft

Die Nutzung personenbezogener Daten in politischen Kampagnen

Auf einen Blick

- Obwohl datengetriebene politische Kampagnen an und für sich kein neues Phänomen sind, stellen die verwendeten Werkzeuge, die Menge der zugänglichen Daten sowie die potenzielle Fähigkeit zur Beeinflussung von Wählern ein neues und herausforderndes Szenario für das Rechtsstaatsprinzip dar.

- Seit dem Aufkommen des partizipativen und sozialen Internets können Internetnutzer jetzt Daten in einem komplexen Netzwerk erzeugen, ohne jedoch verpflichtet zu sein, Objektivität oder journalistische Standards als Säulen der Content-Erstellung zu berücksichtigen.

- Menschen in unterschiedlichen Ländern erhalten ihre Informationen und erfahren Dinge über politische Kandidaten und sonstige politische Fragen zunehmend durch soziale Netzwerke.

- In den vergangenen Jahren haben politische Parteien und Wahlkämpfer in allen Teilen der Welt stark in Online-Werbung investiert, die das Potenzial aufweist, mehr Menschen auf eine effiziente, zielgerichtete und zugängliche Weise zu erreichen.

- Firmen wie Cambridge Analytica sammeln enorme Mengen individueller Daten, verarbeiten diese zwecks Identifizierung und Prognose von noch intimeren individuellen Details und verwenden diese Profile und Prognosen anschließend zur Personalisierung politischer Nachrichten (z. B. zur Werbung auf sozialen Medien) mit dem Ziel einer Unterstützung der taktischen Entscheidungsfindung in Kampagnen.

- Wenn Wähler nicht verstehen, wie ihre Daten zu ihrer eigenen Beeinflussung verwendet werden, sind sie nicht in der Lage, ihre gesetzlichen Rechte in Bezug auf diese Informationen und die angewandten Strategien auszuüben.

- Aktuelle Praktiken einer unbefugten bzw. unrechtmäßigen Verarbeitung personenbezogener Daten haben zu einer starken Zunahme von Falschinformation und „Strategien zum digitalen Astroturfing“ geführt, die in der Lage sind, Bürger mit noch höherer Präzision zu beeinflussen.

- Die Möglichkeit, Lücken zwischen Wahlbestimmungen und den gesetzlichen Rahmenwerken für Wahlkampfaktivitäten unter Einbeziehung personenbezogener Daten zu schließen, hängt von zahlreichen Faktoren ab.

- Diese mangelnde Einheitlichkeit bzw. die falsche Auslegung der Leitlinien der DSGVO im Zusammenhang mit Wahlen könnte zu einem unterschiedlichen Grad des Schutzes personenbezogener Daten in Mitgliedstaaten führen und andere Regionen potenziell negativ beeinflussen.

- Die Wirksamkeit von Datenschutzbestimmungen hängt von der Fähigkeit und institutionellen Artikulierung der unterschiedlichen an diesem Prozess beteiligten Parteien ab.

- Datenschutzbestimmungen sind vollständig auf politische Kampagnen anwendbar und haben die Fähigkeit, die Verringerung der instrumentalen Verwendung personenbezogener Daten zu unterstützen, während sie gleichzeitig die Auswirkungen des Einsatzes von Falschinformation und computergestützter Propaganda zum Zweck der politischen Manipulation vermeiden.

- Ein Datenschutzansatz kann andere Anstrengungen strategisch verstärken und Falschinformationen in Wahlkampagnen durch die Sanktionierung der rechtswidrigen Verarbeitung personalisierter Daten verringern helfen, wodurch er zu einem wirksamen und nützlichen Rechtsinstrument im vorliegenden Kontext wird.

- Einerseits besteht die Rolle öffentlicher Organe und Institutionen darin, mittels ihrer Beschlüsse und Sanktionen die Compliance mit und die Wirksamkeit der Richtlinien der DSGVO zu verstärken. Andererseits haben politische Parteien und Wahlkämpfer die Pflicht zur Erfüllung gesetzlicher Anforderungen und tragen die volle Verantwortung für die Transparenz der Verarbeitung sowie das Vertrauen in die Verarbeitung der personenbezogenen Daten von Wählern.

- Die unbefugte bzw. rechtswidrige Verarbeitung personenbezogener Daten untergräbt – zusammen mit Falschinformationstechniken und der unfairen Verwendung von Bots, Profilen, Deep Fakes und anderen Mitteln – das Vertrauen der Wähler sowie die Integrität politischer Prozesse und sollte daher von Institutionen als Bedrohung der Demokratie betrachtet werden.

Eduardo Magrani

Doktor (Ph. D.) der Rechtswissenschaften und EIZ-Fellow der Konrad-Adenauer-Stiftung e. V. in Deutschland (Hauptabteilung Europäische und Internationale Zusammenarbeit, EIZ-Fellow für Globale Innovationspolitik, Digitalisierung und Künstliche Intelligenz). Professur für Recht und Technologie sowie Recht des geistigen Eigentums an der rechtswissenschaftlichen Fakultät FGV (Getulio Vargas Foundation), IBMEC und Päpstlichen Katholischen Universität von Rio de Janeiro (PUC-Rio) in Brasilien. Präsident des Nationalen Instituts für Datenschutz in Brasilien. Autor der „Digital Culture Trilogy“ in Brasilien „Democracy, Hyperconnectivity and Ethics: a trilogy on digital culture“ (Demokratie, Hyperconnectivity und Ethik: eine Trilogie der digitalen Kultur), die sich mit der Philosophie von Technologie, digitaler Demokratie, Datenschutz, Innovation, Cybersicherheit und künstlicher Intelligenz auseinandersetzt.

Inhaltsverzeichnis

Abstract 6

Einführung 7

1. Das Hacken der Wählerschaft 10

Der Echokammer-/Filterblaseneffekt 14
Erfahrungen in Brasilien: Wahlkampf 2018 16

2. Beachtung der Datenschutzbestimmungen bei Wahlen 30

3. Steigerung der Wirksamkeit und Schließen der Lücken 42

Abschließende Betrachtungen 57

Abstract

Die kontinuierliche Interaktion zwischen intelligenten Geräten, Online-Plattformen, Sensoren und Menschen weist auf das steigende Volumen von Daten hin, die erzeugt, gespeichert und verarbeitet werden und unser tägliches Leben zunehmend in unterschiedlichen Aspekten verändern. Der Kontext der „Hyperconnectivity" kann sowohl dem Staat als auch Unternehmen wirtschaftliche Vorteile bringen sowie Verbrauchern Komfort und Annehmlichkeiten bieten. Auf der anderen Seite bringt diese neue Realität signifikante Herausforderungen für den Raum demokratischer Prozesse mit sich, insbesondere im Zusammenhang mit politischen Kampagnen. Der potenzielle Schaden, der durch Strategien zur politischen Manipulation mithilfe der unbefugten bzw. unrechtmäßigen Verwendung von Daten verursacht werden kann, ist exponentiell, wenn berücksichtigt wird, wie neue Technologien in ihrer Gesamtheit angewendet werden. Dies stellt eine noch nie dagewesene Herausforderung für eine soziale Ordnung dar, deren Zusammenhalt auf dem Rechtsstaatsprinzip, auf Souveränität und auf der Zustimmung ihrer Bürger gegründet ist. Doch auch die Art und Weise, wie sich Demokratien dieser Herausforderung stellen werden, ist ein wesentlicher Faktor politischer Systeme. Erfahrungen aus den vergangenen Jahren zeigen, wie digitale Technologie die Demokratie untergraben und destabilisieren kann. Falschinformationen, algorithmische Manipulation, Beeinflussung von menschlichem Verhalten durch Microtargeting und Social Bots sind einige der aktuell eingesetzten Techniken und basieren meistens auf der unbefugten bzw. unrechtmäßigen Verarbeitung personenbezogener Daten. Zudem können diese Elemente in einzelnen Regionen mit entsprechender Anpassung an deren kulturelle, technologische und persönliche Gewohnheiten unterschiedlich verwendet werden. Bei der Erwägung dieses Kontexts ist es äußerst wichtig, dass Bestimmungen zu Privatsphäre und Datenschutz wirksam gestaltet und gestärkt werden. In der Europäischen Union liefert die Datenschutz-Grundverordnung (DSGVO) einen robusten gesetzlichen Rahmen, der zum Vorbild für eine entsprechende Gesetzgebung in vielen anderen Ländern geworden ist. Trotzdem bestehen gewisse Unterschiede zwischen Datenschutzbestimmungen, die hervorgehoben werden müssen, um festzustellen, wie sie für den Kontext politischer Kampagnen gestärkt und korrekt interpretiert werden können. Die vorliegende Forschungsarbeit beabsichtigt einen Vergleich zwischen der DSGVO und dem brasilianischen Allgemeinen Datenschutzgesetz (LGPD) und untersucht, wie beide Verordnungen bzw. Gesetzeswerke im Kontext der Verwendung personenbezogener Daten in politischen Kampagnen anwendbar sind. Der Einschluss des brasilianischen Szenarios in die vorliegende Analyse erfolgt aus zwei Gründen: (i) Die DSGVO war die Hauptsäule beim Entwurf des LGPD, obwohl letzteres einige Unterschiede in Bezug auf die Beachtung des Gesetzes (Compliance) aufweist, die erwogen werden sollten. Weiterhin (ii) durchläuft die brasilianische Politik einige bedeutende Episoden von Falschinformation und digitalen Astroturfing-Strategien zur politischen Manipulation, die adressiert und tiefer verstanden werden sollten. Abschließend liefert diese Abhandlung eine kritische Analyse der Wirksamkeit beider Gesetzeswerke und schlägt mögliche Lösungen vor.

Einführung

Politische Parteien und Aktivisten bzw. Wahlkämpfer haben, historisch betrachtet, unterschiedliche Kommunikationspraktiken und Technologien angewendet. Heute zeigen sich politische Kampagnen aufgrund der schnellen Entwicklung neuer digitaler Technologien und Kommunikationswerkzeuge zunehmend ausgereifter. Obwohl datenbasierte politische Kampagnen an und für sich kein neues Phänomen sind, stellen die verwendeten Werkzeuge, die Menge der zugänglichen Daten sowie die potenzielle Fähigkeit zur Beeinflussung von Wählern ein neues und herausforderndes Szenario für das Rechtsstaatsprinzip dar.[1]

Die Möglichkeit, gewaltige Datenbanken über Bürger mit Tausenden unterschiedlicher Informationen zu erstellen, die ein ausführliches Bild über Persönlichkeit, Wohnort, Beruf, Aktivitäten und Umfeld dieser Bürger liefern, kann Parteien und Wahlkämpfern einige Vorteile bieten. Millionen von E-Mail-Adressen, Telefonnummern und anderen personenbezogen Daten, wie beispielsweise solche, die im Rahmen von Spendensammlungen, politischen Großveranstaltungen und dem Vertrieb von Handelsartikeln gesammelt werden, gestatten politischen Aktivisten und Wahlkämpfern den Erhalt hochsensibler Informationen über spezifische Zielgruppen und Wähler. In den vergangenen Jahren haben politische Parteien und Wahlkämpfer in allen Teilen der Welt stark in Online-Werbung investiert und damit das Potenzial demonstriert, mehr Menschen auf eine effiziente, gezielte und zugängliche Weise anzusprechen, gelegentlich zu einem Bruchteil der Kosten herkömmlicherer Methoden.[2]

Werbung und Strategien zur politischen Manipulation sind nichts Neues. Doch gibt es keinen Präzedenzfall für die gezielte Ansprache von Menschen auf eine solch intime und detaillierte Weise und in der Größenordnung gesamter Populationen.[3] Diese Anvisierung der Wähler stellt eine Steigerung sowohl der Größenordnung als auch der Wirksamkeit dar. Deshalb sollte sie mit Vorsicht und stets auf der entsprechenden Rechtsgrundlage mit Transparenz, Fairness und Verantwortungsbewusstsein gehandhabt werden. Eine potenzielle Verletzung des Rechts zum Schutz personenbezogener Daten in demokratischen Prozessen, wie beispielsweise Wahlkämpfen, kann andere grundlegende Rechte erheblich beeinflussen. Sie stellt eine echte Bedrohung der Fähigkeit von Bürgern dar, ihre eigenen unabhängigen Entscheidungen zu treffen, oder sogar ihres Rechts auf eigene Einstellung bzw. Meinung, was den fundamentalen Wert ihrer Würde und damit den aller Menschenrechte untergräbt. Die Öffentlichkeit hat das Recht zu erwarten, dass politische Werbung im Einklang mit geltendem Recht erfolgt. Weiterhin müssen alle politischen Parteien und Wahlkämpfer dieselben Datenschutz- und Wahlregeln beachten, unabhängig von der Methode oder von neuen technologischen Entwicklungen.[4]

Die unbefugte bzw. unrechtmäßige Verarbeitung personenbezogener Daten untergräbt zusammen mit Falschinformation und Techniken zum digitalen Astroturfing das Vertrauen der Wähler und die Integrität politischer. Sie sollten daher als Bedrohung für

die Demokratie betrachtet werden.[5] Bürger können nur dann wirklich fundierte Entscheidungen über Kandidaten treffen, wenn sie sicher sind, dass ihre Entscheidungen nicht unfair beeinflusst worden sind. Aus diesem Grund sollten Vertrauen und Zuversicht in die Integrität demokratischer Prozesse nicht geschwächt werden.[6][7]

Berücksichtigt man die Bedeutung der Verarbeitung personenbezogener Daten in diesem Kontext, könnte ein Teil des potenziellen Missbrauchs und der potenziellen Risiken infolge dieses Missbrauchs durch die Anwendung robuster gesetzlicher Rahmenwerke gemindert werden, wie beispielsweise der europäischen und brasilianischen allgemeinen Datenschutzbestimmungen (DSGVO bzw. LGPD). Beide Verordnungen bzw. Gesetze sind auf politische Kampagnen anwendbar und können die instrumentale Verwendung personenbezogener Daten zur unfairen politischen Manipulation verringern. Die Harmonisierung allgemeiner Bestimmungen zu Privatsphäre und Datenschutz mit Wahlgesetzen hat die Macht, wirksame Mechanismen zur Garantie der Rechte und Pflichten in Bezug auf personenbezogene und sensible Daten sicherzustellen, wodurch ein gesundes, rechtmäßiges und ethisches Umfeld in Wahlzeiträumen gestärkt werden kann.[8]

Die Verbindung zwischen Wahlgesetzen und den gesetzlichen Rahmenwerken für Wahlkampfaktivitäten unter Einbeziehung personenbezogener Daten befindet sich jedoch noch in der Entwicklung. Trotz starker Fundamente auf beiden Seiten haben allgemeine Datenschutzbestimmungen, wie beispielsweise die DSGVO und das LGPD, noch keine signifikante Anwendung und Rechtsprechung akkumulieren können, um eine perfekt eindeutige Richtlinie für Compliance und Verantwortlichkeit zu gewährleisten. Zurzeit wird noch debattiert, wie genau diese Bestimmungen auf eine Reihe von Aktivitäten in der Praxis angewendet werden sollten. Die Ausweitung dieses Schutzes auf Kampagnen ist weiterhin ein Ziel, das es zu verfolgen gilt, und wird von Fachleuten auf diesem Gebiet sowie von Gerichten und Datenschutzorganisationen im Detail debattiert.[9]

Die Wirksamkeit von Datenschutzbestimmungen hängt von der Fähigkeit und der institutionellen Artikulierung der unterschiedlichen an diesem Prozess beteiligten Parteien ab. Zur Verhinderung von Manipulation und Praktiken zur Falschinformation werden Aktivitäten in Bezug auf die Verwendung personenbezogener Daten in politischen Kampagnen eine sorgfältige Beobachtung erfordern, nicht nur durch öffentliche Organe wie Gerichte und Datenschutzbehörden, welche die Interpretation harmonisieren und angemessene Richtlinien erstellen müssen, sondern auch durch den privatwirtschaftlichen Sektor.[10]

Die Betrachtung kultureller und normativer Eigenarten mittels Analyse der europäischen und brasilianischen Datenschutzbestimmungen und ihrer potenziellen Auswirkungen auf politische Kampagnen zeigt, dass eine Notwendigkeit für Parteien, Aktivisten, Gerichte, Datenschutzbehörden und private Unternehmen besteht, sich zur Wahrung des Datenschutzes von Nutzern zu verpflichten sowie auf die Nebenwirkungen und Bedrohungen für demokratische Institutionen und die Rechte ihrer Bürger in beiden Kontexten zu reagieren.

1 Information Commissioner's Office (ICO, die britische Datenschutzbehörde) (2018): „Investigation into the use of data analytics in political campaigns: a report to Parliament" (Untersuchung der Verwendung von Datenanalytik in politischen Kampagnen: ein Bericht für das Parlament), https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf, Zugang September 2019.

2 Information Commissioner's Office (ICO, die britische Datenschutzbehörde) (2018): „Investigation into the use of data analytics in political campaigns: a report to Parliament" (Untersuchung der Verwendung von Datenanalytik in politischen Kampagnen: ein Bericht für das Parlament), https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf, Zugang September 2019.

3 Europäischer Datenschutzbeauftragter (2018): „Opinion 3/2018 EDPS Opinion on online manipulation and personal data" (Stellungnahme 3/2018 Stellungnahme des EDSB zu Online-Manipulation und personenbezogenen Daten), https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf, Zugang Oktober 2019.

4 Siehe https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets, Zugang Oktober 2019.

5 Anzeichen aus jüngster Vergangenheit deuten darauf hin, dass sich Wähler des verdeckten Vorhandenseins der Verwendung personenbezogener Daten nicht bewusst sind. Das führt zum Untergraben des Systems der Demokratie mithilfe von computergestützter Propaganda. Siehe Woolley Samuel C., Howard Philip N. (2017): „Computational Propaganda Worldwide" (Weltweite computergestützte Propaganda), Universität Oxford, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, Zugang Oktober 2019.

6 ICO (2019): „Guidance on political campaigning: Draft framework code for consultation" (Leitfaden für politische Kampagnen: Entwurf für einen Rahmenkodex zur Anhörung), https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf, Zugang Dezember 2019.

7 Kaltheuner Frederike (2018): „It's about human dignity and autonomy" (Es geht um menschliche Würde und Autonomie), Digital Society Blog.

8 Die Einhaltung relevanter gesetzlicher Rahmenwerke, wie beispielsweise allgemeiner Datenschutzbestimmungen, hat Auswirkungen auf Parteien, Kandidaten und Berater für politisches Marketing sowie ihre Lieferanten, die neben Internet-Plattformen zur Verantwortung gezogen, beaufsichtigt und, im Fall der Nichtbeachtung der Gesetzgebung durch sie, Sanktionen unterworfen werden müssen. Die herkömmlichen und spezifischen Bestimmungen für politische Kampagnen sind in den meisten Fällen entweder veraltet oder unwirksam, da sie keine modernen Wahlkampfpraktiken widerspiegeln. Die Bedeutung der Verarbeitung personenbezogener Daten im Einklang mit Datenschutzgesetzen während politischer Kampagnen ist wesentlich, um die Integrität von Wahlen und die Autonomie der Wähler sowie das Vertrauen in die Verwendung ihrer Informationen sicherzustellen. Siehe ICO (2019): „Guidance on political campaigning: Draft framework code for consultation" (Leitfaden für politische Kampagnen: Entwurf für einen Rahmenkodex zur Anhörung), https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf, Zugang Dezember 2019.

9 Britto Cruz et al. (2019): „Internet e eleições no Brasil: Diagnósticos e recomendações", InternetLab.

10 Britto Cruz et al. (2019): „Internet e eleições no Brasil: Diagnósticos e recomendações", InternetLab.

1. Das Hacken der Wählerschaft

Microtargeting, Bots und Falschinformationen als neue Herausforderungen für die Demokratie

Die Federal Trade Commission (FTC, staatliche Handelskommission) der USA, Amerikas Verbraucherschutzbehörde, hat sich bereiterklärt, Facebook eine Rekordgeldstrafe von fünf Milliarden US-Dollar aufzulegen: die höchste Geldbuße für Datenschutzverstöße in der Geschichte der FTC. Der Entscheid ist das Ergebnis der Untersuchung der Datenschutzpraktiken des Unternehmens in Bezug auf den Skandal von Cambridge Analytica (CA). Der CA-Fall legte offen, wie personenbezogene Daten zum Microtargeting und zur potenziellen Manipulation von Wechselwählern in den US-Wahlen 2016 missbraucht wurden.[11]

Cambridge Analytica gab an, über bis zu 5.000 Datenpunkte zu jedem US-Wähler zu verfügen, die mithilfe der Profile, Webseiten, Twitter-Nachrichten, Facebook-Profile und Instagram-Bilder von Personen gesammelt worden waren. Das Unternehmen gab vor, durch die Anwendung „psychographischer Analysen" auf seinen Datensatz in der Lage zu sein, die Art von Person jedes Wählers zu bestimmen, einschließlich einer relativ exakten Bewertung individueller Bedürfnisse und Befürchtungen sowie der wahrscheinlichen Verhaltensweise des Wählers.[12]

Psychometrie (oder psychographische Analyse) konzentriert sich auf die Messung psychologischer Merkmale mit der Absicht der Bewertung von Menschen auf der Grundlage von fünf Persönlichkeitsmerkmalen: Offenheit, Bewusstsein, Extroversion, Verträglichkeit/Liebenswürdigkeit und Neurotizismus. Auf der Grundlage dieser fünf Merkmale ist es möglich, wichtige und sensible Informationen über eine Person zu bewerten, die zu unterschiedlichen Zwecken verwendet werden könnten. Vor der Ära des Internets und der Verbreitung sozialer Netzwerke bestand eine der wesentlichen Herausforderungen für eine wirksame Psychometrie in der Schwierigkeit, alle notwendigen Daten zu sammeln, was umfassende Fragebögen hochpersönlichen Inhalts erforderte. Diese Herausforderung wurde mithilfe von Online-Plattformen sowie der Nutzerbeteiligung an sozialen Netzwerken bewältigt.[13] Heute dient Psychometrie größtenteils anderen Zwecken, einschließlich Wahlkampagnen.

Obwohl eine gewisse Uneinigkeit bezüglich der Wirksamkeit psychometrischer Praktiken besteht, zeigen jüngste Forschungen auf dem Gebiet der computergestützten Propaganda und der Soziologie, dass die geistigen Profile von Personen anhand der von ihnen beim Besuch des Internets zurückgelassenen Spuren präzise vorhergesagt werden können. Studien zur Auswirkung von Microtargeting in der Werbung legen nahe, dass psychologisches Microtargeting verdeckt eingesetzt werden kann, um bis zu 40 Prozent mehr Klicks und bis zu 50 Prozent mehr Käufe anzuziehen. Außerdem zeigen die Ergebnisse, dass Marketingfachleute bis zu 63 Prozent mehr Klicks und bis zu 1.400 mehr Konversionen bei Werbekampagnen auf Facebook erzielen können, wenn die Produkte und Marketingnachrichten auf die Persönlichkeitsmerkmale von Verbrauchern abgestimmt sind.[14]

Diese Art von aus digitalen Interaktionen abgeleiteter Auswertung verstärkt die Bedeutung des Verständnisses des Grades, zu dem die Verwendung von Big Data und Psychometrie die Aktivitäten großer Gruppen von Personen beeinflussen kann.[15] Das ist möglicherweise nicht der einzige Grund für das spezifische Resultat der US-Wahlen 2016, doch gibt es Anzeichen dafür, dass sie einen nützlichen Beitrag leistete[16], und das nicht nur in den USA. Facebook hat sich kürzlich bereiterklärt, eine Geldstrafe von

500.000 Pfund Sterling für sein Versagen zu zahlen, die personenbezogenen Informationen britischer Nutzer vor Organisationen wie Cambridge Analytica (CA) zu schützen. Das britische Information Commissioner's Office (ICO, britische Datenschutzbehörde) sagte, Facebook habe einen „echten Verstoß" gegen das Gesetz zugelassen und, unter Verletzung des Datenschutzgesetzes, keine ausreichenden Maßnahmen zur Verhinderung der Datensammlung durch Apps getroffen.[17] [18]

Das ICO erklärte:[19]

> *Unsere Untersuchung ergab, dass Facebook zwischen 2007 und 2014 die personenbezogenen Informationen von Nutzern unfair verarbeitete, indem das Unternehmen Anwendungsentwicklern Zugang zu den Nutzerinformationen ohne deren Einwilligung nach ausreichend klarer Aufklärung gab, und diesen Zugang selbst dann gestattete, wenn Nutzer die App nicht heruntergeladen hatten, sondern lediglich „Freunde" von Personen waren, welche die App heruntergeladen hatten. Weiterhin schütze Facebook die personenbezogenen Informationen nicht, da das Unternehmen keine geeigneten Überprüfungen von Apps und Entwicklern vorgenommen hatte, die seine Plattform verwendeten.*

Abgesehen von der traurigen Berühmtheit des CA-Skandals und seiner Folgen in den USA und im Vereinigten Königreich ergibt sich bei der Analyse der internetbasierten Big-Data-Wirtschaft und ihrer politischen Anwendungen die Schlussfolgerung, dass dieses Phänomen nicht bloß ein einziges Unternehmen betrifft oder auf Ausnahmezeiträume in bestimmten Regionen beschränkt ist. Jüngste Studien haben gezeigt, dass dies weltweit passiert, wo nicht freigegebene personenbezogene Daten von Unternehmen, Parteien und Aktivisten im großen Stil verarbeitet werden, deren Absicht in der Manipulation des Verhaltens von Personen mit der Fähigkeit besteht, Wahlergebnisse unter Einsatz individualisierter Nachrichten mit hoher Wirksamkeit unfair zu beeinflussen. Zudem wird diese Praxis noch wirksamer und manipulativer, wenn Falschinformationen und Techniken zum digitalen Astroturfing verwendet werden.

Der Europäische Datenschutzausschuss (EDSA) erklärt:[20]

> *Politische Parteien, politische Koalitionen und Kandidaten stützen sich zunehmend auf personenbezogene Daten und ausgefeilte Profiling-Verfahren, um Wähler und Meinungsführer zu überwachen und zu adressieren. In der Praxis erhalten Menschen hochgradig personalisierte Nachrichten und Informationen, insbesondere über Plattformen der sozialen Medien, auf der Grundlage ihrer persönlichen Interessen, Lebensgewohnheiten und -werte. Zur Klassifizierung oder Darstellung der Persönlichkeitsmerkmale, der Besonderheiten, der Stimmung und anderer Ansatzpunkte werden Instrumente zur Vorhersage eingesetzt, die Rückschlüsse auf tiefe Persönlichkeitsmerkmale, einschließlich politischer Ansichten und anderer besonderer Kategorien von Daten, zulassen. Die Ausweitung solcher Datenverarbeitungstechniken auf politische Zwecke ist mit erheblichen Risiken nicht nur für das Recht auf Privatsphäre und den Datenschutz, sondern auch für das Vertrauen in die Integrität des demokratischen Prozesses verbunden.*[21]

Trotz verstärkter Anstrengungen von Internet-Plattformen[22], diesen Effekten entgegenzuwirken[23], wächst der Einsatz dieser Techniken durch Regierungen in allen Teilen der Welt entsprechend Oxfords neuem Bericht, und die Strategien sind nicht länger auf große Länder beschränkt. Kleinere Staaten können Internet-Aktivitäten ebenfalls problemlos aufnehmen und verwenden dabei nicht nur personenbezogene Informationen, sondern kombinieren diese mit dem Potenzial von Bots[24], gezielter Falschinformation, gefälschten Profilen und angeworbenen „Trollen".

Forscher am Oxford Internet Institute erstellten eine fallbasierte Analyse von computergestützter Propaganda[25] zum besseren Verständnis ihres globalen Einflusses. Sie kamen zu dem Ergebnis, dass sich die Anzahl von Ländern mit politischen Desinformationskampagnen in den vergangenen zwei Jahren auf mehr als 70 verdoppelt hat, wobei nachweislich mindestens eine politische Partei oder Regierungseinrichtung in jedem dieser Länder an der Manipulation sozialer Medien beteiligt war. Das Weltwirtschaftsforum führte kürzlich die Online-Verbreitung von Falschinformationen als eine der zehn größten Gefahren für die Gesellschaft auf. Forschungsarbeiten haben gezeigt, dass soziale Medien sensationslüsternen Content bevorzugen, unabhängig davon, ob dessen Fakten auf ihre Richtigkeit überprüft wurden oder dieser aus einer verlässlichen Quelle stammt.[26]

Wissenschaftler aus Oxford gaben an, dass Regierungen zunehmend soziale Medien einsetzen, um Menschenrechte zu beschneiden, politische Gegner zu untergraben und Widerspruch zu unterdrücken, einschließlich in Ländern wie Aserbaidschan, Zimbabwe und Bahrain. Der Bericht erklärt weiterhin, dass in Tadschikistan Studenten angeworben wurden, um Fake Accounts aufzusetzen und regierungsnahe Meinungen zu verbreiten.[27] [28] [29] [30] Durch das Mischen von echten Nachrichten mit Falschinformationen und unabhängigem Internet-Content finden Zielwähler auf vielen Online-Seiten Nachrichten, die ihre eigenen Perspektiven bestärken. Hierbei ahnen sie nicht, dass sie zu den wenigen Menschen auf der Welt gehören, die solche Nachrichten erhalten. Weiterhin sind sie sich nicht bewusst, das Ziel einer politischen Kampagne zu sein.[31] [32] [33]

Die Wissenschaftler kamen zu dem Schluss, dass der Großteil der mit Regierungen verknüpften Desinformationsanstrengungen auf deren eigenes Land konzentriert war, wobei jedoch mindestens die folgenden sieben Länder versuchen, Meinungen jenseits ihrer Staatsgrenzen zu beeinflussen: China, Indien, Iran, Pakistan, Russland, Saudi-Arabien und Venezuela. Politische Werbung zielte darauf ab, Bilder, Videos oder anderen Content zu erstellen, welche die Algorithmen sozialer Netzwerke ausnutzen und sich deren verstärkende Wirkung zunutze machen, wobei das virale Potenzial auf jeder Plattform maximiert wird.[34] [35]

Internet-Plattformen weisen oft unzureichende Transparenz in Bezug auf das Beschneiden von Informationen und durch Algorithmen auf, wodurch Verbraucher eine falsche Vorstellung von der Neutralität und dem freien Fluss der Informationen bekommen. In einigen Fällen interagieren Nutzer in Filterblasen, d. h. sie betrachten eine digitale Realität, die von algorithmischen Filtern vorgegeben wird und spezifisch auf den Nutzer zugeschnitten ist. Dabei werden die Bedürfnisse, Wünsche, Ängste und Schwächen der Nutzer auf der Grundlage ihrer personenbezogenen

Daten berücksichtigt. Algorithmusfilterung in Online-Umgebungen gestattet einen Grad von Nutzeranpassung und -anvisierung im deutlich größeren Maßstab, was mit der Zunahme des Szenarios des „Internets der Dinge“ tendenziell beschleunigt wird. Die steigende Anzahl intelligenter, verbundener Geräte in unserer Umgebung wird dazu führen, dass noch mehr personenbezogene Daten über uns gesammelt, gespeichert, verarbeitet und übertragen werden.[36] [37]

Der Echokammer-/Filterblaseneffekt

Der sogenannte Echokammer-/Filterblaseneffekt[38] bezieht sich auf eine definierte Gruppe von Daten, die von allen eingesetzten algorithmischen Mechanismen erzeugt wird, um eine unsichtbare Ausgabe zu erstellen, die auf die Nutzeranpassung der Online-Navigation ausgerichtet ist.[39] Dabei handelt es sich um Content-Anpassung durch die Internet-Plattformen/-Anwendungen zur Steigerung des Nutzererlebnisses und der Werbeeinnahmen für ihre Unternehmen.[40]

Filterung hat sich als Notwendigkeit herausgestellt und wird oft als willkommen betrachtet, da sie dem Nutzer erheblichen Komfort bietet, indem er die von ihm gewünschten Informationen bzw. den gewünschten Content in den meisten Fällen schnell und effizient finden kann. Das ist zum Beispiel das Geschäftsmodell von Netflix, das dem Nutzer gestattet, eine Auswahl von Filmen ausschließlich auf der Grundlage seines Profils zur Verfügung zu haben. Dieses verbesserte Nutzererlebnis wird mithilfe des Vorschlags personalisierter Titel und Filter gewährleistet. Dasselbe Argument für Annehmlichkeit und Erlebnissteigerung gilt für Googles Suchmaschine, Facebooks Chronik, Instagram, LinkedIn, Amazon und viele andere Plattformen und Anwendungen, deren Geschäftsmodell auf Werbung, Microtargeting und dem Profiling von Nutzern basiert.[41]

Wenn man über Annehmlichkeit und Benutzererlebnis hinausschaut, besteht das Problem in der Form und im Übermaß der Filterung, sowohl durch die Unternehmen als auch die Personen selbst, die sich unbewusst selbst beschränken sowie von widersprüchlichen Standpunkten wegbewegen und damit den Wert der Debatte im virtuellen öffentlichen Raum verkümmern lassen[42]. Folglich können Filterblasen Nutzer auf eine algorithmische Prognose beschränken, die lediglich einen spezifischen Ziel-Content auf der Grundlage der Verarbeitung ihrer personenbezogenen Daten liefert.[43] Dadurch ergibt sich ein Problem beim Zugriff auf Informationen, die gesehen werden sollten, um die demokratische Debatte zu bereichern.[44] Aus einer anderen Perspektive betrachtet ist der Internet-Nutzer bei seiner Navigation durch die bekanntesten Seiten heute das Ziel einer Flut von gezielter Werbung, welche die kommerziellen Interessen hinter diesem Filterungs- und Personalisierungsmechanismus aufzeigt.[45]

Wenn digitale Plattformen zu zugeschnittenen Realitätsräumen geformt werden, können Echokammern und Filterblasen erzeugt werden, die Menschen von Dingen isolieren, die sie letztendlich sehen müssen. Dieser Effekt kann als für die Debatte und die Konsensbildung im verbundenen öffentlichen Raum schädlich angesehen werden, da er den Zugang zu Informationen sowie die Autonomie von Personen beschränken und potenziell zu einer gesteigerten Polarisierung und Radikalisierung von Diskursen führen kann.[46] [47] [48]

Es gibt allerdings Divergenzen in Bezug auf den echten Effekt, den Filterblasen und Echokammern[49] heute auf sozialen Plattformen und auch im politischen Kontext darstellen. Eine ungenaue Verallgemeinerung ist zu vermeiden, um eine komplexere Analyse zu gestatten.[50] Simon Hegelich erklärt, dass sich Nutzer nicht wirklich in einer „Blase" befinden:[51] „Sie kommunizieren in Wirklichkeit unterschiedliche Themen in verschiedenen Netzwerken und entscheiden zu jedem Zeitpunkt, wann sie Ideen diskutieren wollen, die über ihre eigenen ideologischen Begrenzungen hinausgehen." Hegelich fügt jedoch hinzu: „Während jeder Nutzer im Prinzip die Option hat, die ursprüngliche Quelle der Information nachzuschlagen und unparteiische Informationen zu erhalten, erfordert ein solches Verhalten allerdings einen Wechsel zur rationalen Logik. Die Architektur sozialer Netzwerke verhindert diesen Wechsel nicht, doch sind Facebook, Twitter usw. für den privaten Austausch zwischen Freunden vorgesehen, wobei Homophilie grundsätzlich willkommen ist (...)."[52]

Trotz der Tatsache, dass einige Divergenzen[53] bezüglich der Auswirkungen von Echokammern und Filterblasen sowie ihrer Variationen in unterschiedlichen Ländern und soziotechnischen Kontexten weiterhin bestehen, sind ihre Existenz und Bedeutung von vielen Wissenschaftlern und Forschern ausgiebig hervorgehoben worden. Obwohl empirische Nachweise zur Untermauerung stärkerer Bedenken über Filterblasen noch konsolidiert werden, können infolge der Verbesserung von Personalisierungstechnologien[54] und der Übernahme der Rolle der Hauptinformationsquelle von Menschen durch personalisierte Nachrichten gewisse Probleme für unsere Demokratie auftreten.[55]

Michela Del Vicario et al. erklären:[56]

> *Nutzer tendieren dazu, sich in Interessengemeinschaften zusammenzufinden, was zu Bestärkung führt und die Neigung zur Bestätigung, Segregation und Polarisation begünstigt. Dies geht auf Kosten der Qualität der Informationen und führt zur Proliferation voreingenommener Schilderungen, die durch gegenstandslose Gerüchte, Misstrauen und Paranoia geschürt werden. Diesen Einstellungen entsprechend scheinen algorithmische Lösungen nicht die besten Optionen zum Aufbrechen einer solchen Symmetrie zu sein.*

Judith Moeller und Natali Helberger erklären:[57]

> *Es lässt sich nicht bestreiten, dass die Art und Weise, auf die Nachrichten verbreitet und konsumiert werden, sich infolge der Proliferation von Profiling- und Targeting-Praktiken tiefgreifend verändert hat. Eine wachsende Anzahl von Nutzern konsumiert Nachrichten-Content (außerdem) über große, hoch personalisierte Informationsvermittler oder -plattformen: Plattformen, die das redaktionelle Ethos und die Verpflichtung zur Vielfalt, zu welcher sich herkömmliche hochwertige Nachrichtenkanäle verpflichtet fühlen, nicht teilen. Insbesondere die Teile der Bevölkerung, für die diese Plattformen die Haupttore zu Informationen darstellen, gehen das Risiko ein, zwar nicht unbedingt in Filterblasen zu enden, aber zumindest nur eingeschränkten Zugang zu stark gefilterten und potenziell zu populären Standpunkten neigenden Informationsquellen (die hauptsächlich in den USA und im Vereinigten Königreich ansässig sind) zu haben. Zusätzlich schafft die Multiplikation von Informations-Content und -quellen online die Notwendigkeit neuer Methoden zur Kuration und Filterung von Nachrichten-Content.*

Angesichts der obigen Bedenken könnte die Idee, dass die Internet-Infrastruktur als öffentlicher Raum das Potenzial hat, die Diskussionen ausreichend stark werden zu lassen, um unterschiedliche Segmente und Interessengruppen zu erreichen und sich somit durch die verschiedenen Netzwerke von Menschen, welche die Gesellschaft ausmachen, zu replizieren, zunehmend zu einer fernen Realität werden.[58] Dies beruht auf der Tatsache, dass die Ausdrücke oft auf Netzwerke von Menschen mit gemeinsamen Interessen sowie auf Kommunikationskanäle, die von den Plattformeigentümern zur Bestärkung dieses Effekts entworfen werden, beschränkt bleiben.[59] Als Konsequenz ergibt sich das Potenzial für eine Fragmentierung und Polarisation der öffentlichen Debatte[60], die mehr fruchtbaren Boden zur politischen Manipulation schafft.[61]

Erfahrungen in Brasilien: Wahlkampf 2018

Ähnlich der Kampagne 2016 von Donald Trump zeigte der brasilianische Wahlkampf 2018 ebenfalls, dass Nachrichten massenhaft über soziale Medien-Plattformen verschickt wurden, um die Wählerschaft zu beeinflussen.[62] Politische Manipulation mithilfe von Falschinformationen, algorithmischer Manipulation, verhaltensorientiertem Microtargeting und Social Bots[63] wurde weitverbreitet eingesetzt und basierte meistens auf der unbefugten bzw. unrechtmäßigen Verarbeitung personenbezogener Daten, wobei außerdem nationale Eigenarten und kulturelle Aspekte ausgenutzt wurden.

Brasilien ist das größte Land Lateinamerikas mit einer Bevölkerung von ungefähr 208 Millionen Menschen. Obwohl 66 Prozent der Brasilianer Zugang zum Internet haben, greifen 49 Prozent nur über ihr Handy auf das Internet zu.[64] Bei einer von Consumer Watch durchgeführten Umfrage gaben Brasilianer die Nutzung sozialer Netzwerke als Hauptgrund für ihren Zugriff auf das Internet an. Brasilien ist eines der Länder, welche die meisten sozialen Plattformen verwenden. Neununddreißig Prozent der nationalen Internet-Nutzer besuchen ihre sozialen Netzwerke mehr als zehn Mal täglich und sind durchschnittlich fünf Stunden täglich online, wobei sie hauptsächlich in sozialen Netzwerken surfen.[65]

Während Facebook und Twitter in der US-Wahlkampagne im großen Stil zum Einsatz kamen, spielte in Brasilien WhatsApp eine bedeutende Rolle.[66] WhatsApp ist zu einer der wichtigsten Waffen für computergestützte Propaganda und Falschinformation im politischen Szenario Brasiliens geworden. Die Nutzerdurchdringung von WhatsApp in Brasilien wurde durch vereinfachte Zugänglichkeit zur Plattform mithilfe von Zero-Rating-Praktiken ermöglicht. Facebook war die erste App, welche die Netzneutralitätsregeln[67] in Brasilien umging. Heute ist WhatsApp mit 120 Millionen Nutzern die im Land am meisten verwendete Chat-App.[68]

Obwohl WhatsApp zu derselben wirtschaftlichen Gruppe wie Facebook gehört, bringt WhatsApp eine neue Schicht von Herausforderungen mit sich. Die App hat eine unterschiedliche Rolle als Sofortnachrichtenplattform und ihre Nachrichten umfassen durchgängige Verschlüsselung. Daher, und trotz ihrer Garantie eines besseren Schutzes der Privatsphäre und personenbezogener Nutzerdaten, ist es zudem schwieriger, Content zu untersuchen und zu moderieren, da selbst das Unternehmen keinen direkten Zugang zum Inhalt der Nachrichten hat (*a priori*).[69]

Die Komplexitäten der Plattform erschwerten demzufolge das Hervorheben des massiven Wahl-Content oder selbst die Versicherung für die Kandidaten, dass die Plattform nicht zu rechtswidrigen Zwecken verwendet würde, wie beispielsweise unfairer politischer Werbung, Verbreitung von Hassreden oder falschen, von automatisierten Prozessen verbreiteten Fakten.[70]

Obwohl WhatsApp keine Werbung gestattet, bieten Marketingunternehmen politische Kampagnendienstleistungen ausschließlich für die Nachrichten-App an. Fortlaufende Untersuchungen in Brasilien zeigen, dass auf politische Marketingkampagnen spezialisierte Drittunternehmen in der letzten Wahlkampagne in Brasilien engagiert waren und bestimmte Gruppen mit dem Zweck der politischen Manipulation anvisierten. Dabei verstießen sie nicht nur gegen die Nutzungsbedingungen der Plattform durch den Einsatz von Techniken zur Verbreitung von Falschinformation mittels Massenversand von Nachrichten (was von der Plattform verboten ist). Vielmehr verwendeten sie zudem unbefugte Datenbanken, womit sie die besten Praktiken des Datenschutzes verletzten.[71] Als gängige Praxis sammeln diese Unternehmen Wählerdaten, wie beispielsweise Telefonnummern auf Veranstaltungen, und bauen auf dieser Grundlage Broadcast-Listen auf, die 20.000 Nutzer erreichen können, um im Durchschnitt zehn Nachrichten pro Tag an jeden Nutzer in der Nachrichten-App zu senden.[72]

Auf der Grundlage der DSGVO-Standards müssen die Möglichkeiten der Verarbeitung personenbezogener Daten, selbst wenn sie auf „öffentlich verfügbaren personenbezogenen Daten“ beruhen und im Wahlkontext verwendet werden, sorgsam erwogen werden, wobei zu berücksichtigen ist, was in spezifischen Situationen passierte, wie beispielsweise im oben erwähnten CA-Fall. Obwohl Ausnahmen hinsichtlich der Einwilligung bestehen können, kann die Verarbeitung in vielen Fällen als rechtswidrig betrachtet werden, da keine grundlegenden Compliance-Schritte durchgeführt wurden, wie beispielsweise die Benachrichtigung der betroffenen Person über die Verarbeitung und die Gewährleistung fundamentaler Datenschutzgrundsätze und -rechte.[73] [74] [75] [76]

Im Oktober 2019 gab WhatsApp erstmalig zu, dass Nachrichten während der letzten Präsidentschaftswahlen in Brasilien auf seiner Plattform mit von Unternehmen gemieteten automatisierten Systemen (Bots)[77] massenhaft verschickt wurden. Dieses Eingeständnis wurde von Ben Supple, Public Policy Officer der Nachrichtenplattform, gemacht, der erklärte, es hätte einen „Verstoß gegen die Nutzungsbedingungen“ gegeben, die das automatisierte massenhafte Verschicken von Content verbieten.[78] Nichtsdestotrotz hatte eine brasilianische Zeitung[79] bereits ein Jahr zuvor, im Oktober 2018, enthüllt, dass Marketingunternehmen zum massenhaften Verschicken politischer Nachrichten, die auch Falschinformation enthielten[80], angeworben wurden.[81] Die Strategie wurde öffentlich bekannt, als die Presse offenlegte, dass Verträge im Wert von ungefähr zwölf Millionen R$ zum Massenversand von Nachrichten sowie zum Kauf von Drittdatenbanken abgeschlossen worden waren. Namen, Geburtsdaten und Identifizierungsnummern älterer Menschen in Brasilien und im Ausland wurden ebenfalls verwendet, um Handychips ohne deren Einwilligung zu registrieren. Diese Handynummern wurden dann zur massenhaften Erstellung von Nachrichten auf WhatsApp und zum Anvisieren von Empfängern auf der Grundlage ihres Einkommens und ihrer geografischen Region eingesetzt. [82]

Daher stellt das Wachstum robotergeführter Maßnahmen eine echte Gefahr für die öffentliche Debatte dar. Sie repräsentieren Gefährdungen für die Demokratie selbst, da sie mit dem Prozess der Konsensbildung im öffentlichen Raum sowie mit der Wahl der Volksvertreter und mit Regierungsabsichten interferieren.[83] Die Abteilung für die Analyse öffentlicher Politik (DAPP) der FGV (Getulio-Vargas-Stiftung) bestätigt die These des Risikos für die Demokratie mit ihrer Offenlegung der rechtswidrigen Einmischung in die Online-Debatte während der 2018[84]-Wahlen[85] und in öffentliche Debatten im Allgemeinen.[86] Planmäßige Accounts für Massenbeiträge sind zu einem Werkzeug für die Manipulation von Debatten auf sozialen Medien geworden. Im Verlauf des Wahlkampfs 2018 waren automatisierte Accounts für 12,9 Prozent von Interaktionen auf Twitter verantwortlich.[87] [88] [89] [90]

Ein ehemaliger Mitarbeiter eines der Unternehmen (Yacows), der den Nachrichtenprozess koordinierte, gab an, eine Liste mit Informationen über zehntausend Personen zum illegalen Zugang zu personenbezogenen Daten zum Senden der Nachrichten verwendet zu haben, wobei die Absicht darin bestand, die von WhatsApp eingerichtete Nummernfilterung zu umgehen. Der Einsatz von Robotern wurde ebenfalls angegeben und es wurde eingestanden, nach jeweils 50 Nachrichten eine Pause von zehn Sekunden eingefügt zu haben, um ebenso die Umgehung der WhatsApp-Sperre zu versuchen. [91] [92] Es könnte sein, dass bis zu 300.000 WhatsApp-Accounts für automatisierte Broadcasts zur Desinformation und zur Koordination nicht gemeldeter politischer Werbung an tausende von WhatsApp-Gruppen verwendet wurden.[93] [94] [95] [96]

Aufgrund von Offenlegungen durch die Medien finden zurzeit Untersuchungen der Beteiligung von Politikern, Parteien und Anhängern an Falschinformation und politischer Manipulation statt. Die Untersuchungen legen wichtige Fakten und Zeugnisse offen. Gleichzeitig enthüllen sie die komplexen Umstände, denen sich insbesondere das Justizsystem bei seinem Kampf gegen gesetzwidriges Verhalten bei digitalen Kampagnen gegenübersieht.[97] [98] [99] [100] [101] [102]

Das neue Modell datengetriebener Kampagnen stellt eine systemische und institutionelle Herausforderung dar, die nicht schnell bewältigt werden kann und eine Kombination aus politischen und regulatorischen Ansätzen erfordert. Verstärkter Datenschutz ist sicherlich ein Teil der Antwort[103]: Die korrekte Durchsetzung der europäischen Datenschutz-Grundverordnung mit ihrer internationalen Reichweite und ihre Verwendung als Modell in anderen Ländern könnte helfen, das Ausmaß des zur politischen Manipulation eingesetzten Data-Mining und Profiling zu mindern.[104] Mit den Worten von Iva Nenadić: „Die Effizienz von Online-Microtargeting hängt zum großen Teil von Daten und Profiling ab. Falls die DSGVO daher wirksam implementiert wird, sollte sie hier durch ihre Verhinderung der gesetzwidrigen Verarbeitung personenbezogener Daten nützlich sein.“[105]

Nach Privacy International Organization: [106]

> *Wo Daten erzeugt werden, sollten Personen in der Lage sein, herauszufinden, welche Unternehmen welche Arten von Daten über sie führen. Profiling erzeugt hochsensible Schlüsse und Vorhersagen über Persönlichkeit, Verhalten oder Überzeugungen von Menschen. (...) Unternehmen, die sensible Daten von Milliarden Menschen in allen Teilen der Welt über Jahre hinweg gesammelt haben, könnten die Fähigkeit haben, das*

tatsächliche Verhalten von Menschen im großen Stil zu verändern. (...) Personen sollten in der Lage sein, Zugang zu diesen Schlüssen und Vorhersagen über sie zu haben, um sie wirksam anfechten oder die Löschung ihrer Profile verlangen zu können.

Personenbezogene Daten sind der Schlüssel zu dieser Debatte. Linda Risso sagt:[107] „Es ist eindeutig, dass Gesetzgeber der Entwicklung hinterherhinken und eine zunehmend breitere Lücke zwischen dem aktuellen Entwicklungsstand der Technologie und dem Schwerpunkt des Gesetzes besteht.[108] Deshalb ist es wesentlich, dass nationale Regierungen die ethischen und rechtlichen Herausforderungen, die von sozialen Medien, computergestützter Propaganda und Datenschutz gestellt werden, schnell bewältigen.[109] Seit 2017 besagen EU-Datenschutzbestimmungen, dass personenbezogene Daten nur in bestimmten Situationen und unter bestimmten Bedingungen verarbeitet werden dürfen. Die Frage, wie das in der Praxis funktionieren wird, bleibt jedoch offen."[110] [111] [112] [113]

---

11 „Die wichtigste Datenquelle war Facebook. Cambridge Analytica hatte über eine Dritt-App unrechtmäßig Daten von bis zu 87 Millionen Facebook-Profilen erlangt, einschließlich Status-Updates, Likes und sogar privaten Nachrichten. Zudem wurde Microtargeting zur individuellen Anpassung von Nachrichten zwecks Beeinflussung des Nutzerverhaltens verwendet." Westby Joe (2019): „The Great Hack: Cambridge Analytica is just the tip of the iceberg" (Der große Hack: Cambridge Analytica ist lediglich die Spitze des Eisbergs), Amnesty Tech, https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/, Zugang Januar 2020.

12 Christopher Wylie, einer der Mitbegründer von Cambridge Analytica und Whistleblower, sagte: „Wir benutzten Facebook zur Ernte der Profile von Millionen von Menschen und bauten Modelle zur Ausnutzung unseres Wissens über sie sowie zur gezielten Adressierung ihrer tiefsten Ängste." Siehe https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting, Zugang Januar 2020.

13 „Kein Facebook-Konto zu haben stellte keinen Schutz dar: Die lange Liste verfügbarer Datenquellen ist nicht auf Facebook beschränkt und die Analyse kann problemlos auf andere Punkte persönlicher Vorlieben angewendet werden. Zusätzlich ist jede Webseite mit dem Facebook-Logo mit Facebook verknüpft, sodass nicht nur Mitglieder, sondern auch Nichtmitglieder, die den Dienst möglicherweise nicht gewählt haben, verfolgt werden können. Es gibt viele ähnliche Quellen für Online-Tracking, wie beispielsweise Web Beacons, von denen die meisten mit ‚Cookies' verknüpft sind, die über Webseiten hinweg verwendet werden können und deren Zugang an interessierte Käufer verkauft werden kann." Isaak, Mina J. Hanna (2018), „User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection" (Nutzerdatenschutz: Facebook, Cambridge Analytica und Datenschutz), IEEE Computer Band: 51 Ausgabe: 8, https://ieeexplore.ieee.org/abstract/document/8436400, Zugang August 2018.

14 Grassegger Hannes, Krogerus Mikael (2017): „The Data That Turned the World Upside Down" (Die Daten, welche die Welt auf den Kopf stellten), Motherboard, https://www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win, Zugang Oktober 2019.

15 Matz S. C., Kosinski M., Nave G., Stillwell D. J. (2017): „Psychological targeting in digital mass persuasion" (Gezielte psychologische Ansprache bei der digitalen Massenüberredung), National Academy of Sciences, siehe auch Moon Y. (2016): „Personalization and personality: Some effects of customizing message style based on consumer personality" (Personalisierung und Persönlichkeit: Einige Wirkungen der Anpassung des Nachrichtenstils auf der Grundlage der Verbraucherpersönlichkeit), Journal of Consumer Psychology, Elsevier.

16 Aufgrund der vielen, am Prozess der politischen Manipulation beteiligten Faktoren – von kulturellen und technologischen bis zu psychologischen/idiosynkratischen – ist es weiterhin schwierig, mit absoluter Klarheit zu sagen, wie diese Manipulation genau erfolgte und wie viele Personen durch diese Techniken manipuliert wurden. Empirische Forschungen zur spezifischen Untersuchung der Online-Kommunikationsprozesse und Ergebnisse sind noch spärlich.

17 Youyou Wu et al. (2015): „Computer-based personality judgments are more accurate than those made by humans" (Computergestützte Persönlichkeitsbeurteilungen sind exakter als von Menschen gefällte Beurteilungen), PNAS. https://www.bbc.com/news/technology-45976300, Zugang Oktober 2019.

18 Information Commissioner's Office (ICO, die britische Datenschutzbehörde) (2018): „Investigation into the use of data analytics in political campaigns: a report to Parliament" (Untersuchung der Verwendung von

Datenanalytik in politischen Kampagnen: ein Bericht für das Parlament), https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf, Zugang September 2019.

19 Information Commissioner's Office (ICO, die britische Datenschutzbehörde) (2018): „Investigation into the use of data analytics in political campaigns: a report to Parliament" (Untersuchung der Verwendung von Datenanalytik in politischen Kampagnen: ein Bericht für das Parlament), https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf, Zugang September 2019.

20 Europäischer Datenschutzausschuss (EDSA) (2019): „Statement 2/2019 on the use of personal data in the course of political campaigns" (Erklärung Nr. 2/2019 zur Verwendung personenbezogener Daten im Rahmen politischer Kampagnen), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf, Zugang Januar 2020.

21 Der Europäische Rat verabschiedete eine Gruppe aus Richtlinien, die politische Parteien zwingen, die EU-Datenschutzregeln einzuhalten. Europäischer Rat (2019), „EP elections: EU adopts new rules to prevent misuse of personal data by European political parties" (Europawahl: neue EU-Vorschriften sollen den Missbrauch personenbezogener Daten durch die europäischen Parteien verhindern), https://www.consilium.europa.eu/en/press/press-releases/2019/03/19/ep-elections-eu-adopts-new-rules-to-prevent-misuse-of-personal-data-by-european-political-parties/, in: Chester J., Montgomery K. C. (2019): „The digital commercialization of US politics – 2020 and beyond" (die digitale Kommerzialisierung der US-Politik – 2020 und darüber hinaus), Internet Policy Review, 8(4).

22 WhatsApp beschränkte zum Beispiel die Anzahl der Mitglieder jeder Gruppe auf 256 und die Anzahl der Weiterleitungen von Nachrichten auf fünf. WhatsApp implementierte außerdem die Notwendigkeit von Berechtigungen, um in einer spezifischen WhatsApp-Gruppe hinzugefügt zu werden, und löschte beinahe 1,5 Millionen Accounts in den letzten brasilianischen Wahlen, die zu einem gewissen Grad an der Automatisierung von Content oder einer sonstigen missbräuchlichen Verwendung der Plattform beteiligt waren. Google wird seine Praxis beenden, Werbeträgern die Fähigkeit zur spezifischen Ausrichtung von Wahlwerbung unter Verwendung von Daten wie öffentlichen Wählerlisten und allgemeinen politischen Zugehörigkeiten zu geben. Facebook erklärte, das Unternehmen werde Deep Fakes entfernen. Twitter entschied im Oktober kategorisch, keine weitere politische Propaganda zu akzeptieren. Google legte im November fest, dass jeder, der politische Werbung in den Vereinigten Staaten kaufen möchte (einschließlich YouTube), die Veröffentlichung nicht länger auf Nutzer abstimmen kann, die nach ideologischem Vorzug gefiltert sind. Siehe https://piaui.folha.uol.com.br/materia/o-algoritmo-da-agora/. Siehe https://www.zdnet.com/article/whatsapp-banned-nearly-half-a-million-accounts-during-brazilian-elections/. Siehe https://faq.whatsapp.com/en/30046788/?lang=en. Siehe https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKBN1X-U2WT. Siehe https://link.estadao.com.br/noticias/empresas,facebook-passara-a-remover-videos-falsos-e-deepfakes-da-rede-social,70003146938?utm_source=facebook:newsfeed&utm_medium=social-organic&utm_campaign=redes-sociais:012020:e&utm_content=:::&utm_term=, Zugang Februar 2020.

23 Ein Problem, das in diesem Zusammenhang nicht übersehen werden sollte, ist die Bedeutung von Aufklärungs- und Schulungsarbeit zum Phänomen von Online-Falschinformation. Eine vom Unternehmen Kaspersky durchgeführte Umfrage, die ein tieferes Verständnis der Art und Weise gewinnen wollte, wie Lateinamerika mit Fake News umgeht, gelangte zu folgenden Ergebnissen: Durchschnittlich wissen 70 Prozent der Lateinamerikaner nicht, wie sie Neuigkeiten im Internet von Fake News unterscheiden können, bzw. sind sich unsicher, ob dies überhaupt möglich ist. Nach Staatsangehörigkeit aufgeschlüsselt sind die Peruaner am wenigsten in der Lage, falsche Neuigkeiten zu erkennen (79 Prozent), gefolgt von den Kolumbianern (73 Prozent) und Chilenen (70 Prozent). Danach kommen die Argentinier und Mexikaner mit 66 Prozent und die Brasilianer (62 Prozent). Siehe https://veja.abril.com.br/tecnologia/62-dos-brasileiros-nao-sabem-reconhecer-uma-noticia-falsa/amp/?__twitter_impression=true&fbclid=IwAR0hLFm_NOTv61xTWYDazqY4Oi_Uf_HFUCnIkqyDJf6A1zJwNdfGlUGM8gE, Zugang Februar 2020.

24 „Bei Bots, d. h. automatisierten, für die Verbreitung computergestützter Propaganda wesentlichen Programmen, handelt es sich um Software, die zur Ausführung einfacher, repetierender roboterhafter Aufgaben bestimmt ist. Sie dienen zur computergestützten Steigerung der menschlichen Fähigkeit, Arbeit online zu erledigen. Social Media Bots sind automatisierte Identitäten, die banale Aufgaben wie Informationssammlung durchführen können, aber auch mit Personen und Systemen kommunizieren können. Sie werden eingesetzt, um rechtmäßige Aufgaben wie die Lieferung von Nachrichten und Informationen auszuführen. Außerdem dienen sie zu schädlicheren Aktivitäten in Verbindung mit Spam und Belästigung. Unabhängig von ihren Verwendungszwecken sind sie in der Lage, Nachrichten schnell zu verbreiten, mit dem Content anderer Nutzer zu interagieren, Trendalgorithmen durchzuführen und dabei als menschliche Nutzer aufzutreten. Politische Bots, d. h. Social Media Bots, die zur politischen Manipulation eingesetzt werden, sind außerdem wirksame Werkzeuge zur Stärkung von Online-Propaganda und Hasskampagnen. Eine Person oder eine kleine Gruppe von Personen kann eine Armee politischer Bots auf Twitter einsetzen, um die Illusion zu erzeugen, dass es sich um einen Konsens im großen Rahmen handelt." Woolley Samuel, Howard Philip (2017): „Computational Propaganda

Worldwide“ (Weltweite computergestützte Propaganda), Universität Oxford, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, Zugang Februar 2020.

25 Woolley Samuel, Howard Philip (2017): „Computational Propaganda Worldwide“ (weltweite computergestützte Propaganda), Universität Oxford, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, Zugang Februar 2020.

26 Woolley Samuel, Howard Philip (2017): „Computational Propaganda Worldwide“ (Weltweite computergestützte Propaganda), Universität Oxford, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, Zugang Februar 2020.

27 „Regierungen und Parteien verwenden ‚Cyber-Truppen‘ zur öffentlichen Meinungsbildung, einschließlich Netzwerken von Bots zur Nachrichtenverstärkung, Gruppen von ‚Trollen‘ zur Belästigung politischer Dissidenten wie Journalisten und Aktivisten sowie Fake Accounts auf sozialen Medien zur fälschlichen Darstellung der Anzahl der an einem Thema beteiligten Personen. Regierungen verbreiten Desinformation, um politische Gegner in Verruf zu bringen, widersprechende Meinungen zu verdecken und sogar in die Angelegenheiten anderer Länder einzugreifen.“ Alba D., Satariano A. (2019): „At Least 70 Countries Have Had Disinformation Campaigns“ (Mindestens 70 Länder haben Desinformationskampagnen betrieben), NY Times.

28 „Falls diese Methoden wirklich so leistungsfähig sind, wie die Unternehmen und ihre Kunden angeben, stellen sie letztendlich eine echte Bedrohung für unsere Fähigkeit dar, unsere eigenen unabhängigen Entscheidungen zu treffen, oder sogar für unser Recht auf eine Meinung. Dadurch wird der grundlegende Wert der Würde untergraben, der allen Menschenrechten zugrunde liegt. Werbung und Propaganda sind nichts Neues, doch gibt es keinen Präzedenzfall für die gezielte Ansprache von Menschen auf eine solch intime und tiefgreifende Weise und in der Größenordnung gesamter Populationen.“ Westby Joe (2019): „The Great Hack: Cambridge Analytica is just the tip of the iceberg“ (Der große Hack: Cambridge Analytica ist lediglich die Spitze des Eisbergs), Amnesty Tech, https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/, Zugang Januar 2020.

29 Isaak, Mina J. Hanna (2018): „User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection“ (Nutzerdatenschutz: Facebook, Cambridge Analytica und Datenschutz), IEEE Computer Band: 51 Ausgabe: 8, https://ieeexplore.ieee.org/abstract/document/8436400, Zugang August 2018.

30 Woolley Samuel, Howard Philip (2017): „Computational Propaganda Worldwide“ (weltweite computergestützte Propaganda), Universität Oxford, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, Zugang Februar 2020.

31 Risso Linda (2017): „Harvesting Your Soul? Cambridge Analytica and Brexit“ (Wird Ihre Seele geerntet? Cambridge Analytica und Brexit), Akademie der Wissenschaften und der Literatur, http://www.adwmainz.de/fileadmin/user_upload/Brexit-Symposium_Online-Version.pdf#page=75, Zugang Dezember 2019. Siehe auch Woolley Samuel C., Howard Philip N. (2017): „Computational Propaganda Worldwide“ (Weltweite computergestützte Propaganda), Universität Oxford, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, Zugang Oktober 2019. Siehe auch Funke D., Flamini D. (2019): „A guide to anti-misinformation actions around the world“ (Ein Leitfaden zu Maßnahmen zur Bekämpfung von Falschinformation in allen Teilen der Welt), https://www.poynter.org/ifcn/anti-misinformation-actions/, Zugang Dezember 2019.

32 Bradshaw S., Howard P. (2019): „The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation“ (Die Ordnung der globalen Desinformation: Globales Verzeichnis 2019 der organisierten Manipulation sozialer Medien), Universität Oxford, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf, Zugang Dezember 2019.

33 Funke D., Flamini D. (2019): „A guide to anti-misinformation actions around the world“ (Ein Leitfaden für Maßnahmen zur Bekämpfung von Falschinformation in allen Teilen der Welt), https://www.poynter.org/ifcn/anti-misinformation-actions/, Zugang Dezember 2019.

34 Alba D., Satariano A. (2019): „At Least 70 Countries Have Had Disinformation Campaigns“ (Mindestens 70 Länder haben Desinformationskampagnen betrieben), NY Times.

35 Woolley Samuel C., Howard Philip N. (2017): „Computational Propaganda Worldwide“ (Weltweite computergestützte Propaganda), Universität Oxford, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, Zugang Oktober 2019.

36 Bayer J. et al. (2019): „Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States. European Parliament“ (Desinformation und Propaganda – Auswirkungen auf das Funktionieren des Rechtsstaatsprinzips in der EU und ihren Mitgliedstaaten. Europäisches Parlament), http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf, Zugang Februar 2020.

37 Anderson J., Rainie L. (2017): „The Future of Truth and Misinformation Online“ (Die Zukunft von Wahrheit und Falschinformation online), Pew Research Center, web/imagining/surveys/2017_survey/Future_of_Info_Environment_Elon_University_Pew_10-18-17.pdf, Zugang Februar 2020.

38 Pariser E. (2011): „The Filter Bubble: What the Internet is Hiding from You“ (Die Filterblase: Was das Internet vor Ihnen versteckt), Penguin Press.

39 Magrani Eduardo (2014): „Democracia Conectada“, Jurua, https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/14106/Democracia%20conectada.pdf?sequence=1&isAllowed=y, Zugang September 2019.

40 „Cookies sind kurz gesagt Zugangsdaten, die aus den ‚digitalen Fußabdrücken‘ bestehen, die zurückbleiben, wenn Nutzer Online-Umgebungen besuchen und mit ihnen interagieren.“ Wu Tim (2011): „The Master Switch: The Rise and Fall of Information Empire“ (Der Hauptschalter: Aufstieg und Niedergang des Informationsweltreichs), Vintage.

41 Magrani Eduardo, Medeiros R. (2019): „The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018“ (Der im Zeitalter von Fake News und Filterblasen gebildete öffentliche Raum: die Erfahrungen in Brasilien 2018), Cyber law.

42 Magrani Eduardo (2014): „Democracia Conectada“, Jurua, https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/14106/Democracia%20conectada.pdf?sequence=1&isAllowed=y, Zugang September 2019.

43 Morozov E. (2013): „To Save Everything, Click Here: The Folly of Technological Solutionism“ (Um alles zu speichern, hier klicken: die Torheit des technologischen „Solutionism“), Public Affairs.

44 Borgesius Z. et al. (2016): „Should we worry about filter bubbles?“ (Sollten Filterblasen uns Sorgen machen?), Internet Policy Review, 5(1).

45 Magrani Eduardo, Medeiros R. (2019): „The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018“ (Der im Zeitalter von Fake News und Filterblasen gebildete öffentliche Raum: die Erfahrungen in Brasilien 2018), Cyber law.

46 Eine kategorische Aussage in dieser Richtung würde weitergehende Untersuchungen erfordern, sodass der spezifische Ansatz zu diesem Punkt über die Grenzen der vorliegenden Studie hinausgehen würde.

47 „Viele Menschen sind sich in keiner Weise bewusst, dass Filterblasen überhaupt existieren. Mehr als 60 Prozent aller Facebook-Nutzer sind sich vollkommen unbewusst, dass Facebook eine Kuration vornimmt, und glauben stattdessen, dass jede einzelne Geschichte von ihren Freunden und den von ihnen gefolgten Seiten in ihrem Nachrichten-Feed auftauchte.” Hern A. (2017): „How social media filter bubbles and algorithms influence the election“ (Wie Filterblasen und Algorithmen in sozialen Medien die Wahl beeinflussen), The Guardian. https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles, Zugang Oktober 2019.

48 Allred K. (2018): „The Causes and Effects of ‚Filter Bubbles‘ and how to Break Free‘ (Die Ursachen und Wirkungen von „Filterblasen“ und wie man sich von ihnen befreien kann), Medium, https://medium.com/@10797952/the-causes-and-effects-of-filter-bubbles-and-how-to-break-free-df6c5cbf919f, Zugang Oktober 2019.

49 Diese Debatte wird außerdem durch die abweichenden Konzepte um beide Begriffe erschwert. Siehe Bruns A. (2019): „Filter Bubbles and Echo Chambers: Debunking the Myths“ (Filterblasen und Echokammern: die Mythen entlarven), Medium, https://medium.com/dmrc-at-large/are-filter-bubbles-real-3be22bd9230e, Zugang Oktober 2019. Siehe auch Moeller J., Helberger N. (2018): „Beyond the filter bubble: Concepts, myths, evidence, and issues for future debates“ (Über die Filterblase hinaus: Konzepte, Mythen, Nachweise und Probleme für zukünftige Debatten), Universität Amsterdam, https://www.ivir.nl/publicaties/download/Beyond_the_filter_bubble__concepts_myths_evidence_and_issues_for_future_debates.pdf, Zugang Oktober 2019.

50 Bruns A. (2019): „Are Filter Bubbles Real?“ (Sind Filterblasen real?), Digital-Future-Serie.

51 Hegelich S., Shahrezaye M. (2017): „Disruptions to political opinion: Political debate in the age of echo chambers and filter bubbles“ (Störungen der politischen Meinung: Politische Debatte im Zeitalter von Echokammern und Filterblasen), KAS Facts and Findings, Nr. 253, https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_49188_2.pdf/d3741812-3abb-c52a-fe75-658665e274d7?version=1.0&t=1539649011639, Zugang Oktober 2019.

52 Hegelich S., Shahrezaye M. (2017): „Disruptions to political opinion: Political debate in the age of echo chambers and filter bubbles“ (Störungen der politischen Meinung: Politische Debatte im Zeitalter von Echokammern und Filterblasen), KAS Facts and Findings, Nr. 253, https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_49188_2.pdf/d3741812-3abb-c52a-fe75-658665e274d7?version=1.0&t=1539649011639, Zugang Oktober 2019.

53 „Solch eine moralische Panik lenkt uns nach Sebastian Meineck von wichtigeren Dingen ab. Erst wenn die Fabel von der Filterblase platzt, kann die Debatte um die Transformation des öffentlichen Raums wirklich beginnen. Diese Debatte wird untersuchen müssen, ob Gesellschaften in allen Teilen der Welt, von Australien bis Brasilien, von Deutschland bis zu den Vereinigten Staaten, zunehmend polarisiert werden oder ob eine solche Polarisierung lediglich sichtbarer wird; (...) diese Transformationen stören bestehende politische Systeme erheblich, lähmen sie sogar manchmal und untergraben den fundamentalen gesellschaftlichen Konsens. Die Debatte wird jedoch ebenfalls anerkennen müssen, dass solche Umwandlungen nicht einfach durch oberflächliche Faktoren wie die Kommunikationstechnologien und Plattformen getrieben werden, die von diesen neuen politischen Akteuren bzw. ihren etablierten Gegnern bevorzugt werden, sondern eher ein Ausdruck von grundlegenderen sozialen, wirtschaftlichen, gesellschaftlichen und politi-

schen Herausforderungen sind. Das bedeutet nicht, dass Such- und soziale Medien-Plattformen fehlerfrei sind. Es besteht in der Tat zurzeit eine akute Notwendigkeit, sie (durch regulatorische oder sonstige Mittel) zu zwingen, mehr zu tun, um Extremisten-Accounts zu entfernen, die Verbreitung von Desinformation zu verhindern und sich einer unabhängigen Überprüfung durch Wissenschaftler zu unterwerfen. In Bezug auf die spezifische Frage nach Filterblasen erscheinen sie jedoch weitgehend schuldlos." Bruns A. (2019): „Filter bubble" (Filterblase), Internet Policy Review.

54 Aufgrund der vielen, am Prozess der politischen Manipulation beteiligten Faktoren – von kulturellen und technologischen bis zu psychologischen/idiosynkratischen – ist es weiterhin schwierig, mit absoluter Klarheit zu sagen, wie diese Manipulation genau erfolgte und wie viele Personen durch diese Techniken manipuliert wurden. Empirische Forschungen zur spezifischen Untersuchung der Online-Kommunikationsprozesse und Ergebnisse sind noch spärlich. Um Zuiderveen et al. zu zitieren: „Empirische Forschung hinsichtlich des Ausmaßes von personalisierter Kommunikation und ihrer Auswirkungen auf den Zugang zu diversen Informationen kann einen Realitätscheck liefern. Empirische Forschung kann dabei helfen, die Prioritäten in der öffentlichen Politik anzupassen und Bereiche zu identifizieren, in denen wir einfach nicht genug wissen, um schlüssige politische Aussagen treffen zu können. (...) falls sich die Personalisierungstechnologie verbessert und personalisierter Nachrichten-Content zur Hauptinformationsquelle von Menschen wird, könnten sich in der Tat Probleme für unsere Demokratie ergeben, was unsere Prüfung empirischer Studien von Medieneffekten gezeigt hat." Zuiderveen Borgesius F. J., Trilling D., Möller J., Bodó B., de Vreese C. H., Helberger N. (2016): „Should we worry about filter bubbles?" (Sollten Filterblasen uns Sorgen machen?), Internet Policy Review, 5(1).

55 Zuiderveen Borgesius F. J., Trilling D., Möller J., Bodó B., de Vreese C. H., Helberger N. (2016): „Should we worry about filter bubbles?" (Sollten Filterblasen uns Sorgen machen?), Internet Policy Review, 5(1).

56 Del Vicario, Michela et al. (2016): „The spreading of misinformation online" (Die Online-Verbreitung von Falschinformationen), Proceedings of the National Academy of Sciences of the United States of America, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4725489/, Zugang Oktober 2019.

57 Moeller J., Helberger N. (2018): „Beyond the filter bubble: Concepts, myths, evidence, and issues for future debates" (Über die Filterblase hinaus: Konzepte, Mythen, Nachweise und Probleme für zukünftige Debatten), Universität Amsterdam, https://www.ivir.nl/publicaties/download/Beyond_the_filter_bubble__concepts_myths_evidence_and_issues_for_future_debates.pdf, Zugang Oktober 2019.

58 „Facebook führte ein gewaltiges psychologisches Experiment an 689.003 Nutzern durch, bei dem ihre Nachrichten-Feeds manipuliert wurden, um die Auswirkungen auf ihre Emotionen zu bewerten. Facebook hat die Fähigkeit, Nutzer sich gut oder schlecht fühlen zu lassen, indem das Unternehmen lediglich leicht den Content justiert, der in ihrem Nachrichten-Feed erscheint. Das Unternehmen verließ sich bei seinem Experiment auf ein automatisiertes System, das positive oder negative Worte auf der Basis eines elektronischen Wörterbuchs identifizierte. Facebook reduzierte den positiven Content in den Nachrichten-Feeds einiger Nutzer. Diese Verringerung des positiven Content führte dazu, dass ein größerer Prozentsatz von Worten in den Status-Updates von Personen negativ und ein kleinerer Prozentsatz positiv war. Bei der Reduzierung der Negativität trat das entgegengesetzte Muster auf. Die Autoren kamen zu dem Schluss, dass diese Ergebnisse nahelegen, dass die von Freunden über soziale Online-Netzwerke ausgedrückten Emotionen unsere eigenen Stimmungen beeinflussen. Das Facebook-Experiment liefert unseres Wissens nach den ersten experimentellen Nachweis für emotionale Ansteckung über soziale Netzwerke im großen Rahmen und unterstützt damit früher in Frage gestellte Behauptungen, dass sich Emotionen mittels Ansteckung über ein Netzwerk ausbreiten." McNeal G. (2014): „Facebook Manipulated User News Feeds to Create Emotional Responses" (Facebook manipulierte Nutzer-Feeds, um emotionale Antworten hervorzurufen), https://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/#10567b1039dc, Zugang Oktober 2019. Siehe auch Ryan C. (2013): „Digital Market Manipulation" (Digitale Marktmanipulation), University of Washington School of Law Research Paper No. 2013–27.

59 Cass Sunstein gibt an, dass Blasenfilter aufgrund des mangelnden Kontakts mit abweichenden Meinungen und der Polarisation von Diskursen, die zu Radikalismus führen, ein ernsthaftes Risiko für das Potenzial des verbundenen öffentlichen Raums darstellen würden. Das wäre ein Problem mit Trends aufgrund der Weiterentwicklung von Nutzeranpassungsalgorithmen, die nicht dessen Lösung, sondern dessen Verschärfung fördern. Sunstein C. (2011): „Republic.com 2.0." (Republik.com 2.0), Princeton University Press. Siehe auch Sunstein C. (2001): „Republic.com" (Republik.com), Princeton University Press.

60 Einzelne Personen haben in diesem Kontext eine wichtige Verantwortung für die Verringerung ihrer eigenen persönlichen Filterblasen. Indem wir unsere Anpassungsmerkmale und das Datensammeln mithilfe von Cookies sowie gezielte Werbung auf Webseiten verstehen und verwalten, können wir die Auswirkungen von Algorithmen auf unseren Content einschränken.

61 Magrani Eduardo, Medeiros R. (2019): „The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018" (Der im Zeitalter von Fake News und Filterblasen gebildete öffentliche Raum: die Erfahrungen in Brasilien 2018), Cyber law. Eine kategorische Aussage in dieser Richtung würde weitergehende Untersuchungen erfordern, sodass der spezifische Ansatz zu diesem Punkt über die Grenzen der vorliegenden Studie hinausgehen würde.

62 Siehe https://www1.folha.uol.com.br/poder/2019/10/whatsapp-admite-envio-massivo-ilegal-de-mensagens-nas-eleicoes-de-2018.shtml, Zugang Oktober 2019.

63 Die Ergebnisse der Studie „Computational Power: Automated Use of WhatsApp in the Elections" (Computergestützte Macht: automatisierte Verwendung von WhatsApp bei den Wahlen), die sich mit dem Einsatz von Bots und WhatsApp bei den Wahlen in Brasilien 2018 beschäftigte, besagen: „Wir identifizierten spezifisch das Vorhandensein starker Elemente eines Einsatzes von Automatisierung zur Förderung der Verbreitung von Informationen unter verschiedenen Gruppen auf WhatsApp. Weiterhin stellten wir eine koordinierte Handlung zwischen verschiedenen Mitgliedern bei ihren Aktivitäten in den Netzwerken von Diskussionsgruppen auf WhatsApp fest. (...) ungefähr 56 Prozent der brasilianischen Wähler sagten, dass ihre Wahl von Präsidentenkandidaten durch soziale Netzwerke beeinflusst wurde. Daher gibt es Hypothesen, die auf die Wirksamkeit dieser Strategie hinweisen, insbesondere in der ersten Wahlrunde, selbst wenn alle Kandidaten in unterschiedlichem Ausmaß und mit unterschiedlichen Strategien von digitalen Kampagnen Gebrauch machten. Unser Verständnis des Einsatzes von Automatisierung und Rechenleistung zur Beeinflussung von Wahlentscheidungen ist zurzeit noch sehr begrenzt", Machado Caio, Konopacki Marco (2018): „Computational Power: Use of Automation on WhatsApp in the Elections; A study on the use of automation tools to boost political campaigns digitally in the 2018 Brazilian elections" (Rechenleistung: Einsatz von Automatisierung auf WhatsApp bei den Wahlen; eine Studie über den Einsatz von Automatisierungswerkzeugen zur digitalen Stärkung politischer Kampagnen bei den Wahlen in Brasilien 2018), ITS Rio.

64 Casaes D., Córdova Y. (2019): „Weaponized Information in Brazil: Digitizing Hate" (Informationen als Waffe in Brasilien: die Digitalisierung des Hasses), Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, Zugang Januar 2019.

65 Casaes D., Córdova Y. (2019): „Weaponized Information in Brazil: Digitizing Hate" (Informationen als Waffe in Brasilien: die Digitalisierung des Hasses), Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, Zugang Januar 2019.

66 „WhatsApp ist zu einem besonders kraftvollen Kampagneninstrument geworden. Aufgrund ihrer einfachen Anwendung, ihrer durchgängigen Verschlüsselung und der Möglichkeit zum Austausch von Nachrichten innerhalb großer Nutzergruppen ist WhatsApp in Ländern wie Indien (Hickok, 2018), Brasilien und anderen Ländern der südlichen Hemisphäre äußerst beliebt. WhatsApp gestattet den Parteien jedoch nicht nur das Zuschneiden von Nachrichten auf präzise Gruppen, sondern bietet außerdem Anonymität. Dadurch ist es einfach, die Identität eines Absenders mithilfe von vorhersagbaren und weit verbreiteten Bedenken bezüglich der Lieferung von ‚Fake News' und Hass anstachelnden Nachrichten falsch darzustellen. Rafael Evangelista und Fernanda Bruno (2019) demonstrieren die bösartige Verwendung von WhatsApp in Brasilien zur Verbreitung von Nachrichten mit rassistischem, frauenfeindlichem und homophobem Inhalt (...). Ihre Analyse legt nahe, dass sich WhatsApp auf eine vertrauensvollere Beziehung zwischen Gruppenmitgliedern verlässt als das innerhalb sonstiger sozialer Medien offenbar ist. Deshalb stellt WhatsApp ein empfänglicheres Medium für die Verbreitung von Falschinformation dar." Siehe Bennett C. J., Lyon D. (2019): „Data-driven elections: implications and challenges for democratic societies" (Datengetriebene Wahlen: Implikationen und Herausforderungen für demokratische Gesellschaften), Internet Policy Review, 8(4). Siehe auch: Evangelista R., Bruno F. (2019): „WhatsApp and political instability in Brazil: targeted messages and political radicalization" (WhatsApp und politische Instabilität in Brasilien: gezielte Nachrichten und politische Radikalisierung), Internet Policy Review, 8(4).

67 Netzneutralität ist das Prinzip der gleichen Behandlung aller über das Internet verschickten Datenpakete unabhängig von ihrem Inhalt, Herkunftsort, Zielort und der Art der zu ihrem Zugang verwendeten Ausrüstung. „Zero-Rating" bedeutet, dass ein Internetanbieter dem Datenverkehr in Verbindung mit einer bestimmten Anwendung bzw. Anwendungsklasse auf der Grundlage einer kommerziellen Vereinbarung einen Preis von Null zuordnet, oder eine unilaterale Entscheidung eines Internetanbieters, die dazu führt, dass ein Teil des Content von der monatlichen Datenobergrenze des Nutzers ausgenommen ist.

68 Casaes D., Córdova Y. (2019): „Weaponized Information in Brazil: Digitizing Hate" (Informationen als Waffe in Brasilien: die Digitalisierung des Hasses), Policy Brief No. 63. Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, Zugang Januar 2019.

69 Gollatz K., Jenner L. (2018): „Hate Speech und Fake News – Zwei verwobene und politisierte Konzepte", HIIG.

70 Martins B., Varon J. (2018): „Data and elections in Brazil" (Daten und Wahlen in Brasilien), Coding Rights.

71 Außerdem dauern Untersuchungen in den Wahlgerichten an, die sich mit nicht offengelegten Zahlungen und Verträgen in Bezug auf Massennachrichtenverbreitung und Falschinformation in der Wahlkampagne 2018 beschäftigen.

72 Weiterhin kamen sogenannte Bons zur Steigerung der Durchdringung in Filterblasen zum Einsatz. Sie erhöhen die Fähigkeit, eine enorme Anzahl von Nachrichten online zu verschicken sowie Gegner anzu-

greifen und Diskussionen aufzubauen. Sie manipulieren Debatten, erzeugen und verbreiten falsche Nachrichten und beeinflussen die öffentliche Meinung, indem sie Nachrichten im großen Rahmen senden und replizieren. Viele Bots haben Hashtags auf Twitter und Facebook reproduziert, die an Bedeutung gewinnen, indem sie automatisierte Beiträge verschicken, um plötzlich zu einem bestimmten Thema entstehende Debatten zu ersticken. Martins B., Varon J. (2018): „Data and elections in Brazil" (Daten und Wahlen in Brasilien), Coding Rights.

73 Ruediger M. (2019): „Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018" (Roboter, soziale Netzwerke und Politik in Brasilien: Studie zur rechtswidrigen Einmischung in die öffentliche Debatte im Internet, den Risiken für die Demokratie und den Wahlvorgang 2018), FGV, http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/, Zugang Juli 2019.

74 Durch ihre Einmischung in Diskussionen erreichen Roboter direkt politische und demokratische Prozesse mittels ihrer Beeinflussung der öffentlichen Meinung. Cordova Y., Doneda D. (2017): „A Place for the Robots in the Elections" (Ein Platz für die Roboter bei den Wahlen), JOTA, https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017, Zugang März 2018.

75 Magrani Eduardo, Medeiros R. (2019): „The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018" (Der im Zeitalter von Fake News und Filterblasen gebildete öffentliche Raum: die Erfahrungen in Brasilien 2018), Cyber law.

76 Siehe https://observa2018.com.br/posts/debate-influenciado-por-robos-volta-a-crescer-e-chega-a-104-das-discussoes-sobre-os-presidenciaveis-no-twitter/, Zugang Oktober 2018.

77 Es ist wichtig zu bemerken, dass automatisierte Accounts auch positive Aspekte für das Leben in sozialen Netzwerken liefern können. Chatbots vereinfachen zum Beispiel den Kundendienst und helfen in einigen Fällen sogar Verbrauchern bei ihrer Verarbeitung von Anfragen und bei der Informationsbeschaffung. Nichtsdestotrotz agiert eine zunehmende Anzahl von Robotern im öffentlichen Raum mit bösartiger Absicht. Social Bots (soziale Roboter) sind von Software kontrollierte Accounts, die Content künstlich erzeugen und Interaktionen mit Nichtrobotern eingehen. Sie versuchen, menschliches Verhalten zu imitieren und als Mensch aufzutreten, um sich in legitime und freiwillige Debatten einzumischen und erzwungene (d. h. nicht organisch entstandene) Diskussionen zu erzeugen. Institute of Technology and Equity (2017): „Experts Explain How the Robot can Influence the Debate in Networks" (Fachleute erklären, wie der Roboter die Debatte in Netzwerken beeinflussen kann), Medium, https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849, Zugang Oktober 2017.

78 Das Studium des Einsatzes von Robotern zeigt bereits deutlich das negative Potenzial dieser Praxis für die politische Auseinandersetzung und die öffentliche Debatte. Eine der offensichtlichsten Schlussfolgerungen in diesem Sinn ist die Konzentration dieser Handlungen an den extremen Polen des politischen Spektrums, wo eine künstliche Steigerung der Radikalisierung der Debatte in Blasenfiltern erfolgt und wo folglich potenzielle Brücken des Dialogs zwischen den unterschiedlichen etablierten politischen Feldern untergraben werden. Daher können Roboter nicht nur Falschinformationen verbreiten, was schädliche Auswirkungen auf die Gesellschaft haben kann, sondern Nutzer auch aktiv daran hindern, sich selbst angemessen zu informieren. Magrani Eduardo, Medeiros R. (2019): „The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018" (Der im Zeitalter von Fake News und Filterblasen gebildete öffentliche Raum: die Erfahrungen in Brasilien 2018), Cyber law.

79 Siehe https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml, Zugang Januar 2020.

80 Eine andere Art von Falschinformationstechnik, die in der Praxis zunehmend beobachtet wird und eine ernste Sorge darstellt, sind „Deep Fakes". Hierbei handelt es sich um eine neue und höher entwickelte Methode, Falschinformationen zu erzeugen. Deep Fakes sind gefälschte Videos oder Audioaufzeichnungen, die genau wie die echte Person aussehen bzw. sich anhören. Es gibt bereits heute Technologien, die Audioaufzeichnungen mit Imitation gestatten, die der Stimme von Menschen sehr ähnlich sind und das Bearbeiten von Videos ermöglichen, in denen das Gesicht einer Person als Teilnehmer erscheint, obwohl diese Person in der Situation nicht aufgetreten ist. Solch ein Eingriff ist bereits im täglichen Leben einer nicht in der Öffentlichkeit stehenden Person äußerst schädigend für ihren guten Ruf und ihr Image. Dieses Risiko wächst exponentiell, wenn Personen des öffentlichen Lebens davon betroffen sind. Audio und editierte Videos können zum Beispiel zur Verleumdung eines bestimmten Kandidaten für eine zur Wahl stehende Position verwendet werden. Am 23. Oktober 2018 wurde in Brasilien ein Video im Internet (hauptsächlich auf WhatsApp) verbreitet, in dem João Doria (PSDB), der Gouverneurskandidat für den Staat São Paulo, angeblich in intimen Szenen mit Frauen zu sehen war. Die Verbreitung eines solchen Videos fünf Tage nach der zweiten Wahlrunde ist äußerst schädigend für das Image des Kandidaten, insbesondere wenn man berücksichtigt, dass Doria als Verfechter traditioneller Familienwerte gilt. Der damalige Kandidat reichte eine Untersuchungsklage bei einem Wahlgericht ein. Zuerst kamen die Untersuchungen in Bezug auf das Video zu dem Schluss, dass es zusammengestellt oder simuliert war. Ein Gutachten erklärte, dass das Gesicht des Kandida-

ten fälschlich in das Video eingefügt worden war und er in einer Situation gezeigt wurde, in der er sich niemals befunden hatte. In der Folge bestätigte ein neues Gutachten jedoch die Echtheit des Videos. Kurz gesagt: Es gab zwei technische Gutachten mit widersprüchlichen Aussagen. Nach der Freigabe des Videos zeigten Umfragen zur Wahlpräferenz eine gewisse Variation der Prozentpunkte jedes Kandidaten. Entsprechend der von Datafolha am 25. Oktober 2018 durchgeführten Umfrage hatte Doria 52 Prozent der Stimmen, während der Prozentsatz am 27. Oktober auf 49 Prozent gefallen war. Unter Berücksichtigung der Intensität der Kampagnen in den Tagen unmittelbar vor den Wahlen und der Überfülle der offengelegten Informationen können wir nicht mit Sicherheit sagen, dass das Video für diese Verringerung direkt verantwortlich war. Tatsache ist, dass die Offenlegung dieses Deep Fake in Verbindung mit widersprüchlichen Expertengutachten nicht ausreichte, um den Sieg des Kandidaten zu verhindern, der mit 51,77 Prozent der gültigen Stimmen gewann. Herauszustellen ist jedoch, dass wir bestätigen können, dass diese Art von Video einen wichtigen Faktor der Schlussphase einer Kampagne darstellen kann. Zudem wird die Realität selbst in Frage gestellt, und es ist nicht länger eindeutig, was wahr oder falsch ist. Diese Situation schafft geistige Verwirrung in der Wählerschaft, die an eine Seite glaubt, ohne dafür solide Argumente zu haben, und sich auf Erzählungen verlässt. Wenn alles andere in Frage gestellt scheint, führt das menschliche Bedürfnis nach einer Antwort dazu, dass sich Menschen an allen möglichen Anhaltspunkten für die Wahrheit festhalten oder sich zuvor gehegten Vorurteilen oder sogar der Selbsttäuschung hingeben. Der Einsatz von Deep Fakes zusammen mit Microtargeting und künstlicher Intelligenz ohne ordnungsgemäße und robuste Reglementierung zu ihrer Kontrolle ist bereits heute eine der bedeutendsten Befürchtungen für zukünftige Wahlen. Magrani Eduardo, Medeiros R. (2019): „The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018“ (Der im Zeitalter von Fake News und Filterblasen gebildete öffentliche Raum: die Erfahrungen in Brasilien 2018), Cyber law.

81 Ortellado Pablo (2018): „Bias on the Internet Does Not Seem to Be Caused by Bubbles“ (Vorurteile im Internet scheinen nicht von Blasen verursacht zu sein), Folha de São Paulo, https://www1.folha.uol.com.br/colunas/pablo-ortellado/2018/02/polarizacao-na-internet-nao-parece-ser-causada-pelas-bolhas.shtml, Zugang Oktober 2018. Siehe auch Mello P. (2018): „Entrepreneurs Campaign Against the PT by WhatsApp“ (Unternehmer führen Kampagne gegen PT [Partido dos Trabalhadores, Partei der Arbeiter] auf WhatsApp), Folha de São Paulo, https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml, Zugang Oktober 2018.

82 Magrani Eduardo, Medeiros R. (2019): „The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018“ (Der im Zeitalter von Fake News und Filterblasen gebildete öffentliche Raum: die Erfahrungen in Brasilien 2018), Cyber law.

83 Bots machen mehr als 50 Prozent des weltweiten Internet-Verkehrs aus. Einige Bots beabsichtigen beispielsweise, Politiker zur Verantwortung zu ziehen, die Geschlechterungleichheit auszumerzen oder die (vielen) Alltagstätigkeiten ihrer Nutzer organisieren zu helfen. Andere Bots zielen dagegen darauf ab, Lügen zu verbreiten, um Konversationen im öffentlichen Raum zu beeinflussen: ein Phänomen, das seit 2014 global an Gewicht gewonnen hat. Diese Bots existieren, wobei kaum jemand weiß, wie sie arbeiten, wer sie entwickelt und von wem sie finanziert werden. Siehe https://g1.globo.com/rs/rio-grande-do-sul/noticia/pesquisa-demonstra-que-repercussao-do-cancelamento-do-queermuseu-foi-insuflada-por-robos-na-internet.ghtml, Zugang März 2017.

84 Ruediger M. (2019): „Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018“ (Roboter, soziale Netzwerke und Politik in Brasilien: Studie zur rechtswidrigen Einmischung in die öffentliche Debatte im Internet, den Risiken für die Demokratie und den Wahlvorgang 2018), FGV, http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/, Zugang Juli 2019.

85 Ruediger M. (2019): „Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018“ (Roboter, soziale Netzwerke und Politik in Brasilien: Studie zur rechtswidrigen Einmischung in die öffentliche Debatte im Internet, den Risiken für die Demokratie und den Wahlvorgang 2018), FGV, http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/, Zugang Juli 2019.

86 Ruediger M. (2019): „Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018“ (Roboter, soziale Netzwerke und Politik in Brasilien: Studie zur rechtswidrigen Einmischung in die öffentliche Debatte im Internet, den Risiken für die Demokratie und den Wahlvorgang 2018), FGV, http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/, Zugang Juli 2019.

87 Im Jahr 2014, als eine Präsidentschaftswahl erstmalig von Robotern in einem bedeutsameren Maß gestört wurde, gab es eine ähnliche Interferenz. Die Bots waren für mehr als zehn Prozent der Interaktionen auf Twitter verantwortlich. Zuvor waren Roboter während des Amtsenthebungsprozesses der vorher-

gehenden Präsidentin Dilma Rousseff für 20 Prozent der Debatte unter den Anhängern von Rousseff verantwortlich gewesen. In der zweiten Runde der Wahlen 2014 wurden 20 Prozent der Interaktionen zugunsten von Aécio Neves von Robotern verursacht. Siehe Ruediger M. (2019): „Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018" (Roboter, soziale Netzwerke und Politik in Brasilien: Studie zur rechtswidrigen Einmischung in die öffentliche Debatte im Internet, den Risiken für die Demokratie und den Wahlvorgang 2018), FGV, http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/, Zugang Juli 2019.

88 „Twitter gibt an, dass das Unternehmen seit Juni 2017 täglich durchschnittlich 130.000 Accounts festgestellt hat, die versucht hatten, Trendthemen mithilfe von Social Bots zu manipulieren. Das soziale Netzwerk behauptet, dass ungefähr 16 Millionen Fake oder Spam Accounts existieren, während Fachleute schätzen, dass diese Zahl größer ist. Diese Dynamik wird „Botnet" genannt, d. h. ein Netzwerk aus Robotern, bei dem Profile auf eine synchronisierte Art und Weise mit derselben Leistungsfähigkeit handeln: ein Profil sendet einen Beitrag und andere retweeten oder antworten oder veröffentlichen etwas Ähnliches. Die allgemeinen Bestimmungen der Plattform geben an, dass es nicht gestattet ist, Twitter-Dienste zur künstlichen Verstärkung oder Unterdrückung von Informationen oder zu einem Verhalten zu verwenden, bei dem das Erlebnis anderer Personen auf Twitter manipuliert oder geschädigt wird. Das soziale Netzwerk erklärt, dass gegen diese Bestimmungen verstoßende Accounts mit verringerter Sichtbarkeit, ihrer Entfernung aus der Twitter-Suchmaschine und sogar einem Bann bestraft werden können." Siehe https://apublica.org/2019/12/como-funciona-um-perfil-robo-no-twitter/, Zugang Januar 2020.

89 „Die Erkennung mittels maschinellem Lernen erfolgt durch Kodierung der Verhaltensmuster aus der Erfassung von Metadaten. Auf diese Weise ist das System in der Lage, Menschen und Roboter automatisch auf der Grundlage der Verhaltensmuster des Profils zu identifizieren. Nutzermetadaten werden als einer der am einfachsten vorherzusagenden Aspekte der Differenzierung zwischen Menschen und Robotern betrachtet und können zu einem besseren Verständnis der Funktionsweise hoch entwickelter Roboter beitragen. Die Identifizierung dieser Roboter oder gehackten Accounts ist jedoch schwierig für diese Systeme. Zusätzlich führt die fortlaufende Evolution von Robotern dazu, dass das aus einer statischen Datenbank aufgebaute System mit der Zeit weniger exakt wird. Es gestattet allerdings die Verarbeitung einer großen Anzahl komplexer Korrelationen und Muster sowie die Analyse einer großen Anzahl von Accounts. Die effizientesten Identifizierungsmechanismen kombinieren unterschiedliche Aspekte dieser Ansätze und erforschen mehrere Dimensionen von Profilverhaltensweisen wie beispielsweise Aktivitäts- und Zeitmuster. Diese Systeme berücksichtigen zum Beispiel, dass echte Nutzer mehr Zeit im Netzwerk mit dem Austausch von Nachrichten und dem Besuch des Content anderer Nutzer verbringen, wie beispielsweise Fotos und Videos, während Roboter-Accounts ihre Zeit damit verbringen, Profile zu durchsuchen und Freundschaftsanfragen zu senden." Ruediger M. (2019): „Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018" (Roboter, soziale Netzwerke und Politik in Brasilien: Studie der rechtswidrigen Einmischung in die öffentliche Debatte im Internet, der Risiken für die Demokratie und des Wahlvorgangs 2018), FGV, http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/, Zugang Juli 2019.

90 Magrani Eduardo, Medeiros R. (2019): „The public sphere forged in the era of fake news and filter bubbles: the Brazilian experience of 2018" (Der im Zeitalter von Fake News und Filterblasen gebildete öffentliche Raum: die Erfahrungen in Brasilien 2018), Cyber law.

91 Simões M. (2018): „Pro-Bolsonaro Groups on WhatsApp Orchestrate Fake news and Personal Attacks on the Internet, Research Says" (Recherchen zeigen, dass Gruppen von Bolsonaro-Anhängern auf WhatsApp Fake News veröffentlichen und persönliche Angriffe im Internet senden), El País, https://brasil.elpais.com/brasil/2018/10/23/politica/1540304695_112075.html?id_externo_rsoc=FB_BR_CM&fbclid=IwAR05Mw9z-XzmjDbYv5OkjAm1hVipWBURMCPyiOORIaxSsy_qNxEjzrpHKxfQ, Zugang Oktober 2018.

92 Siehe https://observa2018.com.br/posts/fraude-nas-urnas-e-kit-gay-tem-maior-impacto-que-outras-noticias-falsas-em-twitter-facebook-e-youtube/, Zugang Oktober 2018.

93 Gianetti E. (2005): „Lies We Live By: The Art of Self-deception" (Lügen, mit denen wir leben: die Kunst der Selbsttäuschung), Companhia das Letras.

94 Es gibt Gesetzesentwürfe im brasilianischen Nationalkongress für Projekte zur Kriminalisierung der Offenlegung von falschen Fakten bzw. Fake News, zum Beispiel Gesetzesentwurf Nr. 9973/2018, 10292/2018, 9931/2018 und 9532/2018 im Repräsentantenhaus. Der Senatsgesetzesentwurf Nr. 246/2018 ist breiter gefasst und beabsichtigt die Aufnahme von Internet-„Maßnahmen zur Bekämpfung der Offenlegung von falschem Content oder anstößigen Internet-Anwendungen." Zusätzlich gibt es Gruppen mit der Absicht der Faktenprüfung. Jedoch könnte in einem Szenario, in dem alles in Frage gestellt ist, der Überfluss wahrer und falscher Informationen zum sogenannten Kontext einer Infocalypse (nach Prof. Aviv Ovadya) führen, welcher die Möglichkeit eines Konsenses auf rationaler und demokratischer Grundlage gefährden könnte. Aus diesem Grund unterstreichen wir oben die Wesentlichkeit, ein Mindestmaß an Konsens über die Realität sowie Achtung für fundamentale ethische Prinzipien zu gewährleisten. Eine ausführliche Auf-

zählung und detaillierte Darstellung aller Gesetzesentwürfe zu diesem Thema würde eine eigene Studie erfordern und über die Grenzen dieses Artikels hinausgehen. Siehe https://www.uol/noticias/especiais/ele-previu-o-apocalipse-das-noticias-falsas.htm, Zugang Januar 2020.

95 Siehe https://www1.folha.uol.com.br/poder/2018/12/fraude-com-cpf-viabilizou-disparo-de-mensagens-de-whatsapp-na-eleicao.shtml. Siehe auch https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml Siehe auch https://www1.folha.uol.com.br/poder/2018/10/entenda-as-irregularidades-envolvendo-uso-do-whatsapp-na-eleicao.shtml, Zugang Januar 2020.

96 Siehe https://riotimesonline.com/brazil-news/brazil/whatsapp-admits-to-illegal-mass, Zugang November 2019.

97 Facebook, das unter zunehmenden Druck geraten ist, mehr gegen Falschinformation zu unternehmen, kündigte ein Update von WhatsApp im Januar an, das die Anzahl der Weiterleitungen einer einzelnen Nachricht durch einen Nutzer auf fünf Weiterleitungen verringert. Siehe https://www.theguardian.com/world/2019/oct/29/europe-accuses-facebook-of-being-slow-to-remove-fake-accounts, Zugang Januar 2020. Siehe auch https://www.theguardian.com/technology/2019/jan/21/whatsapp-limits-message-forwarding-fight-fake-news. Siehe auch https://politica.estadao.com.br/blogs/estadao-verifica/limite-de-encaminhamento-no-whatsapp-nao-consegue-frear-desinformacao-na-plataforma-aponta-pesquisa/?amp&__twitter_impression=true&fbclid=IwAR1X_aDEg7Mlz_0OoCE1piZHkO_TyyMQVgyw9SH-hT4Vc37LbfJ5By6JumU, Zugang Januar 2020.

98 Siehe https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests?CMP=share_btn_fb, Zugang Januar 2020.

99 Yasodora Cordova und Diego Casaes gaben in einem kürzlichen Bericht über den brasilianischen Kontext Folgendes an: „Brasilianer machen alles über WhatsApp, da es „kostenlos“ ist. Von Musikklassen bis zu E-Commerce und Arztterminen: Die App wurde zum zentralen Bestandteil des Funktionierens des Geschäfts- und Familienlebens, insbesondere für stark armutsgefährdete Gemeinschaften. Die brasilianischen Bürger gehören zu den stärksten Nutzern sozialer Medien weltweit, an zweiter Stelle hinter den Philippinen. Bürger sind jedoch oft durch den Content eingeschränkt, den sie über WhatsApp erhalten, und verlieren daher den Kontext und die Gelegenheit, unterschiedliche Versionen online zu prüfen und ihr Wissen zu erweitern. Die Tatsache, dass der gesamte Inhalt auf WhatsApp frei von Internet-Gebühren ist, erleichtert es Personen, Audioaufzeichnungen oder YouTube-Videos (die in WhatsApp öffnen) zu verbreiten. Aufgrund dieses Designs kann WhatsApp als Kanal von Desinformation in vielen Formaten betrachtet werden und ist besonders schädigend in Bezug auf Audios und Videos. Zusammen bildeten YouTube und WhatsApp eine Pipeline der Falschinformation und verbreiteten Verschwörungstheorien, Kampagnenmaterial und politische Propaganda in ganz Brasilien.“ Casaes D., Córdova Y. (2019): „Weaponized Information in Brazil: Digitizing Hate“ (Informationen als Waffe in Brasilien: die Digitalisierung des Hasses), Policy Brief No. 63 Toda, https://toda.org/assets/files/resources/policy-briefs/t-pb-63_casaes-and-cordova_weaponised-information-in-brazil.pdf, Zugang Januar 2019.

100 Evangelista R., Bruno F. (2019): „WhatsApp and political instability in Brazil: targeted messages and political radicalization“ (WhatsApp und politische Instabilität in Brasilien: gezielte Nachrichten und politische Radikalisierung), Internet Policy Review, 8(4), Zugang Oktober 2018. Rafael Evangelista und Fernanda Bruno erklären es wie folgt: Obwohl WhatsApp keinen Dienst zum Microtargeting von Zielgruppen anbietet, ist belegt, dass auf unpolitische Marketingkampagnen spezialisierte Drittunternehmen diese Art von Dienstleistung im Kontext von Wahlen anboten, wobei gelegentlich rechtswidrige Datenbanken zum Einsatz kamen. (...) Der Fall des Einsatzes von WhatsApp bei den Wahlen in Brasilien zeigt, wie eine Überwachungsstruktur auf einem Gruppennachrichtendienst aufgebaut wurde, der angeblich Verschlüsselung zum Nutzerdatenschutz verwendet.“

101 Siehe https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests?CMP=share_btn_fb, Zugang Januar 2020.

102 „Internet Policy Review, 8(4).“ Siehe auch Cesarino L. (2019): „On Digital Populism in Brazil“ (Digitaler Populismus in Brasilien), PoLAR: Political and Legal Anthropology Review, https://polarjournal.org/2019/04/15/on-jair-bolsonaros-digital-populism/, Zugang Januar 2020.

103 Die Europäische Kommission „hat [kürzlich] das Ausgesetztsein der Bürger gegen Online-Desinformation und das Microtargeting von Wählern auf der Grundlage der gesetzeswidrigen Verarbeitung personenbezogener Daten als eine der wichtigsten Herausforderungen für europäische Demokratien anerkannt. Als Antwort darauf hat die EK mehrere Maßnahmen zur Formulierung eines europäischen Ansatzes eingeleitet. (...) Der Leitfaden der Kommission zur Anwendung der DSGVO im Zusammenhang mit Wahlen (EK, 2018d) unterstreicht, dass sie „für alle Akteure im Zusammenhang mit Wahlen gilt“, einschließlich europäischen und nationalen politischen Parteien, europäischen und nationalen politischen Stiftungen, Plattformen, Datenanalyseunternehmen und öffentlichen Behörden mit Verantwortung für den Wahlprozess. Jegliche Datenverarbeitung muss die Prinzipien der DSGVO beachten, zum Beispiel Fairness und

Transparenz, und darf ausschließlich zu vorgegebenen Zwecken erfolgen." Siehe Nenadić I. (2019): „Unpacking the European approach to tackling challenges of disinformation and political manipulation" (Analyse des europäischen Ansatzes zur Bewältigung von Herausforderungen bezüglich Desinformation und politischer Manipulation), Internet Policy Review, 8(4). Siehe auch: Europäische Kommission (2018): „Free and fair European elections – Factsheet, State of the Union", (Lage der Union 2018: Europäische Kommission schlägt Maßnahmen zur Gewährleistung freier und fairer Europawahlen vor) https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681. Siehe auch: Europäische Kommission (2018): „Commission guidance on the application of Union data protection law in the electoral context: A contribution from the European Commission to the Leaders' meeting in Salzburg" (Leitfaden der Kommission zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen. Ein Beitrag der Europäischen Kommission zum Treffen der Führungsspitzen in Salzburg), https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf, Zugang Januar 2019.

104 Westby J. (2019): „The Great Hack': Cambridge Analytica is just the tip of the iceberg" (Der große Hack: Cambridge Analytica ist lediglich die Spitze des Eisbergs), Amnesty Tech, https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/, Zugang Januar 2019.

105 Westby J. (2019): „The Great Hack': Cambridge Analytica is just the tip of the iceberg" (Der große Hack: Cambridge Analytica ist lediglich die Spitze des Eisbergs), Amnesty Tech, https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/, Zugang Januar 2019.

106 Siehe https://privacyinternational.org/learning-topics/data-and-elections, Zugang Januar 2019.

107 Risso Linda (2017): „Harvesting Your Soul? Cambridge Analytica and Brexit" (Wird Ihre Seele geerntet? Cambridge Analytica und Brexit), Akademie der Wissenschaften und der Literatur, http://www.adwmainz.de/fileadmin/user_upload/Brexit-Symposium_Online-Version.pdf#page=75, Zugang Dezember 2019.

108 „Politische Entscheidungsträger sollten verpflichtet sein, mit den sich schnell entwickelnden Innovationen in Technologie- und Marketingbranchen Schritt zu halten und die Verwendungszwecke und Missbräuche digitaler Anwendungen zu politischen Zwecken zu identifizieren, wie beispielsweise die Methode, mit der WhatsApp während der jüngsten Wahlen in Brasilien zur computergestützten Propaganda eingesetzt wurde." In: Chester J., Montgomery K. C. (2019): „The digital commercialization of US politics – 2020 and beyond" (Die digitale Kommerzialisierung der US-Politik – 2020 und darüber hinaus), Internet Policy Review, 8(4), Zugang Januar 2019.

109 „Es ist angemessen zu sagen, dass Aufsichtsbehörden im Allgemeinen die komplexe Vielfalt der durch datengetriebene Kampagnen dargestellten Risiken nur langsam anerkannt haben. Bis vor Kurzem hatten die meisten Datenschutzbehörden zum Beispiel kein aktives Interesse an der Verarbeitung personenbezogener Daten im Zusammenhang mit dem Wahlprozess in ihren Ländern gezeigt. Es gab gewisse frühe Leitfäden und Regelungen zu politischen Kampagnen im Vereinigten Königreich (ICO, 2014) und eine Reihe von Regelungen in Frankreich (CNIL, 2012). In den meisten EU-Ländern und in anderen Ländern, in denen politische Parteien den Bestimmungen von Datenschutzgesetzen unterliegen, beziehen sich solche Regelungen auf relativ eng gefasste Fragen, die aufgrund vereinzelter Klagen bezüglich der Handlungen bestimmter Parteien und Kandidaten während spezifischer Wahlkämpfe aufgetreten sind. In ähnlicher Weise haben sich Wahlaufsichtsbehörden in der Regel mehr mit dem transparenten und effizienten Ablauf von Wahlen beschäftigt, zusammen mit Fragen zur Wahlfinanzierung, und weniger mit Bedenken bezüglich der Verarbeitung personenbezogener Daten der Wählerschaft." Siehe Bennett C. J., Lyon D. (2019): „Data-driven elections: implications and challenges for democratic societies" (Datenbasierte Wahlen: Implikationen und Herausforderungen für demokratische Gesellschaften), Internet Policy Review, 8(4).

110 Europäische Kommission: „Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions" (Vorschlag der Kommission: noch besserer Schutz der Privatsphäre für die gesamte elektronische Kommunikation und moderne Datenschutzvorschriften für die EU-Organe), http://europa.eu/rapid/press-release_IP-17-16_en.htm, Zugang Januar 2019.

111 Woolley Samuel C., Howard Philip N. (2017): „Computational Propaganda Worldwide" (Weltweite computergestützte Propaganda), Universität Oxford, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf, Zugang Oktober 2019.

112 Lane Julia et al. (Hrsgg.) (2014): „Privacy, Big Data, and the Public Good: Frameworks for Engagement" (Datenschutz, Big Data und das Gemeinwohl: Rahmenbedingungen zur Interaktion), Cambridge.

113 Die Europäischen Kommission schlägt ein hohes Maß an Datenschutzbestimmungen für die gesamte elektronische Kommunikation vor und aktualisiert Datenschutzvorschriften für EU-Organe. 2017. Siehe http://europa.eu/rapid/press-release_IP-17-16_en.htm, Zugang Januar 2019.

2. Beachtung der Datenschutz-bestimmungen bei Wahlen

Eine vergleichende Analyse zwischen der EU und Brasilien (DSGVO vs. LGPD)

Zur Analyse der Anwendung von Bestimmungen zum Schutz personenbezogener Daten auf Wahlprozesse in Brasilien und der EU untersucht dieser Abschnitt die relevantesten Ähnlichkeiten und Unterschiede zwischen der europäischen Datenschutz-Grundverordnung (DSGVO) und dem brasilianischen Allgemeinen Datenschutzgesetz („Lei Geral de Proteção de Dados Pessoais", LGPD). Die folgenden Erwägungen untersuchen, wie diese komplizierten Systeme die Grenzen der Datenverarbeitungsfähigkeiten der Kandidaten und Parteien in jeder Gerichtsbarkeit bestimmen, während sie außerdem relevante normative Instrumente spezifisch in Bezug auf Wahlprozesse vorstellen.

Das brasilianische Allgemeine Datenschutzgesetz war weithin auf der Datenschutz-Grundverordnung der EU gegründet. Deshalb bestehen viele Ähnlichkeiten zwischen den beiden Gesetzen. Zuerst gibt es Überschneidungen zwischen den allgemeinen Grundsätzen in beiden Gesetzen. Die DSGVO führt in Artikel 5 sechs Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten an. Das LGPD nennt in Artikel 6 zehn Grundsätze. Beide Verordnungen bzw. Gesetze enthalten die Kernwertvorstellungen von festgelegten und eindeutigen Zwecken, Transparenz, Qualität (Richtigkeit) von Daten, Sicherheit, Verantwortlichkeit, Rechtmäßigkeit und Verarbeitung nach Treu und Glauben (Fairness). Der Kopfteil des brasilianischen Artikels zu den Grundsätzen lautet:

> *Art. 6 Aktivitäten zur Verarbeitung personenbezogener Daten müssen nach Treu und Glauben erfolgen und folgende Grundsätze beachten …*

Die Erwähnung von „Treu und Glauben" (boa-fé) könnte als analog zum Fairness-Grundsatz der DSGVO interpretiert werden. „Boa-fé" ist ein allgemeiner Grundsatz des bürgerlichen Rechts in Brasilien. Seine ausdrückliche Erwähnung im Kopfteil des Artikels in Bezug auf die Grundsätze der Verarbeitung personenbezogener Daten stärkt seine Rolle als interpretative Achse bei der Anwendung des Gesetzes. In der Praxis bedeutet das die Berücksichtigung des Kontexts der Datenerfassung zur Bestimmung der angemessen erwarteten und fairen Verwendung der Daten. Juristen beschreiben dies als „kontextabhängigen Datenschutz":[114]

> *Zusammenfassend betrachtet umfasst die Theorie des kontextabhängigen Datenschutzes deshalb die Erwägung, dass die betroffene Person legitime Erwartungen (Schutz ihrer Daten) in Bezug auf den angemessenen Fluss ihrer Daten haben kann. Der Datenverkehr findet daher nicht in einem Vakuum statt, sondern unter einer Gruppe von Umständen, die seine Integrität bestimmen.*

Abgesehen von vielen Ähnlichkeiten wie dem oben erwähnten Fairnessgrundsatz gibt es allerdings Punkte, in denen sich die beiden Gesetze unterscheiden. Ein solcher Fall ist die Definition von gemeinsam Verantwortlichen. Gemeinsam Verantwortliche sind in Artikel 26 der DSGVO beschrieben, der besagt:

> *Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14*

nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

Es ist wichtig, hervorzuheben, dass derselbe Datensatz viele bestimmte Verantwortliche haben kann, wenn diese ihn zu bestimmten Zwecken verwenden, oder gemeinsam Verantwortliche, wenn diese gemeinsam über die Zwecke der Verarbeitung entscheiden[115]. Das brasilianische Gesetz umfasst dagegen keine ausdrückliche Kategorie gemeinsam Verantwortlicher. Die Verantwortlichkeit wird weiterhin auf der Grundlage der Fähigkeit festgestellt, über die Zwecke der Verarbeitung zu entscheiden, wobei jedoch keine gemeinsame Verantwortlichkeit erwähnt wird. Das Gesetz weist allerdings in einem Fall darauf hin.

In Artikel 42, II, erklärt das LGPD, dass die Verantwortlichen, die direkt an einer Verarbeitungsaktivität beteiligt sind, die gemeinsame Verantwortung für mögliche Verstöße gegen das Gesetz tragen. Dieser Artikel legt eine gemeinsame Verantwortung nahe, indem er besagt, dass bestimmte Akteure unter den Auswirkungen des Gesetzes zusammengefasst werden können. Das ist eine Auslegung, die bei der Festlegung der Steuerungsstruktur politischer Kampagnenanstrengungen berücksichtigt werden sollte. In solchen Fällen ist das besonders wahr, was von einer anderen Rechtsvorschrift zur Haftung von Kandidaten und politischen Parteien untermauert wird. Das brasilianische Gesetz Nr. 9.504/1997 erklärt in Artikel 6, § 5:

§ 5 Kandidaten und ihre Parteien haften gemeinsam und einzeln für Geldbußen aufgrund von Wahlpropaganda …

Daher ist das LGPD vollständig anwendbar auf die Verarbeitung personenbezogener Daten, die von Parteien und Kandidaten durchgeführt wird, sowie auf ihre Kampagnenstrukturen. Im brasilianischen Gesetz wird dies weiter unterstrichen, indem politische Parteien als private Vereinigungen charakterisiert werden, d. h. als Rechtswesenheiten, die unter dieselben rechtlichen Grundsätze fallen wie Privatunternehmen und Nichtregierungsorganisationen.

Die Verantwortlichkeit ist eine entscheidende Frage in beiden Gesetzen, da der Verantwortliche für die Implementierung einer breiten Gruppe aus Anforderungen verantwortlich und in letzter Instanz für mögliche Verstöße haftbar ist. Die Feststellung des Verantwortlichen für personenbezogene Daten kann sich in der Praxis als Herausforderung erweisen, bei der es darum geht, die Person(en) ausfindig zu machen, welche die Fähigkeit hat (haben), Entscheidungen von bedeutender Tragweite über die Zwecke und Mittel der Datenverarbeitung zu treffen. Im Kontext politischer Kampagnen kann sich das als komplexe Bewertung herausstellen:

Die Rolle des Datenverantwortlichen oder Datenverarbeiters/-auftragsverarbeiters muss für jeden Einzelfall bewertet werden. Im Zusammenhang mit Wahlen können eine Reihe von Akteuren Datenverantwortliche sein: Politische Parteien, einzelne Kandidaten und Stiftungen sind in den meisten Fällen Datenverantwortliche. Plattformen und Datenanalyseunternehmen können (gemeinsam) Verantwortliche oder Auftragsver-

arbeiter für eine gegebene Verarbeitung sein, was vom Ausmaß ihrer Kontrolle über die betreffende Verarbeitung abhängt. Nationale Wahlbehörden sind Verantwortliche für die Wählerverzeichnisse[116].

Abgesehen von Verantwortlichen müssen politische Kampagnen ebenfalls zwei weitere Rechtswesenheiten beachten, die an den Beziehungen der Verarbeitung personenbezogener Daten beteiligt sind. Die Datenverarbeitung wird von einem „Auftragsverarbeiter" (DSGVO; im LGPD als *Operador* bezeichnet) durchgeführt, der den Willen und die Strategie des Verantwortlichen umsetzt. Während der Verantwortliche umfassende Entscheidungsbefugnis hat, implementiert der Auftragsverarbeiter lediglich die geplanten Verarbeitungsaktivitäten. Die andere Rechtswesenheit ist der Datenschutzbeauftragte (DSGVO; im brasilianischen Gesetz als *Encarregado* bezeichnet), der als Kommunikationskanal zwischen der betroffenen Person, der Datenschutzbehörde und dem Unternehmen bzw. der Organisation agiert.

Die Rollen des Auftragsverarbeiters und des Datenschutzbeauftragten sind sehr unterschiedlich. Der Auftragsverarbeiter ist an den Verarbeitungsaktivitäten beteiligt und hat den erforderlichen technischen Hintergrund zur Umsetzung der Entscheidungen des Verantwortlichen, dessen Anweisungen er ausführt. Der Datenschutzbeauftragte ist dagegen als „die Manifestation der Aufsichtsbehörde in einer Organisation"[117] beschrieben worden. Diese Rolle sollte idealerweise vom Verantwortlichen und Auftragsverarbeiter unabhängig sein, um eine umfassende Bewertung der Datenverarbeitungsaktivitäten durchführen und die Behörde und betroffenen Personen bei Bedarf über Probleme benachrichtigen zu können[118].

Obwohl sich die Konzepte für den Datenschutzbeauftragten und den *Encarregado* ähneln, sind die beiden in der DSGVO und im LGPD leicht unterschiedlich aufgebaut. Eine wesentliche Unterscheidung besteht darin, dass die Bestellung eines *Encarregado* im Allgemeinen vorgeschrieben ist und der Verzicht auf seine Bestellung eine weitere Vorgabe von der brasilianischen Datenschutzbehörde erfordert (Art. 41, § 3, LGPD). Die DSGVO führt dagegen die Fälle auf, in denen der Datenschutzbeauftragte notwendig ist, obwohl es als gute Praxis gilt, in allen Fällen einen solchen zu bestellen[119].

Das brasilianische Gesetz hat sich vor der Einführung des LGPD in einem beschränkten Ausmaß mit personenbezogenen Daten in Wahlkampagnen beschäftigt. Ein Beispiel bezieht sich auf den Austausch von Daten mit Dritten. Artikel 7, I, und § 5 des LGPD besagen, dass, falls Daten mit Einwilligung gesammelt und verarbeitet werden und einem anderen Verantwortlichen mitgeteilt werden müssen, eine neue spezifische Einwilligung der betroffenen Person erforderlich ist. Falls dies auf einer beliebigen sonstigen Rechtsgrundlage basierte, wären die Pflichten der Transparenz und Verantwortlichkeit sowie alle Rechte der Person und Rechtsgrundsätze weiterhin anwendbar, doch wäre keine vorhergehende Mitteilung an die Person erforderlich. Das würde bedeuten, dass die Übertragung und ihre Zwecke abhängig vom Einzelfall, jedoch vorzugsweise in einem Datenschutz-Folgenabschätzungsbericht (DSFA-Bericht)[120] erfasst werden. Falls berechtigtes Interesse die rechtmäßige Grundlage für die Verarbeitung darstellt, ist es empfehlenswert, eine Interessenabwägung, d. h. eine Abwägung des berechtigten Interesses (Legitimate Interest Assessment, LIA), vorzunehmen[121].

Vor der Einführung des LGPD gab es jedoch bereits Artikel 57-E von Gesetz Nr. 9.504/97 (Bestimmungen zu politischen Parteien), der ein Verbot des Austauschs oder Kaufs von Kontaktadressenlisten zu politischen Propagandazwecken enthielt. Der Artikel besagt:

> *Art. 57-E. Es ist den in Art. 24 aufgeführten Personen verboten, elektronische Verzeichnisse ihrer Kunden zugunsten von Kandidaten, Parteien oder Parteigruppierungen zu verwenden, zu spenden oder zu überlassen.*
>
> *§ 1 Es ist verboten, elektronische Adressenlisten zu verkaufen.*

Dieses allgemeine Verbot des Austauschs von Kontaktinformationen macht das Szenario noch komplizierter. „Elektronische Listen" (*cadastro eletrônico*) dürfen von einer Reihe von Rechtswesenheiten nicht weitergegeben werden, einschließlich ausländischen Rechtswesenheiten oder Regierungen; öffentlichen Verwaltungsbehörden; öffentlichen Dienstleistungsanbietern; Gewerkschaften; gemeinnützigen Organisationen, die ausländische Finanzierung erhalten; Nichtregierungsorganisationen, die öffentliche Finanzierung erhalten; usw. Privatunternehmen im Allgemeinen wurden im Anschluss an eine Entscheidung des Obersten Gerichtshofs zu Fall ADI 4650, der sich mit privaten Spenden an politische Kampagnen beschäftigte, hinzugefügt[122]. Zusätzlich ist jede kommerzielle Nutzung elektronischer Adressenlisten verboten.

Die DSGVO beschäftigt sich nicht ausdrücklich mit der Datenkommerzialisierung. Eine Auslegung nach den Regelungen und Grundsätzen der Verordnung ordnet jedoch an, dass ein Verantwortlicher personenbezogene Daten entsprechend den ursprünglich beabsichtigten Zwecken verarbeiten muss[123]. Dies bedeutet, dass die Übertragung von Daten an Dritte mittels Spende oder Verkauf den ursprünglichen Zweck der Datensammlung erfüllen muss.

In der Praxis bedeuten diese Erwägungen, dass politische Kampagnen die Quelle ihrer Daten und die Zugangsberechtigten sorgfältig prüfen sollten. Falls die ursprüngliche Datensammlung direkt durch die Kampagne mittels Online-Abonnement oder physischem Abonnement erfolgte, sollten alle zukünftigen Verwendungen der Informationen, einschließlich E-Mail-Marketing und Profiling, der betroffenen Person mitgeteilt werden. Falls die ursprüngliche Datensammlung keinen Bezug zu politischen Kampagnen hatte, zum Beispiel im Fall eines Kandidaten mit Kontaktinformationen über seine Wählerschaft mit dem Ziel, ihnen bei bestimmten Problemen im Rahmen der regulären Ausübung seiner politischen Aufgaben zu helfen, sollte man fragen, ob die betroffenen Personen mögliche weitere Verwendungen angemessen erwarten würden[124]. Dies trifft sowohl auf den europäischen als auch auf den brasilianischen Kontext zu. In Brasilien sollten politische Kampagnen zudem weder Spenden von Kontaktlisten annehmen noch letztere kaufen, da das Wahlgesetz solche Praktiken ausdrücklich verbietet.

Der zuvor beschriebene Fall, in dem politische Nachrichten während der Wahlen in Brasilien über WhatsApp verbreitet wurden, ist ein gutes Beispiel für eine Praxis, die gegen diese Pflichten verstoßen würde. Damals wurden spezialisierte Unternehmen angestellt, um solche Nachrichten im großen Stil unter bestimmten Umständen an Kontakte auf Nummernlisten zu senden[125]. Man könnte argumentieren, dass die Personen auf diesen Listen keine angemessene Erwartung bezüglich des Empfangs von

Wahlpropaganda oder politischen Nachrichten über WhatsApp hatten. Die Aktivisten hätten Schwierigkeiten, Nachweise bezüglich einer spezifischen Einwilligung oder sonstigen Rechtsgrundlage für solche Aktivitäten vorzulegen.

Ein ähnliches Problem ist die Sammlung und Behandlung öffentlich verfügbarer Daten. Eine solche Datensammlung im großen Stil kann für Profiling-Aktivitäten[126] verwendet werden, wobei das Kreuzen eindeutiger Datenquellen und -punkte es gestattet, Schlüsse zu ziehen und ein detailliertes Profil einer Person zu erstellen. Alle auf diese Weise gesammelten Daten und die gezogenen Schlussfolgerungen unterliegen Datenschutzbestimmungen, da sie sich „auf eine identifizierte oder identifizierbare natürliche Person beziehen" (Art. 4 DSGVO) oder es sich um „Informationen in Bezug auf eine identifizierte oder identifizierbare natürliche Person" handelt (Art. 5 LGPD). Hierbei handelte es sich um die Grundlage des oben erwähnten Falls von Cambridge Analytica, bei dem das Unternehmen unter Verwendung von Datenanalysetechniken in der Lage war, Wähler in eindeutige Gruppen zu unterteilen – selbst solche Wähler, die keine ausdrückliche Einwilligung zur Sammlung ihrer Daten gegeben hatten[127]. Auf der Grundlage einer Einstufung, welche Informationen als „öffentlich verfügbar" wahrgenommen werden könnten, d. h. mithilfe von Profilen von Nutzern und ihren Freunden gesammelte Informationen, verzerrte CA quasi den demokratischen Prozess mittels Psychometrie und Big Data.

Erwähnungen „öffentlich verfügbarer" Daten im brasilianischen LGPD treten in drei Fällen auf: den Paragraphen 3, 4 und 7 von Artikel 7. Der erste Paragraph beschreibt die Verarbeitung „öffentlich verfügbarer personenbezogener Daten", indem er angibt, dass der ursprüngliche Zweck und das öffentliche Interesse, das ihrer Veröffentlichung zugrunde lag, sowie guter Glaube zu beachten sind. Der zweite Fall behandelt „von der Person offenbar veröffentlichte Daten", wodurch in diesem Fall eine Ausnahme zur Einwilligung geschaffen wurde. Der dritte Fall, bei dem es sich um eine späte Änderung des Gesetzes handelt, gestattet die Verarbeitung solcher Daten zu neuen Zwecken. Es besteht ein offensichtlicher Konflikt zwischen den Paragraphen 3 und 7, da ersterer die weitergehende Verarbeitung auf den ursprünglichen Kontext beschränkt, während letzterer eine Verarbeitung zu neuen Zwecken gestattet. Dies ist wahrscheinlich ein Problem, mit dem sich die neue Nationale Datenschutzbehörde (Autoridade Nacional de Proteção de Dados, ANPD) beschäftigen muss.

In diesem Punkt ist die DSGVO erheblich präziser als das LGPD. Artikel 14 der DSGVO verweist auf die „Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden", sondern zum Beispiel aus öffentlich verfügbaren Daten stammen. Der Artikel enthält eine Reihe von Festlegungen der Pflichten des Verantwortlichen bezüglich der Verarbeitung von Daten. Diese Informationspflichten umfassen unter anderem die beabsichtigten Verwendungszwecke der Daten, den Verarbeitungszeitraum, Namen und Kontaktdaten des Verantwortlichen, die Kategorien der gesammelten Daten, die Zwecke der Verarbeitung, die Empfänger und Quellen der Daten, die Rechte der betroffenen Person auf Berichtigung und das Beschwerderecht bei einer Aufsichtsbehörde.

Auf der Grundlage des LGPD bzw. der DSGVO müssen die Möglichkeiten einer Verarbeitung basierend auf „öffentlich verfügbaren personenbezogenen Daten" von den Behörden sorgfältig erwogen werden. Dabei sind die Geschehnisse in spezifischen

Situationen, wie beispielsweise der Massenversand von WhatsApp-Nachrichten in Brasilien oder der CA-Fall, zu berücksichtigen. Obwohl Ausnahmen bei der Einwilligung in Bezug auf öffentlich verfügbare personenbezogene Daten bestehen können, kann die Verarbeitung in vielen Fällen als rechtswidrig betrachtet werden, indem keine grundlegenden Compliance-Schritte durchgeführt wurden, wie beispielsweise die Benachrichtigung der betroffenen Person über die Verarbeitung und die Gewährleistung grundlegender Datenschutzprinzipien und -rechte.

Aufgrund der vollen Anwendbarkeit der Bestimmungen zum Schutz personenbezogener Daten ist es wichtig, dass sowohl die Parteien als auch die Kandidaten alle notwendigen Vorsichtsmaßnahmen treffen, um die Beachtung aller Grundsätze und Rechte zu gewährleisten. Dies beginnt gewöhnlich mit einer ausführlichen Darstellung der Datenflüsse in der Kampagnenstruktur: eine Aufgabe, die eng mit dem Verantwortungsbereich des Datenschutzbeauftragten zusammenhängt. Das trifft insbesondere auf Fälle zu, in denen sensible Daten verarbeitet werden – eine bei politischen Kampagnen gängige Situation. Da die von Parteien und Kandidaten verwendeten Daten in der Regel die politischen Einstellungen und Meinungen der betroffenen Personen beinhalten, erweist sich die Rolle des Datenschutzbeauftragten als noch wichtiger. Unterschiedliche Kampagnen haben unterschiedliche Anforderungen und Formate, besonders in breiten und diversen Zusammenhängen wie den politischen Szenarien in Brasilien und Europa. Ein erster Schritt besteht in der detaillierten Erfassung aller Punkte, an denen Daten auf beliebige Weise gesammelt, kommuniziert, gespeichert oder verarbeitet werden. Weitere Details klären darüber auf, wer Zugang zu welcher Art von Daten hat, auf welcher Rechtsgrundlage die Verarbeitung regulärer oder sensibler Daten erfolgt, von welcher Dauer die Verarbeitungsaktivitäten sind und welchem Zweck sie dienen.

Ein wesentlicher Unterschied zwischen den beiden Gesetzen besteht in ihrer Behandlung der Datenschutz-Folgenabschätzung (DSFA). DSFA werden in Artikel 35 der DSGVO und in den Artikeln 10, 32 und 38 (unter anderen) des LGPD behandelt. Erstere gibt eine Verpflichtung vor, eine DSFA durchzuführen, wann immer ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ besteht. Dabei wird davon ausgegangen, dass zumindest eine vorläufige Risikoabschätzung für alle Verarbeitungsaktivitäten durchgeführt werden sollte, um ein hohes Risiko und folglich die Verpflichtung zur Durchführung einer DSFA festzustellen[128]. Der umfassende Artikel legt nicht nur die Pflichten des Verantwortlichen fest, sondern auch die Beteiligung des Datenschutzbeauftragten und die Pflichten der Datenschutzbehörde, die für die Festlegung spezifischer Fälle verantwortlich ist, in denen eine DSFA zwingend vorgeschrieben ist.

Das brasilianische Gesetz behandelt dagegen das Thema der Folgenabschätzungen kürzer und erwähnt lediglich, dass die brasilianische Datenschutzbehörde (ANPD) eben diese von Verantwortlichen verlangen und ihren erforderlichen Inhalt festlegen kann. In Bezug auf diesen Punkt besagt Artikel 38 des LGPD:

> *Art. 38. Die nationale Behörde kann den Verantwortlichen anweisen, einen Folgenabschätzungsbericht zum Schutz personenbezogener Daten, einschließlich sensibler Daten, vorzulegen, bezüglich seiner Datenverarbeitungsaktivitäten in Übereinstimmung mit der spezifischen Bestimmung unter Beachtung industrieller Geheimhaltungsbestimmungen.*

Alleinstehender Paragraph. Der im Kopfteil dieses Artikels erwähnte Bericht muss mindestens eine Beschreibung der Arten gesammelter Daten, der angewandten Datensammlungs- und Informationssicherheitsmethoden und der Analyse des Verantwortlichen bezüglich der angewandten Maßnahmen, Sicherheitsvorkehrungen und Minderungsmechanismen enthalten.

Dagegen erklärt Artikel 35 (7) der DSGVO:

Die Folgenabschätzung enthält zumindest Folgendes:

a) *eine systematische Beschrei bung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;*

b) *eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;*

c) *eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und*

d) *die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.*

Wie bei vielen anderen Themen entschied sich das brasilianische Gesetz, die Einzelheiten der DSFA-Verordnung der ANPD zu überlassen. Dabei wird es zum Beispiel um die Entscheidung gehen, welche Repräsentanten verpflichtet sein werden, DSFA durchzuführen und unter welchen Umständen. Das wird durch mindestens zwei Gesetzespunkte bestärkt: Artikel 55-J, XIII und XVIII. Ersterer erklärt, dass die nationale Behörde über die Kompetenz verfügt, Bestimmungen im Detail zu klären und Verfahren für die DSFAs in Fällen festzulegen, in denen ein hohes Risiko für die gesetzlich garantierten Grundsätze und Rechte besteht. Letzterer besagt, dass es in den Zuständigkeitsbereich der Behörde fällt, besondere und vereinfachte Verfahren für kleine und neu gegründete Unternehmen vorzugeben.

Ein weiterer wichtiger Unterschied zwischen den europäischen und brasilianischen Bestimmungen bezieht sich auf die automatisierte Verarbeitung von Daten. In der DSGVO hat die betroffene Person das Recht, in automatisierte Entscheidungsfindungsprozesse, einschließlich Profiling, nicht einbezogen zu werden. Dieses Recht unterliegt den folgenden drei Ausnahmen:

Art 22 Abs 2: Absatz 1 gilt nicht, wenn die Entscheidung:

a) *für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,*

b) *aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder*

c) *mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.*

Falls jedoch eine der Ausnahmen anwendbar ist, garantiert die europäische Verordnung der betroffenen Person das „Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung" (Art. 22 (3)). Wenn das brasilianische LGPD in seiner ursprünglichen Form verabschiedet worden wäre, hätte es eine ähnliche Bestimmung enthalten. Das Gesetz wurde jedoch mittels eines Erlasses des Präsidenten modifiziert, sodass Artikel 20 in seiner gegenwärtigen Form nur das Recht auf eine „Prüfung" automatisierter Entscheidungen garantiert. Demzufolge braucht diese Prüfung nicht durch einen menschlichen Bearbeiter zu erfolgen.

Wichtig ist ein abschließender Hinweis auf eine spezifische Erwägung bezüglich der Verarbeitung personenbezogener Daten zu politischen Einstellungen durch Parteien bei Wahlkampfaktivitäten. Diese Verarbeitung, die wie oben erklärt unter den von den Gesetzen festgelegten Schutz und die festgelegten Einschränkungen fallen würde, wird von Erwägungsgrund 56 der DSGVO interpretiert[129], der eine lockerere Verarbeitung auf der Grundlage öffentlichen Interesses gestattet. Nichtsdestotrotz sollte diese Möglichkeit sorgfältig beachtet werden, um sicherzustellen, dass die Verarbeitung politischer Einstellungen durch politische Parteien im Sinn des Gesetzes erfolgt.

Politische Einstellungen sind von Artikel 9 der DSGVO als besondere Kategorie personenbezogener Daten eingestuft, die einen stärkeren Schutz verdienen. Ihre Verarbeitung ist ausdrücklich untersagt (Art. 9 (1)) und nur in außerordentlichen Fällen zulässig (Art. 9 (2)). Das brasilianische Gesetz hat kein Äquivalent zu Erwägungsgründen und keinen ausdrücklichen Verweis auf die Verarbeitung politischer Einstellungen, mit Ausnahme ihrer Kategorisierung als sensible personenbezogene Daten, dem Äquivalent zu Daten einer besonderen Kategorie in der DSGVO. Dieser offensichtliche Widerspruch wird im nächsten Abschnitt untersucht, in dem wir die Implementierung diskutieren, um einen wirksamen demokratischen Prozess bei Wahlen in Bezug auf den Schutz personenbezogener Daten zu gewährleisten.

Zuvor ist es nichtsdestotrotz wichtig, hervorzuheben, dass es beim Vergleich der Qualität der europäischen Verordnung mit dem brasilianischen Gesetz keine eindeutige Antwort gibt. Das brasilianische Gesetz ist im Allgemeinen flexibler als die DSGVO und diese Flexibilität zeigt sich, wenn man die Anzahl von Rechtsgrundlagen für Verarbeitungsaktivitäten, das Meldesystem nach einer Verletzung des Schutzes, die Höhe der Verwaltungsstrafgelder usw. betrachtet. Das könnte auf der einen Seite als positiver Faktor angesehen werden, da es der Branche mehr Raum zur Anpassung an die Bestimmungen gibt. Auf der anderen Seite könnte dieser Grad von Flexibilität jedoch zu einer Unwirksamkeit des Gesetzes führen, da die für die Verantwortlichen festgelegten Parameter zu subjektiv und die Bestimmungen nicht starr genug sind, um eindeutige Grenzen festzulegen. Zusätzlich legt sie den Datenschutzbehörden eine noch größere Verantwortung auf. In dieser Angelegenheit ist die nationale Behörde in Brasilien im Gegensatz zu den Datenschutzbehörden in der EU weder unabhängig noch autonom, da sie der Präsidentschaft der Republik untersteht. Außerdem steht die Auslegung ihrer Struktur und Körperschaft noch aus. Wenn man die Bedeutung der Datenschutzbehörde bei der Gewährleistung der Wirksamkeit des Gesetzes und der Bereitstellung spezifischer Bestimmungen zu seiner Ergänzung berücksichtigt, führen alle diese Elemente zu Ungewissheit bezüglich der Erfüllung und Wirksamkeit des Datenschutzszenarios in Brasilien.

Trotz ihrer Ähnlichkeit mit dem LGDP ist die DSGVO bewusst geradliniger und objektiver bezüglich der Regulierung des Datenschutzes. Dies ist wiederum Grund zu Lob und Kritik. Einerseits schafft ihre Starrheit ein Klima der Rechtssicherheit, das durch hohe Parameter des Schutzes grundlegender Rechte geprägt ist. Da diese einen kontrollierteren Raum für Ermessensentscheidungen der Aufsichtsbehörden bieten, ist es einfacher, eine harmonisierte Anwendung des Gesetzes innerhalb der Europäischen Union zu erzielen. Andererseits könnte die Verordnung bei ihrem Unterfangen, solche Parameter festzulegen, undurchführbare Bestimmungen enthalten, wie beispielsweise die in Art. 33[130] vorgegebene Bestimmung, die einen Teil ihrer Glaubwürdigkeit rauben könnte, indem sie den Verantwortlichen eine übermäßige Belastung auflegt und unnötige Kosten verursacht.

Deshalb sollte angesichts der Ähnlichkeiten und Unterschiede im Ansatz beider Gesetzeswerke, die positive und negative Kommentare hervorrufen könnten, die Frage nicht die sein, welches Gesetz bessere Bestimmungen umfasst, da dies subjektiv sein kann, sondern wie Compliance und Verantwortlichkeit in beiden Szenarios garantiert werden können. Daran anknüpfend ist das nächste Kapitel einer praktischen Analyse und Aufführung der zu diesem Zweck einzuleitenden Schritte gewidmet.

---

114 BIONI Bruno (2019): „Proteção de dados pessoais: A função e os limites do consentimento“, Forense, S. 319.

115 ICO (2019): „Guidance on political campaigning: Draft framework code for consultation“ (Leitfaden für politische Kampagnen: Entwurf für einen Rahmenkodex zur Anhörung), https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf. Zugang Dezember 2019.

116 Europäische Kommission (2018): „Commission guidance on the application of Union data protection law in the electoral context: A contribution from the European Commission to the Leaders‘ meeting in Salzburg“ (Leitfaden der Kommission zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen. Ein Beitrag der Europäischen Kommission zum Treffen der Führungsspitzen in Salzburg), https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf, Zugang Januar 2019.

117 HEWARD-MILLS D. (2019): „The DPO must be independent, but how?“ (Der Datenschutzbeauftragte muss unabhängig sein, aber wie?), https://iapp.org/news/a/the-dpo-must-be-independent-but-how/, Zugang November 2019.

118 Weitere praktische Schritte zur Rolle des Datenschutzbeauftragten sind im folgenden Abschnitt beschrieben.

119 CNIL (2019): „Devenir délégué à la protection des données“, https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees, Zugang November 2019.

120 EDSA (2019): „Guidelines on Data Protection Impact Assessment (DPIA)“ (Leitlinien zur Datenschutz-Folgenabschätzung (DSFA), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, Zugang November 2019.

121 ICO (2019): „How do we apply legitimate interests in practice?“ (Wie werden wir berechtigten Interessen in der Praxis gerecht?), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/. Siehe auch https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/, Zugang November 2019.

122 Britto Cruz et al. (2019): „Internet e eleições no Brasil: Diagnósticos e recomendações“, InternetLab, S. 32–33.

123 Art. 5 (1) b) der DSGVO.

124 ICO (2019): „Guidance on political campaigning: Draft framework code for consultation“ (Leitfaden für politische Kampagnen: Entwurf für einen Rahmenkodex zur Anhörung), https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf. Zugang Dezember 2019.

125 Siehe „WhatsApp Admits Illegal Mass Messaging Used in Brazil's 2018 Elections" (WhatsApp gibt zu, dass ein rechtswidriger Massenversand von Nachrichten bei den Wahlen in Brasilien 2018 auf der Plattform stattgefunden hat), The Rio Times, https://riotimesonline.com/brazil-news/brazil/whatsapp-admits-to-illegal-mass, Zugang November 2019.

126 DSGVO-Erwägungsgrund 71 definiert Profiling als „jegliche Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für dieselbe entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt."

127 REVELL T. (2018): „How Facebook let a friend pass my data to Cambridge Analytica" (Wie Facebook es zuließ, dass ein Freund meine Daten an Cambridge Analytica weitergab), https://www.newscientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica/, Zugang November 2019.

128 ICO (2019): „Guidance on political campaigning: Draft framework code for consultation" (Leitfaden für politische Kampagnen: Entwurf für einen Rahmenkodex zur Anhörung), https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf, Zugang Dezember 2019.

129 Erwägungsgrund 56: „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."

130 Art. 33: „Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen."

3. Steigerung der Wirksamkeit und Schließen der Lücken

Die Bedeutung der Pflege der Datenhygiene und Beachtung der Bestimmungen bei politischen Kampagnen hat viele Aspekte. Vom Blickpunkt der demokratischen Institutionen betrachtet, ist sie, wie zuvor erörtert, eine Voraussetzung für gesunde Wahlprozesse. In einem Zeitalter der allgegenwärtigen Verbindung und des sofortigen wahllosen Austauschs von Daten können Ideen und Überzeugungen von Online-Filtern geformt werden und wird der öffentliche Raum zwangsläufig mit neuen Informations- und Kommunikationstechnologien überschwemmt. Deren fehlerhafte Funktion, die auf echte Fehler oder ein strukturell mangelhaftes System zurückzuführen sein kann, könnte die Fähigkeit von Personen, einen Konsens und Mittelweg auf eine friedliche und ausgewogene Weise zu finden, kompromittieren, wie kürzlich durch die Einmischung in Wahlprozesse in unterschiedlichen Teilen der Welt offensichtlich wurde.[131]

Vom Standpunkt der Datenverantwortlichen und, in diesem spezifischen Fall, der politischen Parteien und Politiker gesehen, stellt die präzise Beachtung der Regeln nicht nur eine gesetzliche Verpflichtung dar, sondern sollte sich als grundlegende Anforderung an die Darstellung der eigenen Person bzw. Partei gegenüber der Gesellschaft als ethische Person bzw. Partei erweisen, die Aufmerksamkeit, Vertrauen und damit die Stimme der Wähler verdient. Das trifft noch stärker zu, wenn man die jüngsten Fälle berücksichtigt, bei denen Datenverarbeitungstechniken auf politische Kampagnen angewandt wurden, zum Beispiel im Fall von CA und des Einsatzes von WhatsApp bei den Wahlen in Brasilien, und die das Problem in den Vordergrund und die Aufmerksamkeit der Wählerschaft auf dasselbe gelenkt haben. Die Nichtachtung der Privatsphäre von Menschen sowie ihres Rechts auf Datenschutz und Selbstbestimmung im Hinblick auf Informationen sollte sich für das Marketingimage und das öffentliche Image zunehmend als unentschuldbar herausstellen, insbesondere da sich eine zunehmende Anzahl von Menschen dieser Probleme bewusst wird.

Kandidaten und politische Parteien sollten in Bezug auf die Verarbeitung von Daten für ihre Kampagnen bei Wahlprozessen Sorgfalt walten lassen und nach den besten aktuellen Praktiken suchen – nicht nur in ihrem eigenen Interesse, sondern auch im Interesse von betroffenen Personen und der Gesellschaft in ihrer Gesamtheit.[132] Aufgrund der Natur dieser Prozesse wird es sich bei vielen der von ihnen behandelten personenbezogenen Daten, die entweder von ihnen direkt gesammelt oder mittels Analyse- und Profiling-Techniken erschlossen werden, um sensible Daten handeln – eine besondere Kategorie von Daten, die besonderen Schutz verdienen. Es ist nicht nur wichtig, die Beachtung von Rechten und Grundsätzen im Interesse der betroffenen Personen unter Beachtung des Rechtsstaatsprinzips zu garantieren, sondern es ist auch wesentlich, insbesondere in Bezug auf politische Kampagnen, bei denen das öffentliche Image einen zentralen Bestandteil darstellt, demonstrieren zu können, dass Privatsphäre und Datenschutz auf eine ethisch und rechtlich absolut einwandfreie Weise beachtet werden.

Die Zunahme der Datenverstöße erreichte 2019 ihren Höhepunkt mit 5.183 Datenverstößen und 7,9 Milliarden offengelegten Datensätzen in den ersten neun Monaten des Jahres. Das bedeutet eine 33,3-prozentige Steigerung im Vergleich zu 2018[133]. Falls dies eine Andeutung auf zukünftige Trends darstellt, sollte die Datensicherheit eines der Hauptbedenken bei allen Aktivitäten zur Verarbeitung personenbezogener Daten sein. Strafgelder für Datenverstöße können Dutzende Millionen US-Dollar

ausmachen sowie die Aussetzung oder den Ausschluss von Vermögenswerten einschließen. Zur Verhinderung solcher Verluste muss der Verantwortliche die neuesten Sicherheitsstandards anwenden. Wichtige Schritte umfassen zum Beispiel die ordnungsgemäße Schulung aller an der Verarbeitung beteiligten Personen sowie die Verringerung der Anzahl von Personen mit Zugang zu personenbezogenen Daten. Eine aus mehreren Faktoren bestehende Zugangsberechtigung ist ebenfalls eine grundlegende Anforderung, da sie in der Lage ist, die Verwundbarkeit des Systems drastisch zu reduzieren[134]. Weitere Schritte in Richtung auf eine gesteigerte Sicherheit sind die Verringerung der Anzahl von Geräten, auf denen die Daten gespeichert sind, und die Reduzierung der Datenübertragung zwischen Geräten. Verantwortliche können und sollten diese Schritte einleiten, vorzugsweise durch einen Chief Information Security Officer (CISO), bei dem es sich nicht um dieselbe Person wie den Datenschutzbeauftragten handeln sollte[135].

Letzterer spielt eine führende Rolle bei der Gewährleistung, dass dieses gesamte System funktioniert. Er ist dafür verantwortlich, die Beachtung der Datenschutzgesetzgebung zu verfolgen. Das bedeutet, Informationen über die Stellen zu sammeln, an denen Daten verarbeitet werden, und sicherzustellen, dass dabei alle gesetzlichen Anforderungen erfüllt werden. Es bedeutet weiterhin, den Verantwortlichen auf der Grundlage der eigenen Beobachtungen in Bezug auf die Verbesserung der Compliance zu beraten, die Mitarbeiter im Hinblick auf Sicherheitsmaßnahmen und gute Praktiken zu schulen sowie als Verbindungsglied zwischen der Organisation, der Behörde und den betroffenen Personen zu fungieren. Außerdem sollte der Datenschutzbeauftragte unabhängig sein, was schwierig sein kann, wenn er intern angestellt ist.

Beste Praxis besagt, dass der Datenschutzbeauftragte nicht dem Verantwortlichen unterstellt, sondern stattdessen direkt der höchsten Ebene der Entscheidungsfindung in der Leitungsstruktur gegenüber verantwortlich sein sollte. Zur Garantie seiner Unabhängigkeit sollte er weiterhin über die notwendigen Ressourcen (Mitarbeiter, Geräte und Finanzmittel) verfügen, um seine Pflichten ausüben zu können[136]. Abschließend sollte er nicht in eine Position gebracht werden, in der ein Interessenkonflikt besteht, zum Beispiel indem er in IT- oder Personalabteilungen an den Datenverarbeitungsaktivitäten arbeitet oder gearbeitet hat, was hieße, dass er zur Selbstaufsicht gezwungen wäre[137]. Diese Probleme können durch die Anstellung eines externen Datenschutzbeauftragten vermieden werden. Selbst dann ist es jedoch wichtig, dass der Datenschutzbeauftragte den notwendigen Zugang und die notwendigen Ressourcen sowie die erforderlichen technischen Kenntnisse hat.

Alle diese Punkte sind Bausteine einer Datenverarbeitungs- und -sicherheitsstrategie, die mit einer einfachen Bewertung des Datenflusses durch die Betriebsabläufe und der aktuellen diesbezüglichen Risiken beginnt. Zur Gewährleistung der Beachtung der DSGVO und folglich des LGPD (da beide sehr ähnliche Datenschutzgrade aufweisen), sollten sich politische Parteien und Kandidaten mit den aktuellen besten Managementpraktiken und -werkzeugen in Bezug auf Datenflüsse auskennen.

Ein Verantwortlicher sollte in der Lage sein, die Flüsse personenbezogener Daten in seiner Kampagne aus der Vogelperspektive zu betrachten, vorzugsweise mithilfe einer Compliance-Tafel, die von allen beteiligten Verantwortlichen und Auftragsverarbeitern

zu verwenden ist. Dieses zentralisierte Datenverwaltungssystem sollte außerdem die Kontaktangaben aufweisen und den Datenschutzbeauftragten in der Kampagnenstruktur sowie eine vollständige Zuordnung und Steuerung der verarbeiteten und übertragenen Daten und ihren zugehörigen rechtmäßigen Zweck zeigen.

Weiterhin sind die Mitteilungspflichten des Verantwortlichen nach DSGVO und LGPD zu bedenken, einschließlich der (i) Identität und Kontaktangaben des Verantwortlichen und Datenschutzbeauftragten; (ii) der Identifizierung oder Kategorisierung der Empfänger der Daten; (iii) der Zielsetzungen der Verarbeitung sowie ihrer Rechtsgrundlage; (iv) der Dauer der Verarbeitung (v) sowie der Rechte der betroffenen Personen – insbesondere gegebenenfalls der Berichtigung und des Widerrufs der Einwilligung usw.[138] Zusätzlich sollten Verantwortliche in der Lage sein, die Anträge betroffener Personen auf Zugang zu ihren Daten zeitgerecht zu bearbeiten. Diese Anträge stellen Fälle dar, in denen betroffene Personen Zugang zu ihren Daten, die Berichtigung derselben und manchmal auch deren Löschung verlangen könnten.

Der Verantwortliche sollte außerdem Maßnahmen zur Pflege von „Brotkrumen zur digitalen Einwilligung“ einleiten, d. h. ein Verzeichnis der Zeitachse der Einwilligung oder bestimmter Einwilligungen für die Verarbeitung, die eine betroffene Person gegeben bzw. widerrufen hat. Abschließend sollten Genehmigung und Zugangskontrolle granular sein, was bedeutet, dass nur die unverzichtbaren Bearbeiter innerhalb der Kampagnenstruktur Zugang zu den entsprechenden Datengruppen haben sollten. Alle diese Aspekte der Beziehung zwischen dem Auftragsverarbeiter und der betroffenen Person sollten durch einfach zu verwendende Schnittstellen wie beispielsweise Apps und Formulare umgesetzt werden, sodass die betroffene Person ihre Rechte umfassend verstehen kann und der Verantwortliche in der Lage ist, Compliance nachzuweisen[139].

All dies könnte sich nach erheblicher Arbeit anhören, und diese Einschätzung ist richtig. Glücklicherweise gibt es abgesehen von fähigen Fachleuten, die Unternehmen beim Aufbau von Compliance unterstützen können, zurzeit Werkzeuge zur Selbstbewertung bezüglich der DSGVO-Compliance, die sich leicht auf die Anforderungen des LGPD anpassen lassen sollten. Das britische Information Commissioner’s Office (ICO, die britische Datenschutzbehörde) bietet zum Beispiel zahlreiche spezifische Ressourcen einschließlich Compliance-Checklisten für Verantwortliche, Auftragsverarbeiter, Informationssicherheits-, Direktmarketing-, kleine und mittelständische Unternehmen usw. an[140]. Ein weiteres unbezahlbares Werkzeug ist der Privacy Notice Code des ICO, der im Einzelnen behandelt, wie die auf Webseiten und in Apps anzutreffende Datenschutzerklärung (Privacy Notice), eines der am häufigsten für die Kommunikation zwischen dem Verantwortlichen und der betroffenen Person verwendeten Werkzeuge, zur Gewährleistung von Compliance strukturiert sein sollte[141].

Ein kurzer Überblick über diese Werkzeuge zeigt, dass der wesentliche Punkt eines wirksamen Compliance-Programms für die Verarbeitung personenbezogener Daten darin besteht, die an einem Betriebsablauf beteiligten Prozesse zu kennen: das Was, Wo, Wann und Wie der Sammlung und Verarbeitung personenbezogener Daten. Dies sollte bei politischen Kampagnen nicht anders sein: Ein praktischer Ansatz ist notwendig, an dem Marketingfachleute, Designer, Rechtsexperten, Programmierer und ehrenamtliche Helfer beteiligt sind und daran arbeiten, wie betroffene Perso-

nen am besten gegen mögliche Verletzungen ihrer Rechte auf Privatsphäre und Datenschutz geschützt werden können. Diese Studie hat durch das Hervorheben spezifischer rechtlicher Leitfäden und konkreter Situationen gezeigt, dass Datenschutzbestimmungen vollständig auf politische Kampagnen anwendbar sind und die Fähigkeit haben, die Verringerung der instrumentalen Verwendung personenbezogener Daten zu unterstützen, während sie gleichzeitig die Auswirkungen des Einsatzes von Falschinformation und computergestützter Propaganda zum Zweck der politischen Manipulation vermeiden.

Pragmatischer betrachtet sollten politische Kampagnen zumindest die folgenden Empfehlungen auf der Basis der Grundsätze und wichtigsten Leitfäden allgemeiner Datenschutzbestimmungen beachten, wobei stets der Blickwinkel von Gesetzmäßigkeit, Fairness, Transparenz und Verantwortlichkeit zu wahren ist:[142]

Stellen Sie die relevanten Akteure fest: Welche Personen sind Verantwortliche und Auftragsverarbeiter und wer ist der Datenschutzbeauftragte (falls vorhanden)?

- Art. 5 LGPD; Art. 4 DSGVO.
- **Beispiel:** Der Kandidat hat in einer bestimmten politischen Kampagne ein Marketingunternehmen zum Management seines öffentlichen Images angestellt. Alle Entscheidungen bezüglich der Sammlung und Verarbeitung von Daten werden vom Marketingdirektor getroffen. Der Direktor kann als Datenverantwortlicher charakterisiert werden, da er über die Zwecke der Verarbeitung entscheiden kann. Der Kandidat wäre ebenfalls ein Verantwortlicher, da er der Entscheidungsträger in letzter Instanz ist.

Stellen Sie fest, wie die Daten gesammelt und verarbeitet werden, d. h. welchen Lebenszyklus die Daten im Organisationsfluss der Kampagne haben.

- **Maßnahme:** Stellen Sie alle Datensammlungs- und -verarbeitungspunkte fest. Stellen Sie fest, wie viel Zeit vergeht, bis ein einzelner Datenpunkt eliminiert wird. Identifizieren Sie die zur Datenspeicherung verwendeten Geräte bzw. Dienste. Identifizieren Sie, welche Drittparteien Zugang zu den Daten haben.

Stellen Sie fest, welche Daten auf welcher Rechtsgrundlage gesammelt und verarbeitet werden. Legen Sie sensible Daten[143] fest und achten Sie besonders auf deren Rechtsgrundlagen.

- Art. 5, I, II; Art. 7, Art. 11 LGPD; Art. 4, Art. 9 DSGVO.
- **Maßnahme:** Falls es Datenpunkte gibt, für die keine Rechtsgrundlage bestimmt werden kann, sollten diese eliminiert werden, da sie eine Bürde darstellen. Hierbei handelt es sich um grundlegende „Datenhygiene“.

Denken Sie daran, dass Datenminimierung[144] eine gute allgemeine Regel (und ein Grundsatz) ist. Falls keine Notwendigkeit besteht, einen bestimmten Aspekt personenbezogener Daten zu sammeln, sehen Sie von seiner Erfassung ab. Wenn der Zweck der Sammlung erfüllt worden ist, löschen Sie die Daten.

- Art. 15, Art. 16 LGDP; Art. 5, Art. 25 DSGVO.
- **Maßnahme:** Falls keine Notwendigkeit besteht, einen bestimmten Aspekt personenbezogener Daten zu sammeln, sehen Sie von seiner Sammlung ab. Wenn der Zweck der Sammlung erfüllt worden ist, löschen Sie die Daten.

- **Beispiel:** Der Kandidat sammelt Daten von betroffenen Personen, um ihnen eine digitale Kopie des Regierungsplans zu schicken. Falls die Einwilligung strikt zur Verbreitung des besagten Materials gegeben wird: 1. braucht der Kandidat keine weiteren Daten als den Namen und die E-Mail-Adresse der betroffenen Person zu sammeln und sollte die Sammlung auf diese Angaben beschränken; 2. sollte der Kandidat die Daten nach dem Versand des Materials löschen, sofern keine angemessene anderweitige Erwartung auf sonstigen Rechtsgrundlagen bzw. mittels einer neuen spezifischen Einwilligung besteht.

Lassen Sie die gesamte Dokumentation zu Rechtsgrundlagen archivieren.

- **Beispiel:** Der Kandidat hat Daten gesammelt und verarbeitet, um eine Aufzeichnung einzelner Kampagnenspenden nach dem brasilianischen Wahlgesetz zu führen. Der Kandidat sollte eine Aufzeichnung solcher Betriebsabläufe mit Verweis auf die relevanten Gesetze und Rechtsgrundlagen führen, um auf eine mögliche Prüfung vorbereitet zu sein.

Erneuern Sie die bestehende Einwilligung in Übereinstimmung mit den aktuellsten Datenschutzbestimmungen.

- **Maßnahme:** Falls ein neuer Text für die Datenschutzerklärung vorliegt oder Daten betroffener Personen vor Einführung der DSGVO bzw. des LGPD gesammelt wurden, holen Sie eine neue Einwilligung ein oder benachrichtigen Sie die betroffenen Personen über die neue Datenschutzerklärung und Rechtsgrundlage.
- **Beispiel:** Der Kandidat hat bereits eine Kontaktliste im Rahmen von öffentlichen Veranstaltungen und mithilfe eines Webseitenabonnementformulars vor Einführung der DSGVO bzw. des LGPD gesammelt. Er sollte allen Empfängern eine Bitte um Bestätigung ihrer Einwilligung zum Erhalt von politischer Kommunikation schicken. Die Mitteilung könnte zum Beispiel wie folgt lauten: „Wir aktualisieren unsere Datenschutzpraktiken im Einklang mit den jüngsten Datenschutzbestimmungen. Falls Sie unseren Inhalt weiterhin erhalten möchten, klicken Sie bitte auf die folgende Schaltfläche/erneuern Sie Ihr Abonnement bitte auf/[Fügen Sie eine Form der Bestätigung hinzu].“

Geben Sie Informationen an: Denken Sie an die verschiedenen Informationspflichten, die ein Verantwortlicher gegenüber der betroffenen Person hat. Die betroffene Person sollte in der Lage sein festzustellen, welche personenbezogenen Daten gesammelt werden, zu welchem Zweck, über welchen Zeitraum, wer Zugang zu ihnen hat, welcher Prozess zur Beantragung von Zugang zu den Daten verwendet wird, sowie zu ihrer Berichtigung, zur Beantragung ihrer Löschung oder ihrer Übertragung an einen anderen Verantwortlichen usw.

- Art. 9, Art. 18 LGPD; Art. 13, Art. 14 DSGVO.
- **Maßnahme:** Falls die Einwilligung die Rechtsgrundlage darstellt, sollten alle relevanten Informationen im Rahmen der Einwilligungsabgabe bereitgestellt werden. Bei sonstigen Rechtsgrundlagen sollte die betroffene Person einfachen Zugang zu solchen Informationen mittels Antrag oder öffentlichem Zugang (z. B. auf einer Webseite) haben. Falls Daten durch sonstige Mittel, d. h. nicht direkt von der betroffenen Person, gesammelt werden (z. B. öffentlich verfügbare Daten), hat der Verantwortliche eine Reihe von Informationspflichten (siehe relevante DSGVO-Artikel).

Führen Sie eine Aufzeichnung der Verarbeitungsaktivitäten, insbesondere falls berechtigtes Interesse die Rechtsgrundlage darstellt (Art. 30 DSGVO; Art. 37 LGDP). Halten Sie gegebenenfalls eine DSFA[145] bzw. ein LIA[146] bereit.

- Art. 37 LGPD; Art. 30 DSGVO.
- **Maßnahme:** Führen Sie ein Verzeichnis mit folgendem Mindestinhalt: 1. Zweck der Verarbeitung; 2. Beschreibung der Datenkategorien und betroffenen Personen; 3. externe Datenflüsse; 4. angewendete Sicherheitsmaßnahmen; 5. Namen und Kontaktdaten des Verantwortlichen; 6. vorgesehene Fristen für die Löschung jeder Datenkategorie[147].
- **Beispiel:** Eine kleine Kampagne für eine lokale Wahl hat einen Organisationsfluss angewendet, um ein Verzeichnis von Datenverarbeitungsaktivitäten zu führen. Alle über betroffene Personen gesammelten Informationen werden in einer Tabelle mit Kategorien entsprechend der Datenquelle aufgezeichnet. Zum Beispiel werden Daten aus Abonnementformularen entsprechend der Vereinbarung zum Zeitpunkt der Einwilligung als einwilligungsbasierte Daten kategorisiert, enthalten den Namen und die E-Mail-Adresse, werden an den Newsletter-Dienst eines Dritten geschickt, auf einem mit Zwei-Faktor-Berechtigung geschützten, restriktierten Cloud Server gespeichert und auf unbestimmte Zeit aufbewahrt.

Teilen Sie den betroffenen Personen mit, wer ihr Datenschutzbeauftragter ist (falls zutreffend), und bieten Sie ihnen einen einfachen Kommunikationskanal für Anträge auf Zugang durch betroffene Personen.

- Art. 18 LGDP; Art. 12 DSGVO.
- **Beispiel:** Eine Kampagne hat auf ihrer Webseite ein Kontaktformular mit direkter Verbindung zum Datenschutzbeauftragten eingerichtet. Es enthält außerdem spezifische Felder für Zugangsanträge von betroffenen Personen, die mit Vorrang bearbeitet werden.

Vergewissern Sie sich, dass Sprache und Auslegung Ihrer Plattformen geeignet sind, das bestmögliche Verständnis für betroffene Personen zu gewährleisten.

- **Maßnahme:** Verwenden Sie angemessene Typografie (Größe, Farbe, Kontrast, Schrift usw.), Sprache, Bildsymbole, Illustrationen und sonstige Mittel zur Gewährleistung des optimalen Verständnisses unter Berücksichtigung der spezifischen Fähigkeiten der Leser.
- **Beispiel:** Eine Kampagne hat ein Team aus Rechtsfachleuten, Marketingfachleuten und Webdesignern angestellt, die gemeinsam an der Erstellung eines Datenschutzdokuments arbeiten werden, das nicht nur die geforderte Rechtssprache, sondern auch vereinfachten erklärenden Inhalt enthält, den Nichtjuristen verstehen können.

Benachrichtigen Sie Nutzer über ihre Datenschutzrichtlinien und mögliche Aktualisierungen.

- **Maßnahme:** Benachrichtigen Sie Personen über die Verarbeitung ihrer Daten, einschließlich Übertragungen an Dritte, unter Angabe dieser Dritten oder zumindest ihrer Kategorien und des Zeitraums der Verwahrung der Daten.
- **Maßnahme:** Seien Sie möglichst spezifisch, da allgemeine Genehmigungen von keinem der beiden Gesetze anerkannt werden.

- **Beispiel:** Eine Kampagne hat sich entschlossen, Google Analytics auf ihrer Webseite zu verwenden. Außerdem hat sie die Webseite unter Verwendung eines Webseitenbaukastens wie Wix oder Squarespace gebaut. Alle diese Plattformen sammeln Nutzerdaten, was den betroffenen Personen gegenüber erwähnt werden sollte.

Verwalten Sie den Inhalt: Falls die Einwilligung die Rechtsgrundlage darstellt, vergewissern Sie sich, dass sie unter angemessenen Bedingungen erteilt wird. Das erfordert einen multidisziplinären Ansatz von der Rechtsabteilung bis zu IT und Design[148], um sicherzustellen, dass die Einwilligung freiwillig erteilt wird sowie spezifisch, informiert und unmissverständlich ist.

- **Maßnahme:** Erbitten Sie ausdrücklich die Genehmigung zur Sammlung von Cookies und sonstigen identifizierenden Informationen (ausgenommen in Fällen, in denen eine andere angemessene Rechtsgrundlage für die Sammlung besteht)[149].
- **Beispiel:** Der Kandidat hat ein Abonnementformular für einen politischen Newsletter auf seiner Kampagnenwebseite und seine Webseite sammelt Cookies. Die Webseite hat ein vormarkiertes Kästchen, das die Einwilligung zum Erhalt des Newsletter anzeigt. Das wird nicht als gültige Einwilligung betrachtet, und das Kästchen sollte nicht vormarkiert sein. Außerdem weist die Webseite eine Cookie-Erklärung auf, die besagt, dass die „Einwilligung bei Verwendung dieser Webseite als gegeben betrachtet wird". Das wird gleichfalls nicht als gültige Einwilligung betrachtet[150]. Beste Praxis wäre eine informative Haftungsfreistellung, die dem Nutzer gestattet zu wählen, welche Arten von Cookies er zulassen möchte, und die erklärt, welche Cookies für das ordnungsgemäße Funktionieren der Webseite notwendig sind und welche die aktive Einwilligung des Nutzers erfordern, d. h. eine Handlung, die seine Einwilligung widerspiegelt.

Achten Sie besonders auf die Daten von Kindern und Daten einer besonderen Kategorie (sensible Daten), die strengeren Bestimmungen unterliegen.

- Art. 11, Art. 14 LGPD; Art. 8, Art. 9 DSGVO.
- **Maßnahme:** Die Einwilligung sollte spezifisch und hervorgehoben sein und, im Fall von Kindern, von den Eltern oder gesetzlichen Vertretern gegeben werden. (Die DSGVO enthält altersspezifische Regelungen. Siehe den relevanten Artikel.) Die Rechtsgrundlagen für die Verarbeitung sensibler Daten sind einschränkender (siehe relevante Artikel).

Beachten Sie die Datenübertragbarkeit: Vergewissern Sie sich, dass die Daten in einem Format vorliegen, welches ihre Übertragbarkeit gestattet. Hierbei handelt es sich um ein Recht der betroffenen Person sowohl im LGPD als auch in der DSGVO. Die betroffene Person sollte in der Lage sein, ihre Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln" (Art. 20 DSGVO).

- Art. 18 LGDP; Art. 20 DSGVO.

Definieren Sie die Pflichten des Auftragsverarbeiters: Alle von einem Verantwortlichen beauftragten oder ernannten Auftragsverarbeiter sollten einen Datenverarbeitungsvertrag[151] haben, der ihre Verantwortlichkeiten, die Sicherheitsstandards und sonstige rechtliche Anforderungen[152] festlegt.

- Art. 28 DSGVO.
- **Maßnahme:** Setzen Sie einen Datenverarbeitungsvertrag auf, der die Verantwortlichkeiten und Sicherheitsstandards festlegt.

Stellen Sie sicher, dass Ihre Dienstanbieter Compliance gewährleisten sowie die Daten auf eine sichere Art und Weise verwalten und dass die Daten auf einem Server in einem Land gespeichert werden, das die aktuellsten Datenschutzbestimmungen beachtet.

- **Maßnahme:** Prüfen Sie, ob die von diesen Dritten gehandhabten Daten in Ländern mit einem äquivalenten Status hinsichtlich des Datenschutzes gespeichert werden. Die EU hat ein System zur Einstufung der Gesetzgebung von Ländern als äquivalent oder nicht äquivalent eingerichtet.
- **Maßnahme:** Vergewissern Sie sich, dass Ihre Rechtsabteilung die Nutzungsbedingungen eines von Ihnen verwendeten Drittdienstes zur Verwaltung personenbezogener Daten sorgfältig studiert und ihre Compliance mit der DSGVO bzw. dem LGPD analysiert.
- **Beispiel:** Die Kampagne entscheidet sich für eine Datensammlung mithilfe von Google Analytics sowie die Lieferung von Werbung mit der Werbeplattform von Facebook, das Senden von E-Mails über Mailchimp und das Management interner Datenflüsse mithilfe einer technischen Lösung aus Indien. Die Kampagne muss sich vergewissern, dass jeder einzelne der obigen Dienstanbieter die Datenschutzgesetze beachtet, da sie Zugang (wenn auch nur vorübergehend) zu den gesammelten und verarbeiteten personenbezogenen Daten haben werden. Im Fall der technischen Lösung aus Indien sollte die Kampagne bei einer Speicherung der Daten auf einem Server in Indien bestätigen, dass die EU Indiens Compliance mit der DSGVO anerkannt hat. (Im Dezember 2019 war das Land dabei, diesen Status anzustreben, hatte ihn jedoch noch nicht erreicht.)

Managen Sie Verletzungen des Schutzes: Ein Prozess zur Feststellung von Verletzungen des Schutzes und zur Benachrichtigung der Aufsichtsbehörde und betroffenen Personen über Verletzungen des Schutzes sollte vorhanden sein.

- Art. 48 LGPD; Art. 33 DSGVO.
- **Maßnahme:** Sicherheitsverstöße müssen der nationalen Aufsichtsbehörde unverzüglich gemeldet werden (nach DSGVO innerhalb von 72 Stunden). Nur das LGPD schreibt die Benachrichtigung der betroffenen Personen vor, während eine solche Benachrichtigung in der DSGVO nur notwendig ist, wenn ein erhebliches Risiko für die Rechte und Freiheiten der betroffenen Personen besteht.
- **Beispiel:** Die Kampagne hat eine Sicherheitsabteilung, die dafür zuständig ist, Fehler und Mängel im Design und in den Funktionen aller Datenverarbeitungsaktivitäten zu finden. Sie hat außerdem das gesamte relevante Personal dahingehend geschult, wie es auf eine Verletzung des Schutzes zu reagieren hat, einschließlich den an die Aufsichtsbehörde über entsprechende Kanäle zu meldenden Informationen und der Kommunikation mit der Öffentlichkeit.

Managen Sie Sicherheitsrisiken:

- Art. 46 LGPD; Art. 32 DSGVO.
- **Maßnahmen:** Minimieren Sie die Übertragung von Daten zwischen Geräten. Verschlüsseln, pseudonymisieren oder anonymisieren Sie die Daten nach Möglichkeit. Richten Sie interne Sicherheitsleitlinien ein, schulen Sie die Teammitglieder zu Sicherheitsfragen, legen Sie vorgeschriebene Passwortsicherheitsrichtlinien fest und betreiben Sie eine aus mehreren Faktoren bestehende Berechtigungsprüfung[153]. Führen Sie eine Risikobewertung der zur Sammlung, Verarbeitung und Speicherung der Daten verwendeten Infrastruktur durch.
- Compliance als Prozess: Datenschutz hört nicht auf, wenn ein Verantwortlicher eine DSFA schreibt oder den betroffenen Personen Informationen über die Datenschutzrichtlinien der Organisation bereitstellt. Der Datenschutz sollte fortlaufend überwacht, geprüft, aktualisiert und an die Datenverarbeitungskontexte sowie die jüngsten technologischen Fortschritte angepasst werden.

Diese obigen Punkte sind alle ausführbar und an Datenverantwortliche und Verarbeitungsabläufe gerichtet. Ein vollständiges Datenschutzparadigma kann jedoch nur durch die Beteiligung vieler Akteure erreicht werden. Dies bedeutet eine sorgfältige Regulierung und Führung durch nationale Aufsichtsbehörden, insbesondere im Fall von Brasilien, wo das Gesetz viele Punkte dem Ermessen der Datenschutzbehörde überließ, die über Sicherheitsstandards sowie Fälle, in denen eine DSFA notwendig ist, und besondere Bestimmungen für kleine und mittelständische Unternehmen usw. entscheiden wird. Es bedeutet außerdem eine aktive Anstrengung seitens der Judikative zur Abstimmung ihres Verständnisses an die Grundsätze und den Sinn des Gesetzes sowie zur Interpretation schwieriger Fälle und der Erfüllung dieser Grundsätze mit Leben unter Berücksichtigung des Schutzes der betroffenen Personen.

Diese Anstrengungen, den Bestimmungen die nötige Substanz zu geben, haben in Europa bereits begonnen, und in Bezug auf politische Kampagnen ist es interessant, die rechtlichen Debatten zu beobachten, die unmittelbar nach dem Inkrafttreten der DSGVO bezüglich des Erwägungsgrunds Nr. 56 zur Verordnung entstanden sind. Der Erwägungsgrund lieferte eine Interpretation bezüglich der Verarbeitung personenbezogener Daten im Zusammenhang mit Wahlen. Dort lautet es wie folgt[154]:

> *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.*

Die darauffolgenden legislativen Anstrengungen in einigen Mitgliedstaaten unter Berücksichtigung des Erwägungsgrunds führten zu einer Diskussion über die Grenzen einer Verarbeitung in solchen Fällen. Spanien und Rumänien führten Grundlagen für die Verarbeitung personenbezogener Daten bei Wahlkampagnen in ihre nationale Gesetzgebung ein, die auf der Interpretation des öffentlichen Interesses gegründet sind. In Rumänien bedeutete das eine Ausnahme bezüglich der Einwilligung zur Verarbeitung personenbezogener Daten zu Wahlzwecken. Sie gestattete zum Beispiel der

rumänischen Post den Abschluss eines Vertrags mit der Sozialdemokratischen Partei des Landes zur Lieferung von politischem Kampagnenmaterial an ausgewählte Populationen unter Verwendung der Daten der Post über ältere Rentner[155].

Auf ähnliche Weise gestattete ein nationales Gesetz in Spanien politischen Parteien die Sammlung personenbezogener Daten aus öffentlich verfügbaren Quellen, wie beispielsweise sozialen Netzwerken, und ihre Verwendung zum Profiling von Wählern. Die Bestimmung modifiziert das spanische Wahlgesetz durch die Hinzufügung von Artikel 58 bis, der besagt[156]:

> **Artikel 58 bis. Verwendung von technologischen Werkzeugen und personenbezogenen Daten bei Wahlaktivitäten.**
>
> 1. *Die Sammlung personenbezogener Daten in Bezug auf politische Einstellungen von Personen durch politische Parteien bei ihren Wahlaktivitäten muss durch öffentliches Interesse begründet sein und darf nur durchgeführt werden, wenn angemessene Garantien bestehen.*
> 2. *Politische Parteien, Koalitionen und Wahlgruppierungen dürfen personenbezogene Daten, die sie von Webseiten und sonstigen, öffentlich zugänglichen Quellen erhalten haben, zu Wahlkampfaktivitäten während des Wahlzeitraums verwenden.*
> 3. *Das Verschicken von Wahlpropaganda mithilfe von elektronischen Mitteln oder Nachrichtensystemen und die Verbreitung von Wahlpropaganda in sozialen Netzwerken oder auf äquivalenten Plattformen mittels Beauftragung Dritter wird nicht als kommerzielle Kommunikationsaktivität betrachtet.*
> 4. *Die oben erwähnten Werbeaktivitäten müssen ihre Wahlkampfnatur eindeutig klarstellen.*
> 5. *Der Empfänger muss über eine einfache und kostenlose Methode zur Ausübung seines Rechts auf Widerspruch verfügen.*

In der Praxis könnten die Bestimmungen des spanischen Gesetzes als nachlässiger in Bezug auf den Schutz personenbezogener Daten interpretiert werden, in diesem Fall die besondere Datenkategorie politischer Einstellungen, die den spezifischen Gegenstand des Erwägungsgrunds darstellen. Erwägungsgrund 56 sollte als Spezifizierung von Artikel 9 der DSGVO interpretiert werden, die unter Punkt (2) g) die Verarbeitung behandelt, die „aus Gründen eines erheblichen öffentlichen Interesses erforderlich“ ist. Daher sollten sowohl die Darlegungen des Erwägungsgrunds als auch, insbesondere, der Artikel bei der Implementierung solcher Bestimmungen im nationalen Gesetz beachtet werden.

Erwägungsgrund 56 verlangt, dass die Zusammenstellung solcher Daten zu politischen Einstellungen für „das Funktionieren des demokratischen Systems in einem Mitgliedstaat“ erforderlich und durch „geeignete Garantien“ abgedeckt ist. Artikel 9 (2) g) ist strenger und erwähnt die Notwendigkeit eines „erheblichen“ öffentlichen Interesses sowie eine Verarbeitung, die 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[157].

Der Fehler des spanischen Gesetzes, der vom Obersten Gericht des Landes in einem Fall im März 2019 erkannt wurde, liegt darin, dass weder „angemessene und spezifische Maßnahmen“ vorgesehen waren noch ein „erhebliches öffentliches Interesse“ festgestellt worden war[158].

In der Praxis ging das Gesetz das Risiko ein, eine willkürliche Verarbeitung sensibler Daten unter direkter Verletzung der DSGVO zu gestatten und die Bürger Praktiken auszusetzen, die den beim Skandal von Cambridge Analytica eingesetzten Praktiken ähnelten. Zu diesem Punkt und angesichts solcher Kontroversen bezüglich der Verwendung sensibler personenbezogener Daten bei Wahlkampagnen veröffentlichte der Europäische Datenschutzausschuss (EDSA) im März 2019 seine „Erklärung Nr. 2/2019 zur Verwendung personenbezogener Daten im Rahmen politischer Kampagnen[159]“. Die Erklärung liefert fünf konkrete Empfehlungen und Klarstellungen für die Mitgliedstaaten:

I. *Personenbezogene Daten, aus denen politische Meinungen hervorgehen, stellen eine besondere Kategorie von Daten nach der Datenschutz-Grundverordnung (DSGVO) dar. Grundsätzlich ist die Verarbeitung solcher Daten verboten und unterliegt einer Reihe eng auszulegender Voraussetzungen, wie der ausdrücklichen, spezifischen, umfassend informierten und freiwillig erteilten Einwilligung der betroffenen Personen;*

II. *Personenbezogene Daten, die öffentlich gemacht oder von einzelnen Wählern geteilt wurden, auch wenn sie keine Daten darstellen, die politische Meinungen erkennen lassen, unterliegen nach wie vor dem EU-Datenschutzrecht. Beispielsweise kann die Verwendung personenbezogener Daten, die über soziale Medien erhoben werden, nicht durchgeführt werden, ohne dass die Verpflichtungen in Bezug auf Transparenz, Zweckbindung und Rechtmäßigkeit erfüllt werden;*

III. *Selbst wenn die Verarbeitung rechtmäßig ist, müssen Organisationen ihre anderen Pflichten nach der Datenschutz-Grundverordnung einhalten, einschließlich der Transparenz- und Informationspflichten. Die politischen Parteien und die Kandidaten müssen in der Lage sein, nachzuweisen, wie sie den Grundsätzen des Datenschutzes, insbesondere den Grundsätzen der Rechtmäßigkeit, Fairness und Transparenz, Rechnung tragen;*

IV. *Ausschließlich automatisierte Entscheidungen einschließlich des Profilings, bei denen die Entscheidung die betroffene Person rechtlich oder in ähnlicher Weise erheblich beeinträchtigt, sind beschränkt. Der EDSA interpretiert die Beeinflussung der Wahlstimme einer Person als „rechtliche Beeinflussung“ der betroffenen Person;*

V. *Bei gezielter Ansprache sollten die Wähler angemessene Informationen erhalten, in denen erläutert wird, warum sie eine bestimmte Botschaft erhalten, wer dafür verantwortlich ist und wie sie ihre Rechte als betroffene Personen wahrnehmen können.*

Mit diesen Empfehlungen bietet der EDSA den Gesetzgebern der Mitgliedstaaten eindeutige Leitlinien zur Interpretation von Artikel 9 (2) g) und Erwägungsgrund 56 in Bezug auf Wahlprozesse. Das ist wesentlich, da eine unvollständige Anwendung der von der Verordnung verlangten Garantien und Anforderungen zu Situationen führen könnte, die direkt gegen den Sinn des Gesetzes verstoßen, wie es in zuvor erwähnten Fällen geschah. In diesem Zusammenhang ist es interessant, die spanischen und rumänischen Fälle mit den von Italien und Frankreich verfolgten Ansätzen zu vergleichen. In Italien können nach Feststellung der Datenschutzbehörde des Landes im Jahr 2014 im Internet öffentlich verfügbare, personenbezogene Daten nicht zur politi-

schen Kommunikation verwendet werden, mit Ausnahme von ursprünglich zu diesem Zweck veröffentlichten Daten. In Frankreich verlangt eine 2016 vorgenommene Aktualisierung der Empfehlungen zur politischen Kommunikation der französischen nationalen Datenschutzkommission (CNIL) aus dem Jahr 2012 die spezifische Einwilligung zur rechtmäßigen Sammlung und zum Profiling der personenbezogenen Daten von Wählern[160].

Der Verantwortliche sollte immer daran denken, dass die Datenschutzgesetze um die betroffene Person und ihre Rechte herum ausgelegt sind und ein ermächtigendes System für Geschäftspraktiken und Innovationen um Daten schaffen, allerdings innerhalb der Grenzen von Privatsphäre und Datenschutz, bei denen es sich um tief in Persönlichkeitsrechten und menschlicher Würde verwurzelten Garantien handelt. Deshalb sollten Praktiken, wie beispielsweise das Kaufen von Listen von Datenmaklern und das willkürliche Profiling betroffener Personen, die in einem Szenario vor der Einführung von Datenschutzbestimmungen gängig waren und unter anderem zu Wahlzwecken eingesetzt wurden[161], unter diesem neuen Paradigma vermieden werden. Zusätzlich hat der Schutz personenbezogener Daten wie zuvor erwähnt eine direkte Auswirkung auf die Qualität von Wahlprozessen, da diese Daten eine notwendige Eingabegröße für Psychometrie und andere Techniken darstellen, die bei ihrer Anwendung auf politische Kampagnen eine echte Auswirkung auf Wahlergebnisse haben.

In Europa und Brasilien werden sich die Behörden dieses Risikos zunehmend bewusst, was aus den Maßnahmen des EDSA zur Harmonisierung der nationalen Gesetzgebungen und einer ordnungsgemäßen Auslegung von Erwägungsgrund 56 hervorgeht. In Brasilien nahm das Oberste Wahlgericht vor Kurzem Bestimmungen in seinen letzten Gesetzesentwurf für die anstehenden Kommunalwahlen auf, die auf eine Einschränkung der Verbreitung von Falschinformationen abzielen, insbesondere über soziale Medien und digitale Anwendungen.

Die Harmonisierung allgemeiner Datenschutzbestimmungen mit Wahlbeschlüssen sowie die Beachtung der Bestimmungen zur Informationsverarbeitung sollten als Priorität betrachtet werden mit der Gewalt, wirksame Mechanismen gegen die missbräuchliche Verwendung personenbezogener Daten während Wahlperioden sicherzustellen, die einen Beitrag zu einem fairen Wahlumfeld leisten.

---

131 Aus der Perspektive von betroffenen Personen erscheinen neue Datenschutzbestimmungen offenbar vorteilhaft, da sie auf eine gesteigerte Autonomie von betroffenen Personen abzielen. Autonomie bringt jedoch die Verantwortung mit sich, souverän über seine eigene Identität entscheiden zu müssen. Sie bereichert die persönliche Freiheit, verlangt allerdings gleichzeitig eine grundlegende Veränderung der Art und Weise, wie Menschen ihre Beziehung zu Datenverantwortlichen sowie den von ihnen angebotenen Dienstleistungen und Produkten sehen und letztendlich Ihres Verständnisses, wie eine Datenökonomie und -gesellschaft sein sollte.

132 Obwohl allgemeine Datenschutzbestimmungen in vielen Ländern bereits gelten, haben viele politische Entscheidungsträger immer noch kein klares Verständnis davon, was bezüglich der Datenverarbeitung erlaubt ist, welche übergreifenden Implikationen bestehen und wie wichtig dieses Thema ist. Daher sind die Anstrengungen zur Schaffung des Bewusstseins und der Fähigkeiten nicht nur für Bürger, sondern auch für politische Entscheidungsträger, wichtig und fortlaufend und sollten verstärkt werden, um das richtige Verständnis und die Durchsetzung der geltenden Bestimmungen zu gewährleisten.

133 Siehe „Risk Based Security (2019), Data Breach“ (Risikobasierte Sicherheit (2019), Datenverstoß) QuickView Report: 2019 Q3 trends.

134 AMIGORENA F. (2019): „The Myths of Multifactor Authentication. DARKReading“ (Die Mythen der Multifaktor-Zugangsberechtigung. DARKReading), https://www.darkreading.com/endpoint/authentication/the-myths-of-multifactor-authentication/a/d-id/1336262.

135 GDPR Informer (2017): „Data Security 101: Access Controls & Planning“ (Datensicherheit 101: Zugangskontrollen & Planung), https://gdprinformer.com/gdpr-articles/data-security-101-access-controls-planning.

136 HEWARD-MILLS D. (2019): „The DPO must be independent, but how?“ (Der Datenschutzbeauftragte muss unabhängig sein, aber wie?), https://iapp.org/news/a/the-dpo-must-be-independent-but-how/, Zugang November 2019.

137 Siehe DSGVO-Info, https://gdpr-info.eu/issues/data-protection-officer/, Zugang November 2019.

138 Siehe Art. 13 DSGVO sowie Art. 9 und 18 LGPD.

139 FINUCANE B. (2018): „A Post-GDPR Checklist for Political Parties“ (Eine Checkliste für politische Parteien nach Einführung der DSGVO), CPO Magazine, https://www.cpomagazine.com/data-protection/a-post-gdpr-checklist-for-political-parties/, Zugang November 2019.

140 Hier finden Sie eine Liste von Checklisten: <https://ico.org.uk/for-organisations/data-protection-self-assessment/>.

141 Hier finden Sie den Code: <https://www.pdpjournals.com/docs/88625.pdf>.

142 Diese Liste basiert hauptsächlich auf den zuvor angegebenen Ressourcen, nämlich den ICO-Checklisten und der Checkliste für politische Parteien von Finucane. Sie spiegelt außerdem die Bestimmungen der DSGVO bzw. des LGPD sowie die Analyse beider Rechtsdokumente durch den Autor wider. Falls sonstige Quellen hinzugezogen wurden, sollten sie in einer Fußnote angegeben sein.

143 Die „Daten besonderer Kategorie“ der DSGVO werden im LGPD als „sensible Daten“ (dados sensíveis) bezeichnet.

144 ICO (2019): „Principle (c): Data minimization“ (Grundsatz (c): Datenminimierung), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/, Zugang November 2019.

145 Das ICO hat eine DSFA-Vorlage hier bereitgestellt: https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf.

146 Wenn man sich bei der Datenverarbeitung auf berechtigtes Interesse beruft, empfiehlt das ICO die Durchführung eines „Legitimate Interest Assessment“ (Bewertung des berechtigten Interesses). Das trägt zu Verantwortlichkeit und Transparenz bei und sichert das Unternehmen im Fall einer Prüfung ab. Das LIA umfasst die drei Kernaspekte der Grundlage des berechtigten Interesses: Zweck, Notwendigkeit und die Ausgewogenheit zwischen diesen Interessen sowie den Interessen, Rechten und Freiheiten der betroffenen Person. Weitere Informationen zum LIA sowie eine LIA-Vorlage finden Sie auf https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/, Zugang Januar 2020.

147 BIONI Bruno (2019): „A obrigação de registro das atividades de tratamento de dados“, GEN Jurídico, http://genjuridico.com.br/2019/08/27/registro-tratamento-de-dados/, Zugang Dezember 2019.

148 ICO (2019): „Privacy notices, transparency, and control: Data protection: a code of practice on communicating privacy information to individuals“ (Datenschutzerklärungen, Transparenz und Kontrolle: Datenschutz: ein Verhaltenskodex zur Kommunikation von Datenschutzinformationen an Personen), https://www.pdpjournals.com/docs/88625.pdf, Zugang November 2019.

149 USTARAN Eduardo (2019): „Getting cookie consent right“ (Cookie-Einwilligung richtig gestalten), Infolaw, https://www.infolaw.co.uk/newsletter/2019/11/getting-cookie-consent-right/, Zugang Dezember 2019.

150 CJEU (2019): „Judgment of the Court (Grand Chamber) of 1 October 2019, Case C-673/17“ (Urteil des Gerichts (Große Kammer) vom 1. Oktober 2019, Fall C-673/17), http://curia.europa.eu/juris/liste.jsf?language=en&num=C-673/17, Zugang Dezember 2019.

151 Siehe „What is a GDPR data processing agreement?“ (Was ist ein DSGVO-Datenverarbeitungsvertrag?), https://gdpr.eu/what-is-data-processing-agreement/, Zugang November 2019.

152 Hier finden Sie eine Vorlage für einen Datenverarbeitungsvertrag: https://gdpr.eu/wp-content/uploads/2019/01/Data-Processing-Agreement-Template.pdf.

153 GDPR.EU. Compliance-Checkliste: https://gdpr.eu/checklist/, Zugang November 2019.

154 Erwägungsgrund 56. Verfügbar auf: <https://gdpr-info.eu/recitals/no-56/>.

155 Siehe https://www.hotnews.ro/stiri-politic-23066729-exclusiv-contractul-prin-care-posta-livreaza-plian-tele-psd-sunt-vizati-toti-pensionarii-inclusiv-cei-care-primesc-pensia-cont-card-posta-obligat-trimita-psd-informatii-din-baza-date-pensionarii.htm, Zugang November 2019.

156 „Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales. 1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas. 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral. 3. El envío

de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán ninguna consideración de actividad o comunicación comercial. 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral. 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición."

157 GONZÁLEZ E. G. (2019): „The good, the bad and the ugly: Spanish electoral system act: A tale with a happy ending." (The Good, the Bad and the Ugly: der Akt des spanischen Wahlsystems: eine Geschichte mit einem glücklichen Ende), Secuoya, https://secuoyagroup.com/2019/06/the-good-the-bad-and-the-ugly-spanish-electoral-system-act-a-tale-with-a-happy-ending/, Zugang Dezember 2019.

158 „De lo anterior se concluye que la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclaman nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. […] La declaración de inconstitucionalidad y nulidad se basa, como se ha dicho en el fundamento jurídico anterior, en que la Ley Orgánica 3/2018 no ha fijado por sí misma, como le impone el Art. 53.1 CE, las garantías adecuadas por lo que respecta específicamente a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. Ello constituye una injerencia en el derecho fundamental a la protección de datos personales de gravedad similar a la que causaría una intromisión directa en su contenido nuclear." Sentencia. Recurso de Inconstitucionalidad núm. 1405–2019. Verfügbar auf: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/2019-1405STC.pdf, Zugang November 2019.

159 Siehe EDSA-Erklärung 2/2019 zur Verwendung personenbezogener Daten im Rahmen politischer Kampagnen. Verfügbar auf: https://edpb.europa.eu/our-work-tools/our-documents/ostalo/statement-22019-use-personal-data-course-political-campaigns_pt. Zugang November 2019.

160 Siehe EDSB-Stellungsnahme 3/2018: Stellungnahme des EDSB zu Online-Manipulation und personenbezogenen Daten. Verfügbar auf: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf, Zugang Dezember 2019.

161 Siehe „Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election" (Privatsphäre von Wählern: Was Sie für die Wahlen 2016 über Ihre digitalen Spuren wissen sollten), EFF, https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election, Zugang November 2019.

Abschließende Betrachtungen

Die Kultur der „Hyperconnectivity“, in der wir leben, bringt trotz zahlloser und unbestrittener Vorteile für die Bürger auch signifikante Herausforderungen für demokratische Räume mit sich. In diesem Zusammenhang ist es wichtig, der neuen Art und Weise der Kampagnenführung in unserer modernen Datenwelt besondere Aufmerksamkeit zu schenken und geeignete und effiziente Bestimmungen zur Gewährleistung fairer Wahlen vorzuschlagen.

Obwohl datengetriebene politische Kampagnen an und für sich kein neues Phänomen sind, stellen die verwendeten Werkzeuge, die Menge der zugänglichen Daten sowie die potenzielle Fähigkeit zur Beeinflussung von Wählern ein neues und herausforderndes Szenario für das Rechtsstaatsprinzip dar.

In den vergangenen Jahren haben politische Parteien in allen Teilen der Welt stark in Online-Werbung investiert, die das Potenzial aufweist, mehr Menschen auf eine effiziente und zielgerichtete Weise zu erreichen. Jüngste Erfahrungen, wie im Fall von Cambridge Analytica und bei den letzten Wahlen in Brasilien, haben jedoch gezeigt, wie Strategien zur politischen Manipulation von Wählern durch Falschinformation, algorithmische Manipulation, verhaltensorientiertes Microtargeting und Social Bots in diesem Szenario weit verbreitet eingesetzt wurden. Zusätzlich basieren diese Strategien meistens auf der unbefugten bzw. unrechtmäßigen Verarbeitung personenbezogener Daten, wie es im Fall von Cambridge Analytica, bei der Wahlkampagne in Brasilien 2018 und in anderen Fällen beobachtet wurde.

Mit den Worten von Colin Bennett und David Lyon:[162]

> *Fragen zur legitimen Verarbeitung personenbezogener Daten über die Wählerschaft sind der Kern der Antwort auf jede dieser größeren Fragen. Die Durchführung von Wähleranalytik und das Microtargeting politischer Nachrichten, einschließlich der Lieferung sogenannter Fake News, hat eine direkte Beziehung zur programmierten Werbung und zu den unpersönlichen Algorithmen, die einzelne Bürger oft ohne deren Kenntnis und Einwilligung anvisieren. Jetzt treten bekannte Fragen zur Privatsphäre in dieser hitzigen internationalen Debatte über demokratische Praktiken zu Tage, und Aufsichtsbehörden, wie beispielsweise Datenschutzbehörden, finden sich im Mittelpunkt einer globalen Diskussion über die Zukunft der Demokratie. Demzufolge „sind Privatsphäre und Datenschutz in der Vergangenheit selten große politische Fragen gewesen. Das hat sich jetzt geändert.“*

Daher kann ein Teil der möglichen missbräuchlichen Verwendungen und Risiken infolge von Missbrauch unter Berücksichtigung der Bedeutung der Verarbeitung personenbezogener Daten in diesem Kontext durch die Anwendung robuster gesetzlicher Rahmenwerke für die Regulierung personenbezogener Informationen gemindert werden. Als Beispiele gelten die DSGVO in Europa und das kürzlich verabschiedete brasilianische Datenschutzgesetz (LGPD), das bald in Kraft treten wird.

Diese Studie hat durch das Hervorheben spezifischer rechtlicher Leitfäden und konkreter Situationen gezeigt, dass Datenschutzbestimmungen vollständig auf politische Kampagnen anwendbar sind und die Fähigkeit haben, die Verringerung der instrumentellen Verwendung personenbezogener Daten zu unterstützen, während sie gleichzeitig die Auswirkungen des Einsatzes von Falschinformation und computergestützter Propaganda zum Zweck der politischen Manipulation vermeiden. Deshalb kann ein Datenschutzansatz andere Anstrengungen, zum Beispiel durch die Privatwirtschaft, strategisch verstärken, und Falschinformationen bei Wahlkampagnen durch die Sanktionierung der rechtswidrigen Verarbeitung personalisierter Daten verringern helfen, wodurch er zu einem wirksamen und nützlichen Rechtsinstrument im vorliegenden Kontext wird.

Einerseits besteht die Rolle öffentlicher Organe und Institutionen darin, mittels ihrer Beschlüsse und Sanktionen die Compliance mit den Richtlinien des LGPD und der DSGVO sowie deren Wirksamkeit zu verstärken. Andererseits haben die politischen Parteien die Pflicht zur Erfüllung gesetzlicher Anforderungen und tragen die volle Verantwortung für die Transparenz der Verarbeitung und den guten Glauben an die Verarbeitung der personenbezogenen Daten von Wählern.

Die unbefugte bzw. rechtswidrige Verarbeitung personenbezogener Daten untergräbt zusammen mit Falschinformationstechniken und der unfairen Verwendung von Bots, Profilen, Deep Fakes und anderen Mitteln das Vertrauen der Wähler sowie die Integrität politischer Prozesse. Daher sollte es von Institutionen als Bedrohung der Demokratie betrachtet werden.

---

162 Bennett C. J., Lyon D. (2019): „Data-driven elections: implications and challenges for democratic societies“ (Datengetriebene Wahlen: Implikationen und Herausforderungen für demokratische Gesellschaften). Internet Policy Review, 8(4).

Obwohl datengetriebene politische Kampagnen an und für sich kein neues Phänomen sind, stellen die verwendeten Werkzeuge, die Menge der zugänglichen Daten sowie die potenzielle Fähigkeit zur Beeinflussung von Wählern ein neues und herausforderndes Szenario für das Rechtsstaatsprinzip weltweit dar. Wie mit dieser Herausforderung umgegangen werden kann und welche Möglichkeiten Rechtsnormen zum Schutz personenbezogener Daten hierbei spielen können, erläutert die vorliegende Studie am Beispiel des europäischen und brasilianischen Rechtsrahmens.

Konrad-Adenauer-Stiftung e. V.