Big Data-Revolution, Überwachung und soziale Medien: Gefahr für die Demokratie?[1]

Martin Kahl[2]

Universität Hamburg

Abstract

Unternehmen, Sicherheitsbehörden und politische Organisationen sammeln und verwerten eine Unmenge persönlicher Daten zur Verbesserung von Verhaltensprognosen und zur Verhaltenssteuerung. Setzt man diese Entwicklung mit Kernelementen demokratischer Willensbildung wie der autonomen Meinungsbildung, der selbstbestimmten Grenzziehung zwischen Privatheit und Öffentlichkeit und der Vermittlungsaufgabe öffentlicher Medien in Beziehung, so werden an vielen Stellen tiefgreifende Veränderungen und Probleme deutlich. Die gesellschaftlichen und politischen Folgen der massenhaften Erhebung und Auswertung persönlicher Daten sind aus demokratietheoretischer Perspektive jedoch erst in Ansätzen behandelt worden. Der Beitrag illustriert gegenwärtige Überwachungspraktiken und erörtert ihre komplexen, teilweise gegenläufigen Folgen mit Blick auf die Grundbedingungen demokratischer Willensbildung.

Keywords: Big Data-Revolution, Überwachung, soziale Medien, Privatheit, Demokratie

> *We know where you are. We know where you've been. We can more or less know what you're thinking about.*
> Eric Schmidt, CEO Google

Die Sammlung und Auswertung großer Datenmengen, die Menschen weltweit in ihrer täglichen Lebenspraxis hinterlassen, hat einen solchen Umfang angenommen, dass seit einiger Zeit von einer „Big Data-Revolution" gesprochen wird (Mayer-Schönberger/Cukier 2013; Baecker 2007; Morozov 2014). Beteiligt hieran sind in der Hauptsache Unternehmen, darunter Internetfirmen und kommerzielle Auskunfteien, Regierungen und Sicherheitsbehörden, sowie seit einiger Zeit auch politische Organisationen, etwa Parteien und ihre Kampagne-

[1] Ich danke den anonymen Gutachterinnen und Gutachern für die konstruktive Kritik und Kommentare.

[2] Martin Kahl ist Wissenschaftlicher Referent am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH): kahl@ifsh.de. Zu seinen Forschungsthemen gehören Terrorismus und Terrorismusbekämpfung, Radikalisierung und Überwachung.

DOI: http://dx.doi.org/10.18753/2297-8224-98

Agenturen. Sie verwenden zwar nur zum Teil die gleichen Datenquellen und verfolgen je nach ihren Organisationszielen unterschiedliche Interessen, ihnen allen geht es jedoch um die Prognose und Steuerung von Verhalten. Das Bild ist nicht vollständig ohne die Nutzerinnen und Nutzer, die Telekommunikationsdiensten und sozialen Medien über Verbindungsdaten hinaus freiwillig viele persönliche Daten preisgeben.[3] Zwar gibt es immer wieder Stimmen, die vor den Folgen dieser Entwicklungen für Privatheit und Demokratie warnen, so zuletzt angesichts der Verwendung von Facebook-Daten durch das Unternehmen Cambridge Analytica im Rahmen politischer Kampagnen.[4] Öffentliche Debatten darüber, was mit den massenhaft erhobenen und ausgewerteten Daten geschieht, sind mit Ausnahme kurzzeitiger Erregungswellen, wie es sie auch nach den Enthüllungen Edward Snowdens gegeben hat, bisher jedoch nur schwach ausgeprägt (Hegemann/Kahl 2016; Pohle/Audenhove 2017; Steiger et al. 2017).

Die gesellschaftlichen und politischen Folgen der massenhaften Erhebung und Auswertung persönlicher Daten sind aus demokratietheoretischer Perspektive erst in Ansätzen behandelt worden. Angesichts der jungen und dynamischen Entwicklung des Feldes *Big Data* sowie seiner Komplexität kann dies nicht überraschen. Dieser Beitrag versucht aufzuzeigen, was sich zu den Auswirkungen von Big Data-Analysen auf demokratische Kernprozesse gegenwärtig aussagen lässt. Anders gefragt: Was lässt sich angesichts der der von Internetfirmen, Sicherheitsbehörden und politischen Organisationen vorgenommenen umfassenden Sammlung, Analyse und Nutzung einer Vielzahl privater Daten an Aussagen zu den Bedingungen der autonomen Herausbildung eigener Wertüberzeugungen im Schutze der Privatheit treffen sowie zu der Möglichkeit, diese anschließend selbstbestimmt in einen öffentlichen Prozess des Meinungsaustausches einzubringen?

Neben einem kurzen Kapitel, das begriffliche Klärungen vornimmt, enthält der Artikel drei weitere Teile. Um die Tragweite der Big Data-Revolution verstehbar und die hinter ihr liegenden Interessen nachvollziehbar zu machen, gibt der erste von ihnen einen Überblick über die Praktiken der Nutzung von Big Data durch kommerzielle Unternehmen, darunter auch die großen Internetkonzerne, durch Sicherheitsbehörden und durch politische Organisationen. Dabei wird insbesondere auf die sozialen Medien als Datenquelle und -verwerter eingegangen. Der zweite Teil entwickelt demokratietheoretische Kernkriterien anhand derer die Folgen von Big Data für Demokratie und Gesellschaft bewertet werden können. Der dritte Teil beleuchtet anschließend das komplexe Verhältnis von Big Data, Privatheit, Öffentlichkeit und demokratischer Willensbildung vor dem Hintergrund der demokratietheoretischen Grundannahmen. Er zeigt dabei Entwicklungsstränge auf, die in ihrer Wirkung nicht leicht zu erfassen und die durchaus gegenläufig sind. Auf der einen Seite lässt sich sagen, dass der Bereich des Privaten durch Big Data immer weiter aufgelöst wird. Die Individuen werden gründlich auf Vorlieben, Einstellungen und Verhaltensmuster durchleuchtet, um ihr Verhalten gezielter prognostizieren und lenken zu können (Amoore 2014), während die Prozesse der Datenerhebung und -auswertung selbst undurchsichtig bleiben. Das Zusammenwirken von

[3] Bauman und Lyon (2013) haben die Beteiligung an einer solchen Art der Verwertung von Daten „liquid surveillance" genannt. Lyon (2015: 146) spricht an anderer Stelle von einer „surveillance culture", in der Überwachung und ihre Techniken zum alltäglichen Leben dazugehören und an der man sich aktiv beteiligt.

[4] So erklärte die deutsche Justizministerin Katarina Barley am 22. März 2018 in einem Interview (BMJV 2018), die Vorgänge seien eine Gefahr für die Demokratie.

Facebook und Cambridge Analytica hat dies deutlich gezeigt. Auf der anderen Seite steht die Beobachtung, dass auf Big Data-Analysen basierende Beeinflussungsversuche trotz des hohen Aufwandes keinesfalls klare Ergebnisse und nur verführte Konsumenten oder angepasste Wählerinnen und Wähler hervorbringen, sondern dass zunehmende politische Polarisierungen zu beobachten sind, dies insbesondere auch in den sozialen Medien. Der Befund gewinnt dadurch an Komplexität, dass die Diskurse in den sozialen Medien einer algorithmischen Steuerung durch die Anbieterfirmen unterliegen und durch manipulative Eingriffe verzerrt werden. Aus demokratietheoretischer Sicht sind insgesamt so zwar viele Problemstellen sichtbar, ein einfaches Fazit lässt sich gegenwärtig jedoch nicht ziehen.

Was sind Big Data und was ist Überwachung?

Big Data zeichnen sich einer weit verbreiteten Definition zufolge durch drei Merkmale aus: ihren großen Umfang (Volume), die hohe Geschwindigkeit ihrer Generierung und Verarbeitung (Velocity) sowie die große Vielfalt bzw. Heterogenität der genutzten Datentypen und -quellen (Variety) (Gartner Research 2013).[5] Auf Big Data beruhende Analysen versuchen über automatisierte Datentechniken (*Data Mining*) aus umfangreichen, komplexen und nur schwach strukturierten Datensätzen anwendbare Informationen zu destillieren. Ein besonderes Spezifikum stellt die Verknüpfung von Daten aus unterschiedlichen Kontexten dar, um über sie neue, bisher unentdeckte und nicht-antizipierbare Korrelationen aufzuzeigen, Muster zu entdecken und diese Erkenntnisse für praktische Zwecke, etwa soziale Regulierung und Verhaltenssteuerung, einzusetzen (Andrejevic/Gates 2014: 186; siehe zur Frage der Kontexte insbesondere auch Nissenbaum 2010). Nimmt man diese Ziele als Maßgabe, kann man für das Sammeln und Aufbewahren von Daten auch dann Rechtfertigungen anführen, wenn zum Zeitpunkt ihrer Aufzeichnung noch kein unmittelbarer Verwendungszweck sichtbar ist.

Für die Sammlung und Auswertung großer Datenmengen sind je nach den Anlässen und Zielen unterschiedliche Begriffe verwendet worden. *Surveillance* ist David Lyon (2007a: 14) zufolge „the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction". Die Definition Lyons ist nicht akteursspezifisch, sie schließt sowohl die Überwachung durch staatliche Stellen als auch durch Privatunternehmen ein. Überwachung ist dieser Definition zufolge jedoch spezifisch in ihrer Zielstellung, geht es hier doch um die systematische, routinemäßig vorgenommene Erhebung von persönlichen Daten zu dem Zweck der Beeinflussung und Kontrolle. Kurz, sie beruht auf gezielten Interventionen, um bestimmte Informationen zu erlangen. Roger Clarkes (2016) Kunstwort *Dataveillance* meint in Abweichung von einer solchen eher klassischen Überwachung – wenn auch nicht ganz trennscharf – die Aufzeichnung der Daten von Individuen oder Gruppen über unterschiedliche digitale Plattformen hinweg. Die Sammlung und Zusammenführung der Daten geschieht ohne die oft sehr spezifische Zweckbestimmung der

[5] Big Data sind „high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making" (Gartner Research 2013).

klassischen Überwachung und ist den Datenproduzenten oft gar nicht bewusst.[6] Mayer-Schönberger und Cukier (2013: 30) haben einen weiteren Begriff eingeführt, der nicht nur die Sammlung und Verwertung von Daten umfasst, sondern auch deren Produktion. Mit *Datafication* bezeichnen sie den Prozess der Transformation sozialer Aktionen in Online-Daten, also etwa die Kommunikation und das Hinterlassen von Daten in Form von *Tweets*, darüber hinaus aber auch die Wertschaffung aus diesen Daten durch die Anbieter. Die unterschiedlichen Begriffe erfassen so verschiedene Ausschnitte dessen, was heute an Datenproduktion und -auswertung vorgenommen wird und weisen auf die Komplexität dieser Vorgänge hin. Sie beziehen sich zudem nicht allein auf staatliche Maßnahmen zur Speicherung und Auswertung von Daten, sondern auch auf die Maßnahmen anderer Einrichtungen. Der in diesem Beitrag verwendete Begriff *Überwachung* schließt diesen Begriffsverwendungen folgend auch die Sammlung, Zusammenführung und Auswertung von Massendaten durch kommerzielle Unternehmen und politische, nicht-staatliche Organisationen ein.

Die Nutzung von Big Data durch Unternehmen, Sicherheitsbehörden und politische Organisationen

Big Data werden durch Unternehmen, staatliche Institutionen, darunter auch die Sicherheitsbehörden, und politische Organisationen so umfassend und auf so vielfältige Weise genutzt, dass eine detaillierte Darstellung aller Verwendungen an dieser Stelle nicht vorgenommen werden kann. Jede der erwähnten Gruppen verfolgt spezifische Interessen und verwendet die Daten entsprechend. Bei dieser Nutzung bestehen Kooperationen und Symbiosen zwischen ihnen, aber auch deutliche Differenzen. Die Ausführungen in diesem Abschnitt sollen die komplexen Verflechtungen und Dynamiken, an denen die beschriebenen Akteursgruppen beteiligt sind, lediglich illustrieren, um im weiteren Fortgang des Beitrags die Folgen für Gesellschaft und Demokratie bewerten zu können. Sie befassen sich zudem zwar nicht ausschließlich, aber doch vorrangig mit den sozialen Medien als Datenquelle und -verwerter.

Big Data, Unternehmen und Social Media

Social Media-Plattformen wie Facebook, Internetkonzerne wie Google und Amazon, aber auch klassische Branchen wie Versicherungen, Banken und Auskunfteien sammeln Daten und nehmen allesamt Big Data-Analysen vor, um Prognosen zu treffen und das Verhalten ihrer Zielgruppen zu beeinflussen. Facebook, Google und Twitter sammeln sämtliche Daten, die ihre Nutzerinnen und Nutzer zur Verfügung stellen und werten sie vornehmlich zu dem Zweck aus, Werbung an sie individuell anzupassen. Sie haben unterschiedliche Tools entwickelt, die das Nutzerverhalten differenziert aufzeichnen und auswerten, um diese Anpassung im Sinne ihrer Werbekunden und zur eigenen Gewinnsteigerung vornehmen zu können. Sie gestalten ihr Angebot und ihren Webaufritt zudem so, dass die User möglichst lange auf ihrer

[6] „Dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons“ (Clarke 2016). Die Unterscheidung zwischen surveillance und dataveillance entspricht mit Blick auf die Folgen in etwa der Unterscheidung Monahans in *differential* und *automatic control* (siehe Monahan 2010: 97-98).

Plattform verweilen. Auch dies dient der Steigerung des Absatzes von Werbung. Das Ziel von Online-Versendern und Streamingdiensten wie Amazon ist es, die Kaufabsichten der Kunden zu prognostizieren und ihre Aufmerksamkeit durch entsprechende Offerten auf die infrage stehenden Produkte zu lenken (Turow 2007; Christl/Spiekermann 2016: 11-21; Christl 2017: 6). Beide Varianten von Internetkonzernen benötigen für ihren Geschäftserfolg also die fortlaufende Sammlung und Auswertung persönlicher Daten, so die Suchanfragen, das Surfverhalten, Äußerungen zu Vorlieben und Interessen, aber beispielsweise auch das Konsumverhalten, die Finanzsituation oder den Familienstand. Im Kern geht es diesen Konzernen darum, „durch die Dauerbeobachtung ihrer Kunden verborgene emotionale Anreize" zu setzen und auf diese Weise ihre Produkte besser zu verkaufen (Morozov 2015: 4; siehe auch Greenfield 2017).[7]

Die Daten dienen ihnen jedoch nicht allein zur gezielten Platzierung von Werbung oder der Erhöhung des Warenumsatzes, sondern werden an Dritte weiterverkauft, die sie wiederum entlang der eigenen Geschäftsinteressen kategorisieren und weiterverwenden, Banken beispielsweise in Bezug auf Kreditwürdigkeit und Kaufkraft (Becker 2017). Eine Reihe von Internetkonzernen kauft zudem selbst offline gewonnene Daten von kommerziellen Auskunfteien zu ihren Beständen hinzu. Bis zum Bekanntwerden des Geschäftsgebarens von Cambridge Analytica bestanden Kooperationen etwa zwischen Facebook und den großen Auskunfteien Acxiom, Oracle Datalogix und Transunion sowie den Marketingfirmen WPP und Experian (Krempl 2017a; Angwin et al. 2016; Chassot 2018). Auch Google versucht Online- und Offlinedaten stärker miteinander zu vernetzen und über die Anreicherung von Nutzerprofilen mit externen Daten noch genauere Prognosen und Steuerungseffekte zu erzielen. Neben der Erlangung differenzierter Profile besteht ein weiteres Ziel solcher Vernetzungen in der Prüfung, inwieweit online lancierte Anzeigen tatsächlich das Kaufverhalten beeinflussen (Christl 2017; Kleinz 2017).

Festgehalten und auswertet werden von den großen Internetkonzernen nicht nur Vorgänge wie Postings im Internet und gegebenenfalls Käufe mittels Kreditkarten, sondern über entsprechende Anwendungen auch Vorgänge wie die Eingabegeschwindigkeit über die Tastatur, die Fehlerhäufigkeit bei der Eingabe, die Lesezeit bei Tweets und vieles mehr (Oremus 2017). Mit dem *Internet der Dinge* wird sich der Trend zur Ausweitung und Fusion der Datenquellen noch weiter fortsetzen. Die Auswertung von Daten etwa von *intelligenten* Stromzählern aus den Haushalten lassen dann Rückschlüsse auf Verhaltensmuster der Stromkundinnen und -kunden zu (Wolfangel 2017). Der konventionelle Handel ist gegenwärtig bemüht, über Facebook und Google gesammelte Daten in Verbindung mit eigenen WLAN-Trackern für die Produktwerbung in seinen Warenhäusern nutzbar zu machen (Jansen 2017) und will so ebenfalls von Big Data profitieren.

Die Sammlung, Fusion und Auswertung von Nutzerdaten durch Internetkonzerne und Auskunfteien beruht auf einem so breiten Spektrum von Quellen, dass sich auch umsichtige Individuen diesen Vorgängen nicht vollständig entziehen können. So sammelt Facebook auch Daten von Personen, die nicht seine eigenen Nutzerinnen oder Nutzer sind. Wenn WhatsApp die Adressbücher auf Smartphones ausliest, werden auch die Daten solcher Personen erfasst

[7] Für Hinweise, dass die Anwendung psychologisch zugeschnittener Werbung es ermöglicht, das Verhalten großer Gruppen von Menschen zu beeinflussen siehe Matz et al. (2017).

und an Facebook übertragen, die diese Anwendung nicht nutzen. Dies geschieht im Regelfall ohne deren ausdrückliche Zustimmung (Riese 2017).[8] Auch über Schnittstellen auf Webseiten und von Apps, die nicht zu Facebook gehören, fließen Daten ohne ausdrückliche Zustimmung der Nutzerinnen und Nutzer an den Konzern und werden von ihm verwertet (Bundeskartellamt 2017). In diesen Fällen greift nicht einmal das ohnehin umstrittene Modell der *informierten Einwilligung*, mittels derer Nutzerinnen und Nutzer den softwareanbietenden Unternehmen die in den AGBs festgelegte Erhebung und Verarbeitung von persönlichen Daten gestatten.[9]

Dieser kurze Überblick bietet einen Eindruck, wie kommerzielle Firmen mittels ausgefeilter Analysetools und Querverbindungen zwischen vielen unterschiedlichen Datenquellen differenzierte Profile von Millionen von Menschen erstellen. Sie enthalten Daten zu den Vorlieben der Nutzerinnen und Nutzer, ihren weltanschaulichen Orientierungen, ihrem Konsumverhalten, ihrer Wohn- und Lebenssituation und weiteren soziodemographischen Faktoren. Die Datennetze werden immer enger und die Individuen selbst verlieren mit der Ausweitung dieser Art von Überwachung immer mehr die Kontrolle darüber, wer was über sie weiß und wozu dieses Wissen verwendet wird.

Big Data und Sicherheitsbehörden

Mit den Enthüllungen Edward Snowdens im Jahr 2013 ist deutlich geworden, dass auch die Sicherheitsbehörden vieler Staaten massenhaft Daten aus unterschiedlichsten Quellen schöpfen. Die Erhebungsorte und -methoden sowie die rechtlichen Voraussetzungen für die Sammlung und Auswertung der Daten durch diese Behörden unterscheiden sich naturgemäß von jenen für kommerzielle Unternehmen. Seit einiger Zeit zeichnet sich der Trend ab, Sicherheitsbehörden – und unter diesen insbesondere auch den Geheimdiensten – einen breiteren Zugang auch zu solchen behördlichen Datenbanken zu gewähren, die nicht zur Gefahrenabwehr angelegt worden sind. Zudem sollen einige der Großdatenbanken auf europäischer Ebene wie das Schengen Informationssystem, die Fingerabdruckdatenbank für Asylbewerber oder das Europäische Strafregisterinformationssystem zusammengeführt oder intensiver vernetzt werden. Dies soll sogenannte *Kreuztreffer* und differenziertere Verdächtigenprofile ermöglichen (European Commission 2017a).

Informationen versuchen die Sicherheitsbehörden darüber hinaus ganz wesentlich auch über den Zugriff auf Telekommunikationsdaten, einschließlich der Datenverkehre im Internet, zu erlangen. In einer ganzen Reihe von Staaten sind die Telekommunikationsanbieter per Gesetz dazu verpflichtet, die Metadaten zu Telefon- und Internetverbindungen für eine vorge-

[8] Dessen ungeachtet enthalten bestimmte Klassen von Daten aufgrund ihrer Eigenschaften stets auch Daten über andere Personen (siehe Heesen/Matzner 2015: 164).

[9] Diese auf dem Prinzip der individuellen Selbststimmung aufbauende Erlaubniskonstruktion ist aufgrund des Machtungleichgewichts zwischen den Dienste-Anbietern und den individuellen Anwendern kritisiert worden: Nur wenn sie den AGBs zustimmen, können sie die Dienste nutzen, eine andere Möglichkeit haben sie nicht. Ein Verzicht auf die Dienstleistungen kann jedoch zu erheblichen Einschränkungen im Alltag und bei der gesellschaftlichen Teilhabe führen. Zudem, so wird argumentiert, ist es den Nutzerinnen und Nutzern kaum möglich, die Folgen der Einwilligung in die Verarbeitung ihrer Daten vollständig zu überblicken, zumal sich bestimmte Verwendungsmöglichkeiten der Daten erst zu einem späteren Zeitpunkt zeigen (Hofmann/Bergemann 2017; Worms/Gusy 2012: 98).

schriebene Zeitdauer zu speichern. Der Zugriff auf die gespeicherten Daten bedarf zumeist einer richterlichen Genehmigung. Die Abschöpfung der Datenverkehre von Ausländern ist in der Regel unter weniger strengen Voraussetzungen gestattet. Geheimdienste fangen unter anderem Daten direkt an den Datenleitungen ab und nutzen eigene Analysetools zur Auswertung der gesammelten Daten. Wie von Edward Snowden an die Öffentlichkeit gebrachte Dokumente zeigen, betreiben der amerikanische Geheimdienst National Security Agency (*NSA*), die britische Government Communications Headquarters (*GCHQ*) und andere westliche Geheimdienste ein weltweit und verdachtsunabhängig operierendes System zur Datenabschöpfung. Sie sammeln und analysieren in großem Umfang die Daten der Kundinnen und Kunden von Telekommunikations- und Internetdienstleistern – darunter auch Daten von Facebook und Twitter (de Goede 2017: 25). Die Programme der NSA etwa greifen weltweit auf Glasfaser-Kabelverbindungen zu, um Daten abzufangen (*Tempora*) und zu sammeln (*Upstream*, *Quantuminsert*). Eine gezielte Auswertung erfolgt über Analysewerkzeuge wie *XKeyscore*, das mit dem *PRISM*-Programm verknüpft ist. PRISM analysiert Konsumentendaten, die über Social Media- und Cloud-Plattformen erhoben werden. Die Dienste können somit auf eine große Fülle von Daten zugreifen, die die Nutzerinnen und Nutzer von Telekommunikationsdiensten, Webseiten, sozialen Medien oder Apps hinterlassen.

Zwischen Geheimdiensten und kommerziellen Dienstleistern bestehen viele Überschneidungen. Sie beziehen sich nicht nur auf die Datenquellen, sondern auch auf die verwendeten Analysetechnologien. So werden die über das Google-Tracking von Webseiten gewonnenen Daten beispielsweise nicht nur von Google selbst ausgewertet, sondern auch von der NSA (Soltani et al. 2013). Wie weit Telekommunikations- und Internetdienstleister mit den Geheimdiensten aber tatsächlich kooperieren, ist nicht leicht erkennbar. Die großen amerikanischen Telekommunikationsfirmen, Social Media-Unternehmen und Softwarehersteller haben nach den Snowden-Enthüllungen behauptet, von der Abschöpfung der über sie abgewickelten Datenverkehre keine Kenntnis gehabt zu haben. Ein Großteil der weltweiten Glasfaserkabel aber ist für die NSA durch Sicherheitsabkommen mit privaten Unternehmen zugänglich (vgl. Lyon 2015: 144).

Auch bei den Sicherheitsbehörden spielen Big Data-Analysen bei der Auswertung der in großem Umfang erhobenen Daten eine wichtige Rolle. Zum einen dient dies dem Zweck, konkrete Straftaten aufzuklären, zum anderen aber auch, kriminelle Absichten bereits im Vorfeld erkennen zu können. Big Data-Analysen sollen solche Einstellungs- und Verhaltensmerkmale ausfindig machen, die darauf hinweisen, dass eine Straftat begangen werden könnte.[10] Es geht nun nicht mehr allein darum, konkret etwa die Identität eines Terroristen zu kennen, sondern potentielle Täter anhand von bestimmten Mustern auszumachen und *Risikoscores* zu erstellen (Ulbricht 2017: 18-19). Anhand dieser Scores kann dann beispielsweise bestimmten Personen an den Landesgrenzen die Einreise verweigert werden. Was in diese *datenbasierten Risikowerte* eingeht, ist in der Regel intransparent und aufgrund komplexer Rechenvorgänge, denen Algorithmen zugrunde liegen, rückwirkend oftmals nicht mehr zu entschlüsseln. Was als verdächtig gilt, wird so in gewisser Weise durch die Daten selbst erst algorithmisch konstruiert (Brayne 2017), sollen sie doch Zusammenhänge anzeigen, die ansonsten

[10] Siehe hierzu etwa die Homepage der von der CIA mitfinanzierten Firma Palantir, www.palantir.com.

nicht ohne weiteres erkennbar sind (Andrejevic und Gates 2014: 186). Während es Geheimdiensten vor allem darum geht, über die Auswertung von abgeschöpften Daten organisierte Straftaten, einschließlich terroristischer Anschläge, zu verhindern bzw. zu ihrer Aufklärung beizutragen, suchen Polizeibehörden gegenwärtig noch darüber hinaus nach Wegen, wie durch datengestützte frühzeitige Interventionen langfristige Verhaltensänderungen (im Sinne der Veränderung des Habitus) erreicht werden können (Clarke et al. 1997; Garland 2008). Wie bei den kommerziellen Anbietern, so entsteht damit auch auf sicherheitsbehördlicher Seite ein immer engeres Datennetz, in das eine Unzahl privater Daten eingewoben ist.

Big Data und politische Organisationen

Neben kommerziellen Unternehmen und Sicherheitsbehörden suchen auch politische Gruppierungen und Organisationen nach neuen Möglichkeiten der Verhaltensbeeinflussung mittels Big Data. Insbesondere in den Vereinigten Staaten sind auf Basis einer Vielzahl von Datenquellen, auch solcher der großen Internetfirmen, im Rahmen politischer Kampagnen Profile angelegt und zur gezielten Versendung von Botschaften zum Zweck der Mobilisierung – etwa im Rahmen von Wahlkampagnen – genutzt worden. Bennett (2015: 371) hat mit Bezug auf die USA von „voter surveillance" gesprochen, die dazu diene, Wählerinnen und Wähler in hoch umkämpften Wahlkreisen individuell ansprechen zu können. Hierzu würden sämtliche zur Verfügung stehenden Daten über die Wählerschaft beschafft und mittels ausgefeilter Data Mining- und Analysetools ausgewertet.

Nicht erst im März 2018 (Rosenberg et al. 2018), sondern bereits 2016 haben Berichte über die Tätigkeit des Unternehmens Cambridge Analytica im Rahmen des Wahlkampfs von Donald Trump Aufmerksamkeit erregt. Cambridge Analytica hat nach eigenen Angaben auf Basis von Social Media-Daten, darunter solchen von Facebook, Online-Persönlichkeitstests und von Auskunfteien hinzugekaufter Daten Millionen Profile von Wahlberechtigten angelegt, entsprechend derer diese dann, vor allem auf dem Weg der sozialen Medien, individuell angesprochen worden sind (Grassegger/Krogerus 2016). Die von Cambridge Analytica annoncierte durchschlagende – und in diesem Fall wahlentscheidende – Wirkung des von ihr angeblich verwendeten „OCEAN-Modells"[11] wird durchaus skeptisch beurteilt (Mützel 2016). Dennoch ist erkennbar, wie intensiv gegenwärtig die Bemühungen sind, Big Data auch zur politischen Beeinflussung zu nutzen. Facebook und Google spielen bei solchen Wahlkampagnen inzwischen eine zentrale Rolle. Sie bieten ihren Kunden aus der Politik ein komplettes Spektrum an digitalen Marketingtools und -techniken für den Einsatz in politischen Kampagnen. Facebook hat einen eigenen Stab für politisches Kampagnenmarketing, der seine Kundinnen und Kunden aus der Politik intensiv berät und unterstützt. Da Facebooks Datenbestände mit den Klarnamen der User verbunden sind, können diese individuell angesprochen werden, etwa nach Alter, Geschlecht, Wahlbezirk oder Interessen. Auch Google versucht an dem Markt zu

[11] „OCEAN" steht für Openness (Aufgeschlossenheit), Conscientiousness (Gewissenhaftigkeit), Extraversion (Geselligkeit), Agreeableness (Verträglichkeit) und Neuroticism (Neurotizismus). Cambridge Analytica besitzt nach eigenen Angaben Persönlichkeitsprofile von 220 Millionen Amerikanerinnen und Amerikanern, die auf diesen fünf Faktoren basieren. Ob das Modell von Cambridge Analytica im US-Wahlkampf so tatsächlich verwendet wurde, ist umstritten, siehe die Ausführungen von Hegelich (2017: 110-111). Inzwischen gibt es Hinweise, dass sich Cambridge Analytica die den Profilen zugrundeliegenden Daten auf unrechtmäßige Weise beschafft hat (Rosenberg et al. 2018).

partizipieren und bietet seine eigenen Instrumente für das politische Marketing (Chester/Montgomery 2017).

Auch in Europa sind Bemühungen zu beobachten, Big Data für politische Kampagnen im Verbund mit sozialen Medien zu nutzen. Alle größeren deutschen Parteien haben im Bundestagswahlkampf 2017 *Microtargeting* betrieben, d.h. die Wählerinnen und Wähler wurden gezielt über individualisierte Wahlwerbung angesprochen. Die Parteien konnten hierfür Werkzeuge und Daten von Facebook nutzen, die der Konzern sonst für das Ausspielen zielgenauer kommerzieller Werbung einsetzt (Hausen/Kogel 2017). Auf welchen Daten genau die Auswahl politischer Botschaften beruht hat und auf Basis welcher Überlegungen das *Microtargeting* und der Einsatz von *Dark Posts* bei solchen politischen Anzeigen, die nur bestimmten Zielpersonen zugespielt werden und für andere nicht sichtbar sind, vorgenommen worden ist, blieb dabei weitgehend ungeklärt, da die Parteien sich bis auf wenige Ausnahmen geweigert haben, entsprechende Informationen herauszugeben.[12]

Ein immer dichteres Datennetz

Der illustrative Überblick zeigt, dass Unternehmen, Sicherheitsbehörden und politische Organisationen in großen Mengen Daten von Individuen sammeln und auswerten, um über die Erkennung von Mustern und Profilen Steuerungseffekte zu erzielen (McCulloch/Wilson 2007; Holzer 2017). Internetfirmen und Social Media-Plattformen verarbeiten hierzu die Daten ihrer Kundinnen und Kunden, greifen aber etwa über Adressbücher auf Smartphones und Analysetools auf Webseiten auch auf Daten von Nichtkunden zu. Zudem kaufen sie Daten von Dritten, wie etwa den großen Auskunfteien, hinzu. Unternehmen klassischer Branchen wie etwa Banken erwerben auf der anderen Seite wiederum die Daten von Internetfirmen und werten sie entsprechend ihrer Geschäftszwecke aus. Auch die Sicherheitsbehörden, unter ihnen die Geheimdienste, sammeln Daten aus den sozialen Medien und analysieren sie in der Hauptsache zur Gefahrenabwehr und zur Strafverfolgung. Politische Organisationen nutzen in massivem Ausmaß Daten für politische Werbekampagnen. Sie greifen hierzu auf die sozialen Medien gleichzeitig als Datenquelle und als Kommunikationsmedium zurück.

Auch wenn die Datennetze, in die die Individuen auf diese Weise eingebunden sind, eng geknüpft sind, kann aufgrund der unterschiedlichen Interessen der Beteiligten nicht von einer spannungsfreien Kooperation oder sogar Verschwörung zwischen ihnen ausgegangen werden (hierzu differenziert: Stalder 2017: 234-237). So haben sich etwa Telekommunikationsanbieter und Internetprovider immer wieder gegen die Vorratsspeicherung positioniert, die Herausgabe von Daten an Sicherheitsbehörden verweigert und ihren Kunden Verschlüsselungstechnologien angeboten. Fügt man alles zu einem Gesamtbild zusammen, so scheint es dennoch angemessen, von einem „Überwachungskomplex“ im Sinne einer fluiden funktionalen Verflechtung unterschiedlicher Akteure, Prozesse und Arrangements zu sprechen (Lyon 2015; Hayes 2012).[13]

[12] Es gab allerdings Bemühungen unabhängiger Organisationen und einiger Zeitungen, dieser Intransparenz entgegenzuwirken (Angwin/Larson 2017).

[13] Haggerty/Ericson (2000) und Wood (2013) reden von einer „surveillant assemblage“.

Demokratietheoretische Kriterien: Politische Willensbildung und Öffentlichkeit

Die hier im Überblick dargestellten Entwicklungen im Bereich Big Data sind auf komplexe Weise miteinander verschlungen, vielgestaltig, dynamisch und noch so neu, dass sich ihre genauen Konturen vorerst nur schwer bestimmen lassen. Dennoch soll der Versuch unternommen werden, einige ihrer Folgen mit Blick auf Demokratie und Gesellschaft aufzuzeigen. Der Schwerpunkt der Überlegungen liegt dabei auf Big Data im Zusammenhang mit den sozialen Medien.

Um etwas zu den Folgen von Big Data für Demokratie und Gesellschaft aussagen zu können, bedarf es geeigneter Bewertungskriterien. Es liegt nahe, sie demokratietheoretisch herzuleiten und auf die gegenwärtigen Verhältnisse anzuwenden. Nun gibt es aber eine ganze Reihe unterschiedlicher Demokratietheorien. Sie fassen ihren Gegenstand jeweils anders und führen abweichende Kriterien dafür ins Feld, was eine Demokratie ausmacht und welche Bedingungen zu ihrem Funktionieren gegeben sein müssen. An dieser Stelle soll lediglich ein auf demokratietheoretische Kernannahmen reduziertes Kriterienbündel herangezogen werden.

So unterschiedlich moderne Demokratietheorien inhaltlich auch ausgerichtet sein mögen, sie halten funktionierende demokratische Gemeinwesen ohne die Möglichkeit sowohl der ungehinderten Formung eigener Präferenzen als auch der Verbreitung der eigenen Meinung nicht für vorstellbar. Hierzu bedarf es umfassender Informations- und Partizipationsrechte für die Bürgerinnen und Bürger. Ob dabei von Individuen mit vorpolitisch existierenden Präferenzen und fixen Identitäten ausgegangen wird, die durch geeignete Institutionen und in politisch bindenden Entscheidungen ihre politisch-gesellschaftliche Repräsentanz finden, wie dies die liberalen Demokratietheorien betonen (Locke 1977 [1689], Mill 2011 [1859], Dahl 1989, Rawls 2003), oder aber Identitäten sich über soziale Vermittlung formen und Präferenzen sich in einem offen und rational geführten Diskurs bilden, wie beispielsweise republikanische und Theorien deliberativer Demokratie hervorheben (Dryzek 1990, Habermas 1992), ist in diesem Zusammenhang nicht entscheidend. Grundlegend ist vielmehr das Vorhandensein persönlicher Autonomie als Grundlage eines offenen und rationalen Entscheidungsfindungsprozesses, zu dem prinzipiell alle Bürgerinnen und Bürger in gleichberechtigter Art und Weise beitragen können, sofern sie dies wollen (Buchstein 2016: 31-33). Eigene Wertüberzeugungen, Vorstellungen und Interessen autonom entwickeln und diese selbstbestimmt in einen öffentlichen Prozess des Meinungsaustausches einzubringen zu können, sind demnach ein Wesensbestandteil der Demokratie. Dies trifft selbst dann zu, wenn ein breites Konzept individueller Autonomie zugrunde gelegt wird, welches eine solche Autonomie immer auch als Ergebnis intersubjektiver Praxis, als Resultat sozialer Anerkennungsbeziehungen, sieht (Seubert 2012: 101; Becker/Seubert 2016; siehe auch Cohen 2013).

Als konstitutiv für die Demokratie gilt gleichzeitig, dass die Individuen und sozialen Gruppen die Kontrolle über das behalten, was von ihren Meinungen und Ansichten an die Öffentlichkeit gelangen soll und was nicht. Die Bürgerinnen und Bürger müssen darauf vertrauen können, dass das, was in bestimmten sozialen Sphären und den dazugehörigen privaten Kommunikationsräumen (Becker/Seubert 2016: 75; Rule 2012: 65) geäußert und getan wird, nicht „registriert und später zur Profilbildung oder zur Vorhersage von Einstellungen und Verhalten genutzt wird“ (Roßnagel/Nebel 2015: 458). Abwehr- und Partizipationsrechte

spielen hier zusammen, denn die Möglichkeit, frei und selbstbestimmt an diesen Prozessen teilnehmen zu können, setzt geschützte Räume voraus, sowohl den der geschützten Privatheit, in dem sich das Selbst bilden kann, als auch den in seiner Offenheit und deliberativen Qualität geschützten öffentlichen Raum. Beide bieten den Bürgerinnen und Bürgern Schutz vor Willkür. Das Recht auf Privatheit soll dem Wissen des Staates über seine Bevölkerung Grenzen setzen, um ihre Freiheit zu wahren und ihre Rolle als Mitglied der politischen Gemeinschaft selbst bestimmen zu können. Der beteiligungsoffene und Widerspruch ermöglichende öffentliche Raum soll einen Missbrauch der aus dem Gewaltmonopol resultierenden Übermacht des Staates verhindern.

Den Medien – in der Vergangenheit waren dies in der Hauptsache Zeitungen, Zeitschriften, Radio und Fernsehen – wird dabei eine besondere Funktion als Informationsmittler sowohl für die Regierten als auch die Regierenden zugeschrieben. Sie bieten ihnen öffentliche Foren zur Begründung und Legitimierung ihrer Forderungen und Entscheidungen sowie zu ihrer Kritik. Über die Medien vermittelt findet dieser Funktionszuschreibung zufolge eine öffentliche Auseinandersetzung statt, die trotz aller Gegensätze an einem gemeinschaftlich gebildeten, am Gemeinwohl orientierten Diskursergebnis ausgerichtet bleibt (Richter 2015: 47).

Die Folgen der intensiven Sammlung, Analyse und Nutzung privater Daten für die Herausbildung eigener Wertüberzeugungen und die Möglichkeit, diese Überzeugungen in der Öffentlichkeit zu vertreten, werden im Folgenden diskutiert.

Big Data und die Folgen: Anpassung, Big Nudging und Manipulation?

Unternehmen, Sicherheitsbehörden und politische Organisationen verfolgen, wie gezeigt, unterschiedliche, teils sich ausschließende Interessen und manche Konsequenz aus dieser Entwicklung zeichnet sich erst ab oder ist umstritten. Dennoch lässt sich ein Trend durchaus identifizieren, nämlich der, dass den Bürgerinnen und Bürgern immer stärker die Kontrolle darüber entgleitet, wer über ihre Daten verfügt, wer sie weitergibt und was mit diesen Daten geschieht. Für einen bestimmten Zweck erhobene Daten werden zunehmend für weitere Zwecke und im Zusammenhang mit anderen Daten genutzt. Das Kerninteresse von Big Data-Analysen besteht ja gerade darin, über die Entdeckung von Korrelationen und Mustern aus einer möglichst großen Zahl von Daten aus unterschiedlichsten Quellen Vorhersagen über das Verhalten von Individuen und Gruppen zu ermöglichen oder zu verbessern und in Steuerungskonzepte und -prozesse umzusetzen. Kurz: Eine der bedeutsamsten Folgen der gegenwärtigen Entwicklungen, an denen Unternehmen, Sicherheitsbehörden und politische Organisationen in der im ersten Teil beschriebenen Weise beteiligt sind, ist der zunehmende Kontrollverlust des Individuums über die eigenen Daten und damit verbunden die schrittweise Auflösung des Privaten.

Mit Blick auf die grundsätzlichen Funktionsbedingungen von Demokratien ist in diesem Zusammenhang immer wieder darauf hingewiesen worden, dass bereits die Ungewissheit darüber, was andere an Privatem über ein Individuum oder eine Gruppe in Erfahrung bringen können, das Vertrauen darin untergräbt, frei und selbstbestimmt am öffentlichen Leben partizipieren und politische und gesellschaftliche Missstände kritisieren zu können (Seubert 2012: 104). Wenn ökonomische, staatliche und politische Akteure Daten in einer Weise sammeln

und verknüpfen, durch die die Kontrolle des Individuums über sie verloren geht, gefährdet dies dieser Argumentation zufolge die Demokratie als „freiheitlich-egalitäre Kommunikationspraxis“ (Becker/Seubert 2016: 76), in der alle Mitglieder über ihre Kommunikationsakte selbst bestimmen und über die sie die bestehenden Verhältnisse kritisieren können. Das Private kann dann nicht länger „als Ressource und Gegenmodell zu (aus subjektiver Perspektive) präformierten und fremdbestimmten Handlungsräumen“ dienen (Heesen/Matzner 2015: 159). Nicht erst der konkrete Missbrauch von privaten Daten, sondern bereits das Unwissen darüber, wer sich Zugang zu diesen Daten verschaffen kann, birgt die Gefahr einer vorauseilenden Anpassung an das als *normal* erachtete (hierzu ausführlich: Hempel et al. 2011): Die Menschen unterlassen dann Handlungen oder Äußerungen, von denen sie annehmen, dass sie sie verdächtig machen oder als unzuverlässig erscheinen lassen könnten (Mitrou 2010: 138).[14]

Big Data-Analysen in der aufgezeigten Form werden deshalb in zweifacher Hinsicht als folgenreich erachtet: sie wirken sowohl *normbildend* als auch *verhaltensbestimmend* (Roßnagel/Nebel 2015: 456). *Normbildend* bedeutet, dass sie über die analysierten Daten vorgeben, was als normales Verhalten gelten kann. Sie bilden den Standard, anhand dessen Abweichungen überhaupt erst definierbar und entdeckbar werden. Als Folge solcher Vorgaben droht der Verlust an „intellektueller Diversität und exzentrischer Individualität“ (Richards 2013: 1946), die für eine lebendige, funktionsfähige und sich stets selbst erneuernde Gesellschaft in einer Demokratie notwendig sind. Mit *verhaltensbestimmend* ist die Anpassung des Verhaltens von Personen an den so vorgegebenen Standard gemeint, sei es, um für sich selbst Vorteile zu erlangen, sei es, um nicht durch abweichendes Verhalten auffällig zu werden (Krasmann 2011; Bauman/Lyon 2013).

Beispiele aus China zeigen, wie intensiv staatliche auf Big Data setzende Überwachung zur Kontrolle und Normierung des Verhaltens der Bevölkerung schon jetzt verfolgt wird: Dort sind bereits an vierzig Standorten Experimente im Gange, die darauf zielen, die *soziale Vertrauenswürdigkeit* der Bürgerinnen und Bürger über ein Sozialkreditpunktesystem zu ermitteln. Eine zentrale Datenbank, über die das Verhalten von Individuen, Unternehmen und Institutionen mittels Big Data und Künstlicher Intelligenz erfasst und beurteilt werden kann, ist im Aufbau und soll bis 2020 fertiggestellt werden. Wer sich nicht den gesellschaftlichen und politischen Ordnungsvorstellungen der Behörden unterwirft, wird von dem System entsprechend eingestuft, soziale Nachteile, etwa eine ausbleibende Beförderung, drohen. Minuspunkte gibt es für das Einreichen regierungskritischer Petitionen aber auch bereits für das Über-

[14] Auch das deutsche Bundesverfassungsgericht hat diese Verbindung in seinem Volkszählungsurteil von 1983 hergestellt. Demnach bedarf ein freiheitlich demokratisches Gemeinwesen der selbstbestimmten Mitwirkung seiner Bürgerinnen und Bürger, die nicht durch einen Anpassungszwang aufgrund Unsicherheiten hinsichtlich des Verbleibs und der Nutzung ihrer Daten beschränkt werden darf: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“ (Bundesverfassungsgericht 1983, Randnummer 172).

queren einer roten Ampel (Ankenbrand 2017; Bandurski 2017; Dorloff 2017). Bestimmte Vorstellungen der chinesischen Regierung über *funktionierende* Gesellschaften sollen auf diese Weise durchgesetzt, nicht gewünschte soziale (und politische) Verhaltensweisen unterdrückt werden.

In liberalen Demokratien ist eine solche direkte Verhaltenssteuerung sicher sehr viel schwieriger umzusetzen als in China, aber auch für diese gilt: je mehr Daten zur Verfügung stehen, desto lückenloser können Mechanismen der Verhaltenssteuerung greifen (instruktiv hierzu Lobe 2017). Nun könnte eingewandt werden, dass es schon seit langem nicht nur Beeinflussungen von Konsumenten, sondern auch von Wählerinnen und Wählern und die Überwachung durch Sicherheitsbehörden gibt. Dem ist grundsätzlich zuzustimmen, aber die Detailliertheit und Tiefe des Wissens über die Individuen durch die allgegenwärtige Sammlung und Auswertung elektronischer Daten ist doch ohne Vorbild. Auf Big Data-Analysen beruhende Beeinflussungskonzepte haben damit ein weit größeres Potential als das bekannte und umstrittene Konzept des *nudging*, welches Verhalten durch das geschickte Arrangement von Auswahlmöglichkeiten in eine gewünschte (als *vernünftig* erachtete) Richtung lenken will (Thaler/Sunstein 2014). Es ist deshalb sinnvoll, zwischen einem solchen allgemeineren *social shaping* in Form des *nudging* und auf die Verwendung von Big Data setzende Versuche spezifischerer Verhaltensbeeinflussung zu unterscheiden. Um diesen Unterschied auch begrifflich zu erfassen, hat Helbing (2015) für die letztgenannte Praxis den Begriff *Big Nudging* vorgeschlagen, Yeung (2017) spricht in diesem Zusammenhang von *Hypernudge*. Mögliche Anwendungsfelder für diese Art der Beeinflussung gibt es unzählige, von der Gesundheitsvorsorge bis zur Radikalisierungsprävention. Genutzt wird in einigen dieser Felder – wie gezeigt – auch der Datenschatz der sozialen Medien. Demokratietheoretisch relevant sind solche, auf Big Data gestützten Beeinflussungsversuche, weil sie in einem Spannungsverhältnis zu dem Kriterium der autonomen Herausbildung eigener Wertüberzeugungen im Schutze der Privatheit stehen.

Eine besondere Rolle in diesem Spannungsverhältnis nehmen die sozialen Medien selbst ein, denn die von ihnen erhobenen, mittels Big Data-Analysen strukturierten und an die User verteilten Daten machen eine subtile Gestaltung der Informationsumgebung bis auf die Ebene des Individuums hinunter möglich. Die Social Media-Anbieter folgen dabei zuerst ihren eigenen Geschäftsinteressen, also dem Verkauf von Werbung.

Wenn man nun genauer nach der Bedeutung der nach ihren eigenen Logiken funktionierenden sozialen Medien für den politischen Prozess in Demokratien fragt, sind mit Blick auf Meinungsbildung und Öffentlichkeit zunächst zwei Einschränkungen zu machen. Zum einen ist darauf zu verweisen, dass sie bei weitem nicht die einzige – und in vielen Gesellschaften auch nicht die wichtigste – Quelle für politische Informationen bilden. Untersuchungen (KANTAR TNS 2017; Schmidt et al. 2017) zum Informationsverhalten der Bevölkerung in verschiedenen westlichen Demokratien haben gezeigt, dass in den meisten von ihnen eine deutliche Mehrheit noch immer konventionelle Medienquellen wie Fernsehsendungen und Zeitungsberichte zur Informationsgewinnung heranzieht. Die Nutzung von sozialen Medien zu diesem Zweck – mit weitem Vorsprung vor YouTube, WhatsApp und Twitter rangiert dabei Facebook – ist deutlich geringer. Sie ist in vielen Ländern über die Jahre allerdings angestiegen und insbesondere bei jüngeren Menschen weit verbreitet. Laut der Mediengewich-

tungsstudie der Landesmedienanstalten hat das Internet in der Altersgruppe der 14- bis 29-Jährigen mit 51,9 Prozent bereits erheblich mehr Einfluss für die Meinungsbildung als das Fernsehen mit 19,2 Prozent (KANTAR TNS 2017). Allerdings ist die Nutzung von sozialen Medien zu Zwecken der Information im Zeitraum von 2016 bis 2017 in vielen Staaten leicht zurückgegangen, was auf eine gewisse Sättigung hindeutet (Reuters 2017; Hölig/Hasebrink 2017). Die zweite Einschränkung bezieht sich auf die Frage der Fragmentierung der politischen Öffentlichkeit durch die sozialen Medien. Hier ist festzuhalten, dass die Existenz von Teilöffentlichkeiten, an denen nicht alle Mitglieder einer Gesellschaft teilnehmen, nichts grundsätzlich Neues ist.[15] Auch die weiter oben dargestellte idealtypische Funktionszuschreibung für die Medien in Demokratien und die von ihnen hergestellte Öffentlichkeit ist bereits seit längerem insbesondere von Vertreterinnen und Vertretern postdemokratischer Positionen mit Hinweis auf eine *Neoliberalisierung* und *Elitisierung* der Medienberichterstattung problematisiert worden (Ritzi 2014: 257).

Es gibt bei den sozialen Medien insbesondere im Vergleich zu den klassischen Medien hinsichtlich der Meinungsbildung im öffentlichen Raum und der Informationsumgebung aber doch einen wichtigen Unterschied: Die Verteilung von Informationen erfolgt hier nicht entlang inhaltlicher Relevanz, die aus journalistischen Kriterien gewonnen wird, sondern entlang des individuell *möglicherweise Interessanten*, welches auf Basis des vorherigen Nutzerverhaltens der Individuen ermittelt wird (Lischka/Stöcker 2017: 22). Die algorithmisch bestimmten Informationsflüsse adressieren die Nutzerinnen und Nutzer dabei „nicht als politische Bürger, sondern als Datenquelle, deren Präsenz auf der Plattform gehalten werden soll, um fortlaufend aktuelle Informationen über unser Interaktionsverhalten zu gewinnen“ (Hofmann 2017: 14). Algorithmische Prozesse bestimmten für einen Großteil der Nutzerinnen und Nutzer sozialer Medien also, wie und mit welchen Nachrichtenangeboten sie in der digitalen Sphäre versorgt werden. Sie gestalten den gesellschaftlichen Diskurs mit, indem sie „Mitteilungen priorisieren und so die Öffentlichkeit strukturieren“ (Lischka/Stöcker 2017: 6). Kurz: Jeder User bekommt nur das zu sehen, was er sehen soll und zwar auf Basis dessen, was man über ihn weiß. Dies ist den Nutzerinnen und Nutzern oft nicht bewusst und Prozesse hinter der Gestaltung ihrer Informationsumgebung sind für sie auch kaum nachvollziehbar. Eine transparente Kommunikation, die als konstitutiv für den öffentlichen Raum und die demokratische Meinungsbildung gilt, ist damit grundsätzlich nicht gegeben (Calhoun 1993; Gerhards/Schäfer 2010; Cohen 2013: 1913).

Bei politischen Kampagnen, die über soziale Medien geführt werden, stellt sich das Problem des Zuschnitts der Informationsumgebung auf Basis von Big Data besonders scharf. Hier geht es nicht um die Gestaltung der Informationsumgebung der Nutzerinnen und Nutzer gemäß den monetären Interessen der sozialen Medien selbst, sondern gemäß den politischen Interessen von Auftraggebern im Rahmen von Wahlkampagnen. Mit Blick auf demokratische Willensbildungsprozesse sind hier zwei Fragen auseinanderzuhalten: zum einen, ob derartige auf Big Data gestützte Beeinflussungsversuche – unabhängig vom tatsächlichen Erfolg – aus demokratietheoretischer Perspektive statthaft sind, zum anderen, ob sie gegenwärtig bereits so wirksam sind, dass durch sie Wahlausgänge entscheidend verändert werden können.

[15] Heesen und Matzner (2015: 153-154) etwa unterscheiden zwischen episodischen Begegnungen in der Öffentlichkeit, Versammlungsöffentlichkeiten, Massenmedienöffentlichkeiten und komplexen Öffentlichkeiten durch digitale Techniken.

Als unstatthaft müssen sie den gängigen Demokratietheorien zufolge dann gelten, wenn durch ihr Wirken die Transparenz und Offenheit des demokratischen Willensbildungsprozesses nachhaltig gefährdet wird. Hierzu gibt es gegenwärtig kein einheitliches Urteil. Während auf der einen Seite befürchtet wird, dass eine disaggregierende Informationsverteilung bei Kampagnen im Vorfeld von Wahlen Standards gleicher Teilhabe am politischen Prozess auflöst (Haggerty/Samatas 2010: 6), gibt es auf der anderen Stimmen, die solche Strategien als besondere, demokratiestärkende Aufmerksamkeit der Parteien für ihre Wählerinnen und Wähler interpretieren und die sie lediglich als Fortschreibung einer seit langem gepflegten Ansprache an die Wählerschaft verstehen, die zum politischen Wettbewerb dazugehört (Bedford-Strohm 2016; Kreiss 2017). Es sind ferner Stimmen vertreten, die betonen, dass es durch *Dark Posts* gelingen könnte, gerade solche Nutzerinnen und Nutzer anzusprechen, die politisch einem anderen Lager zuzuordnen sind und hierdurch etwaige Echokammern zu überwinden (Papakyriakopoulos et al. 2017: 334).[16]

Auch was die Frage der tatsächlichen Wirkung von Strategien wie denen des *Microtargetings* angeht, also ob sie bereits signifikante Beeinflussungen von Wahlergebnissen möglich gemacht haben, herrscht in der bisherigen Forschung keine Übereinstimmung. Es überwiegt insgesamt deutliche Zurückhaltung. Demnach gilt es zu berücksichtigen, dass die Wirksamkeit von Beeinflussungsstrategien von einem ganzen Bündel an Faktoren abhängig ist, so etwa von bereits vorhandenen politischen Spaltungen in einer Gesellschaft (Überblick bei Chen/Potenza 2018; Hersh 2015).

Ungeachtet der unterschiedlichen Ansichten hinsichtlich der Legitimität und Wirksamkeit politischer Kampagnen mittels sozialer Medien ist an dieser Stelle noch einmal festzuhalten, dass es einen deutlichen Einschnitt in einen offenen demokratischen Willensbildungsprozess darstellt, wenn Wählerinnen und Wählern etwa über Facebook personalisierte Wahlwerbung zugespielt wird, dies auf Basis des vorherigen Nutzerverhaltens der Angesprochenen geschieht und die Auswahlkriterien für die Botschaften ungeklärt bleiben (Trinkwalder 2017). Es entsteht auf diese Weise das Problem der Intransparenz, der Fragmentierung des öffentlichen Raumes und eines kaum zu überprüfenden Chamäleon-Verhaltens von Politikerinnen und Politikern, die den Wählerinnen und Wählern je nach deren Profil genau jeweils das versprechen, was sie vermeintlich hören wollen. Die Folgen für den politischen Diskurs durch die Verwendung von Dark Posts hat Dachwitz so beschrieben:

> *Wahlplakate, Radio- und Fernsehspots konnten von allen BürgerInnen und auch von der politischen Konkurrenz rezipiert werden. Damit waren die eigenen Botschaften für alle vergleich- und vor allem anfechtbar. Widersprüchliche Versprechen an unterschiedliche Gruppen konnten entlarvt und öffentlich diskutiert werden. Andere politische Akteure konnten widersprechen und auf dieser Grundlage einen politischen Diskurs führen* (Dachwitz 2017).

Wenn auch die gezielte Verbreitung von Wahlwerbung über die sozialen Medien in Europa noch nicht das Ausmaß wie in den USA erreicht hat, wo die Datenschutzbestimmungen deutlich mehr erlauben, so sind auch die hier zu beobachtenden Entwicklungen mit Blick auf die

[16] Eine Echokammer kann verstanden werden als „an isolated space on the web, where the ideas being exchanged essentially just confirm one another" (Quattrociocchi 2016).

Transparenz des politischen Wettbewerbs keineswegs zu vernachlässigen oder wegzudiskutieren.[17]

Die „computational politics" (Tufekci 2014), welche politische Kommunikation in zunehmend personalisierte, private Transaktionen verwandeln und damit den Raum, in dem Öffentlichkeit stattfindet, grundlegend umwandeln, haben noch weitere Folgen. Sie tragen auf komplexe Weise dazu bei, dass sich bereits vorhandene gesellschaftliche Polarisierungen verstärken.

In den USA und Europa werden über die sozialen Medien in großem Umfang Äußerungen verbreitet, die sich vehement gegen die jeweilige Regierungspolitik, Mainstreammeinungen und -medien richten. Sie werden vielfach *geliked* oder geteilt. Zu den gegenwärtig beobachtbaren Polarisierungen haben sicher realweltliche Ereignisse beigetragen, in Europa etwa die massenhaften Fluchtbewegungen. So haben sich Aufrufe von einzelnen Individuen und politischen Gruppierungen zur Ausgrenzung von Minderheiten und Forderungen nach internationaler Abgrenzung gemehrt, etwa nach einem Austritt aus internationalen und regionalen Organisationen oder nach der Abschottung der eigenen Wirtschaft.

Es mag zwar auf den ersten Blick beruhigen, dass gegenwärtig keine Verhältnisse beobachtbar sind, in denen die Bürgerinnen und Bürger lediglich eine schweigende und apathische Rolle spielen und in denen die herrschenden (neoliberal orientierten) Eliten die Demokratie – bei gleichzeitiger Unversehrtheit der institutionellen Ordnung – zu einer reinen Inszenierung degradiert haben (Crouch 2008).[18] Von einem *naturwüchsigen* Dissens *von unten* – das macht den Sachverhalt so überaus komplex – kann man aber auch nicht so ohne weiteres sprechen. Mehrere Aspekte spielen hier ineinander.

Zwar können individuell motivierte Beiträge in den sozialen Medien erhebliche Resonanz finden (Allcott/Gentzkow 2017), was als individuelle Meinungsäußerung daherkommt, kann aber auch auf organisierte Gruppierungen zurückgehen, die sich die durch Algorithmen gesteuerte Informationsverbreitung und die mit ihnen verbundenen Verstärkereffekte über lancierte *Computerpropaganda* zunutze zu machen versuchen. Durch sie sollen Diskussionen manipuliert, der politische Gegner demobilisiert und Unterstützung für die eigene Position auf Twitter, Facebook oder Instagram simuliert werden (Neudert 2017).[19] Diese Gruppierungen sind nicht mit Billigung der Social Media-Betreiber am Werk, wie dies im Falle direkter Wahlwerbung durch Parteien der Fall ist, sie agieren vielmehr ohne deren Wissen. Vermutet werden hinter solcher Propaganda Geheimdienste, auf eigene Faust vorgehende politische Aktivisten oder Hacker. Eine Studie des Internet-Instituts der Universität Oxford hat gezeigt, dass in der jüngsten Vergangenheit *Social Bots* bei der Verbreitung entsprechender Inhalte eine wichtige Rolle eingenommen haben (Woolley/Howard 2017, siehe auch Krempl 2017b). *Social Bots*, die zu einem guten Teil Falschmeldungen enthalten, werden automatisch generiert und täuschen in Bezug auf bestimmte Meldungen bzw. Tweets eine größere Verbreitung

[17] Simon Hegelich von der Technischen Universität München und seine Mitarbeiterinnen und Mitarbeiter konnten auch für Deutschland zeigen, dass es möglich ist ohne Verletzung von Datenschutzbestimmungen aus Facebook Daten zu extrahieren und damit Microtargeting zu betreiben (Papakyriakopoulos et al. 2017).

[18] Siehe zu verschiedenen Varianten der Postdemokratie Ritzi (2014).

[19] Computational propaganda bezieht sich Neudert (2017: 4) zufolge auf „autonomous scripts and algorithms tasked with the manipulation of public opinion online".

und damit eine größere Popularität vor, als tatsächlich durch reale Nutzerinnen und Nutzer gegeben. Auch sie sollen Aufmerksamkeitstrends für bestimmte Themen steigern, Unbehagen hervorrufen, Unsicherheit verbreiten und die Ansichten politischer Gegner desavouieren (Nimmo/Bajoran 2014). Bots nutzen die algorithmisch gesteuerte Verteilung von Inhalten in den sozialen Medien geschickt aus; es gibt Hinweise dafür, dass die durch Bots hervorgerufenen Verzerrungseffekte durch die algorithmische Relevanzermittlung noch zusätzlich verstärkt werden (siehe hierzu Hegelich 2016; Kühl 2017; Stöcker 2017). Die Aufdeckung und Kontrolle solcher organisierten Beeinflussungsstrategien hat sich als überaus schwierig erwiesen (Weedon et al. 2017; Stamos 2017; Dwoskin et al. 2017; US Senate 2017).

Selbst wenn die sozialen Medien zu den beschriebenen politischen Zwecken *gekapert* werden, ist stets im Blick zu behalten, dass die Social Media-Anbieter die Verbreitung der User-Mitteilungen weiter ihren Geschäftsinteressen gemäß steuern und damit noch immer „die Kontrolle über den Informationsfluss nicht bei den Produzenten, sondern den Betreibern der sozialen Netzwerke liegt“ (Hofmann 2017: 14). Die Informationen sind also nach wie vor *kuratiert* (Lischka/Stöcker 2017; Kaiser/Rauchfleisch 2017) und zumindest bei der Verstärkung bereits vorhandener Polarisierungen müssen die Anbieter sich aufgrund ihrer gewinnorientierten algorithmengesteuerten Verteilung von Informationen und der damit verbundenen Effekte – auch über Bots – einen Anteil zurechnen lassen (Lischka/Stöcker 2017). Untersuchungen zeigen, dass Inhalte, die ungewöhnlich sind, aufgrund der Verteilungsmechanismen in den sozialen Medien mehr Reichweite in den Netzwerken erlangen. Zu ihnen zählen insbesondere auch solche, die polarisieren sowie vielerlei Falschmeldungen. Die Geschäftsinteressen der sozialen Medien führen dazu, dass sie gerade solche Beiträge stärker bewerben, um die Nutzerinnen und Nutzer weiter auf der Social Media-Plattform zu halten (Vosoughi et al. 2018).

Der Befund zu diesen Entwicklungen ist uneinheitlich: Interpretationen, die die Beeinflussungsmacht ökonomischer, sicherheitsbehördlicher und politischer Eliten hervorheben und die darauf hinweisen, dass die Online-Medien ihren Nutzerinnen und Nutzern die neu verliehenen Beteiligungsmöglichkeiten „jederzeit wieder entziehen können“ (Stalder 2017: 230), steht eine merkbare, andauernde Polarisierung in eben diesen Medien gegenüber. Die sozialen Medien haben mit ihrer Gewinnorientierung selbst zu den Verschärfungen der Polarisierungen beigetragen, wenn ihnen einige ihrer Auswüchse momentan auch selbst über den Kopf zu wachsen scheinen. Im September 2017 hat Facebook bekannt gegeben, dass im Vorfeld der amerikanischen Präsidentschaftswahlen versucht worden sei, über die Schaltung von Anzeigen in dem sozialen Medium gesellschaftliche Spaltungen in den USA (mit besonderem Schwerpunkt auf der Ostküste) voranzutreiben, etwa bei Themen wie Einwanderung und Waffenbesitz (Stamos 2017). Die Regierungen demokratischer Staaten versuchen selbst immer stärker reglementierend in die Prozeduren der sozialen Medien einzugreifen. Gegenwärtig konzentrieren sich ihre Bemühungen vor allem auf Gewaltaufrufe, Hetz- oder Hasskommentare in den sozialen Medien. Sie sollen durch Upload-Filter unterbunden oder durch die

Anbieter sozialer Medien nach entsprechenden Hinweisen selbst entfernt werden.[20] Mit Blick auf die Meinungsfreiheit ist dies heikel, es bleibt aber zu berücksichtigen, dass auch ohne solche Reglementierungen das Problem der Intransparenz und Fragmentierung der Öffentlichkeit bleibt. In den sozialen Medien sind die Bedingungen für eine autonome Herausbildung eigener Wertüberzeugungen im Schutze der Privatheit sowie für die Möglichkeit, diese anschließend selbstbestimmt in einen öffentlichen Prozess des Meinungsaustausches einzubringen stets durch Gewinnabsichten beschränkt.

Kein einfaches Fazit

Was die hier in Umrissen dargestellten Auswirkungen von Big Data für die Zukunft politischer Willensbildung in Demokratien bedeuten, ist noch schwer genau zu fassen und in seiner gesellschaftlichen und politischen Wirkung über eine längere Zeitstrecke kaum zuverlässig abzuschätzen. Es ergibt sich insgesamt ein komplexes Gebilde aus Überwachung, technisch gesteuerten Informationsprozessen und individueller Sorglosigkeit bei der Datenabgabe. Kennzeichen des Überwachungskomplexes sind eine schrittweise Auflösung von Privatheit durch die Verwendung von Big Data und die Intransparenz der in ihm ablaufenden Prozesse. Zusammen mit der zunehmenden Fragmentierung politischer Öffentlichkeit sind hier aus demokratietheoretischer Sicht gleich drei Problemstellen angesprochen.

Insbesondere in den sozialen Medien bilden sich fragmentierte, konkurrierende Öffentlichkeiten, die, wenn überhaupt, dann als Antipoden aufeinander Bezug nehmen (Diener 2017) und ein über lange Jahre als stabil betrachteter gesellschaftlicher Grundkonsens scheint politischen Polarisierungen Platz zu machen. Zur Erfassung des Gesamtbildes sind nicht nur die Überwachungspraktiken durch Unternehmen und Sicherheitsbehörden und die gezielte Verbreitung von Wahlwerbung durch politische Organisationen in den Blick zu nehmen, sondern auch die Mitteilungen der vielen Nutzerinnen und Nutzer sozialer Medien selbst, unter die sich zudem nur schwer identifizierbare organisierte Akteure mischen, sowie darüber hinaus die spezifische Art und Weise, wie die Daten und Mitteilungen der User durch die sozialen Medien in ihren Netzwerken verteilt werden. Am Beispiel des Zusammenwirkens von Facebook und Cambridge Analytica hat sich gezeigt, wie aus reinem Profitstreben vorgenommene Big Data-Analysen zu politischen Zwecken genutzt werden können. Politische *Propaganda* ist zwar kein neues Thema, durch die datengestützten Techniken zur schnellen und auf individuelle Einstellungen zugeschnittenen Verbreitung von Nachrichten hat sie inzwischen dennoch eine neue Dimension gewonnen.

Es bleibt eine der Aufgaben sozialwissenschaftlicher Forschung, die mit Big Data-Analysen verbundenen Mechanismen und Umwälzungen sowie die dazugehörigen Praktiken zu analysieren und ihre Folgen für Politik und Gesellschaft aufzuzeigen. Hatte sich die Demokratieforschung in der Vergangenheit bereits mit dem Phänomen „Medien-Demokratie“ auseinandergesetzt und angesichts medienvermittelter „Wirklichkeiten“ Gewinne und Verluste für die

[20] Zu Bemühungen der Europäischen Kommission zu Upload-Filtern und einem Verhaltenskodex für Internetanbieter: European Commission (2017b). Das deutsche Netzwerkdurchsetzungsgesetz (Bundesgesetzblatt 2017) schreibt den Betreibern sozialer Medien unter anderem vor, inkriminierte Inhalte innerhalb von 24 Stunden zu löschen; siehe auch Stefan Krempl (2017c).

Demokratie bilanziert (Donges 2015), so stehen tiefergehende Untersuchungen zur „Soziale Medien-Demokratie“ noch aus.[21] Ruppert et al. (2017) haben gefordert, mehr zu „Data Politics“ zu forschen, wenn hierzu nicht sogar ein neues Forschungsfeld zu etablieren, denn „data and politics are inseparable. Data is not only shaping our social relations, preferences, and life chances but our very democracies“. Es lässt sich schon jetzt feststellen, dass die Nutzerinnen und Nutzer moderner Kommunikationstechnologien und -medien „in Datenlandschaften leben, in denen sie selbst, ob sie wollen oder nicht, als Datenkörper eingelassen sind, welche ihrerseits ständig Daten erzeugen“ (Ochs 2015: 176). Konzepte der Privatheit im Informationszeitalter, hier ist Julie Cohen (2012: 114) zuzustimmen, sollten dieses komplexe Geflecht berücksichtigen und das autonome liberale Selbst und das dominierte postmoderne Selbst als entgegengesetzte Endpunkte fassen, zwischen denen unterschiedliche Formen und Intensitätsgrade der Beeinflussung denkbar sind. Sie hat zur Beschreibung dieser Art der Beeinflussung über gezielte Wissensproduktion den Begriff Modulation verwendet:

> *Modulation is a mode of privacy invasion, but it is also a mode of knowledge production designed to produce a particular way of knowing and a mode of governance designed to produce a particular kind of subject. Its purpose is to produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories* (Cohen 2013: 1917).

Über die sozialen Medien hinaus gehört zu den Folgen der mit Big Data-Analysen verbundenen Mechanismen und Umwälzungen auch, dass die Lebenschancen von Menschen durch für sie intransparente Datenerfassungssysteme und algorithmisch gesteuerte Big Data-Kategorisierungen nachhaltig beeinflusst werden (Lyon 2003; 2007b). Dies ist selbst dann der Fall, wenn die den Kategorisierungen zugrundeliegenden Algorithmen nicht so arbeiten wie intendiert (O’Neil 2016). Strukturierte Daten nehmen eine immer wichtigere Rolle im Leben der Menschen ein – sei es bei der Vergabe von Krediten, Wohnungen und Arbeitsplätzen, bei Einreisen in andere Länder oder beim Zutritt zu geschützten Bereichen wie etwa Flughäfen (Johnson/Wayland 2010; Smolak 2015). Gleichzeitig gestaltet sich die demokratische Kontrolle komplexer technischer Systeme und ihrer Wirkungen schwierig (Sclove 1995), ein Befund, der durch das intransparente Gebaren von Social Media-Firmen, Geheimdiensten und politischen Parteien sowie angesichts der zunehmenden Fragmentierung der Öffentlichkeit noch an Bedeutung und Aktualität gewinnt (Richards 2013: 1935; Morozov 2013; Helbing et al. 2015). In weiten Teilen der Bevölkerungen hat sich bisher jedenfalls kaum öffentlicher Protest gegen die massenhafte Sammlung und Auswertung ihrer Daten erhoben (Krasmann 2011¸ Pörksen 2016; Bauman et al. 2014; Monahan 2010).

Literaturverzeichnis

Allcott, Hunt, Matthew Gentzkow (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives,* 31(2), 211-236.

[21] Siehe auch Schaal (2015: 299), der feststellt, dass „die grundlagentheoretische Reflexion des Bedeutungswandels zentraler demokratietheoretischer Kategorien nach dem digital turn noch in den Kinderschuhen“ steckt.

Amoore, Louise (2014). Security and the Claim of Privacy. *International Political Sociology*, (8)1, 108-112.

Andrejevic, Mark, Kelly Gates (2014). Editorial. Big Data Surveillance: Introduction. *Surveillance & Society*, 12(2), 185-196.

Angwin, Julia, Jeff Larson (2017). *Help Us Monitor Political Ads Online – ProPublica launches a "PAC" to scrutinize campaign ads on Facebook*. Pro Publica. 7.9.2017. Zugriff am 8.9.2017 auf https://www.propublica.org/article/help-us-monitor-political-ads-online.

Angwin, Julia, Surya Mattu und Terry Parris Jr. (2016). *Facebook Doesn't Tell Users Everything It Really Knows About Them*. Pro Publica, 27.12.2016. Zugriff am 8.5.2017 auf https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them.

Ankenbrand, Hendrik (2017). *China plant die totale Überwachung*. faz net, 22.11.2017. Zugriff am 22.11.2017 auf http://www.faz.net/aktuell/wirtschaft/nationales-punktesystem-china-plant-die-totale-ueberwachung-15303648.html.

Baecker, Dirk (2007). *Studien zur nächsten Gesellschaft*. Frankfurt/M.: Suhrkamp.

Bandurski, David (2017). *Ihr werdet schon sehen*. TAZ online, 20.7.2017. Zugriff am 21.7.2017 auf https://www.taz.de/!5431172/

Bauman, Zygmunt, David Lyon (2013). *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon und R.B.J. Walker (2014). After Snowden. Rethinking the Impact of Surveillance. *International Political Sociology,* 8(2), 121-144.

Becker, Carlos, Sandra Seubert (2016). Privatheit, kommunikative Freiheit und Demokratie. *DuD - Datenschutz und Datensicherheit*, 40(2), 73-78.

Becker, Philipp von (2017). *Im Panoptikum des Datenkapitalismus*. Telepolis, 1.1.2017. Zugriff am 2.1.2017 auf https://www.heise.de/tp/features/Im-Panoptikum-des-Datenkapitalismus-3574113.html.

Bedford-Strohm, Jonas (2016). *Ein Hoch auf die Datenanalyse im Wahlkampf*. Huffington Post, 10.12.2016. Zugriff am 11.12.2016 auf http://www.huffingtonpost.de/jonas-bedfordstrohm/ein-hoch-auf-die-datenana_b_13459744.html.

Bennett, Colin J. (2015). Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications. *Surveillance & Society*, 13(3/4), 370-384.

BMJV (Bundesministerium der Justiz und für Verbraucherschutz) (2018). *Zitat Dr. Katarina Barley*. Homepage BMJV. Zugriff am 23.4. 2018 auf http://www.bmjv.de/SharedDocs/Zitate/DE/2018/032218_Funke_Facebook.html.

Brayne, Sarah (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, 82(5), 977–1008.

Buchstein, Hubertus (2016). *Typen moderner Demokratietheorien – Überblick und Sortierungsvorschlag*. Wiesbaden: Springer VS 2016.

Bundesgesetzblatt (2017). *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG)*. Bundesgesetzblatt, Jahrgang 2017 Teil I Nr. 61, ausgegeben zu Bonn am 7. September 2017.

Bundeskartellamt (2017). *Hintergrundinformationen zum Facebook-Verfahren des Bundeskartellamtes*. Dezember 2017. Zugriff am 9.3.2018 auf http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Diskussions_Hintergrundpapier/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=5.

Bundesverfassungsgericht (1983). Urteil vom 15. Dezember 1983 · Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil).

Calhoun, Craig (1993). *Habermas and the Public Sphere*. Cambridge (Mass.): MIT Press.

Chassot, Sylviane (2018). *Wer sind die Datenhändler, von denen Facebook sich zurückzieht?* NZZ-online, 29.3.2018. Zugriff am 29.3.2018 auf https://www.nzz.ch/wirtschaft/wer-sind-die-datenhaendler-von-denen-facebook-sich-zurueckzieht-ld.1370595.

Chen, Angela, Alessandra Potenza (2018). *Cambridge Analytica's Facebook data abuse shouldn't get credit for Trump*. The Verge, 20.3.2018. Zugriff am 23.3.2018 auf https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting.

Chester, Jeff, Kathryn C. Montgomery (2017). The role of digital marketing in political campaigns. *Internet Policy Review*, 6(4). DOI: 10.14763/2017.4.773.

Christl, Wolfie (2017). *Corporate Surveillance in Everyday Life – How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*. Vienna: Cracked Labs Institute for Critical Digital Culture. Zugriff am 25.11.2017 auf http://crackedlabs.org/en/corporate-surveillance

Christl, Wolfie, Sarah Spiekermann (2016). *Networks of Control, A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Vienna: Cracked Labs Institute for Critical Digital Culture. Zugriff am 25.11.2017 auf http://crackedlabs.org/en/networksofcontrol.

Clarke, Roger (2016). *Dataveillance* Zugriff am 26.10.2017 auf http://www.rogerclarke.com/DV/Intro.html#DV.

Clarke, Ronald, Graeme Newman und Shlomo Shoham (1997). *Rational Choice and Situational Crime Prevention – Theoretical Foundations*. London: Routledge.

Cohen, Julie E. (2012). *Configuring the Networked Self*. New Haven, CT: Yale University Press.

Cohen, Julie E. (2013). What Privacy Is For. *Harvard Law Review*, 126, 1904-1933.

Crouch, Colin (2008). *Postdemokratie*. Frankfurt/M.: Suhrkamp.

Dachwitz, Ingo (2017). *Wahlkampf in der Grauzone: Die Parteien, das Microtargeting und die Transparenz*. netzpolitik.org, 1.9.2017. Zugriff am 8.9.2017 auf https://netzpolitik.org/2017/wahlkampf-in-der-grauzone-die-parteien-das-microtargeting-und-die-transparenz/.

Dahl, Robert A. (1989). *Democracy and Its Critics*. New Haven: Yale University Press.

De Goede, Marieke (2017). The Chain of Security. *Review of International Studies*, 44(1), 24–42.

Diener, Andrea (2017). *Die Twitterinsel der AfD-Getreuen*. faz.net, 28.12.2017, Zugriff am 10.3.2018 auf http://www.faz.net/aktuell/feuilleton/medien/chaos-communication-congress-die-twitterinsel-der-afd-getreuen-15361701.html.

Donges, Patrick (2015). Mediendemokratie. In: Lembcke, Oliver W., Claudia Ritzi und Gary S. Schaal (Hg.). *Zeitgenössische Demokratietheorie, Band 2: Empirische Demokratietheorien*. Wiesbaden: SpringerVS, 103-124.

Dorloff, Axel (2017). *China auf dem Weg in die IT-Diktatur*, Deutschlandfunk online, 9.9.2017. Zugriff am 10.9.2017 auf http://www.deutschlandfunk.de/sozialkredit-system-china-auf-dem-weg-in-die-it-diktatur.724.de.html?dram:article_id=395440.

Dryzek, John S. (1990). *Discursive Democracy. Politics, Policy, and Political Science*. Cambridge: Cambridge University Press.

Dwoskin, Elizabeth, Adam Entous und Craig Timberg (2017). *Google uncovers Russian-bought ads on YouTube, Gmail and other platforms*. Washington Post, 9.10.2017. Zugriff am 18.10.2017 auf https://www.washingtonpost.com/news/the-switch/wp/2017/10/09/google-uncovers-russian-bought-ads-on-youtube-gmail-and-other-platforms/?utm_term=.16136f6c0151.

European Commission (2017a). *Communication from the Commission to the European Parliament, the European Council and the Council, Tenth progress report towards an effective and genuine Security Union*. COM(2017) 466 final. Brussels, 7.9.2017.

European Commission (2017b). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms*. COM(2017) 555 final, Brussels, 28.9.2017.

Garland, David (2008). *Kultur der Kontrolle – Verbrechensbekämpfung und soziale Ordnung in der Gegenwart*. Frankfurt/M.: Campus Verlag.

Gartner Research (2013). *IT Glossary*. Zugriff am 8.10.2017 auf http://www.gartner.com/it-glossary/big-data/.

Gerhards, Jürgen, Mike S. Schäfer (2010). *Is the internet a better public sphere? Comparing old and new media in the USA and Germany*. Berlin: Sage.

Grassegger, Hannes, Mikael Krogerus (2016). *Ich habe nur gezeigt, dass es die Bombe gibt*. Das Magazin, 48, 3.12.2016. Zugriff am 20.12.2016 auf https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/.

Greenfield, Adam (2017). *Radical Technologies: The Design of Everyday Life*. New York: Verso.

Habermas, Jürgen (1992). *Faktizitat und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*. Frankfurt am Main: Suhrkamp.

Haggerty, Kevin D., Minas Samatas (2010). Introduction – Surveillance and democracy: an unsettled relationship. In: Haggerty, Kevin D., Minas Samatas (Hg.). *Surveillance and Democracy*. Abington: Routledge, 1-16.

Haggerty, Kevin D., Richard V. Ericson (2000). The Surveillant Assemblage. *British Journal of Sociology*, 51(4), 605-622.

Hausen, Johannes, Dennis Kogel (2017). *Mit diesen mächtigen Tools machen die Parteien Wahlkampf auf Facebook*. Motherboard, 21.9.2017. Zugriff am 23.9.2017 auf https://motherboard.vice.com/de/article/yw3pex/mit-diesen-machtigen-tools-machen-die-parteien-wahlkampf-auf-facebook.

Hayes, Ben (2012). The Surveillance-Industrial Complex In: Ball, Kirstie, Kevin D. Haggerty und David Lyon, (Hg.). *Routledge Handbook of Surveillance Studies*. Abingdon: Routledge, 167-175.

Heesen, Jessica, Tobias Matzner (2015). Politische Öffentlichkeit und Big Data. In: Richter, Philipp (Hg.). *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data*. Baden-Baden: Nomos, 151-167.

Hegelich, Simon (2016). *Invasion der Meinungs-Roboter*. Analysen & Argumente, KAS, September 2016, Ausgabe 221.

Hegelich, Simon (2017). Psychologische Kriegsführung. *c't – magazin für computertechnik*, 19/2017, 110-111.

Hegemann, Hendrik, Martin Kahl (2016). (Re-)Politisierung der Sicherheit – Legitimation und Kontestation geheimdienstlicher Überwachung nach Snowden. *Zeitschrift für Internationale Beziehungen*, 23(2), 8-42.

Helbing, Dirk (2015). *"Big Nudging" – zur Problemlösung wenig geeignet*. Spektrum der Wissenschaft, 12.11.2015. Zugriff am 8.10.2017 auf http://www.spektrum.de/kolumne/big-nudging-zur-problemloesung-wenig-geeignet/1375930.

Helbing, Dirk, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari und Andrej Zwitter (2015). *Digitale Demokratie statt Datendiktatur*. Spektrum der Wissenschaft, 17.12.2015. Zugriff am 8.10.2017 auf http://www.spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933.

Hempel, Leon, Susanne Krasmann und Ulrich Böckling (Hg.) (2011). *Sichtbarkeitsregime*. Leviathan Sonderheft 25, Wiesbaden: VS Verlag.

Hersh, Eitan D. (2015). *Hacking the Electorate*. Cambridge: Cambridge University Press.

Hölig, Sascha, Uwe Hasebrink (2017). *Reuters Institute Digital News Survey 2017 – Ergebnisse für Deutschland*. Hamburg: Verlag Hans-Bredow-Institut (Arbeitspapiere des Hans-Bredow-Instituts Nr. 42), Juni 2017.

Hofmann, Jeanette (2017). Demokratie im Datenkapitalismus – Das Verhältnis von Medien und Macht muss neu vermessen werden, *WZB-Mitteilungen*, Heft 155, März 2017, 14-17.

Hofmann, Jeanette, Benjamin Bergemann (2017). *Die informierte Einwilligung: Ein Datenschutzphantom*. netzpolitik.org, 1.6.2017. Zugriff am 18.9.2017 auf https://netzpolitik.org/2017/die-informierte-einwilligung-ein-datenschutzphantom/.

Holzer, Boris (2017). *Dem Verbrechen auf der Datenspur*. faz.net, 5.11.2017, Zugriff am 5.11.2017 auf http://www.faz.net/aktuell/wissen/geist-soziales/big-data-dem-verbrechen-auf-der-datenspur-15257647.html.

Jansen, Jonas (2017). Der gläserne Kunde, *Frankfurter Allgemeine Woche*, 39/2017, 38-40.

Johnson, Deborah G., Kent A, Wayland (2010). Surveillance and transparency as sociotechnical systems of accountability. In: Haggerty, Kevin D., Minas Samatas (Hg.). *Surveillance and Democracy*. Abington: Routledge, 19-33.

Kaiser, Jonas, Adrian Rauchfleisch (2017). *YouTubes Algorithmen sorgen dafür, dass AfD-Fans unter sich bleiben*. Motherboard, 22.9.2017, Zugriff am 23.9.2017 auf

https://motherboard.vice.com/de/article/59d98n/youtubes-algorithmen-sorgen-dafur-dass-afd-fans-unter-sich-bleiben.

KANTAR TNS (2017). *Intermediäre und Meinungsbildung, Mediengewichtungsstudie 2017-I*. Zugriff am 8.11.2017 auf https://www.die-medienanstalten.de/themen/forschung/intermediaere-und-meinungsbildung/.

Kleinz, Torsten (2017). *Beschwerde gegen Googles Offline-Tracking*. heise online, 1.8.2017, Zugriff am 2.8.2017 auf https://www.heise.de/newsticker/meldung/Beschwerde-gegen-Googles-Offline-Tracking-3788615.html.

Krasmann, Susanne (2011). Der Präventionsstaat im Einvernehmen, In: Hempel, Leon, Susanne Krasmann und Ulrich Böckling (Hg.). *Sichtbarkeitsregime*. Leviathan Sonderheft 25, Wiesbaden: VS Verlag, 53-70.

Krempl, Stefan (2017a). *Werbe-Tracking: Facebooks Kooperation mit Datenhändlern in der Kritik*. heise online, 2.1.2017. Zugriff am 7.1.2017 auf https://www.heise.de/newsticker/meldung/Werbe-Tracking-Facebooks-Kooperation-mit-Datenhaendlern-in-der-Kritik-3585647.html.

Krempl, Stefan (2017b). *Oxford-Studie: Computergestützte Propaganda untergräbt die Demokratie*. heise online, 27.06.2017. Zugriff am 16.10.2017 auf https://www.heise.de/newsticker/meldung/Oxford-Studie-Computergestuetzte-Propaganda-untergraebt-die-Demokratie-3756264.html.

Krempl, Stefan (2017c). *"Missing Link": Manipulation, Meinungsfreiheit und Propaganda bei Facebook & Co*. heise online, 15.10.2017. Zugriff am 16.10.2017 auf https://www.heise.de/newsticker/meldung/Missing-Link-Manipulation-Meinungsfreiheit-und-Propaganda-bei-Facebook-Co-3861634.html?artikelseite=all.

Kreiss, Daniel (2017). Micro-targeting, the quantified persuasion. *Internet Policy Review*, 6(4), DOI: 10.14763/2017.4.774.

Kühl, Eike (2017). *Hetze mit System*. ZEIT online, 14.9.2017. Zugriff am 15.9.2017 auf http://www.zeit.de/digital/internet/2017-09/facebook-afd-geschlossene-gruppen-bundestagswahl.

Lischka, Konrad und Christian Stöcker (2017). *Digitale Öffentlichkeit – Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen*. Arbeitspapier im Auftrag der Bertelsmann Stiftung, Juni 2017.

Lobe, Adrian (2017). *Willkommen in der smarten Stadt – wo die Diktatur der Daten herrscht*. Neue Zürcher Zeitung, 13.11.2017. Zugriff am 17.11.2017 auf https://www.nzz.ch/feuilleton/die-stadt-wird-zum-computer-ld.1326729.

Locke, John (1977)[1689]. *Zwei Abhandlungen über die Regierung*. Suhrkamp, Frankfurt am Main.

Lyon, David (2003). Surveillance as social sorting: Computer codes and mobile bodies. In: Lyon, David (Hg.). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. London: Routledge, 13-30.

Lyon, David (2007a). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, David (2007b). Surveillance, security and social sorting: Emerging research priorities. *International Criminal Justice Review*, 17(3), 161-170.

Lyon, David (2015). The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society*, 13(2), 139-152.

Matz, Sandra, Michal Kosinski, Gideon Nave und David J. Stillwell (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of the United States of America (PNAS)*, Early Edition, 17.10.2017. Zugriff am 21.11.2017 auf www.pnas.org/cgi/doi/10.1073/pnas.1710966114.

Mayer-Schönberger, Viktor, Kenneth Cukier (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.

McCulloch, Jude, Dean Wilson (2015). *Pre-crime, Pre-emption, Precaution and the Future*. London: Routledge.

Mill, John Stuart (2011) [1859]. *Über die Freiheit*. Hamburg: Meiner.

Mitrou, Lilian (2010). The Impact of Communications Data Retention on Fundamental Rights and Democracy: The case of the EU Data Retention Directive. In: Haggerty, Kevin D., Minas Samatas (Hg.). *Surveillance and Democracy*, Abington: Routledge, 127-147.

Monahan, Torin (2010). Surveillance as governance. In: Haggerty, Kevin D., Minas Samatas (Hg.). Surveillance and Democracy, Abington: Routledge, 91-110.

Morozov, Evgeny (2013). The real privacy problem. MIT Technology Review, 22.10.2013. Zugriff am 8.11.2017 auf http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/.

Morozov, Evgeny (2014). Datenagenten in eigener Sache – Die Zukunft der Demokratie im Big-Data-Zeitalter. In: Nassehi, Armin (Hg.) *Kursbuch 177. Privat 2.0*, Hamburg: Murmann Verlag, 102-114.

Morozov, Evgeny (2015). „Ich habe doch nichts zu verbergen". *Aus Politik und Zeitgeschichte*, 65(11–12), 3-7.

Mützel, Daniel (2016). *Was an dem Bomben-Artikel, den alle geteilt haben, falsch ist*. Motherboard, 6.12.2016. Zugriff am 20.12.2016 auf http://motherboard.vice.com/de/read/was-an-dem-big-data-artikel-den-gerade-alle-teilen-falsch-ist-und-warum-er-trotzdem-wichtig-ist.

Neudert, Lisa-Maria N. (2017). Computational Propaganda in Germany: A Cautionary Tale. In: Woolley, Samuel, Philip N. Howard, (Hg.). *Working Paper 2017.7*. Oxford, UK: Project on Computational Propaganda. Zugriff am 6.11.2017 auf http://comprop.oii.ox.ac.uk.

Nimmo, Ben, Donara Bajoran (2017). *#BotSpot: Memes Target Der Spiegel, Merkel, German far-right Twitter activists use bots to make hashtags trend*. DFRLab, 14.9.2017. Zugriff am 8.11.2017 auf https://medium.com/dfrlab/botspot-memes-target-der-spiegel-merkel-678a2fc52b05.

Nissenbaum, Helen (2010). *Privacy in Context – Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

O'Neil, Cathy (2016). *Weapons of Math Destruction*. New York: Crown.

Ochs, Carsten (2015). BIG DATA – little privacy? Eine soziologische Bestandsaufnahme, In: Richter, Philipp (Hg.). *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data*. Baden-Baden: Nomos, 169-186.

Oremus, Will (2017). *Twitter's New Order*. Slate, 5.3.2017. Zugriff am 10.10.2017 auf http://www.slate.com/articles/technology/cover_story/2017/03/twitter_s_timeline_algorithm_and_its_effect_on_us_explained.html.

Papakyriakopoulos, Orestis, Morteza Shahrezaye, Andree Thieltges, Juan Carlos Medina Serrano und Simon Hegelich (2017). Social Media und Microtargeting in Deutschland. *Informatik-Spektrum*, 40(4), 327-335.

Pohle, Julia, Leo Van Audenhove (2017). Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change. *Media and Communication*, 5(1),1-6.

Pörksen, Bernhard (2016). *Alles vergeben, alles egal?* DIE ZEIT online, 8.12.2016. Zugriff am 12.9.2017 auf http://www.zeit.de/2016/49/empoerung-effekt-medien-skandale-ueberwachung-privatsphaere.

Quattrociocchi, Walter (2016). *How does misinformation spread online?* World Economic Forum (WEF). Zugriff am 9.3.2018 auf https://www.weforum.org/agenda/2016/01/q-a-walter-quattrociocchi-digital-wildfires/.

Rawls, John (2003). *Politischer Liberalismus*. Frankfurt am Main: Suhrkamp.

Reuters (2017). *Reuters Digital News Report 2017*. Reuters Institute/University of Oxford. Zugriff am 4.11.2017 auf http://www.digitalnewsreport.org/.

Richards, Neil M. (2013). The Dangers of Surveillance. *Harvard Law Review*, 126, 1934-1965.

Richter, Philipp (2015). Big Data und demokratische Willensbildung aus verfassungsrechtlicher Sicht. In: Richter, Philipp (Hg.). *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data*. Baden-Baden: Nomos, 45-67.

Riese, Dinah (2017): *Meine Kontakte, deine Kontakte*. faz.net, 3.7.2017. Zugriff am 18.11.2017 auf http://www.faz.net/aktuell/feuilleton/medien/weitergabe-von-kontakten-durch-whatsapp-vor-gericht-15085153.html.

Ritzi, Claudia (2014). *Die Postdemokratisierung politischer Öffentlichkeit, Kritik zeitgenössischer Demokratie – theoretische Grundlagen und analytische Perspektiven*. Wiesbaden: SpringerVS.

Rosenberg, Matthew, Nicholas Confessore und Carole Cadwalladr (2018). *How Trump Consultants Exploited the Facebook Data of Millions*. New York Times, 17.3.2018. Zugriff am 18.3.2018 auf https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Roßnagel, Alexander und Maxi Nebel (2015). (Verlorene) Selbstbestimmung im Datenmeer. Privatheit im Zeitalter von Big Data. *DuD – Datenschutz und Datensicherheit*, 39(7), 455-459.

Rule, James B. (2012). „Needs" for surveillance and the movement to protect privacy, In: Ball, Kirstie, Kevin D. Haggerty und David Lyon (Hg.). *Routledge Handbook of Surveillance Studies*. Abingdon: Routledge, 64-71.

Ruppert, Evelyn, Engin Isin und Didier Bigo (2017): Data Politics. *Big Data & Society*, 4(2), 1-7.

Schaal, Gary S. (2015). E-Demokratie. In: Lembcke, Oliver W., Claudia Ritzi und Gary S. Schaal (Hg.). *Zeitgenössische Demokratietheorie, Band 2: Empirische Demokratietheorien*. Wiesbaden: SpringerVS, 279-305.

Schmidt, Jan-Hinrik, Lisa Merten, Uwe Hasebrink, Isabelle Petrich, Amelie Rolfs (2017). *Zur Relevanzvon Online-Intermediären für die Meinungsbildung*. Hamburg: Verlag des Hans-Bredow-Insituts (Arbeitspapiere des Hans-Bredow-Instituts Nr. 40), März 2017.

Sclove, Richard E. (1995). *Democracy and Technology*. New York: Guilford Press.

Seubert, Sandra (2012). Der gesellschaftliche Wert des Privaten. *DuD – Datenschutz und Datensicherheit*, 36(2), 100-104.

Smolak, Harald (2015). *Maschinen haben keine Menschlichkeit*. Zeit online, 6.11.2015. Zugriff am 7.11.2017 auf http://www.zeit.de/karriere/beruf/2015-10/big-data-bewerbung-jobsuche-gefahr.

Soltani, Ashkan, Andrea Peterson und Barton Gellman (2013). *NSA uses Google cookies to pinpoint targets for hacking*. Washington Post, 10.12. 2013. Zugriff am 8.9.2017 auf https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking.

Stalder, Felix (2017). *Kultur der Digitalität*. Frankfurt/M: Suhrkamp.

Stamos, Alex (2017). *An Update on Information Operations on Facebook*, 6.9.2017. Zugriff am 9.10.2017 auf https://newsroom.fb.com/news/2017/09/information-operations-update/.

Steiger, Stefan, Wolf J. Schünemann und Katharina Dimmroth (2017). Outrage without consequences? Post-Snowden discourses and governmental practice in Germany. *Media and Communication*, 5(1), 7-16.

Stöcker, Christian (2017). *Social-Media Manipulation – Propagandisten hetzen über Bande*. Spiegel online, 17.9.2017. Zugriff am 7.10.2017 auf http://www.spiegel.de/wissenschaft/mensch/social-media-manipulation-propagandisten-hetzen-ueber-bande-a-1167921-druck.html.

Thaler, Richard H., Cass R. Sunstein (2014). *Nudge: Wie man kluge Entscheidungen anstößt*. Berlin: Ullstein.

Trinkwalder, Andrea (2017). Präzisionswahlkampf. *c't – magazin für computertechnik*, 19/2017, 106-111.

Tufekci, Zeynep (2014). *Engineering the public: Big data, surveillance and computational politics*. First Monday, 19(7). Zugriff am 20.11.2017 auf http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097.

Turow, Joseph (2007). *Niche Envy – Marketing Discrimination in the Digital Age*. Cambridge (Mass.): MIT.

Ulbricht, Lena (2017). Machtkämpfe um Big Data – Bürger und Verbraucher müssen geschützt werden. *WZB-Mitteilungen*, Heft 155, März 2017, 18-21.

US Senate (2017). *The Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, Hearing: Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions*, 31.10.2017. Zugriff am 1.11.2017 auf https://www.judiciary.senate.gov/meetings/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions.

Vosoughi, Soroush, Deb Roy und Sinan Aral (2018). The spread of true and false news online. *Science,* 359(6380), 1146-1151.

Weedon, Jen, William Nuland und Alex Stamos (2017). *Information Operations and Facebook Security*, 27.4.2017, Version 1.0, Facebook. Zugriff am 1.11.2017 auf https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

Wolfangel, Eva (2017). *Sorge um Sicherheit von smarten Stromzählern*. SZ online, 24.8. 2017. Zugriff am 25.8.2017 auf http://www.sueddeutsche.de/wissen/smart-home-sorge-um-sicherheit-von-smarten-stromzaehlern-1.3637580.

Wood, David Murakami (2013). What Is Global Surveillance? Towards a Relational Political Economy of the Global Surveillant Assemblage. *Geoforum*, 49(Oct.), 317–326.

Woolley, Samuel C., Philip N. Howard (2017). Computational Propaganda Worldwide: Executive Summary. In: Samuel Woolley and Philip N. Howard (Hg.). *Working Paper 2017.11*. Oxford, UK: Project on Computational Propaganda. Zugriff am 13.11.2017 auf http://comprop.oii.ox.ac.uk/

Worms, Christoph, Christoph Gusy (2012). Verfassung und Datenschutz. Das Private und das Öffentliche in der Rechtsordnung. *DuD – Datenschutz und Datensicherheit*, 36(2), 92-99.

Yeung, Karen (2017). 'Hypernudge': Big Data as a mode of regulation by design, Information. *Communication & Society*, 20(1) 2017, 118-136.