

Ihre Artikelauswahl als PDF



Inhaltsverzeichnis



1.	Microtargeting. Persönliche Daten als politische Währung	3
----	--	---

Microtargeting. Persönliche Daten als politische Währung

Von Wolfie Christl

7.6.2019

forscht und publiziert über Datenökonomie, Algorithmen und Tech-Plattformen und ist Leiter des unabhängigen Forschungsinstituts Cracked Labs in Wien.

cw@crackedlabs.org

Spätestens seit 2016, mit der Wahl Donald Trumps zum US-Präsidenten, dem Brexit-Referendum sowie den Datenskandalen um Facebook und Cambridge Analytica, tobt eine globale Debatte über digitale Kommunikation und Demokratie. Die einst mit dem Internet verbundenen emanzipatorischen Hoffnungen sind in den Hintergrund getreten. Kaum ein Wahlkampf, bei dem nicht über die digitale Verbreitung von Falschmeldungen oder Hetze diskutiert oder gar versteckte Manipulation vermutet wird. Auch kommerzieller Datenmissbrauch und die Macht der Tech-Plattformen sind in den Fokus gerückt.

Parlamente in aller Welt haben Untersuchungen angestoßen. Ironischerweise war es ausgerechnet der Einsatz von Daten in politischen Kampagnen, der die Debatte über unsere digitale Infrastruktur erst ausgelöst hat. Es geht dabei unter anderem um datengetriebenes "Microtargeting" – also um Praktiken, bei denen kleine Gruppen auf Basis von Datenanalysen mit fein abgestimmter Kommunikation politisch beeinflusst werden sollen.[1] Parteien, politische Kampagnen und andere Lobbys nutzen heute umfassende Daten über die Bevölkerung, insbesondere im Online-Bereich. Wie funktioniert Microtargeting? Welche Rolle spielen Facebook und die datenbasierte Klick-Ökonomie? Und was bedeutet das für Gesellschaft und Demokratie?

Cambridge Analytica und die Trump-Wahlkampagne

Es ist kein Wunder, dass die Beteiligung der Datenfirma Cambridge Analytica bei den Kampagnen für den Brexit und die Wahl Trumps Besorgnis erregt hat. Das Unternehmen hat umfassende Datenbanken über ganze Bevölkerungen zusammengestellt, mit Tausenden Merkmalen pro Person. Mit Hilfe eines Online-Quiz wurde auf Profildaten von 87 Millionen Facebook-NutzerInnen zugegriffen und diese mit Informationen aus Wahlregistern und von privaten Datenhandelskonzernen verknüpft.[2] Dazu war Cambridge Analytica Teil eines undurchsichtigen Firmennetzwerks, das sowohl für Regierungen und militärische Informationsoperationen in Afghanistan als auch für zwielichtige Wahlkampagnen rund um den Globus gearbeitet hat – etwa in den Philippinen, Indien, Pakistan und Kenia.[3]

Die Trump-Kampagne hat im letzten Monat vor der Präsidentschaftswahl fast eine Million US-Dollar täglich für Online-Werbung ausgegeben, mit einem Fokus auf wenige Bundesstaaten.[4] Eigenen Angaben zufolge wurden dabei Listen von WählerInnen mit bestimmten Merkmalen an Facebook geschickt. Die Plattform hat die entsprechenden NutzerInnen identifiziert und als adressierbare Zielgruppen zur Verfügung gestellt. Darüber

hinaus hat Facebook nach Personen mit ähnlichen Merkmalen gesucht. Damit konnten viele kleine Gruppen mit angepassten Inhalten versorgt werden – zum Teil auch, um sie zu verunsichern und von der Wahl abzuhalten.[5] Botschaften, Formulierungen und Gestaltung wurden dabei laufend getestet und vermessen, um die effektivsten Kombinationen zu finden. Dazu wurden täglich bis zu 100000 unterschiedliche Varianten von digitalen Werbeanzeigen eingesetzt.[6]

Welche Rolle die Daten- und Analysekapazitäten von Cambridge Analytica dabei genau gespielt haben, ist nach wie vor nicht geklärt. Die Firma hat sich aggressiv selbst vermarktet, die Effektivität ihrer "psychometrischen" Datenanalysen wird allerdings infrage gestellt.[7] Generell sind die Aussagen von Beteiligten wegen ihrer Eigeninteressen mit Vorsicht zu genießen.[8] Medienberichten zufolge hat Facebook die Trump-Kampagne aber auch in internen Dokumenten als Musterbeispiel für eine "innovative" Nutzung der Plattform dargestellt und dabei die permanenten Tests an ahnungslosen NutzerInnen hervorgehoben. Trump hat laut Facebook in den Monaten vor der Wahl 44 Millionen US-Dollar investiert und dabei in Summe 5,9 Millionen Varianten von Inhalten getestet, Clinton hingegen "nur" 66000 Varianten.[9]

Ist Microtargeting also für den Wahlsieg von Trump verantwortlich? Allein sicher nicht. Aber hat es eine Rolle gespielt? Welche Wirkung haben derartige Praktiken? Die Antwort ist: Wir wissen es nicht genau. Ein kürzlich veröffentlichter Überblick zum Forschungsstand diagnostiziert "fehlende Transparenz und viele offene Fragen".[10] Klar ist: Es ist ein riesiges Geschäft. 2018 hat Facebook mit der selektiven Einblendung von Inhalten 55 Milliarden US-Dollar eingenommen, Google gar 113 Milliarden Dollar.[11] Mit politischer Werbung hat Facebook in den USA allein seit Mai 2018 über 550 Millionen Dollar erwirtschaftet.[12] In Großbritannien ist der Anteil, den politische Kampagnen für digitale Werbung ausgeben, von 0,3 Prozent im Jahr 2011 auf 43 Prozent im Jahr 2017 gestiegen.[13]

Auch wenn Parteien in Europa betonen, Datenschutz zu respektieren, machen auch sie sich vielfach eine Infrastruktur zunutze, die letztlich auf permanenter Echtzeit-Überwachung großer Teile der Bevölkerung beruht. Digitales Marketing basiert auf komplexen Mechaniken, die sowohl aus der Makro- wie aus der Mikroperspektive betrachtet werden müssen. So kann Online-Targeting im Einzelfall ungenau sein und große Streuverluste in Kauf nehmen – aber in Summe trotzdem Verhalten verändern. Meist sind nicht Einzelne das Ziel, sondern Gruppen mit bestimmten Eigenschaften. Basis ist trotzdem die flächendeckende Erfassung und Verknüpfung von Daten auf individueller Ebene. Um zu verstehen, wie Online-Targeting eingesetzt werden kann, ist es notwendig, die Funktionsweise der digitalen Klick-Ökonomie genauer zu betrachten.

Beeinflussungsmaschine Klick-Ökonomie

Seit etwas mehr als zehn Jahren werden Daten zur individuellen Adressierung von Online-Werbung eingesetzt.[14] Wenn wir heute eine Website besuchen oder eine App nutzen, wird unser Profil im Hintergrund innerhalb von Millisekunden an den Höchstbietenden versteigert. Wer die Auktion gewinnt, darf eine Botschaft einblenden. Gleichzeitig werden bei jedem Klick Dutzende bis Hunderte Drittfirmen informiert.[15] Diese ergänzen damit ihre digitalen Profile und vermessen, wie wir auf die eingeblendeten Botschaften reagieren. Beahlt wird meist nicht pro Einblendung, sondern nur, wenn im Anschluss bestimmte Verhaltensweisen zu beobachten sind.[16] Das definierte Ziel kann etwa der Klick auf einen Link sein, das Ansehen eines Videos, eine Registrierung, ein Kauf oder Anderes. Wird dieses Ziel erreicht und die adressierte Person verhält sich wie geplant – klickt also zum Beispiel auf einen Link – spricht man von einer "Konversion" (also einer "Bekehrung"). Viele Anbieter versuchen darum, mit Daten über unseren Alltag möglichst gut

vorherzusagen, wie wir uns künftig verhalten werden, und verkaufen dieses Wissen unzählige Male pro Sekunde. Die Ökonomin Shoshana Zuboff hat für diesen Hochfrequenzhandel mit menschlichem Verhalten den Begriff "Überwachungskapitalismus" etabliert.[17]

Unsere Kommunikationsinfrastruktur ist heute auf vielen Ebenen von dieser Logik geprägt. Nicht nur soziale Beziehungen, sondern auch mediale Inhalte und öffentliche Debatten werden immer mehr von digitalen Umgebungen geformt, die auf die Maximierung von Klicks und Interaktionen sowie auf die Verwertbarkeit von Verhalten hin optimiert sind. Dabei ist die Klick-Ökonomie stark von Betrug geprägt: Stimmen aus der Industrie schätzen, dass ein Viertel der Klicks nicht von realen Menschen stammen und Werbetreibenden dadurch ein Schaden von 20 bis 50 Milliarden US-Dollar pro Jahr entsteht.[18] Außerdem werden NutzerInnen gern mit Anzeigen auf Websites mit qualitativ fragwürdigen Inhalten gelockt, die wiederum Werbeanzeigen enthalten und dabei mehr einbringen als die Anzeigen, mit denen sie dorthin gelockt wurden – eine Art Pyramidenspiel.[19] Auch durch politische Angstmake lässt sich mit Online-Werbung Geld verdienen: Vieles deutet etwa darauf hin, dass obskure Websites im US-Wahlkampf 2016 aus rein ökonomischen Motiven irreführende Informationen verbreitet haben, weil diese einfach viel geklickt werden.[20] Natürlich nutzen auch traditionelle Boulevardmedien diese Dynamiken. Ein österreichischer Chefredakteur hat bezüglich Klick-Maximierung offen über das symbiotische Verhältnis mit einer politischen Partei gesprochen.[21]

Im Unterschied zu früher kann heute aber nicht nur das Zielpublikum einer bestimmten Zeitung oder einer TV-Sendung angesprochen werden. Es können quer durch die Bevölkerung Menschen mit bestimmten Eigenschaften gefunden und adressiert werden – durch die flächendeckende Erfassung und Verknüpfung personenbezogener Daten über viele Firmen hinweg. In einer Studie des US-Forschungsinstituts Data & Society ist von einer "digitalen Beeinflussungsmaschine" die Rede, die sowohl kommerziell als auch politisch genutzt werden könne.[22]

Rasterfahndung und Verhaltensmanagement mit Facebook

Facebook spielt mittlerweile eine wichtige Rolle in der Politik. Ausgangspunkt für den Einsatz sind die sogenannten Seiten von Parteien und PolitikerInnen auf der Plattform. Deutsche Parteien betreiben jeweils bis zu 1500 Facebook-Seiten, von Ortsgruppen bis zur Bundesebene.[23] Diejenigen, die einer solchen Seite bereits aktiv auf Facebook folgen, können über diesen Kanal mit Inhalten "bespielt" werden. Aber nur ein Bruchteil von ihnen bekommt die Postings wirklich zu sehen. Die "organische" Reichweite – jene, die ohne Zuzahlung erreicht wird – ist im Laufe der Jahre auf ein Minimum gesunken.[24] Bezahlung schafft hier Abhilfe: Postings können dadurch an deutlich mehr – oder an ganz bestimmte – NutzerInnen ausgespielt und Interaktionen gezielt verstärkt werden. Die Reichweite erhöht sich auch, wenn viele interagieren – wenn also ein Posting mit einem "Like" versehen, kommentiert oder geteilt wird. Gegen Geld können diejenigen, die bereits interagiert haben, zusätzlich als Werbeträger benutzt werden. Im Optimalfall entsteht eine selbstverstärkende Dynamik und die Inhalte verbreiten sich "viral". Dies alles als "Werbung" zu bezeichnen, greift eigentlich zu kurz.

Facebook bietet viele Funktionen an, um in diese Dynamiken einzugreifen. Dazu sortiert die Plattform ihre NutzerInnen in Hunderttausende Kategorien entlang demografischer Eigenschaften, Interessen und Verhaltensweisen – darunter viele sensible Attribute, aus denen etwa die politische Einstellung abgeleitet werden kann.[25] Parteien können beliebig viele dieser Kategorien kombinieren, um kleine Gruppen anzusprechen. Diese Art der Rasterfahndung kann auch in Kombination mit Postings eingesetzt werden, die nicht allgemein öffentlich sichtbar sind. Diese sogenannten *dark posts* sehen so aus wie andere

Inhalte einer Facebook-Seite, können aber gezielt nur bestimmten Gruppen eingeblendet werden. Auch wenn eine Partei nur rudimentäre Targeting-Kategorien wählt, um etwa schlicht möglichst viele NutzerInnen in einem Land zu erreichen, nutzt sie die geballte Datenmacht der Plattform in ihrer ganzen Tiefe. Denn die Facebook-Algorithmen sind daraufhin optimiert, auch in diesem Fall unter allen NutzerInnen im Land diejenigen zu finden, für die die Inhalte "relevant" sind und die wahrscheinlich reagieren.[26]

Eine zentrale Komponente der Targeting-Mechanismen auf Facebook sind die sogenannten Audiences.[27] Im einfachsten Fall handelt es sich dabei um Listen von NutzerInnen, die sich aus den gewählten Kategorien ergeben – etwa alle Single-Männer über 50 in Leipzig, die sich für Glücksspiel, nicht aber für die SPD interessieren. Alternativ besteht eine Audience aus NutzerInnen, die bereits mit den eigenen Inhalten interagiert haben – etwa all diejenigen, die ein Posting kommentiert haben, sich für eine bestimmte Wahlkampfveranstaltung "interessieren" oder sich – als Beispiel – mindestens zehn Sekunden lang ein Video über "Chemtrails" angesehen haben.

Digitale Zwillinge und Daten abseits von Facebook

Genau genommen sind Audiences auf Facebook keine statischen Listen, sondern dynamische Bündel aus Regeln. Welche NutzerInnen enthalten sind, wird abhängig von deren Verhalten in Echtzeit aktualisiert. Es können viele unterschiedliche Audiences verwaltet und verknüpft werden. Schließlich kann Facebooks mächtige "Lookalike"-Mechanik dazu genutzt werden, um digitale Zwillinge zu finden – also Personen mit möglichst ähnlichen Verhaltensweisen. Politische Kampagnen können so zum Beispiel mit eigens erstellten – und nur für bestimmte Gruppen sichtbaren – Inhalten eine kleine Zahl von wütenden Menschen in einer Audience "einfangen". Facebook sucht dann über die Bevölkerung hinweg nach ähnlichen und besonders aktiven Personen, die als Hebel zur Reichweitensteigerung eingesetzt werden können. In Österreich waren im Wahlkampf 2017 zum Beispiel nur 8900 Personen für die Hälfte aller Facebook-Kommentare verantwortlich[28] – lohnenswerte Ziele.

Audiences können auch auf Basis von Daten erstellt werden, die außerhalb von Facebook erfasst wurden. Einerseits können politische Kampagnen den sogenannten Facebook-Pixel in ihre Websites und Apps einbauen – ein kleines Programm, das Nutzungsdaten an die Plattform überträgt. Wer die betroffenen Websites oder Apps nutzt, wird von Facebook identifiziert und in Echtzeit Teil einer Audience, die dann dort weiter eingesetzt werden kann. Andererseits können mit sogenannten Custom Audiences Listen mit Namen, Telefonnummern oder E-Mail-Adressen an Facebook geschickt werden.[29] Die Trump-Kampagne hat höchstwahrscheinlich Custom Audiences dazu genutzt, um durch Datenanalysen erstellte Listen von WählerInnen hochzuladen – und dann diese und ähnliche Personen adressiert.[30]

Facebook verkauft eine Vielzahl an Funktionen, die es ermöglichen, NutzerInnen zu finden, die sich wahrscheinlich wie gewünscht verhalten – also auf bestimmte Inhalte klicken, sie kommentieren oder teilen – und hilft dabei nach, dass sie sich so verhalten. Denn die Anregung möglichst vieler Interaktionen liegt dem Geschäftsmodell der Plattform zugrunde. Je provokativer die Inhalte, desto günstiger wird es, sie bezahlt zu verstärken. Basis dafür sind die Datenbestände von Facebook. Mit dem Facebook-Pixel und Custom Audiences potenzieren sich die Möglichkeiten, denn damit können politische Kampagnen jegliches Verhalten außerhalb der Plattform zur Grundlage für ihre Aktivitäten auf Facebook machen. Letztlich kann so alles zur Audience werden – egal ob ein Auszug aus einer Wählerdatenbank, die BesucherInnen eines ganz bestimmten Artikels auf einer Website oder Listen von Personen, die von Datenhandelsfirmen oder Analysedienstleistern wie Cambridge Analytica zusammengestellt wurden.[31]

Das manipulative Potenzial vervielfacht sich, sobald mit NutzerInnen so lange experimentiert wird, bis sie sich verhalten wie gewünscht – wenn sie also etwa einen Beitrag aufrufen oder teilen. Facebook bietet diesbezüglich an, automatisiert verschiedene Kombinationen von Texten, Bildern und Videos zu testen.[32] Vor Jahren hat die Plattform selbst derartige Experimente gemacht: Dabei wurde bei Millionen von ahnungslosen NutzerInnen die Reihenfolge und Gewichtung der eingeblendeten Inhalte manipuliert, ein anderes Mal wurden Aufforderungen, wählen zu gehen, eingeblendet. In beiden Fällen habe sich – so heißt es in von Facebook publizierten Studien – die Wahlbeteiligung bei den betroffenen Gruppen leicht erhöht.[33]

Trumps Team hat auch abseits von Wahlen Tausende Facebook-Werbeanzeigen im Einsatz, nach eigenen Angaben "um zu testen und zu lernen".[34] Bislang gibt es nur eine Studie, in der systematisch untersucht wurde, welchen Arten von Targeting europäische NutzerInnen auf Facebook ausgesetzt sind. Basis waren 85 Personen, denen zwischen April 2017 und Juli 2018 insgesamt 71000 bezahlte Postings eingeblendet wurden. Bei 17 Prozent der Anzeigen wurde Lookalike-Targeting eingesetzt, bei acht Prozent Verhaltensdaten von externen Websites oder Apps, und bei zwei Prozent wurden Daten genutzt, die via Custom Audiences hochgeladen wurden.[35] Über den konkreten Einsatz durch die Politik gibt es jedoch kaum belastbare Daten. Sowohl Lookalike-Targeting[36] als auch der Facebook-Pixel[37] dürften auch in der EU oft eingesetzt werden, Custom Audiences zumindest zum Teil.[38] In jedem Fall ist der Einsatz von Facebook für politische Kampagnen in vieler Hinsicht datenschutzrechtlich fragwürdig.[39]

Google bietet ähnliche Funktionen, inklusive der Einbindung von extern erfassten Daten. Abseits der großen Plattformen können derartige Audiences – also regelbasierte Listen über Einzelpersonen und deren Verhalten – nahezu grenzenlos und in Echtzeit zwischen Hunderten Anbietern verschoben werden.[40]

Wählerdaten in den USA und der EU

Online-Microtargeting ist im Grunde die konsequente Weiterentwicklung traditioneller Instrumente: Politische Kampagnen setzen schon seit Langem datenbasierte Methoden ein, um UnterstützerInnen zu mobilisieren, Unentschlossene zu überzeugen, Mitglieder zu rekrutieren, Freiwillige einzubinden oder Spenden zu akquirieren – und umgekehrt um andere Kampagnen zu sabotieren.[41] Zunehmend wird auf der Grundlage von Datenanalysen entschieden, welche Gruppen mit welchen Botschaften auf welchen Kanälen angesprochen werden – von Hausbesuchen und traditioneller Werbung auf Plakaten, in Zeitungen und im Fernsehen über die Ansprache via Post, E-Mail und Telefon bis zu den genannten Methoden auf Facebook und anderen Plattformen. In den USA nutzen Parteien dazu spätestens seit 2004 umfassende Datenbanken mit Informationen über die gesamte Bevölkerung. Neben Daten aus Wahlregistern werden Profile von privaten Firmen zugekauft. Auch die bei Hausbesuchen gesammelten Daten werden eingespeist.[42]

In Kombination mit Daten aus Wahlergebnissen, Geo- und Soziodemografie, Fokusgruppen und Umfragen werden statistische Modelle erstellt, mit denen die Wahlbevölkerung in größere bis sehr kleine Gruppen unterteilt wird. Darüber hinaus wird für jede Person eine Prognose über das Wahlverhalten berechnet.[43] Die Analysen dienen einerseits der Kampagnensteuerung, andererseits werden damit Listen von Personen erstellt, die dann etwa zu Hausbesuchen führen oder als Custom Audience auf Facebook hochgeladen werden. Schließlich wird versucht, jeden Kontakt mit der Kampagne, jeden Besuch einer Wahlveranstaltung und jede Werbeeinblendung zu erfassen. Diese Vermessung ist der eigentliche Ausgangspunkt, denn die Kampagnensteuerung erfolgt

anhand von Kennzahlen und Scores – bis auf die individuelle Ebene. Die NGO Tactical Tech hat die politische Nutzung von Daten überall in der Welt untersucht und dabei über 300 private Dienstleister identifiziert, darunter auch Datenfirmen aus Europa.[44]

In Großbritannien verwenden Parteien zentralisierte Wählerdatenbanken ähnlich wie in den USA.[45] In anderen europäischen Ländern setzt man – soweit bekannt – auf die Segmentierung der Bevölkerung ohne flächendeckende Erfassung von Einzelpersonen. Dabei werden Daten auf der Ebene von mehreren Haushalten oder Straßenzügen zugekauft.[46] In Österreich ist hingegen kürzlich bekannt geworden, dass die Österreichische Post an mehrere Parteien Daten über Einzelpersonen inklusive politischer Affinitäten verkauft hat.[47] Wo jedenfalls sehr wohl auch in der EU eine viel weitergehende Verknüpfung personenbezogener Daten stattfindet, ist einerseits im gesamten Online-Bereich und andererseits, wenn es um Personen geht, deren Daten – zumindest formal – mit "Zustimmung" verarbeitet werden, weil sie in irgendeiner Form Kontakt mit der Kampagne hatten. Dabei werden Kampagnenplattformen und Apps eingesetzt, die selektive Hausbesuche koordinieren und personalisierte Nachrichten verschicken – sowie E-Mail-Adressen und andere Daten sammeln. Parteimitglieder und andere Personen werden mit verhaltenspsychologisch optimierten Belohnungsmechaniken "spielerisch" in Kampagnen eingebunden. Sie erhalten etwa für jeden Hausbesuch und jeden digital geteilten Beitrag virtuelle Punkte und steigen dadurch in einer Rangliste auf, mit der Aussicht auf ein Treffen mit der Spitzenkandidatin.[48]

Neben Eigenentwicklungen sticht hier Nationbuilder heraus, eine integrierte Kampagnen- und Datenplattform, die weltweit tausendfach eingesetzt wurde – sowohl von Trump und 3000 anderen politischen Kampagnen in den USA als auch von der Wahlkampagne des heutigen französischen Präsidenten Emmanuel Macron.[49] Nationbuilder bietet tief greifende Funktionen zur Verknüpfung personenbezogener Daten aus vielen Quellen und mit Social-Media-Plattformen, die in der EU bereits Gegenstand behördlicher Untersuchungen waren.[50] Die Plattform zeichnet alle Kontakte und Aktivitäten auf, berechnet deren ökonomischen Wert und überträgt damit die datenbasierten Wachstumsstrategien der Tech-Konzerne auf politische Kampagnen.[51]

Chancen, Risiken, Handlungsoptionen

Wie wirkt sich datenbasiertes Microtargeting letztlich gesellschaftlich aus? Was die potenziell positiven Wirkungen angeht, gibt es die Hoffnung, dass diese Art der gezielten Ansprache politische Mobilisierung, Interesse und Partizipation stärken und damit gar die Wahlbeteiligung erhöhen könnte. Kampagnen könnten thematisch vielfältiger werden und BürgerInnen angesichts beschränkter Aufmerksamkeit besser informierte Wahlentscheidungen treffen. Zudem könnten sich Vorteile für kleinere politische AkteureInnen ergeben – solange nicht auch finanzstarke Kräfte entsprechend aufgerüstet haben.[52]

Umgekehrt bedroht exzessive Datenerfassung durch politische Parteien Privatsphäre und Autonomie. Dies kann eine abschreckende Wirkung hinsichtlich freier Meinungsäußerung und politischer Beteiligung haben. An kleine Gruppen angepasste Kommunikation ermöglicht gezielte Irreführung bei minimaler Nachvollziehbarkeit. Selbst wenn keine plumpen Falschinformationen zum Einsatz kommen, können unterschiedliche Schwerpunkte hervorgehoben werden, was zu einer verzerrten Wahrnehmung politischer Prioritäten führen kann. Microtargeting macht es außerdem sehr viel ökonomischer, diejenigen Teile der Bevölkerung, die als nicht mobilisierbar eingestuft werden, auszuschließen. In Summe könnte datenbasiertes Microtargeting gesellschaftliche Debatten fragmentieren sowie das Vertrauen in Politik und demokratische Institutionen weiter unterminieren.[53]

Können damit tief greifende politische Überzeugungen auf Knopfdruck manipuliert werden? Natürlich nicht. Wenn es Effekte gibt, sind sie sehr viel indirekter. Möglicherweise sind die geschilderten Praktiken nicht einmal sonderlich wirksam, erzeugen aber trotzdem Kollateralschäden für Öffentlichkeit und Demokratie – oder wir sehen erst die Anfänge dessen, was möglich ist.

Was also tun? Unbestritten ist, dass viel mehr Forschung nötig ist und Online-Targeting auf allen Ebenen transparent werden muss – nicht nur Inhalte, Kanäle und Zeiträume, sondern auch Budgets und genutzte Daten müssen nachvollziehbar sein. Datenschutzrecht muss auch bei politischen Parteien durchgesetzt werden, insbesondere im Online-Bereich, bei Kampagnenplattformen sowie bei der Verknüpfung unterschiedlicher Datenbanken. Darüber hinaus müssen EU-weit die Regeln für politische Werbung an das digitale Zeitalter angepasst werden. Wo für Chancengleichheit und Demokratie nötig, haben sich Parteien auch schon früher auf Beschränkungen bei Wahlwerbung geeinigt. Viele Problematiken stellen sich aber sowohl im kommerziellen als auch im politischen Bereich – von personalisierter Manipulation und Experimenten in digitalen Umgebungen bis zur Macht der Tech-Plattformen.

Fußnoten

1. Vgl. Frederik J.Z. Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, in: Utrecht Law Review 1/2018, S. 82–96.
2. Vgl. Jeff Chester/Kathryn C. Montgomery, The Role of Digital Marketing in Political Campaigns, in: Internet Policy Review 4/2017, (<https://policyreview.info/archives/2017/issue-4>).
3. Vgl. House of Commons/Digital, Culture, Media and Sport Committee, Disinformation and "Fake News": Interim Report, London 2018, S. 17, S. 53ff., S. 298.
4. Vgl. Donald Trump and Hillary Clinton's Final Campaign Spending Revealed, 9.12.2016, (<http://www.theguardian.com/us-news/2016/dec/09/trump-and-clintons-final-campaign-spending-revealed>).
5. Vgl. Joshua Green/Sasha Issenberg, Inside the Trump Bunker, With Days to Go, 27.10.2016, (<http://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go>).
6. Vgl. Lois Beckett, Trump Digital Director Says Facebook Helped Win the White House, 9.10.2017, (<http://www.theguardian.com/technology/2017/oct/08/trump-digital-director-brad-parscale-facebook-advertising>).
7. Vgl. Dave Karpf, Will the Real Psychometric Targeters Please Stand Up?, 1.2.2017, (<https://civichall.org/civicist/will-the-real-psychometric-targeters-please-stand-up>).
8. Vgl. Andreas Jungherr, Einsatz digitaler Technologie im Wahlkampf, in: Harald Gapski et al. (Hrsg.), Medienkompetenz, Bonn 2017, S. 92–101.
9. Vgl. Ryan Mac/Charlie Warzel, Congratulations, Mr. President: Zuckerberg Secretly Called Trump After The Election, 19.7.2018, (<http://www.buzzfeednews.com/article/ryanmac/congratulations-zuckerberg-call-trump-election-2016>).
10. Vgl. Landesanstalt für Medien NRW, Forschungsstand: Microtargeting in Deutschland und Europa, Düsseldorf 2019.
11. Vgl. Mozilla, Internet Health Report v.1.0, 2018, S. 66f., (<https://internethealthreport.org/2018>).
12. Vgl. Facebook, Werbebericht, (<http://www.facebook.com/ads/archive/report>), Zugriff am 28.4.2019.
13. Vgl. UK Electoral Commission, Digital Campaigning. Increasing Transparency for Voters, Juni 2018, S. 4, (<https://t1p.de/bqgy>).
14. Vgl. Wolfie Christl/Sarah Spiekermann, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Wien 2016, S. 118.

15. Vgl. Wolfie Christl, Corporate Surveillance in Everyday Life, Juni 2017, S. 44ff., (https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf).
16. Vgl. z.B. Yu (Jeffrey) Hu/Jiwoong Shin/Zhulei Tang, Incentive Problems in Performance-Based Online Advertising Pricing, in: Management Science 7/2016, S. 2022–2038.
17. Vgl. Shoshana Zuboff, Das Zeitalter des Überwachungskapitalismus, Frankfurt/M. 2018. Siehe auch den Beitrag von Zuboff in dieser Ausgabe (*Anm. d. Red.*).
18. Vgl. Pixelate, Desktop Click Fraud Has Risen From 20% to 25% in 2017, 31.5.2017, (<http://blog.pixelate.com/desktop-ad-click-fraud-rising-stats-data-2017>); Laurie Sullivan, Brands Lose Up To An Estimated \$50 Billion Annually From Ad Fraud, 5.3.2019, (<http://www.mediapost.com/publications/article/332752>).
19. Vgl. Jake Bialer, Inside The World Of Ad Arbitrage: An Analysis of 272,220 Taboola Ads, 10.10.2018, (<https://medium.com/@jbialer/cc044a54881c>).
20. Vgl. z.B. Dan Tynan, How Facebook Powers Money Machines for Obscure Political "News" Sites, 24.8.2016, (<http://www.theguardian.com/technology/2016/aug/24/facebook-clickbait-political-news-sites-us-election-trump>).
21. Vgl. "Zu weit weg von der Bevölkerung", Interview von Markus Huber mit Richard Schmitt, in: Fleisch Magazin 30/2016.
22. Vgl. Anthony Nadler/Matthew Crain/Joan Donovan, Weaponizing the Digital Influence Machine. The Political Perils of Online Ad Tech, 17.10.2018, (<https://datasociety.net/output/weaponizing-the-digital-influence-machine>).
23. Vgl. Jörg Diehl et al., How the German Right Wing Dominates Social Media, 29.4.2019, (<http://www.spiegel.de/international/germany/a-1264933.html>).
24. Vgl. Brandon Lee, The Death of Social Media Organic Reach and How to Overcome It, 4.9.2018, (<http://www.curatti.com/death-social-media-organic-reach>).
25. Vgl. José González Cabañas et al., Unveiling and Quantifying Facebook Exploitation of Sensitive Personal Data for Advertising Purposes, USENIX Security Symposium, Baltimore 15.–17.8.2018, (<http://www.usenix.org/conference/usenixsecurity18/presentation/cabanass>).
26. Vgl. Muhammad Ali et al., Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes, 3.4.2019, (<https://arxiv.org/abs/1904.02095>).
27. Für eine Beschreibung von Audiences/Targeting siehe Facebook, Zielgruppen, (<http://www.facebook.com/business/help/168922287067163>), Zugriff am 25.4.2019.
28. Vgl. Sofia Palzer-Khomenko et al., Facebook: 8900 User bestimmten Wahlkampf-Diskurs, 2.1.2018, (<http://www.mokant.at/1802-facebook-user-wahlkampf-diskurs>).
29. Vgl. Christl (*Anm.* 15), S. 47.
30. Vgl. Antonio García Martínez, How Trump Conquered Facebook – Without Russian Ads, 23.2.2018, (<http://www.wired.com/story/how-trump-conquered-facebook-without-russian-ads>).
31. Vgl. ebd.
32. Vgl. Florian Litterst, Facebook Dynamic Creative, 18.11.2017, (<http://www.adsventure.de/facebook-dynamic-creative>).
33. Vgl. Christl (*Anm.* 15), S. 77.
34. Gary Coby auf Twitter, 24.5.2018, (<https://twitter.com/GaryCoby/status/999764292181340163>).
35. Vgl. Athanasios Andreou et al., Measuring the Facebook Advertising Ecosystem, Network and Distributed System Security Symposium, San Diego, 24–27.2.2019, (<http://www.eurecom.fr/publication/5779>).
36. Vgl. Tom Dobber et al., Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques, in: Internet Policy Review 4/2017, (<https://policyreview.info/archives/2017/issue-4>).
37. Vgl. Peter Teffer, Tory and National Front Websites Hid Facebook Tracking Pixel, 13.4.2018, (<https://euobserver.com/justice/141589>).
38. Vgl. Information Commissioner's Office, Democracy Disrupted? Personal Information

- and Political Influence, 11.7.2018, (<https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf>).
39. Vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit, 1.4.2019.
 40. Vgl. Christl (Anm. 15), S. 49f.
 41. Vgl. Balázs Bodó et al., Political Micro-Targeting: A Manchurian Candidate or Just a Dark Horse?, in: Internet Policy Review 4/2017, (<https://policyreview.info/archives/2017/issue-4>).
 42. Vgl. Luke Bunting, The Evolution of American Microtargeting: An Examination of Modern Political Messaging, in: Butler Journal of Undergraduate Research 1/2015, (<https://digitalcommons.butler.edu/bjur/vol1/iss1/2>).
 43. Vgl. Colin J. Bennett, Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America?, in: International Data Privacy Law 4/2016, S. 261–275.
 44. Vgl. Tactical Technology Collective, "Data and Politics project" overview, 2018–2019, (<https://tacticaltech.org/projects/data-politics>).
 45. Vgl. Bennett (Anm. 43).
 46. Vgl. Simon Kruschinski/André Haller, Restrictions on Data-Driven Political Micro-Targeting in Germany, in: Internet Policy Review 4/2017, (<https://policyreview.info/archives/2017/issue-4>).
 47. Vgl. Addendum, Wenn die Post Partei ergreift, 7.1.2019, (<http://www.addendum.org/datenhandel/parteiaffinitaet>).
 48. Vgl. Mario Voigt/Rene Seidenglanz, Trendstudie. Digital Campaigning in der Bundestagswahl 2017, Dezember 2017, S. 70–74, (<https://t1p.de/3of2>); Dobber et al. (Anm. 36).
 49. Vgl. Chris O'Brien, How Nationbuilder's Platform Steered Macron's En Marche, Trump, and Brexit Campaigns to Victory, 14.7.2017, (<https://venturebeat.com/2017/07/14/how-nationbuilder-helped-emmanuel-macron-secure-a-landslide-in-frances-legislative-elections>).
 50. Vgl. z.B. Judith Duportail, The 2017 Presidential Election: The Arrival of Targeted Political Speech in French Politics, Dezember 2018, (<https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-france.pdf>).
 51. Vgl. Fenwick McKelvey/Jill Piebiak, Porting the Political Campaign: The Nationbuilder Platform and the Global Flows of Political Technology, in: New Media & Society 3/2018, S. 901–918.
 52. Vgl. Borgesius et al. (Anm. 1), S. 84ff.
 53. Ebd., S. 87ff.



Dieser Text ist unter der Creative Commons Lizenz veröffentlicht. [by-nc-nd/3.0/de/](http://creativecommons.org/licenses/by-nc-nd/3.0/de/) (<http://creativecommons.org/licenses/by-nc-nd/3.0/de/>)

Der Name des Autors/Rechteinhabers soll wie folgt genannt werden: [by-nc-nd/3.0/de/](http://www.bpb.de/apuz/292349/microtargeting-persoennliche-daten-als-politische-waehrung)
 Autor: Wolfie Christl für Aus Politik und Zeitgeschichte/bpb.de

Online-URL

<http://www.bpb.de/apuz/292349/microtargeting-persoennliche-daten-als-politische-waehrung>

Impressum

Diensteanbieter
gemäß § 5 Telemediengesetz (TMG)
Bundeszentrale für politische Bildung
Adenauerallee 86
53113 Bonn
redaktion@bpb.de