1 Big Data im öffentlichen Diskurs: Hindernisse und Lösungsangebote für eine Verständigung über den Umgang mit Massendaten

1.1 Big Data und Datenschutz im politischen Diskurs: Einführung und Bestandsaufnahme

Was Big Data betrifft, so ist die öffentliche und politische Debatte in Deutschland über Sinn und Unsinn, über Nutzen- und Schadenspotenziale noch ohne erkennbares Ergebnis im Sinne eines gesellschaftspolitischen Mehrheitskonsenses. Zu den Protagonisten von Big Data gehören nicht nur die großen Internetkonzerne, sondern auch die deutschen Industrieunternehmen, deren Manager angesichts von kritischen Stimmen schon mal vor einer „kleingeistig geführten Angstdebatte" (Busch 2018, S. 10) warnen. Diese ‚Angstdebatte' wiederum lässt sich an einer regelrechten Veröffentlichungswelle festmachen, die kritische Positionen einnimmt und deren Beginn ziemlich genau zu datieren ist. Im Sommer 2013 enthüllte der ehemalige CIA-Mitarbeiter Edward Snowden das ganze Ausmaß der Überwachungs- und Spionagepraxis von Geheimdiensten und löste damit die sogenannte NSA-Affäre aus. Einen zusätzlichen Schub erhielt die Protestwelle im Frühjahr 2018 durch das Eingeständnis von Facebook, dass die englische Analysefirma Cambridge Analytica mehr als 50 Mio. Datensätze von Nutzern ohne deren Kenntnis im US-Wahlkampf von Donald Trump eingesetzt hatte (The Guardian 2018).

Ängste vor dem Überwachungsstaat sind vor dem Hintergrund der eigenen geschichtlichen Erfahrung mit dem totalitären NS-Regime offensichtlich gerade in Deutschland leicht zu wecken. So hatte schon die 1983 geplante, verglichen mit den heute diskutierten Datenpraktiken harmlose, Volkszählung eine massive Protestbewegung bis hin zum Boykott ausgelöst. Schon damals ging es um die

Dieses Kapitel wurde von Susanne Knorre verfasst

S. Knorre et al., *Die Big-Data-Debatte,*
https://doi.org/10.1007/978-3-658-27258-6_1

prinzipielle Frage, welchen Nutzen die Datenerhebung hat, welche Risiken damit verbunden sind und wie das Eine sichergestellt werden kann, ohne das Andere zu ignorieren. Für Infrastrukturplanung und Wohnungsbau benötigte der Staat aktuelle Daten seiner Bürger, die Gegner befürchteten den Missbrauch dieser Daten (‚gläserner Bürger') und malten die Schreckensvision eines beginnenden Überwachungsstaats an die Wand. Erst das Urteil des Bundesverfassungsgerichts, aufgrund dessen die Regierung einige Teile des Zensus anpassen musste, führte zu Rechtsfrieden. Das Urteil gilt seitdem als Geburtsstunde des deutschen Datenschutzrechtes, das in diesem Sinne 1990 novelliert wurde.

Heute steht wieder die Frage im Raum, wie mit (personenbezogenen) Daten umzugehen ist – allerdings in einem völlig veränderten Umfeld, das durch Internet, Big Data und künstliche Intelligenz gekennzeichnet ist und in dem auf der anderen Seite die Nutzer ‚permanently online, permantly connected' sind. Es geht auch um mehr als ‚nur' Marktforschung, um personalisierte Werbung, um Wettbewerbsvorsprung durch Kunden- und Userdaten oder den Profit einiger großer Online-Konzerne. Es geht um eine gesamtgesellschaftliche Richtungsentscheidung, die sich mit ebenso grundsätzlichen wie vielschichtigen Themen wie der Abgrenzung von Privatem und Öffentlichem, mit der Gewichtung von Werten und Normen oder dem Verhältnis von Ökonomie und dem Primat der Politik befasst. Will man eine solche Richtungsentscheidung herbeiführen, dann bedarf diese ihrerseits eines mehrheitsfähigen Verständnisses über einen geeigneten politischen und rechtlichen Handlungsrahmen.

Der Umgang mit personenbezogenen Daten bzw. Massendaten unter den Bedingungen der dritten Dekade des 21. Jahrhunderts verlangt neue Antworten. Es bestehen Risiken wie Überwachung, Missbrauch und Diskriminierung; neue ethische Probleme stellen sich, wenn Entscheidungen auf Algorithmen und Maschinen verlagert werden. Aber es geht auch um die Chancen auf ein besseres Leben, das mit Hilfe von Big Data und künstlicher Intelligenz in der Medizin, im Verkehr und im Wohnbereich gesünder, sicherer, komfortabler und ressourcenschonender zu werden verspricht.

1.1.1 Nutzen und Schutz von Daten: Überlegungen zur Analyse eines politischen Diskurses

Vor diesem Hintergrund soll in diesem Essay den Fragen nachgegangen werden, wie der Umgang mit Daten im politischen Diskurs thematisiert wird, wie der aktuelle Stand dieses Diskurses zu beschreiben ist und welche Implikationen sich daraus für die weitere Entwicklung von sinnhaften und mehrheitsfähigen

Konventionen bzw. Normen und Regeln unterschiedlicher Art und Reichweite ergeben. Diese Überlegungen münden in die Suche nach geeigneten, wirkungsvollen Handlungs- bzw. Steuerungsoptionen.

Dazu wird zunächst beschrieben, welche Merkmale der öffentliche Diskurs über die Dichotomie von Schutz und Nutzen von Daten aufweist, um diese Ergebnisse dann mit den entsprechenden Beobachtungen und Interpretationen des politischen Diskurses im engeren Sinne in Beziehung zu setzen bzw. zu vergleichen. Dieses Vorgehen wurde gewählt, weil davon ausgegangen wird, dass die öffentlichen, nach wie vor wesentlich über Massenmedien ausgetragenen Argumentationen ihrerseits den politischen Diskurs im engeren Sinne zwischen Entscheidungsträgern und pluralistischen Interessengruppen maßgeblich beeinflussen.

Die Frage, ob mit der Nutzung von Massendaten aller Art eher Vorteile und Verbesserungen oder eher Nachteile bzw. Risiken verbunden sind, ist thematisch als eine typische Fortschrittsdebatte zu beurteilen. D. h. alle kommunikativ Handelnden bringen jeweils ihre subjektiven Zukunftserwartungen, Ängste und Hoffnungen in ihre Argumentationen mit ein. Es geht schließlich um äußerst komplexe Zusammenhänge mit vielen Unsicherheiten, ja vor allem mit vielen ‚unknown unknowns', die auch nicht von Experten unstreitig einzuschätzen sind. Dennoch – und darin liegt die besondere gesellschaftliche und politische Herausforderung – muss darüber, wie wir morgen mit den in unabsehbarer Menge und Verknüpfungen erhobenen und gespeicherten Daten umgehen wollen, bereits heute eine Verständigung erzielt werden. Und zwar weniger deshalb, weil es einen zusätzlichen konkreten Steuerungsanspruch z. B. mittels Gesetzgebung einzulösen gilt, sondern weil eine solche Verständigung zur Legitimierung demokratischer Entscheidungen ganz grundsätzlich notwendig ist, will man nicht in eine vordemokratische Expertokratie verfallen. Dass solche Verständigungen immer nur von begrenzter zeitlicher Dauer sein können, gilt hier dementsprechend ebenfalls als gesetzt, denn schließlich gibt es zu jeder Entscheidung – sei es in der Politik, sei es in Unternehmen oder bei den Bürgern und Nutzern von Daten – immer eine Alternative. Die notwendige Folge ist eine permanente argumentative Auseinandersetzung über mögliche, bessere Alternativentscheidungen.

Es gibt wohl kaum ein Politikfeld, in dem dieses Kontingenzprinzip so deutlich wird wie im Falle von Big Data bzw. den damit in Verbindung stehenden politischen und rechtlichen Lösungsangeboten. Die breite, von allen Seiten kritische Diskussion um die EU-Datenschutzgrundverordnung hat dies noch einmal ganz konkret vorgeführt. Die Öffentlichkeit ist geprägt von Erzählungen, die – nicht zuletzt basierend auf Alltagserfahrungen – vielstimmig sind und auf die Fülle möglicher Alternativkonzepte zum Umgang mit Massendaten aufmerksam

machen. Damit geht es aber zugleich um eine Verständigungsdebatte über Zwecke und Ziele, es geht um Deutungshoheiten, mithin Machtinteressen in einem interessenbeladenen Politikfeld. Narrationen, also der Akt des Erzählens, und die mit ihnen konstruierten Narrative gelten deshalb inzwischen über die Wissenschaftsdisziplinen hinweg als maßgeblicher Faktor, der Einfluss auf grundlegende soziale, politische und auch ökonomische Entwicklungen ausübt (Shiller 2017).

Gesellschaftliche und politische Konflikte sind dementsprechend als Konflikte der Interpretation zwischen konkurrierenden Narrativen zu sehen (Gadinger et al. 2014, S. 34). Das bedeutet im Umkehrschluss, dass es notwendig und sinnvoll ist, Narrative zu konstruieren, um überhaupt zu einem mehrheitsfähigen Konsens über Nutzen und Grenzen von Big Data zu gelangen. Deshalb versucht dieser Essay, wesentliche Elemente des öffentlichen wie politischen Diskurses anhand von Narrativen zu beschreiben, die verwendet werden, damit komplexe Phänomene jenseits von Zahlen, Formeln oder Algorithmen überhaupt zum Gegenstand des öffentlichen Diskurses gemacht werden können (Gadinger et al. 2014, S. 9 ff.).

Die im Kontext von Big Data zu entdeckenden Geschichten werden in ihren wesentlichen Konstruktionen nachvollzogen und die beabsichtigten und unbeabsichtigten Wirkungen interpretiert, sie werden aber nicht abschließend vermessen (Blatter et al. 2017, S. 31 ff.). Methodisch bedeutet dies, dass unter Punkt 6 Narrationen im öffentlichen Diskurs anhand von aktuellen Presseveröffentlichungen, Fachliteratur und Sekundärerhebungen rekonstruiert, in ihren jeweiligen Kontext eingeordnet und interpretiert werden. Dasselbe geschieht anschließend unter Punkt 8 mit politischen Narrationen, die aber darüber hinaus noch anhand von Gesetzestexten, Parteiprogrammen und Interviews interpretativ analysiert werden. Damit lässt sich die Wirkmächtigkeit von herrschenden Narrativen beschreiben und analysieren, wie sie in der Öffentlichkeit zu beobachten sind.

1.1.2 Big Data, Künstliche Intelligenz und Algorithmen: Begriffe und Konzepte in der Diskussion

Auch wenn Experten Ausmaß und Qualität unterschiedlich beschreiben, so sind sie sich doch einig in der Aussage, dass die Big-Data-Technologie eine dramatische Veränderung für Wirtschaft und Gesellschaft bedeutet. Der Oxford-Professor Viktor Mayer-Schönberger spricht von „einem Daten-getriebenen Neustart des Marktes, der zu einer fundamentalen Umgestaltung unserer Wirtschaft führen wird, die wohl so bedeutsam sein wird wie die industrielle Revolution, eine Neuerfindung des Kapitalismus“ (Mayer-Schönberger und Ramge 2018, S. 3). Mit Big Data habe „die zweite Welle der Digitalisierung“ begonnen, meint Aljoscha

Burchardt (2018, S. 13), Wissenschaftler am Deutschen Forschungszentrum für Künstliche Intelligenz. Die erste Welle wurde durch die Digitalisierung analoger Datenträger (z. B. Foto, Film, Text, akustische Signale) angestoßen, die Digitalisierung beschränkte sich aber weitgehend auf das Speichern der Daten und ihre Wiedergabe. Jetzt werden die Daten für Maschinen verstehbar.

„Big Data ist nicht weniger als die dritte große Welle von Innovationen, nach dem World Wide Web Mitte der 90er Jahre und Social Media Mitte der 2000er. Big Data ist ein Paradigmenwechsel, wie wir Informationstechnologie einsetzen." So beschreibt der Data Scientist Jörg Blumtritt (2015) das Phänomen. Datenintensive Forschung gilt Microsoft-Analytikern als vierte wissenschaftliche Revolution und Motor gesellschaftlicher und wirtschaftlicher Entwicklung, das sogenannte vierte Paradigma (Hey et al. 2009 zitiert in Schwerk et al. 2018, S. 2). Big Data wird somit als eine disruptive Technologie bewertet, die gravierende Auswirkungen für viele Branchen und gesellschaftliche Bereiche mit sich bringen wird, in einigen Branchen wird sie Arbeitsplätze vernichten, gleichzeitig aber auch hohe Produktivitäts- und Wohlstandssteigerungen sowie neue Arbeitsplätze schaffen. Die Unternehmensberatung McKinsey erwartet dadurch weltweit ein Wertschöpfungspotenzial von jährlich mehr als 3,5 Billionen Dollar (McKinsey Global Institute 2018) – das wäre in etwa so viel wie derzeit das Bruttoinlandsprodukt von Deutschland.

Die Fülle der zur Verfügung stehenden Daten und die Fähigkeit, sie zu verarbeiten, verändern Wirtschaft und Gesellschaft grundlegend. Mayer-Schönberger und Ramge (2018) zufolge wandelt sich die Wirtschaft dadurch vom Finanzkapitalismus zum Datenkapitalismus. Um die Wahlhandlungen der Menschen zu koordinieren, stehe nun nicht mehr nur eine Variable, der Preis, zur Verfügung. An die Stelle des häufig zu ineffizienten Lösungen führenden Preismechanismus trete die Koordination mittels Daten. So erlaubten die neuen technologischen Möglichkeiten, dass die Menschen ihre Transaktionen entlang ihrer Präferenzen, die sich in einer Fülle von Daten ausdrücken, zu einem optimalen Ergebnis zusammenführen.

Richtig eingesetzt, könne Big Data über eine nahezu perfekte Personalisierung der Kommunikation in vielen Bereichen, von Bildung über medizinische Versorgung bis hin zum Klimawandel, nachhaltige Lösungen ermöglichen (Mayer-Schönberger und Ramge 2018, S. 12).

> Man muss kein Anhänger utopischer oder dystopischer Science-Fiction sein, um zu erkennen, dass wir uns möglicherweise an der Schwelle zu einer faszinierenden, radikalen Veränderung in der Evolution der Menschheit befinden, wie es sie seit einem Jahrtausend nicht mehr gegeben hat. Revolutionen dieser Art verlaufen niemals reibungslos. Sie sind fast immer chaotisch, undurchsichtig und voller ethischer Fußangeln. (Groth et al. 2018, S. 28)

Folgt man den überwiegenden Darstellungen, dann zeichnet sich Big Data durch vier ‚V' aus: Das erste V steht für ‚Volume' und besagt, dass mit den exponentiell wachsenden Analyse- und Speicherkapazitäten, die sich dem Moore'schen Gesetz zufolge alle 12 bis 24 Monate verdoppeln, auch die weltweit für die Analyse zur Verfügung stehenden Daten exponentiell zunehmen. Die Computerchips werden immer leistungsfähiger, kleiner und preiswerter, der Grad der Vernetzung nimmt zu und eine Vielzahl von Geräten und Alltagsgegenständen ist mit Sensoren ausgestattet, die einen kontinuierlichen Datenstrom liefern. Das macht Analysen und Vorhersagen billiger. Mit dem zunehmenden Datenvolumen in direkter Beziehung steht das zweite V: ‚Velocity', also die Geschwindigkeit, mit der gigantische Datenvolumina heute verarbeitet werden können bis hin zur Analyse in Echtzeit.

Das dritte V bedeutet ‚Variety' und bezieht sich auf die Vielfalt der unterschiedlichen Datenquellen und Datenformate, die verarbeitet und miteinander verknüpft werden können, um daraus Erkenntnisse zu gewinnen. Das betrifft Daten aus den unterschiedlichsten Bereichen, von strukturierten demografischen Statistiken bis hin zu unstrukturierten Daten in Form von Text-, Audio-, Bild- und Video-Dateien insbesondere aus den sozialen Netzwerken. Das vierte V – ‚Veracity' für Zuverlässigkeit – betrifft die Anforderung an die Datenqualität im Sinne von Richtigkeit und Vertrauenswürdigkeit. Das heißt, die mit einer Big-Data-Analyse erzielten Erkenntnisse sind von der Qualität der Daten und der Analysemethode abhängig. Nur mit validen Daten und einem adäquaten Verarbeitungsverfahren sind vertrauenswürdige Ergebnisse möglich.

Big Data bezeichnet also die Verarbeitung von Massendaten unterschiedlichster, auch unstrukturierter, komplexer und sich ändernder Informationen mithilfe von Algorithmen und/oder Künstlicher Intelligenz. Zeichnete sich ein klassischer Analyseprozess bislang durch das Überprüfen von Hypothesen mittels Datenerhebungen aller Art aus, um daraus Aussagen über Kausalitäten zu gewinnen, so besteht er nun vor allem darin, den jeweils vorgefundenen Datenstrom auszubeuten, sprich maschinell nach Zusammenhängen zwischen Variablen, d. h. nach Korrelationen, zu durchforsten.

Unter dem mathematischen Begriff Algorithmus ist eine Rechen- oder Verarbeitungsvorschrift zur Lösung genau definierter Probleme zu verstehen, die von Maschinen abgearbeitet werden können. Algorithmen in Navigationssystemen errechnen die schnellste Verbindung zwischen zwei Orten oder verbessern bei der Textverarbeitung die Rechtschreibung. Aber nicht alle Situationen sind im Voraus modellartig zu erfassen. Für das autonome Fahren etwa braucht es ein System, das lernfähig ist und auch in neuen Situationen richtig (intelligent) zu entscheiden weiß. Hier ist Künstliche Intelligenz erforderlich, man braucht lernfähige Algorithmen beziehungsweise maschinelles Lernen, um Muster in komplexem

Datenmaterial zu erkennen und zu deuten. Und sie müssen in der Lage sein, diese Muster auch auf neue Daten anzuwenden und sich selbstständig in einem begrenzten Rahmen Lösungswege zu erarbeiten.

Für diesen Prozess müssen zwei Bedingungen erfüllt sein: Zum einen benötigt das System riesige Datenmengen, um den Algorithmus zu trainieren. So hat Google alle im Internet vorhandenen Texte in sein Sprachübersetzungstool eingegeben, um alle möglichen Muster des Gebrauchs von Wörtern zu trainieren (Mayer-Schönberger und Ramge 2018, S. 78). Zum anderen braucht das System beständiges Feedback, um sich selbst an neue und veränderte Umstände anpassen zu können. Big Data und Algorithmen bzw. Künstliche Intelligenz sind also komplementäre Elemente. Wohl deshalb werden die drei Begriffe oft synonym verwendet, um diese neue Stufe der Verarbeitung von gigantischen Datenvolumina zu beschreiben. Es ist die Verbindung dieser drei Elemente, die das Potenzial für technologische Sprünge erzeugt.

1.1.3 Arten, Herkunft und Nutzer von Daten: Annäherung an eine Dual-Use Technologie

Um Massendaten nutzen zu können, müssen sie zuvor allerdings analysierbar gemacht werden. Kein Problem ist das bei sogenannten strukturierten Daten, insbesondere solchen, die als Zahlen oder Buchstaben in Tabellenform erfasst sind und die sich in Datenbanken z. B. von Suchmaschinen leicht und schnell durchsuchen lassen. Hinzukommen aber die sogenannten unstrukturierten Daten, die z. B. als Textdateien, Präsentationen, Videos, Audiodaten unbearbeitet vorliegen, d. h. in einer nicht formalisierten, oft nutzergenerierten Struktur von den Nutzern selbst ins Netz gestellt werden (‚user generated content') und in denen nicht zuletzt das Verhalten von Menschen, deren Präferenzen und Stimmungen aufgezeichnet werden, und zwar unabhängig davon, ob diese explizit geäußert werden oder nicht. Um sie dennoch analysieren zu können, kommen Verfahren wie Text- und Spracherkennung oder Stimmanalysen zum Einsatz. Damit sind unstrukturierte Daten ebenfalls zu analysieren, denn die in ihnen gespeicherten Informationen lassen sich in strukturierte Daten umwandeln, dementsprechend durchsuchen und schließlich auf Korrelationen überprüfen.

Unstrukturierte Daten enthalten also latente Informationen, z. B. über Persönlichkeitsmerkmale oder Emotionen, die dann neben den demografischen Daten wie Alter, Geschlecht oder Wohnort für die personalisierte Ansprache genutzt werden, um den Nutzer beispielsweise ganz banal in seinen persönlichen Präferenzen für Streaming-Dienste, aber genauso auch in seinen Sicherheitsbedürfnissen

bzw. Ängsten zu adressieren. Mit derselben Zielsetzung lassen sich auch ‚Likes' bei Facebook oder Statusmeldungen in Messenger-Diensten analysieren, die dann nicht nur sehr zeitnahe Stimmungsbilder über die Nutzer liefern können, sondern sogar Vorhersagen ermöglichen, mit welchen Emotionen zu welcher Zeit bei den Nutzern zu rechnen ist (Farnadi et al. 2014; Youyou et al. 2015).

Daten kommen auf verschiedensten Wegen zustande. Die älteste Form systematischer Datenerhebung ist ein hoheitlicher Akt: die Volkszählung. Aufgrund militärischer und fiskalischer Interessen erfassten Staaten schon früh Bevölkerung und Ressourcen. Eine regelmäßige, lückenlose, systematische Erhebung solcher Daten für die amtliche Statistik ist in Europa seit der zweiten Hälfte des 19. Jahrhunderts in Gebrauch. Gesetzliche Anordnungen wurden erlassen, um Geburten, Heiraten und Todesfälle für das amtliche Melderegister zu erfassen. „Erstmals vermaßen Gesellschaften sich selbst und legten darüber Archive an" (Osterhammel 2009, S. 62). Melderegister sammeln und speichern auch heute noch persönliche Daten wie Namen, Adresse, Geburts- und Sterbetag, Staatsangehörigkeit, Religion, Familienstand und Steuerklasse und geben auch Dritten darüber – entgeltlich – Auskunft.

Viele Daten werden aber auch durch individuelle Bereitstellung der Endnutzer (im Folgenden nur noch Nutzer) erzeugt. Das geschieht etwa in Form von Selbstauskünften, um eine bestimmte Leistung eines Unternehmens in Anspruch nehmen zu können. Dabei handelt es sich häufig um besonders sensible Daten wie etwa Einkommen, Vermögen und Schulden bei einem Kreditantrag oder die eigenen Gesundheitsdaten und Krankheitsgeschichte bei der Krankenversicherung. Genauso wie bei den staatlichen Meldeämtern geschieht die Preisgabe dieser Daten nicht freiwillig, denn ohne die Selbstauskünfte würde kein Vertrag zustande kommen.

Die meisten Daten fallen heute aber automatisch bei der Nutzung bestimmter Geräte oder Technologien (z. B. Smartphone, Computer, Kunden- oder Kreditkarte, Auto) an. Bei den elektronischen Spuren, die dabei entstehen, handelt es sich um Daten, da sie durch bestimmte technische Kennungen (z. B. Telefonnummer, IP-Adresse, Bankkonto-Nummer, Fahrzeug-Identitätsnummer) einer individuellen Person zuzuordnen sind, die beispielsweise für einen Vertragsabschluss ihre persönlichen Daten angeben muss. So lassen sich aus den besuchten Webseiten beim Surfen im Internet leicht persönliche Interessen sowie politische, religiöse oder sexuelle Einstellungen ableiten. Durch die Verknüpfung von Cookies, die beim erstmaligen Besuch von Webseiten gespeichert werden, können Informationen über den Nutzer zu aussagekräftigen Persönlichkeitsprofilen zusammengefügt werden. Durch die Verknüpfung der Cookies ist der Nutzer möglicherweise auch für solche Internetanbieter identifizierbar, denen der Nutzer selbst keine persönlichen Daten offenbart hat.

Aus E-Mails und Telefonaten lassen sich Rückschlüsse auf das soziale Umfeld des Users ziehen. Es gibt inzwischen fast keine menschliche Aktivität mehr, die nicht digitale Spuren hinterlässt. Der wichtigste Datenproduzent ist heute das Smartphone, das dem Telefonanbieter den Aufenthaltsort verrät, aus dem sich Bewegungsprofile ableiten lassen. Ein Smartphone ist heute in der Regel mit mindestens 12 bis 15 Sensoren bestückt, etwa GPS, Barometer, Beschleunigungssensor, Magnetometer für die Himmelsrichtung, Rotationssensor, Näherungssensor, Helligkeitssensor. Manche verfügen auch über ein Thermometer, einen Feuchtigkeitssensor, einen Fingerabdrucksensor oder Gesichtserkennung. Diese Sensoren erhöhen den Bedienungskomfort, aber lassen mittels einer App auch leicht erkennen, ob der Besitzer des Smartphones gerade schläft, geht, ob und wie er Auto fährt oder in welchem Stock eines Gebäudes er sich aufhält (Hajek 2018, S. 56). Interessant ist das nicht nur für Überwachungsorgane, sondern etwa auch für Autoversicherungen, die ihre Prämien am Fahrverhalten orientieren wollen.

Die Menschen, die nicht digital erfasst werden, sind heute schon in der Minderheit. Weltweit nutzen rund 2,6 Mrd. Menschen ein Smartphone, 3,2 Mrd. sind per Smartphone oder Computer in den Sozialen Medien unterwegs, vier Milliarden nutzen das Internet. Insgesamt waren im Jahr 2016 rund 6,4 Mrd. Endgeräte mit dem Internet verbunden, bis 2020 soll die Zahl auf 20,8 Mrd. anwachsen. Im Schnitt nutzt jeder Mensch heute 3,64 internetfähige Endgeräte, 26,7 Apps und ist auf sieben unterschiedlichen Internetplattformen unterwegs (Srinivasan 2018).

Die Autos von heute sind fahrbare, mit dem Internet verbundene Computer, die Daten über Fahrverhalten und Bewegungsprofile an die Autohersteller (und demnächst vermutlich an Autoversicherungen und Anbieter von autonomem Fahren) senden. Abermillionen Kunden- und Kreditkarten hinterlassen Spuren der getätigten Finanztransaktionen. Sogenannte Wearables, also Sensoren, die am Körper getragen werden, wie etwa Fitness-Tracker, übertragen laufend medizinische Daten. Ein steter Datenstrom fließt aus den mit dem Internet verbundenen technischen Sensoren in Häusern und Wohnungen, die der Überwachung und Optimierung von Energie- und Wasserverbrauch dienen. Immer mehr Kameras werden im öffentlichen Raum installiert, um Gesetzesübertreter abzuschrecken und mittels Gesichtserkennung identifizieren zu können.

Zu diesen von Nutzern generierten Daten kommen weitere hinzu – Stichwort Internet of Things. Sensoren in den Fabriken überwachen und steuern die Produktion, sie erfassen beispielsweise Drehzahl, Temperatur, Vibration oder Klangmuster, um drohenden Verschleiß rechtzeitig zu erkennen. Sensoren im öffentlichen Bereich weisen freie Parkplätze aus und helfen den Verkehr zu verflüssigen. Schätzungen zufolge sollen im Jahr 2030 weltweit 100 Billionen

Sensoren im Einsatz sein. Schon jetzt sind es pro Person 140. Das Zusammenwachsen von vier großen Trends – künstliche Intelligenz, Big Data, die Verbreitung von Sensoren und Mobilität – schaffen eine sich selbst beschreibende Welt, so Philip Evans (2018, S. 144) von der Boston Consulting Group.

Wer nutzt all diese Daten und worin genau besteht der Nutzen? Das zeigt beispielsweise der Unterschied zwischen Amazon und einem traditionellen Einzelhändler. Letzterer fragt einen Kunden direkt nach seinen Wünschen, wenn der seinen Laden betritt. Stimmen die geäußerten Kundenpräferenzen mit dem Produktangebot des Händlers überein und stimmt der Preis, kommt es zum Kauf. Amazon dagegen erfasst die Präferenzen der Besucher auf seiner Internetseite nicht durch direkte Fragen, sondern es analysiert die Spuren, die ein Besucher jedes Mal auf der Website hinterlässt, wenn er sie aufsucht: für welche Produkte er sich interessiert, wann und wie lange er sie ansieht, welche Kundenbewertungen er liest und was er schließlich kauft. Beim traditionellen Handel ist der Kontakt zum Kunden immer nur punktuell und meist auf verschiedene Verkäufer verteilt und wird nicht oder nur selten systematisch ausgewertet. Amazon dagegen kann aufgrund des gespeicherten kontinuierlichen Datenstroms ein immer klareres Muster der jeweiligen persönlichen Präferenzen und Bedürfnisse seiner Kunden erkennen. Und da Amazon mit seinem riesigen Warenangebot das Kaufhaus-Prinzip ‚Alles unter einem Dach' befolgt, lässt sich aus dem Kundenverhalten ein immer umfassenderes, differenzierteres Persönlichkeitsprofil zusammenfügen.

Wer über die Daten verfügt, hat einen Informationsvorsprung und damit einen Wettbewerbsvorteil. Das gilt für Amazon, Zalando, Booking.com, Netflix, Spotify, Apple, Airbnb, die Produkte oder Dienstleistungen verkaufen. Das gilt aber ebenso für Suchmaschinen wie Google oder Yahoo und für Soziale Netzwerke wie Facebook oder WhatsApp, die mit diesen persönlichen Datenprofilen personalisierte Werbeplätze verkaufen (wie nun auch Amazon) und damit die Verlage ihrer wichtigen traditionellen Erlösquelle berauben. Aus Sicht dieser Unternehmen sind Daten eine strategische Ressource für ihre Unternehmenspolitik in Vertrieb und Marketing und bei der Generierung von Werbeerlösen. So urteilt der britische Economist: Die wertvollste Ressource der Welt ist nicht länger Öl, sondern sind Daten (Economist 2017). Das disruptive Potenzial zeigt sich nicht nur in der Verlagsbranche, wo der Zuwachs an digitaler Werbung fast ausschließlich von Google und Facebook vereinnahmt wird, sondern auch im Einzelhandel. In den USA entfällt die Hälfte des Online-Umsatzes inzwischen allein auf Amazon. Während der stationäre Handel stagniert oder schrumpft, boomt der E-Commerce (Saal 2017).

Insofern überrascht es nicht, dass E-Commerce, Suchmaschinen und Soziale Medien Schrittmacher in der kommerziellen Verwertung von Daten sind. Die Kunden- und Nutzerdaten sind die Basis für Marktforschung und Business-Planung, für zielgerichtetes personalisiertes Marketing, für Upselling und Crossselling, für eine effiziente Einkaufspolitik, Senkung der Logistikkosten, Preisoptimierung und individuellen Kundenservice (Customer Relationship Management). Die Daten nutzen die Unternehmen entweder selbst oder sie verkaufen sie an andere Unternehmen. Sie senken dadurch ihre Kosten, expandieren Nachfrage und Marktanteil und reduzieren Risiken. Inzwischen ist Big Data auch für weitere Branchen zum Thema geworden, egal ob sie im B2C- oder im B2B-Bereich tätig sind. Chatbots im Kundenservice entlasten branchenübergreifend das Personal. Neben Marketing, Vertrieb und Logistik helfen Big-Data-Technologien bei der Optimierung von Abläufen, bei der Steuerung und Überwachung der Fertigung bis hin zur Personalrekrutierung.

Die eigentliche Komplexität der öffentlichen Diskussion über Big Data resultiert aber weniger aus der Vielfalt der Anwendungsmöglichkeiten. Vielmehr ergibt diese sich aus der Tatsache, dass es sich um sogenannte Dual-Use-Technologien (Bunk und Goldschmidt 2016) handelt, die zugleich zweckbestimmt und zweckentfremdet eingesetzt werden können. Selbst wenn Konsumenten z. B. durch bessere Produktauswahl und niedrigere Preise profitieren, eröffnet Big Data zugleich die Möglichkeiten jedweder Überwachung. Autonomes Fahren macht derzeit hauptsächlich dann Schlagzeilen, wenn ein Wagen dieser Generation in einen Unfall verwickelt ist. Es ermöglicht aber auf der anderen Seite positive Auswirkungen auf Verkehrssicherheit, Fahrkultur und Energieverbrauch. Dass Überwachungstechnologien, insbesondere wenn sie auf der Erfassung biometrischer Daten beruhen, die informationelle Selbstbestimmung gefährden können, gehört inzwischen zum Allgemeinwissen. Dass sie aber zugleich mehr Sicherheit ermöglichen, nicht nur gegenüber äußeren Feinden (z. B. durch Luftraumüberwachung und Bodenbeobachtung), sondern auch gegenüber Terroristen und Verbrecher im Inneren, ist wiederum die andere Seite der Medaille.

Der Einsatz von Smart-Grid-Technologien beim Stromverbrauch hilft nicht nur den Versorgungsunternehmen bei der Vorhersage des Strombedarfs und trägt damit zur Einhaltung ihrer Gewinnziele bei. Sie hilft zugleich den Konsumenten, den Stromverbrauch der einzelnen Geräte zu diagnostizieren, Stromfresser zu identifizieren und mehr Preissensibilität zu entwickeln – mit entsprechend positiven Folgen für Energieverbrauch, Umwelt und Klima. Der Einsatz von Big Data in der Medizin beschwört nicht nur die Gefahr des ‚gläsernen Patienten' herauf, sondern macht auch genauere Diagnosen und Erfolg versprechende Operationen

möglich und lässt Durchbrüche in der medizinischen Forschung und der Gesundheitsversorgung erwarten. Sensoren und Überwachungskameras auf den Straßen erheben nicht nur ein individuelles Bewegungsprofil, sie verbessern auch Verkehrsplanung und sorgen für weniger Staus.

Als Dual-Use-Technologie kann Big Data sowohl zum Schlechten wie zum Guten des Menschen, für gesellschaftlich akzeptierte und nicht akzeptierte Zwecke, für individuelle Profitinteressen genauso wie für das Gemeinwohl eingesetzt werden. Nur in wenigen Bereichen wie etwa bei der Wetterprognose ist der flächendeckende Einsatz von Big Data als nicht ambivalent einzuschätzen. Die Ambivalenz bzw. Janusköpfigkeit von Big Data in seinen Anwendungsmöglichkeiten spiegelt sich im diffusen öffentlichen Meinungsbild wider.

1.1.4 Diffuses Bild: Was bislang über die öffentliche Einschätzung von Datennutzung erhoben wurde

Zum ersten Mal systematisch erfragte das Institut für Demoskopie Allensbach (2013) die Meinung der Deutschen zu Big Data im Jahr 2013 als Schwerpunkt für den alljährlich von ihm erstellten Sicherheitsreport. Die Demoskopen konstatierten darin eine „grundsätzlich ablehnende Haltung“ (Institut für Demoskopie Allensbach 2013, S. 15) der Bevölkerung gegenüber dem umfangreichen Sammeln und Auswerten von persönlichen Daten. 72 % machten sich große oder etwas Sorgen, dass Unternehmen persönliche Daten missbrauchen, 63 %, dass der Staat die Bürger zu sehr überwacht. Selbst bei Mitgliedern von sozialen Netzwerken, die einen tendenziell freizügigeren Umgang mit ihren persönlichen Daten an den Tag legen, fanden 58 % das umfangreiche Sammeln und Auswerten von Kundendaten durch Unternehmen nicht in Ordnung. Und 78 % (Mitglieder von sozialen Netzwerken: 74 %) forderten strengere Vorgaben für Unternehmen, die persönliche Daten ihrer Nutzer sammeln und auswerten.

Etwas differenzierter wurde die Einstellung allerdings, wenn nach konkreten Anwendungen von Big Data gefragt wurde. Mit deren Hilfe Straftaten aufzuklären oder den Bedarf an Kindergärten besser planen zu können, fand große Zustimmung. Überwiegend auf Ablehnung stießen aber die meisten anderen Big-Data-Anwendungen wie Erleichterung von Einkäufen im Internet, Prüfung der Kreditwürdigkeit durch Banken, Hinweise auf Beiträge im Internet oder auf Produkte von Unternehmen. Diese Umfrage war insbesondere deswegen aufschlussreich, weil sie in zwei Etappen erfolgte: Der erste Teil fand statt, als noch wenig von den Snowden-Enthüllungen über das Abhörprogramm des US-Geheimdienstes NSA bekannt war, der zweite Teil, als es ein breites

Medienecho gefunden hatte. Obwohl der NSA-Skandal nur staatlichen Missbrauch zum Gegenstand hatte, ging die Akzeptanz bei allen Anwendungen – staatlichen und unternehmerischen – deutlich zurück, am geringsten aber bei der Aufklärung von Straftaten.

Die jüngeren Umfragen zu diesem Thema ergeben ein ähnlich diffuses, oft sogar widersprüchliches Bild, schwankend zwischen Bejahung und Ablehnung dieser Technologie und stark abhängig von ihrer konkreten Anwendung. Auch dürfte die jeweils für die Technologie verwendete Terminologie eine Rolle spielen. Anders als die Allensbach-Umfrage von 2013 fanden die größeren quantitativen Erhebungen des Jahres 2018 nicht anhand des Begriffs Big Data statt. Sie behandeln das Thema unter dem positiver konnotierten Begriff ‚Künstliche Intelligenz' oder dem eher technokratisch anmutenden Begriff ‚Algorithmus'.

Ein durchweg positives Stimmungsbild zum Einsatz Künstlicher Intelligenz verkündet der Digitalverband Bitcom (2018a), dessen Institut Bitcom-Research im Februar 2018 eine repräsentative Meinungsumfrage unter Deutschen über 14 Jahren durchführte. Danach sehen 55 % diese Technologie mehr als Chance, nur 41 % gewichten die Gefahren höher. Ihr Einsatz erzielt hohe Zustimmungsraten in folgenden Bereichen: Prognose von Umweltphänomenen (93 %), Bekämpfung von Finanzkriminalität (92 %), Vermeidung von Staus (86 %), Früherkennung von Krankheiten (81 %), Prognose von Straftaten (61 %), selbstfahrende Fahrzeuge (58 %) (Bitkom 2018; Neuerer 2018). Dieses Ergebnis der Umfrage, die nicht komplett veröffentlicht wurde, verwundert nicht, denn alle Fragestellungen unterstellten einen konkreten, positiven Nutzen, aber keinen Missbrauch.

Zu erheblich skeptischeren Ergebnissen kommt eine ebenfalls repräsentative Umfrage der GfK für den Bundesverband deutscher Banken vom Juni 2018, obwohl sie gleichfalls den Terminus Künstliche Intelligenz verwendet (GfK 2018). Danach kennen 75 % der Deutschen diesen Begriff, aber jeder Vierte hat davon noch nie gehört. Im Gegensatz zu den Ergebnissen der Bitkom-Umfrage verbindet ein Großteil der Deutschen damit eher Befürchtungen (63 %), lediglich 37 % sehen Chancen. Auch können nur 36 % sich vorstellen, die Künstliche-Intelligenz-Anwendung eines selbstfahrenden Autos zu nutzen – rund 20 Prozentpunkte weniger als bei der entsprechenden Bitkom-Umfrage. Das Fazit dieser Umfrage: Generell ist das Misstrauen in digitalgesteuerte Prozesse weiterhin groß.

Das bestätigt auch eine neue Umfrage des Instituts für Demoskopie Allensbach im Auftrag der Bertelsmann-Stiftung (Fischer und Petersen 2018). Sie verwendet dabei nicht den Begriff ‚Künstliche Intelligenz', sondern fragt nach dem Einsatz von Algorithmen, um bei den Befragten nicht den falschen Eindruck zu

erwecken, es handele sich um Software, die genauso intelligent wie der Mensch ist. Danach haben 72 % den Begriff Algorithmus schon einmal gehört, aber 45 % der Befragten fiel spontan nichts dazu ein. Nur zehn Prozent der Befragten gaben an zu wissen, wie Algorithmen funktionieren. Das Wissen darüber, dass Computerprogramme Entscheidungen treffen oder Empfehlungen abgeben, ist für einzelne Anwendungsbereiche sehr unterschiedlich. Die höchste Nennung erzielte mit 55 % der Einsatz individualisierter Werbung im Internet. Dass Algorithmen bei der Diagnose von Krankheiten oder bei der Beurteilung des Risikos, ob ein Straftäter rückfällig wird, eingesetzt werden können, ist nur 28 % beziehungsweise 18 % geläufig. 79 % der Befragten fühlen sich unwohl bei dem Gedanken, dass Computer über sie entscheiden könnten. Insgesamt verbinden nur 18 % mehr Chancen mit dieser Technologie, 36 % dagegen mehr Risiken, fast die Hälfte der Deutschen (46 %) sind in dieser Frage unentschieden.

Ein wiederum ähnliches Stimmungsbild zeichnet die YouGov-Umfrage vom August 2018 (YouGov 2018). Knapp jeder Zweite (45 %) nimmt zwar ein ausgeglichenes Nutzen-Risiko-Verhältnis wahr, ein Viertel (26 %) bewertet das Risiko allerdings als höher, nur 15 % hingegen sehen den Nutzen höher. Das Ergebnis weicht nur geringfügig von der eben erwähnten Bertelsmann-Umfrage (Fischer und Petersen 2018) ab. Erneut zeigt sich ein etwas differenzierteres Ergebnis, wenn nach konkreten Anwendungen gefragt wird, allerdings auch hier mit insgesamt hohen Ablehnungsquoten.

Trotz einiger Unterschiede in der Anlage der Umfragen und ihren Ergebnissen zeigt sich – wenig überraschend – keine klare Meinungsbildung gegenüber dem Einsatz von Big Data, Künstlicher Intelligenz und Algorithmen. Die Umfragen lassen bei einer klaren Mehrheit der Befragten ein deutliches Unbehagen gegenüber Big Data und Künstlicher Intelligenz erkennen, eine verschwommene Angst vor Kontrollverlust, eine zumindest abwartende, zum Teil aber auch geradezu fatalistische Grundhaltung.[1] Im Vergleich zu den Risiken werden die Chancen zur Verbesserung des Lebens durch den Einsatz von Künstlicher Intelligenz und Big Data, also etwa in Medizin, Mobilität, Energie und Umwelt, offensichtlich weniger stark gewichtet. Die Nutzung von Big Data wird stattdessen vor allem mit der Optimierung von Marketing und Werbung durch die großen Internetkonzerne verbunden. Mögliche Trade-offs in puncto Datenschutz werden nur in Bezug auf

[1]Dass dies keine spezifische deutsche Befindlichkeit ist, zeigt eine Umfrage des Pew Research Center. Danach gaben 91 % der Amerikaner schon 2014 an, dass sie die Kontrolle darüber verloren haben, wie Unternehmen ihre persönlichen Daten sammeln und nutzen (Madden 2014).

wenige Anwendungsfelder toleriert, in denen der erwartete Nutzen relativ höher eingeschätzt wird als die damit einhergehenden Risiken, wie das beispielsweise die Erhebungen für den Einsatz von Big Data in der Medizin nahelegen.

Vor dem Hintergrund dieser diffusen Stimmungslage, eines jetzt schon unübersichtlichen Themenfeldes sowie einer sich äußerst dynamisch weiter entwickelnden Technologie lässt sich annehmen, dass der Meinungsbildungsprozess ganz wesentlich davon abhängt, welche Narrative den öffentlichen Diskurs beherrschen. Sie sind so gesehen ein unverzichtbares Mittel, um eine komplexe, letztlich nicht oder nur begrenzt überschaubare Problemstellung überhaupt mit einem relevanten Grad an Öffentlichkeit aushandeln zu können. An den sichtbar dominierenden Narrativen lässt sich infolgedessen ablesen, in welchem Stadium sich dieser Aushandlungsprozess befindet und in welche Richtung er weiterlaufen kann, in welche aber auch nicht.

1.2 Von Konflikten und Kollisionen: Big Data als Gegenstand öffentlicher Narrationen

Eine erste Näherung an die öffentlichen Erzählungen rund um das Themenfeld Big Data zeigen die Bücher, die ausgerechnet Amazon beim Stichwort Big Data auswirft. Dort finden sich neben vielen Ratgebern für die betriebliche Praxis und einigen differenzierten Darstellungen vor allem Bücher mit alarmistischen und dystopischen Titeln (Amazon 2018).[2]

Ähnliches zeigt bereits ein erster Blick auf die Medienrezeption des Themas ‚Big Data' in Verbindung mit Datenschutz in den Jahren 2017/18. Hier lassen sich wiederkehrende Muster in den Darstellungen erkennen, die ebenfalls stark von skeptischen Konnotationen und Furchtappellen geprägt sind. Um diese erste

[2]Hier nur eine kleine Auswahl aus der Amazon-Vorschlagsliste: Stefan Aust und Thomas Ammann. Digitale Diktatur: Totalüberwachung Datenmissbrauch Cyberkrieg; Yvonne Hofstetter. Sie wissen alles: Wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen; Yvonne Hofstetter. Das Ende der Demokratie: Wie die künstliche Intelligenz die Politik übernimmt und uns entmündigt; Michael Keller und Josh Neufeld. Big Data: Das Ende der Privatheit?; Jaron Lanier. Zehn Gründe, warum du deine Social Media Accounts sofort löschen musst; Markus Morgenroth. Sie kennen dich! Sie haben dich! Sie steuern Dich! Katharina Nocun. Die Daten, die ich rief. Wie wir unsere Freiheit an Großkonzerne verkaufen; Cathy O'Neil. Angriff der Algorithmen; Michael Schröder und Axel Schwanebeck (Hrsg.) Big Data – In den Fängen der Datenkraken: Die (un-) heimliche Macht der Algorithmen.

Beobachtung zu überprüfen, wurden 169 Artikel aus dem Medienset DER SPIEGEL, DIE WELT, DIE ZEIT, F. A. Z. Frankfurter Allgemeine Zeitung, FOCUS, Handelsblatt, Süddeutsche Zeitung und taz (jeweils Printausgabe, vom 01.09.2017 bis 01.09.2018, Abfrage über die GENIOS-Datenbank) analysiert und kategorisiert.

Anhand des narrativen Grundgerüsts bestehend aus einem episodischen Ablauf, den ‚Helden' und anderen Akteuren sowie den Erzählplots lassen sich im untersuchten Material Erzählungen rekonstruieren. Dabei wird sichtbar, dass der öffentliche Diskurs zum Umgang mit personenbezogenen Daten vom ‚Big-Brother'-Narrativ dominiert wird, das zumindest in den westlichen Industrienationen fest verwurzelt ist. Wie dieses Narrativ entstanden ist und welche Rezeption es insbesondere in Deutschland bislang erfahren hat, wird im Folgenden skizziert. Darauf aufbauend wird überprüft, welche Erzählelemente in der aktuellen öffentlichen Diskussion wiederzufinden sind.

1.2.1 Ein Narrativ wird entdeckt: ‚Big Brother' in der Kampagne gegen die Volkszählung 1983

Hunderte Initiativen hatten sich gegründet, zu Tausenden marschierten Protestierende durch die Straßen. Ihr Ziel: Boykott der 1983 geplanten Volkszählung, die im Jahr zuvor noch unter der sozialliberalen Koalition von allen damals im Bundestag vertretenen Parteien beschlossen worden war. Gegen die Volkszählung formierte sich in den achtziger Jahren innerhalb kurzer Zeit eine der größten Protestbewegungen der Bundesrepublik, die weit über das Milieu der AKW- und Nachrüstungsgegner hinausreichte.

Bedrohungsszenarien einer totalen Kontrolle wurden mit dem Narrativ des ‚Big Brother' unterlegt und entfalteten enorme politische Sprengkraft. Diese Figur hatte George Orwell (1949) unter dem Eindruck der totalitären Systeme Faschismus und Kommunismus in seinem dystopischen Roman „1984" entworfen. Darin erzählt er die Horrorvision einer Welt, in der die Menschen durch Überwachungskameras, Abhörgeräte und andere Informationssysteme der totalen Kontrolle in dem Ein-Parteien-Staat Ozeanien, angeführt von einer Parteielite und der eher mythischen Gestalt des ‚Big Brother' unterworfen sind. Die Figur des ‚Big Brother' gehört seitdem zu den politisch wirkungsmächtigsten, tief verwurzelten Narrativen, die sich über Generationen hinweg in verschiedenen Spielarten und Kontexten zeigt.

In fast allen gesellschaftspolitischen Debatten über staatliche (oder jetzt auch: unternehmerische) Erfassung und Verarbeitung persönlicher Daten diente und dient ‚Big Brother' als Metapher für Überwachung und Verlust von Privatheit.

Auf sie trifft zu, was „große Erzählungen“ (Gadinger et al. 2014, S. 11) ausmacht, deren Wirkmächtigkeit „schließlich nicht so sehr in ihrer ereignisunabhängigen Kohärenz, sondern in ihrer Unschärfe und in ihren inneren Spannungen“ (Gadinger et al. 2014, S. 11) liegt. Insofern ist das ‚Big-Brother‘-Bild mehr als nur eine Erzählung, es ist zu den „Meta-Narrativen“ (Gadinger et al. 2014, S. 26) zu zählen, „die als übergeordnete Sinnordnungen Orientierung für ‚kleinere‘ Erzählungen bieten“ (Gadinger et al. 2014, S. 26). Schon in den sechziger und siebziger Jahren wurde Orwells „1984“ in politischen Debatten der USA von Demokraten und Republikanern gleichermaßen genutzt, um ihre Kritik etwa an der Planung des National Data Center, der Datenschutzpolitik, der Watergate-Affäre oder an staatlicher Bürokratie metaphorisch zuzuspitzen (Neuroth 2014).

Als 1983 in Deutschland die Volkszählung anstand, traf der Roman mit der symbolischen Gestalt des ‚Big Brother‘ den kritischen Zeitgeist der achtziger Jahre, zumal Orwells „1984“ unmittelbar bevorstand. Die Metapher ‚Big Brother is watching you‘ brachte die wachsenden Ängste vor Videoüberwachung im öffentlichen Raum, Rasterfahndung, Abhörwanzen, Datenbanken und Berufsverboten auf den Punkt. Obwohl das politische System der Bundesrepublik keineswegs mit Orwells Totalitarismus vergleichbar war, wurde das Sprachbild des Big Brother aus dem Roman in dem von Orwell angeführten Kontext herausgelöst und auf die Bundesrepublik übertragen. Es war die Bundesrepublik, die in der Nachfolge des totalitären NS-Staates gesehen wurde und wo man glaubte, den Anfängen wehren zu müssen, gemäß dem fulminanten Diktum Bertolt Brechts „Der Schoß ist fruchtbar noch, aus dem das kroch“ (Brecht 1981, S. 2000). Zu diesem Klima grundsätzlichen Misstrauens gegen den Staat, seine Sicherheitsorgane und die neuen Möglichkeiten der Datenerfassung trug auch das Buch „Die restlose Erfassung: Volkszählen, Identifizieren, Aussondern im Nationalsozialismus“ (Aly und Roth 1984) bei. In dieser Studie, die von den Autoren auch mit der Absicht vorgelegt wurde, die geplante Volkszählung zu verhindern, weisen diese nach, dass die NS-Vernichtungslager ohne die Erfassung der Daten nicht möglich gewesen wären.

Hatte Orwells Roman nach den ersten Ausgaben 1949 keine besondere Auflagenentwicklung gezeigt, sprang er zwischen 1982 und 1984 auf die Bestsellerliste des „Spiegel“. Das Magazin machte Orwell in der ersten Ausgabe des Jahres 1983 sogar zum Titel: Vom Cover mustert ein Auge streng den Leser, darunter die Titelzeile „Der Orwell-Staat“ (Der Spiegel 1/1983). In der Hausmitteilung schrieb die Chefredaktion: „Die Zukunft, die Orwell mit so nachhaltigem Welterfolg aus- und schwarzgemalt hat, diese Zukunft des „Großen Bruders“, des allgegenwärtigen, alles kontrollierenden Staates, sie hat schon begonnen.“ (Der Spiegel 1/1983) In der Titelgeschichte mit der Headline: „Die neue Welt von

1984“ heißt es: „Der gläserne Mensch ist da, seine Daten sind gespeichert. Der technisch perfekte Überwachungsapparat harrt seines politischen Missbrauchers: 1983 ist ‚1984‘. Die Gefahren des ‚großen Bruders‘ sind nicht mehr bloß Literatur. Sie sind nach dem heutigen Stand der Technik real“ (Der Spiegel 1/1983).

Auch der Schriftsteller Günter Grass, der sich ja immer auch als politischer Mahner verstand, bemühte dieses Narrativ Anfang der achtziger Jahre in Wahlkampfreden für die SPD, die er mit dem Titel „Orwells Jahrzehnt“ versah. Darin interpretierte er, genauso wie die Gegner der Volkszählung, Orwells Fiktion nicht, wie von diesem intendiert, als Kritik an (damals) bestehenden Verhältnissen und als Warnung, sondern als Prophetie, die sich schon teilweise bewahrheitet hatte und deren Realisierung im Jahr 1984 unmittelbar bevorstand (Neuroth 2014, S. 75).

Die Opposition gegen die staatliche Sicherheitspolitik und die Volkszählung war zugleich auch Reaktion auf eine Fortschrittsdebatte. Große Teile der Bevölkerung zeigten sich verunsichert oder sogar verängstigt durch die damals neuen Technologien wie Computer, Datenbanken und Gentechnik. Erst kurz zuvor hatte IBM den ersten PC auf den Markt gebracht, das Time-Magazin wählte erstmals nicht eine ‚Person des Jahres‘, sondern eine ‚Maschine des Jahres‘: den Personal Computer. Die neuen Techniken machten Angst, Szenarien von Massenarbeitslosigkeit durch Computer und zunehmender Entfremdung durch eine ‚seelenlose Technologie‘ kursierten.

Die Protestbewegung war erfolgreich, das Bundesverfassungsgericht stoppte die Volkszählung und hob Ende 1983 das zugrunde liegende Gesetz auf, da es in einigen Punkten das Recht auf informationelle Selbstbestimmung verletzt sah. Auf Grundlage des BVerfG-Urteils erarbeitete der Bundestag ein neues Gesetz und die Volkszählung fand schließlich 1987 statt.

1.2.2 ‚Big Brother‘ reloaded: Die Erzählung von Edward Snowden

Im Sommer 2013 enthüllte der CIA-Mitarbeiter Edward Snowden das ganze Ausmaß der Überwachungs- und Spionagepraxis der amerikanischen Geheimdienste und löste damit den NSA-Skandal aus. Die Affäre rief erstmals einer breiten Öffentlichkeit ins Bewusstsein, welche Möglichkeiten Big-Data-Technologien bei der Erfassung und Verarbeitung elektronischer Daten bei der Telefon- und Internetüberwachung bieten. Als zudem bekannt wurde, dass die NSA sogar die deutsche Bundeskanzlerin ins Visier genommen und ihr Handy jahrelang abgehört hatte, schlugen die Wellen besonders hoch. Politik und Medien mussten zur Kenntnis nehmen, dass die NSA bei Auslandsspionage nicht an amerikanische

Datenschutzgesetze gebunden war und Garantien zum Schutz der Privatsphäre nur für Amerikaner, aber nicht für befreundete Regierungen galten.

Es ist eine Ironie der Geschichte, dass Merkels empörter Kommentar „Abhören unter Freunden – das geht gar nicht“ sich nur wenige Monate später gegen sie selbst wendete, als bekannt wurde, dass der dem Kanzleramt unterstehende deutsche Bundesnachrichtendienst ebenfalls Ziele in befreundeten Staaten ausspähte. Obwohl das deutsche Datenschutzgesetz dem Staat enge Grenzen beim Umgang mit persönlichen Daten setzt, wurde auf einmal sichtbar, wie leicht jemand Objekt der anlasslosen und unterschiedslosen Erfassung und Speicherung jedweder Daten durch ausländische Geheimdienste werden konnte, die zudem noch gegenseitig Informationen austauschten. Vermutlich ist der Begriff Big Data in Deutschland durch die NSA-Affäre deutlich negativ konnotiert. Wie die bereits erwähnte Allensbach-Studie aus dem Jahr 2013 festhält, hatten die Enthüllungen Snowdens die Einstellung der Bevölkerung zu Big Data negativ beeinflusst. Die hier verwendete Medienanalyse zeigt bis ins Jahr 2018 die vielfache Verwendung von Konstrukten wie ‚Gedankenpolizei‘ oder des ‚Gläsernen Menschen‘. Der assoziative Schritt von Big Data zu Big Brother ist ja auch naheliegend.

Die Snowden-Erzählung ist nach wie vor eine der Storys, die am häufigsten in den Medien aufgegriffen wird, wenngleich sie durchaus changiert zwischen Heldengeschichte und Judas-Erzählung (Gladinger et al. 2014, S. 17 ff.). Ist Snowden nun der Held, der die Welt vor totalitaristischen Praktiken warnt, oder ist er ein Verräter, der die Sicherheit des Westens gefährdet und beim Feind in Moskau Unterschlupf findet? Hier ist die typische Vieldeutigkeit starker Erzählungen zu beobachten, die noch nicht zu einem Ende geführt sind und die für alle Seiten noch Spielraum für Erzähl-Interventionen bieten, in dem weiter ausgelotet wird, in welche Richtung die Diskussion über Big Data und Big Brother sich final entwickeln wird. Wem die Rolle des Big Brothers zugeschrieben wird und wer der Retter in der Not ist, ergibt sich als Konstrukt aus den jeweiligen öffentlichen Diskursen.

Während die Ambivalenz dieser Erzählung in den Vereinigten Staaten anhält, solange Snowden dort langjährige Gefängnisstrafen drohen, setzte sich in Deutschland schnell die Heldenerzählung, zusätzlich aufgeladen mit dem Big-Brother-Narrativ, als vorherrschende Interpretation durch. „Erschreckend aktuell: George Orwells ‚1984‘. Unheimliche Verwandtschaft zwischen NSA und dem ‚Großen Bruder‘“ (Schulz-Ojala 2013) lautete beispielsweise die Headline eines Artikels im Tagesspiegel. Selbst der ehemalige Präsident des Bundesnachrichtendienstes Hansjörg Geiger sah sich zu der Warnung veranlasst: „Die neue mögliche Quantität der Überwachung schafft eine neue Qualität. Das ist falsch, das ist Orwell.“ (zitiert in Schulz-Ojala 2013). Die Verkaufszahlen von „1984“ stiegen wieder (Lindner 2017).

1.2.3 Die Manipulation: Die Erzählung von der Beeinflussung des US-Wahlkampfs 2016

Einen zusätzlichen Schub und zugleich eine zusätzliche Variante erhielt die ‚Big-Brother'-Erzählung im Frühjahr 2018 durch die Offenbarung eines Whistleblowers, dass sich die englische Datenanalysefirma Cambridge Analytica (CA), in der der Trump-Unterstützer Robert Mercer investiert war, mehr als 50 Mio. Datensätze von Facebook-Nutzern widerrechtlich und ohne deren Kenntnis sich angeeignet und im US-Wahlkampf von Donald Trump eingesetzt hatte. So ist es kein Wunder, dass Fragen des Daten- und Verbraucherschutzes, die Angst vor dem ‚gläsernen Bürger' und die Sorge vor Missbrauch persönlicher Daten durch Staat und Konzerne in der gesellschaftlichen Debatte über Big Data erneut in den Vordergrund traten.[3]

Cambridge Analytica war schon zuvor zu einer zweifelhaften Berühmtheit geworden: Anfang Dezember 2016, wenige Wochen nach Trumps Wahl, schrieb die Schweizer Zeitschrift „Das Magazin" über dieses Unternehmen eine mehrseitige Geschichte mit der Überschrift „Diese Firma weiss [sic], was Sie denken" und erläuterte das im Vorspann so: „Cambridge Analytica kann mit einer neuen Methode Menschen anhand ihrer Facebook-Profile minutiös analysieren. Und verhalf so Donald Trump mit zum Sieg" (Grassegger und Krogerus 2016). Demnach hatte Trump seinen Wahlsieg Big Data und der Manipulation der Wähler durch den massenhaften Einsatz von Psychografie (der Vermessung der Persönlichkeit) auf Facebook-Konten und Mikrotargeting zu verdanken. Angeblich war CA mit der Methode in der Lage anhand von zehn Facebook-Likes eine Person besser einzuschätzen als etwa ein Arbeitskollege.

Mit individualisierten Werbebotschaften hätten die Trump-Helfer demnach nicht nur potenzielle Wähler ansprechen, sondern vor allem potenzielle Clinton-Wähler von den Wahlurnen fernhalten können, rühmte sich CA nach der Wahl. Dazu gehörten beispielsweise Videos mit Fake-News, in denen Hillary Clinton schwarze Männer angeblich als Raubtiere bezeichnete und die Afroamerikanern zugespielt wurden. Facebook habe sich als bester Wahlhelfer erwiesen, zitieren die Schweizer Journalisten einen Trump-Mitarbeiter. Ihr Fazit: „Es ist ein Treppenwitz der Geschichte, dass Trump oft über die Wissenschaft schimpfte, aber wohl dank ihr die Wahl gewann" (Grassegger und Krogerus 2016). Dass Steve Bannon,

[3]Mehr als 80 % aller ausgewerteten Artikel aus der hier durchgeführten Medienanalyse erwähnen explizit den Fall von Cambridge Analytica.

Trumps Berater und zuvor Herausgeber der ultrarechten Breitbart News, damals als Vizepräsident Cambridge Analytica de facto führte, verlieh der Geschichte zusätzliche Plausibilität und Brisanz. Die Medien flogen denn auch auf sie, in den sozialen Medien wurde sie tausendfach geteilt, zumal in den USA Storys mit ähnlichem Tenor erschienen. Die Geschichte von der Manipulation der US-Wahl mithilfe von Big Data und Fake-News war geboren.

Die „Bild"-Zeitung berichtete groß (Bild 2016). In Großbritannien beschrieb ein Blogger die Methode des Wähler-Targeting auf Basis psychologischer ‚Schwächen' als „Orwellian" (Brown 2018). Die französische Internetzeitung Mediapart titelte den Artikel von Duparc und Hourdeaux (2018): Cambridge Analytica, die Big-Brother-Wahl von Donald Trump. Fertig war die Story, dass „Donald Trump der sinistre Manipulator des Social Web ist und es möglich ist, das Social Web dergestalt zu manipulieren, dass alle Nutzer nach dem Takt eines Big Brother tanzen", kommentierte der Internet-Blogger Thomas Knüwer (2016). Wie groß der Einfluss von CA auf den US-Wahlkampf tatsächlich gewesen ist, bleibt umstritten. Spiegel-Online schrieb dazu: „Das sagenhafte Echo, das solche Geschichten […] im Moment erfahren, hängt wohl auch mit dem Schock und der allgemeinen Verunsicherung nach dem Trump-Sieg zusammen, den viele nicht für möglich gehalten haben" (Reinhold und Schnack 2016). Die Mitgründerin von „Algorithm Watch", Lorena Jaume-Palasi, hält die Cambridge-Analytica-Affäre lediglich für die „Inszenierung eines Skandals" (Witzeck 2018), da CA „seine algorithmische Methode der ‚Psychometrics' nie genutzt" (Witzeck 2018) habe. Man wisse nicht, ob sie funktioniere. Die Wähler von Trump hätten Fox News gesehen und kaum soziale Medien genutzt (Witzek 2018). Im Mai 2018 stellte CA einen Insolvenzantrag.

Dass sich die Manipulationslegende trotzdem so zählebig zeigt, liegt womöglich auch daran, dass US-Präsident Donald Trump nach seiner Wahl Anlass für Assoziationen zu George Orwells „1984" gab. Als er beispielsweise behauptete, keine andere Vereidigung habe jemals ein so großes Publikum gehabt wie seine, und ihm seine Beraterin Kellyanne Conway mit der Bemerkung beistand, dies seien ‚alternative Fakten' zog die Presse sofort Parallelen zu dem ‚Wahrheitsministerium' von „1984". Der Roman selbst wurde wieder stärker nachgefragt, auf der Bestsellerliste von Amazon sprang er auf Platz eins, der Verlag druckte 75.000 Exemplare nach (Lindner 2017).

In Deutschland hat der Schriftsteller Daniel Kehlmann ein Nachwort zur Neuausgabe geschrieben. Er erkenne unter Trump zwar keine totalitären Tendenzen wie in Orwells „1984", sagt Kehlmann (2017), aber er sieht „Überscheidungen" etwa derart,

> dass Wahrheit ununterbrochen ständig neu definiert wird, […] dass das System der Diktatur vor allem dadurch sein kann, was es ist, indem es die absolute Bestimmungsmacht darüber hat, was Wahrheit ist. Und […] das ist eine Parallele, die sehr wohl existiert. (Kehlmann 2017)

Orwells Roman „1984" mit ‚Big Brother', ‚Wahrheitsministerium' und ‚Neusprech' scheint also weiterhin den Nerv unserer Zeit zu treffen. Das Narrativ ist so stark verwurzelt, dass es sofort aufgegriffen wird, wenn sich in unserer heutigen Welt Parallelen zu den Figuren, Institutionen und Handlungen des Romans erkennen lassen.

1.2.4 Spione im Kinderzimmer: Die Erzählung vom Verlust der Privatsphäre

Im Februar 2017 verbot die Bundesnetzagentur dem amerikanischen Spielzeughersteller Genesis, seine sprechende Puppe „My Friend Cayla" in Deutschland zu verkaufen. In die Puppe mit den blauen Augen und dem blonden Haar war ein Mikrofon eingebaut. Sprachen Kinder mit ihr, wie das Kinder mit ihrer Puppe so tun, wurde das über Funktechnik und eine App auf dem Smartphone per Internet mit den Servern des US-Konzerns Nuance Communications verbunden und das biometrische Stimmprofil erfasst. Die Puppe war intelligent. Stellten Kinder ihr eine Frage, antwortete die Puppe – eine einfache Variante von Sprachassistenten wie Alexa, nur nicht als solche gekennzeichnet. Die Bundesnetzagentur stufte sie deshalb als versteckte, sendefähige Anlage ein – ein illegales Spionagegerät. Die App gab viele persönliche Daten weiter, inklusive Adressbuch des Smartphones, ohne Datenschutzerklärung. Für den Hersteller waren die Daten wie auch die kindlichen Gespräche nützlich für Marktforschung und Produktentwicklung.

Auch der amerikanische Hersteller Mattel hatte in den USA, wo Datenschutz eine weit geringere Rolle als in Deutschland spielt, eine sprechfähige Puppe auf den Markt gebracht. „Hello Barbie" war mit den Servern von Mattel verbunden, die Reaktion und Sprache der Kinder verarbeiteten. Mattel versprach sich davon ebenfalls Marktforschung mit dem Ziel, neue Dienstleistungsangebote zu entwickeln für Kinder und Eltern. Letztere wurden mit der Funktion geködert, das Gespräch zwischen Kind und Puppe auch an die Eltern zu senden. Ein verlockendes Angebot für Helikopter-Eltern, die besorgt über jeden kleinen Schritt ihrer Kinder wachen wollen und so ihr ‚gläsernes Kind' mit Mattel teilen würden. Mattel hat die Puppe jedoch vom Markt genommen, nachdem Datenschützer der Firma den „Big Brother Award" verliehen hatten.

Was von den Spielzeugherstellern versucht wurde, bediente erneut die Ängste einer flächendeckenden Überwachung ohne mögliche private Rückzugsorte. Das schon einige Jahre alte Zitat von Facebook-Chef Zuckerberg, dass Privatheit nicht mehr die soziale Norm sei, wurde in den Medien erneut kritisch diskutiert. Der hohe Empörungsfaktor, den diese an sich kleine Geschichte aufweist, hängt allerdings nicht zuletzt mit der Machtasymmetrie zwischen Kindern und Konzernen zusammen. Spione sind schon schlimm, aber im Kinderzimmer, das geht gar nicht – so unisono der Medientenor. Vermutet wurde eine einfache strategische Überlegung: Wer als Kind schon ohne Privatsphäre aufgewachsen ist, wird sich als Erwachsener kaum noch dagegen auflehnen. Eine weitere Variante bzw. Fortsetzung dieser Geschichte von der Überwachung von Kindern bot dann im Dezember 2017 die Serie mit dem bildhaften Titel „Arkangel“ aus der Netflix-Produktion „Black Mirror“. Regisseurin Jody Foster wirft darin einen dystopischen Blick auf eine bereits mögliche Totalüberwachung von Kindern und Jugendlichen.

1.2.5 Die Apokalypse: Die Erzählung vom digitaltotalitären Staat

Wer Hinweise für die freiheitsgefährdenden Potenziale von Big Data sucht, der braucht seine Fantasie aber nicht weit in die Zukunft schweifen zu lassen. Es reicht, sich die Berichte über China anzuschauen. Für den englischen Economist (2016) ist es das ehrgeizigste Experiment digitaler sozialer Kontrolle in der Welt. So wie Banken im kapitalistischen Westen die Kreditwürdigkeit von Kunden durch Scoring abbilden, will China das soziale und politische Verhalten seiner 1,4 Mrd. Einwohner in einem Punkte-System erfassen. Bis 2020 soll ein umfassendes Sozialkredit-System, ein sogenannter Super-Score, mit dem Ziel entstehen, das Verhalten der gesamten Gesellschaft im Sinne einer harmonischen sozialistischen Gesellschaft zu beeinflussen (Sachverständigenrat für Verbraucherfragen 2018, S. 61 ff.).

Danach erhalten Bürger, Firmen und Behörden Punkte für im sozialistischen Sinn tugendhaftes Verhalten, etwa berufliche Auszeichnungen oder soziales Engagement, und Punkteabzüge bei schlechtem Verhalten, beispielsweise für Verkehrsvergehen, Steuerhinterziehung oder die Vernachlässigung der alten Eltern oder auch, wenn man allein in zu großen Wohnungen lebt oder ausländische Luxusautos fährt. Wer eine höhere Punktzahl erreicht, kann mit schnellerer Beförderung im Job oder schnellerer Zuweisung von staatlichen Wohnungen rechnen, eine niedrige Punktzahl wirkt sich negativ auf die Bewilligung von Reisen ins Ausland, Schulplätze für die Kinder, auf die Wohnungssuche oder auch die Nutzung von Autobahnen aus.

Offiziell wird das System mit dem Ziel begründet, mehr Verlässlichkeit im wirtschaftlichen und sozialen Leben bewirken zu wollen. Dadurch sollen korrupte Funktionäre und Unternehmen mit schlechten oder gefälschten Produkten an den Pranger gestellt werden. Aber das System lässt sich eben auch gegen jedwedes unerwünschte Verhalten einsetzen, welches vermeintlich die soziale Ordnung unterminiert oder nationale Verteidigungsinteressen gefährdet. Das Sozialkreditsystem gilt deshalb als „ein Upgrade des chinesischen Überwachungsstaates" (Mazur 2018).

Die chinesischen Sicherheitsgesetze geben dem Staat unbeschränkten Zugang zu fast allen persönlichen Daten. Erfasst werden Hotelaufenthalte, Eisenbahnfahrten und Flüge und in manchen Orten schon der Autoverkehr. Großflächige Überwachungssysteme überwachen den Alltag der Chinesen. Installiert sind derzeit rund 200 Mio. Kameras, vier Mal so viele wie in den USA, und bis 2020 sollen noch mal 100 Mio. hinzukommen. Wie das funktioniert, zeigt sich schon heute in einigen Städten. Bildschirme groß wie Reklametafeln zeigen Bilder von Fußgängern samt Namen und Personalausweisnummer, die bei Rot über die Ampel gehen und mit Hilfe von Gesichtserkennung identifiziert wurden. Andere Tafeln stellen die Namen von Leuten, die ihre Schulden nicht bezahlen, an den Pranger.

China ist heute schon der weltweit größte Markt für Überwachungstechnologie. Regierungsgelder fließen in die Erforschung von Technologien zur Identifizierung von Personen anhand ihrer Gesichter, ihrer Kleidung und sogar ihres Gangs. Experimente laufen, den Personalausweis durch eine App von WeChat zu ersetzen. Eine Kamera mit Gesichtserkennungssoftware gleicht das Gesicht mit der registrierten ID ab. Die Polizei wird mit Spezialbrillen zur Gesichtserkennung ausgerüstet. Was Überwachungstechnologien betrifft, können sich chinesische High-Tech-Firmen mit den besten der Welt messen. In einem Technowettbewerb des US-Geheimdienstes zur Gesichtserkennung belegte das chinesische Start-up Yitu Technology 2017 den ersten Platz (Mazur 2018).

Zur Kontrolle des Internets blockiert China mit der Great Firewall den Zugang westlicher Internetseiten. Der Staat bietet den chinesischen Internetgiganten Alibaba, Tencent und Baidu, die der staatlichen Aufsicht unterliegen, lukrative Geschäftsfelder, indem er sie vor ausländischer Konkurrenz schützt. Dafür stellen sie ihm die Daten ihrer Nutzer zur Verfügung. Das nächste Ziel ist, die verschiedenen Teilelemente zu integrieren zu einer 360-Grad-Überwachung. Dann wäre der erste digitale totalitäre Staat vollendet. „Pekings Pläne für das digitale China stellen sogar George Orwells düstere Vision des totalen Überwachungsstaats in den Schatten" (Steltzner 2018, S. 19 f.).

Dass dies bei der Bevölkerung auf breiten Widerstand stößt, ist so bald nicht zu erwarten. Nach einer Online-Befragung von etwa 2200 chinesischen Internetnutzern durch die Freie Universität Berlin begrüßten 80 % der Befragten solche Sozialkreditsysteme, und 80 % lassen sich schon freiwillig bewerten (Kostka 2018). Die hohe Zustimmung liegt nach Ansicht der Studienleitung daran, dass die meisten von den Systemen profitieren. Das Ergebnis überrascht vor dem kulturellen Hintergrund Chinas wenig, da es nicht über eine dem Westen ähnliche Tradition bürgerlicher Freiheiten und Privatheit verfügt. Auch im kulturell ähnlichen Singapur, wo mithilfe eines ehemaligen amerikanischen Geheimdienstexperten schon vor einigen Jahren ebenfalls ein auf Big-Data-Anwendungen basierendes Super-Score-Programm installiert wurde, gibt es bei der Bevölkerung keinen wirklichen Protest. Die Mehrheit der Bürger hat die Überwachung als notwendig akzeptiert, um Terrorismus und ‚Selbstradikalisierung' zu bekämpfen. Zwischen der Bevölkerung und der Regierung gibt es einen ‚sozialen Kontrakt'. Sie verzichte bewusst auf bestimmte bürgerliche Rechte und individuelle Freiheiten im Austausch für grundlegende staatliche Garantien: Sicherheit, Bildung, bezahlbare Wohnungen und Gesundheitsversorgung (Harris und Castelao 2014).

1.2.6 Die Verselbstständigung der Maschine: Die Erzählung vom unkontrollierbaren Auto

Zwei weitere Narrative lassen sich aus der Medienanalyse rekonstruieren, die etwas anders gelagert sind als die Überwachungs-Dystopie von „1984", aber in der öffentlichen Diskussion ebenfalls als prägend anzusehen sind. Mit dem Begriff ‚Künstliche Intelligenz' verbinden sich nämlich etwas andere narrative Elemente als mit Big Data. Eine hohe Intelligenz, die aber künstlich ist, lässt sich zu anderen, konkreteren Bildern verdichten als die unsichtbaren, weniger greifbaren Big Data-Phänomene. Hier liegen die Kollisionen und Konflikte in dem Bild der sich verselbstständigenden Maschine, der außer Kontrolle geratenen Roboter und autonomen Fahrzeuge. Begriffe wie ‚Killer-KI', die insbesondere für militärische Anwendungen verwendet werden, oder Narrative wie der ‚Aufstand der Maschinen' prägen die Medientexte.

Besonders prägnant ist dies anhand der Erzählungen von Unfällen mit autonom fahrenden Autos zu beobachten, die im Frühjahr 2018 die Medien füllten. Sie berichteten ausführlich, als beispielsweise ein Tesla gegen einen Lastwagen prallte und der Fahrer starb oder als eine Fußgängerin von einem autonom fahrenden Uber-Auto tödlich verletzt wurde. Aber auch jeder kleinere Unfall mit

Sachschaden war eine Schlagzeile wert. Dabei kann den Medien nicht der Vorwurf undifferenzierter Berichterstattung gemacht werden. So berichteten sie im Tesla-Fall, dass die untersuchende Behörde die Schuld bei dem Fahrer sah, der trotz Aufforderung das Lenkrad nicht in die eigenen Hände nahm. Im Uber-Fall zitierten sie auch die Einschätzung von Experten, dass der Fahrer auch keine Chance gehabt hätte, den Unfall zu vermeiden, wenn das Fahrzeug konventionell gesteuert worden wäre. Ebenfalls weisen die Medien zumeist darauf hin, dass die Testfahrzeuge noch nicht die Endstufe Level 5 erreicht haben, bei der die Fahrzeuge ohne Lenkrad und Bremsen und damit ohne einen Fahrer, der zur Not eingreift, auskommen.

Dennoch ist die erhöhte Medienaufmerksamkeit für diese Fälle aufschlussreich: Ging es bisher bestenfalls um Assistenzsysteme, die den Fahrer in bestimmten Situationen unterstützen, soll autonomes Fahren im Endzustand den Fahrer völlig ersetzen. Das Auto hört auf, ein Objekt in der Hand des Fahrers zu sein und wird zum eigenständig handelnden Subjekt. Die Vision eines fahrerlosen Autos war aber immer schon ambivalent. Der Dualismus zwischen ‚Wunderbarem und Unheimlichem' ist schon in der Kurzgeschichte des Science-Fiction-Schriftstellers David H. Keller „The Living Machine" von 1935 angelegt. Sie handelt von der Erfindung des selbstfahrenden Autos, das den Menschen anfangs Nutzen bringt in Form von weniger Unfällen etc., dann aber auf einmal außer Kontrolle gerät und Jagd auf Menschen macht. „Dieses imaginäre Phantasma des Kontrollverlusts über die fahrerlosen Maschinen wird sich als dominantes Muster durch das 20. Jahrhundert ziehen", urteilt Fabian Kröger (2015, S. 42). Dieses Narrativ ist typisch für die von technologischen Umbrüchen gekennzeichnete Moderne. Es steht für die Ängste vor dem Kontrollverlust angesichts einer Entwicklung, die von ihren Urhebern nicht mehr eingefangen werden kann und sich letztlich gegen ihren Schöpfer richtet.

1.2.7 Die globale Gier: Die Erzählung von der Weltherrschaft der ‚Frightful 5'

Es war die New York Times, die am 10.5.2017 zuerst das Bild von den ‚Frightful 5' verwendete und damit die Internetkonzerne Google, Apple, Facebook, Amazon und Microsoft meinte, abgekürzt GAFAM. Angesichts der Mächtigkeit, die den fünf großen US-Internetkonzernen zugeschrieben wird, ist es nur folgerichtig, dass die Sprachbilder, mit denen sie beschrieben werden, ganz überwiegend aus dem politischen bzw. militärischen Sprachgebrauch kommen. Wird das Verhältnis der Konzerne untereinander beschrieben, dann sind ‚Kampf der Supermächte'

oder ‚Kalter Krieg' viel gebrauchte Metaphern. Geht es um die Beschreibung des Verhältnisses der Konzerne zu ihren Stakeholdern, dann dominieren in den hier analysierten Medien Metaphern wie ‚Techno-Feudalismus', ‚digitale Diktatur', ‚digitaler Kolonialismus' oder ‚digitaler Imperialismus'. Die Botschaft ist klar: Hier entsteht ein politisch und gesellschaftlich nicht gewünschtes Machtgefüge, dem durch entsprechende staatliche Interventionen Einhalt geboten werden muss. Politische Metaphern sind immer zugleich Rufe nach einer politischen Lösung, unabhängig davon, ob und wie sie sich faktisch realisieren lässt.

Die Erzählung von den ‚Fürchterlichen 5', die eine neue Weltherrschaft begründen, ist insofern als Weitererzählung der eben beschriebenen Narrationen zu sehen, die auf dem Big-Brother-Meta-Narrativ beruhen. Insbesondere Facebook sieht sich in den deutschen Medien im Zusammenhang mit der Cambrigde-Analytica-Geschichte breiter Kritik ausgesetzt. „So wurden die einstigen Lieblinge des digitalen Zeitalters in atemberaubender Geschwindigkeit zu dunklen Mächten einer dystopischen Zukunft" (Knop 2018).

Ausdruck fand diese Schurkengeschichte wiederum in der Belletristik. Einer, der diese erzählerische Marktlücke über das Ende der Privatheit im Zeitalter der großen Internetkonzerne frühzeitig erkannt hat und den Faden von Orwells „1984" weiterspinnt, ist Dave Eggers (2013) mit seiner Erzählung „Circle". Der Roman stieß in Deutschland auf große Resonanz, er wurde häufig in den Medien besprochen und stand laut Wikipedia schon zwei Wochen nach Erscheinen der deutschen Übersetzung ganz oben auf den Bestsellerlisten. Eggers Dystopie ist die Terrorherrschaft des Digitalen, die freiwillige Unterordnung in eine totale Überwachungsgesellschaft. Im Gegensatz zu Orwells „1984" erwächst die Horrorvision nicht in einem diktatorischen System, sondern in der hippen, gesunden Welt einer freiheitlichen Gesellschaft.

Im Mittelpunkt steht ein fiktives Internetunternehmen, das wie eine Fusion aus Google, Facebook und Twitter scheint und das sich, nicht unähnlich den Digitalkonzernen im Silicon Valley, hehre Ideale auf die Fahnen geschrieben hat. In diesem Fall sind das ‚Leidenschaft, Partizipation, Transparenz', die sich allerdings, und das ist der Kern der Geschichte, im Verlauf der Handlung geradezu zwangsläufig in ihr Gegenteil verkehren: „Aus Freiwilligkeit wird Zwang, aus Aufklärung Despotismus, aus Einzigartigkeit Konformität", schreibt der Kritiker der FAZ (Bernard 2014). Dem Einzelnen ist es nicht möglich, sich dieser Offenheit zu entziehen, Transparenz wird zu Totalüberwachung. Die klaren Bezüge zu Facebook sind gewollt: ‚Alles Private ist Diebstahl', sagt die Roman-Protagonistin. Oder, wie die Schriftstellerin Margaret Atwood (2013) in einer Rezension schreibt: „The brave new world of virtual sharing and caring creates monsters."

Fazit Fasst man diese Rekonstruktionen zusammen, dann ist schnell zu sehen, dass in der von den Medien transportierten gesellschaftlichen Debatte über Big Data die Angst vor dem ‚gläsernen Bürger' und die Sorge vor Missbrauch personenbezogener Daten durch Staat und Konzerne im Vordergrund stehen. Wie alle Risiken sind auch die Risiken von Big Data grundsätzlich als soziale Repräsentationen einer angenommenen Gefährdung zu sehen, d. h. Risiken sind allgemein geteilte Vorstellungen über oft komplexe Sachverhalte. Sie werden in den kommunikativen Beziehungen geformt und beruhen weniger auf technisch-naturwissenschaftlichen Wahrscheinlichkeiten, sondern vielmehr auf subjektiv-qualitativen Kriterien von persönlicher Betroffenheit. Die faktische Ambivalenz der Dual-Use Technologie wird narrativ in eine Richtung aufgelöst, nämlich in Richtung der zweckentfremdeten, nicht akzeptablen Nutzung. Deutlich zu erkennen sind immer wieder Varianten der Big-Brother-Erzählung, die im öffentlichen Diskurs das stärkste Narrativ bilden.

Um in der narrativen Analyse zu bleiben: Alle hier skizzierten Erzählungen verbleiben in den typischen Erzählphasen, die sich mit Konflikten und deren Kollisionen beschäftigen, die zwischen Antagonisten ausgetragen werden oder die Protagonisten, in diesem Falle den Bürger und Nutzer, selbst in Gestalt innerer Konflikte beschäftigen. In Bezug auf die Episodenabfolge lässt sich dementsprechend feststellen, dass die Problemlösung sowie die daraus folgenden Konsequenzen nicht eindeutig auftauchen. Wiederkehrende Narrative, die umgekehrt positive Ergebnisse, einen glücklichen Ausgang oder eine kreative Lösung thematisieren, sind jedenfalls nicht zu finden.[4] Vor allem aber verfängt keinesfalls die Erzählung der ‚Frightful 5', dass sie mit ihrem Handeln eine bessere Welt schaffen, in der die Digitalisierung ein globales Dorf schafft, in dem alle miteinander freundschaftlich vernetzt sind und gemeinsam Gutes schaffen.

1.3 Nutzen und Schutz von Daten des Bürgers im politischen Diskurs

Vor dem Hintergrund dieser öffentlichen Diskussion findet der politische Diskurs im engeren Sinn zwischen den involvierten Entscheidungsträgern statt. Dieser politische Diskurs ist zunächst einmal von Paradoxien geprägt, die sich aus dem

[4]Erkennbar sind durchaus Versuche, positive Metaphern zu bilden, z. B. vom ‚Datenschatz', im Vergleich zu konträren Metaphern wie ‚Datenflut' oder ‚Datenrausch', aber im untersuchten Material sind diese zahlenmäßig deutlich geringer.

Dual-Use-Phänomen ergeben: Regierungen versuchen, dem unkontrollierten Umgang mit personenbezogenen Daten Grenzen zu setzen, möchten aber durchaus selbst von Big Data profitieren, z. B. indem Daten genutzt werden, um die richtigen ‚Nudges' für sozial gewünschtes Verhalten, von reduziertem Drogenkonsum bis zu mehr Steuerehrlichkeit, setzen zu können. Und natürlich stellt sich die grundlegende Frage nach der Vereinbarkeit von zwei gegenläufigen Interessen: Wie soll der Datenschutz in Zeiten von Big Data und künstlicher Intelligenz geregelt werden, um Missbrauch persönlicher Daten und monopolistische Strukturen zu vermeiden, ohne aber gleichzeitig die Chancen dieser Technologie für Wohlstand und wissenschaftlichen Fortschritt zu verbauen? Diese Paradoxien spiegeln sich durchgängig im politischen Diskurs wider bzw. bestimmen dort die Argumentationslinien.

Um diesen Paradoxien besser gerecht zu werden, mag es opportun erscheinen, statt Big Data den Begriff Künstliche Intelligenz in den Vordergrund zu stellen, der vermutlich weniger angstbeladen ist und ohnehin häufig synonym mit Big Data verwendet wird. Der Koalitionsvertrag von CDU/CSU und SPD für die 19. Legislaturperiode verzichtet völlig auf den Begriff Big Data, obwohl ihr der Themenkomplex sieben Absätze wert ist (Bundesregierung 2018). Im Masterplan der Bundesregierung unter dem Titel „Eckpunkte der Bundesregierung für eine Strategie Künstliche Intelligenz" (Bundesministerium für Bildung und Forschung 2018) findet der Begriff Big Data immerhin zweimal Erwähnung, von Künstlicher Intelligenz ist insgesamt 17 Mal die Rede. Allerdings zeigt diese Strategie der Diskursbeeinflussung bislang noch kaum Wirkung. Schon das weiterhin vorherrschende Narrativ der sich verselbstständigenden Maschine, das mit dem Begriff der Künstlichen Intelligenz verbunden ist, hat dies gezeigt.

Dementsprechend kommt die hier angestellte Medienanalyse zu dem Ergebnis, dass – die direkten Medienbeiträge von Regierungs- oder Kommissionsvertretern ausgeklammert – zwischen September 2017 und 2018 kaum zwischen Big Data und Künstlicher Intelligenz differenziert wurde, wenn es um die generell skeptische, von konfliktbeladenen Narrativen geprägte Diskussion geht. Dennoch wird diese Beobachtung weiter zu überprüfen sein, denn ebenso unverkennbar ist, dass mit der Verwendung des Begriffs Künstliche Intelligenz der Fokus der Betrachtung auf die möglichen Anwendungen bzw. den Nutzen von Big Data verschoben wird. Die Medienanalyse weist in diesem Zusammenhang einen eindeutigen Schwerpunkt bei den dargestellten Anwendungen aus, nämlich das Themenfeld Medizin.

1.3.1 Datenschutz im Fokus der Gesetzgebung: Rechtliche Regelungen für den Umgang mit personenbezogenen Daten

Die bisherige Gesetzgebung zum Datenschutz ist als ein Zwischenstand zu betrachten, in dem die gesellschaftspolitische Diskussion bzw. der politische Diskurs zum Umgang mit Big Data quasi eingefroren ist.

Im Urteil zur Volkszählung 1983 hat das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung unter den Bedingungen der modernen Datenverarbeitung definiert als „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten“ (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2018).

Wie im Einzelnen mit personenbezogenen Daten zu verfahren ist, regeln das Bundesdatenschutzgesetz, die Datenschutzgesetze der Länder und seit 2018 die Datenschutzgrundverordnung (DSGVO). Danach ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nur erlaubt, wenn die betroffene Person dem zuvor schriftlich zugestimmt hat und sie über den Zweck aufgeklärt wurde. Dabei gelten die Grundsätze der Datensparsamkeit und der Datenvermeidung, soll heißen, dass so wenig personenbezogene Daten wie möglich verwendet und diese, wenn möglich, anonymisiert oder pseudonymisiert werden. Der Datenschutz ist als klassisches Abwehrrecht gegenüber einem möglicherweise übergriffigen Staat entstanden.

Als personenbezogene Daten gelten etwa Name, Telefonnummer, E-Mail-Adresse oder IP-Adresse. Besonders geschützt sind Informationen über ethnische Herkunft, politische, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Die Bürger haben ein Auskunftsrecht, ob und welche Daten gespeichert sind, aus welchen Quellen sie stammen und zu welcher Verwendung sie dienen. Sie können die Berichtigung falscher Daten, ihre Löschung oder Sperrung verlangen. Jeder hat das Recht, der Nutzung seiner Adressdaten für Werbung oder Markt- und Meinungsforschung zu widersprechen und eine Sperrung seiner Daten zu verlangen.

Die Datenschutz-Grundverordnung der EU (DSGVO), die im Mai 2018 in Kraft trat, soll den Schutz personenbezogener Daten bei der Verarbeitung durch Staat und Privatwirtschaft noch verbessern und gleichzeitig den freien Datenverkehr im europäischen Binnenmarkt gewährleisten. Sie gilt für die EU-Märkte und ist insofern

auch für die großen amerikanischen Internet-Konzerne auf europäischem Boden verbindlich.[5] Dabei sind folgende Grundsätze maßgeblich (Bundesministerium der Justiz und für Verbraucherschutz 2018):

- Personenbezogene Daten werden nur so verarbeitet, wie es bei der Erhebung kommuniziert wurde.
- Der Zweck der Datenverarbeitung muss vorher festgelegt werden. Eine Weitergabe der Daten bedarf der Zustimmung der Datengeber.
- Es sollen nur die dem Zweck angemessenen Daten erhoben werden (‚Datensparsamkeit').
- Daten müssen korrekt sein, fehlerhafte müssen korrigiert oder gelöscht werden. Dazu kommt ein ‚Recht auf Vergessen werden' bei personenbezogener Daten.
- Die Daten sollen nur so lange gespeichert werden, wie es der Zweck verlangt.
- Daten müssen vertraulich behandelt und durch technische und organisatorische Maßnahmen vor unrechtmäßiger Verarbeitung geschützt werden, die vonseiten des Unternehmens, das die Daten erhebt, in das Produkt oder die Dienstleistung einzubauen sind (‚Data Privacy by Design').
- Datenerhebende Unternehmen sind rechenschaftspflichtig gegenüber Öffentlichkeit und Behörden.

Die dort formulierten Grundprinzipien geben zugleich wichtige Schlagwörter des politischen Diskurses wieder: Zweckbestimmung, Transparenz, Integrität, Vertraulichkeit, Rechenschaftspflicht, Verantwortlichkeit oder Treu und Glauben. Diese Grundprinzipien sind darauf ausgerichtet, öffentliches Vertrauen herzustellen (Szidzek und Bolsinger 2018, S. 33 ff.). Es geht um Vertrauen in die Handlungsfähigkeit der Politik, die Big Data bzw. deren Anwender in Gestalt der ‚Frightful 5' nicht unkontrolliert wirken lässt. Es geht aber indirekt um Vertrauen in eben jene Unternehmen und Institutionen, die sich auf der Grundlage der DSGVO rechtmäßig verhalten müssen.

Zusätzlich formuliert die DSGVO ein Recht auf Datenportabilität, also das Recht, beim Verlassen eines Anbieters die eigenen Daten mitzunehmen, sowie ein Kopplungsverbot: Danach darf die Nutzung der Plattform nicht mehr an die

[5]Facebook nennt das neue Datenschutz-Gesetz der EU denn auch als Grund für die Stagnation seiner Nutzerzahlen in Europa, nicht den Cambridge-Analytica-Skandal (Welt 2018).

Einwilligung der Nutzer zu einer Datenverarbeitung gekoppelt werden. Eindeutig gilt dies beispielsweise für Online-Shops. Umstritten ist jedoch, ob es legal ist, wenn das Geschäftsmodell der Plattform darin besteht, eine kostenlose Leistung durch die Abgabe von Daten zu finanzieren, die für Werbezwecke genutzt werden. Außerdem fordert die EU die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen.

Noch nicht verabschiedet ist die Novellierung der ePrivacy-Verordnung, die den Schutz des Privatlebens und der personenbezogenen Daten in der elektronischen Kommunikation zum Ziel hat. Dadurch soll die Verwendung beispielsweise von Cookies, Tracking und Adblocker neu geregelt werden. Während bisher Cookies erlaubt sind, solange der Nutzer nicht widerspricht, soll nach Vorstellung der EU-Kommission in Zukunft der Nutzer jedem Cookie einzeln und nachweisbar zustimmen müssen und Cookies in der Voreinstellung des Browsers generell verhindern können. Dagegen läuft auch die traditionelle Verlagsbranche Sturm, denn dadurch würde das Geschäftsmodell des Affiliate Marketing trockengelegt. Denn mithilfe der Cookies erkennt ein Händler, von welchen Webseiten der Kunde inspiriert wurde, seine Verkaufsplattform anzuklicken, die Grundlage für die Provision. Springer-Chef Mathias Döpfner wettert denn auch: Das sei die „Taliban-Variante des Datenschutzes, bei dem es nicht um Verbraucherschutz, sondern um die Zerstörung eines Geschäftsmodells geht“ (Altrogge und Schade 2018).

1.3.2 Kritik von allen Seiten: Daten- und Verbraucherschützer versus Innovationstreiber

Genau das, nämlich klare Maßnahmen gegen die umfassende Registrierung des Nutzerverhaltens im Internet mithilfe von Cookies, fordert beispielsweise der ehemalige Bundesdatenschutzbeauftragte Peter Schaar. Er sieht ein Spannungsverhältnis zwischen dem Interesse an der ökonomischen Verwertung der Daten und dem Datenschutzrecht, das auf den Grundsätzen der Erforderlichkeit und Zweckbindung aufbaut. Wenn diesen Grundsätzen nicht Rechnung getragen werde, dann drohten „Verlust der Privatsphäre und der informationellen Selbstbestimmung, Machtkonzentration, Manipulation und gegebenenfalls Diskriminierung“ (Schaar 2017a, S. 114).

Zwar sei die EU-DSGVO selbst schon „eine gute Basis für ein zeitgemäßes Datenschutzrecht“ (Schaar 2017b, S. 4). Allerdings gehen ihm wie anderen Daten- und Verbraucherschützern die Bestimmungen nicht weit genug. Ihre Kritik entzündet sich insbesondere an folgenden Punkten:

- Überwachung: Infolge der Verknüpfung von immer mehr Daten zu lückenlosen Persönlichkeitsprofilen droht der Verlust der Privatsphäre. Unter bestimmten Bedingungen lassen sich auch anonymisierte Datenanalysen re-anonymisieren.
- Kontrollverlust: Die Nutzer wissen nicht mehr, welche Daten über sie gespeichert werden. Wenn automatisierte Entscheidungen mit Hilfe von Algorithmen vollzogen werden, so können diese Entscheidungen falsch sein. Außerdem leidet das Vertrauen in Entscheidungsprozesse, wenn sie mit Hilfe von Algorithmen vollzogen werden, die kaum jemand versteht.
- Manipulation (Filterblasen): So zeigt der Newsstream auf Facebook dem User vor allem die Beiträge an, die mit seiner politischen Meinung übereinstimmen. Verstärkt wird das durch Social Bots, die in der Lage sind, natürliche Sprache zu produzieren und sinnvolle Texte zu schreiben und die mit Hilfe von Algorithmen automatisch in sozialen Netzen die ‚richtige' Message für ihr jeweiliges Publikum posten.
- Diskriminierung: Bei der Klassifizierung von Menschen anhand von Scorewerten, wie sie Banken zur Bewertung der Kreditwürdigkeit prinzipiell schon seit Langem vornehmen, besteht die Gefahr, dass angesichts von Big Data auch Faktoren einfließen, die den Vorgaben des Gleichbehandlungsrechts widersprechen, wie etwa Geschlecht, ethnische Herkunft, Religion, Hautfarbe und sexuelle Orientierung. So können besondere User-Gruppen bei der Wohnungsvermietung, Kreditvergabe, Wartedauer in einer Hotline ober der Eingruppierung in Versicherungstarife benachteiligt werden.
- Negative Verteilungseffekte: Bei individualisierten Preisen besteht die Gefahr, dass diejenigen Verbraucher mehr zahlen müssen, aus deren Profil zu schließen ist, dass sie in einer Notlage und besonders auf ein Produkt oder eine Dienstleistung angewiesen sind. Spezifische genetische Dispositionen können durch diesen Mechanismus zum Ausschluss von einer Versicherungsleistung oder zu einem teureren Tarif führen.
- Lock-in-Effekte: Da Facebook, WhatsApp, LinkedIn, Xing und andere ähnlich geartete Social-Media-Plattformen die Kommunikation nur innerhalb der eigenen Mitgliedschaft gestatten, werde den Nutzern erschwert, den Anbieter zu wechseln und es den Sozialen Medien ermöglicht, „den Mitgliedern einseitig die Bedingungen zu diktieren, unter denen ihre Daten verarbeitet und ausgewertet werden" (Schaar 2017b, S. 2). Stattdessen gelte es, die Kommunikation über die Plattformgrenzen hinweg zu ermöglichen.
- Digitale Daten- und Machtkonzentration: Die großen Internetplattformen und Social-Media-Kanäle hätten Vorteile beim Datenzugang (etwa durch Netzwerkeffekte) und dadurch auch bei datenbezogenen Geschäftsmodellen. Diese Asymmetrie am Markt führe zu Marktverzerrungen.

Auf der anderen Seite wurde die DSGVO bei Inkrafttreten in Deutschland aus der entgegengesetzten Richtung zum Gegenstand von kritischer Berichterstattung. Geradezu Hohn und Spott wurde über hanebüchene Auflagen insbesondere für kleine und mittlere Unternehmen ausgegossen. Kritisiert wird darüber hinaus grundsätzlich, dass Datenschutz und die DSGVO die Möglichkeiten von Big Data auf wichtigen anderen Gebieten einschränken. Besonders im Gesundheitswesen sei der deutsche und europäische Datenschutz eine der größten Barrieren nationaler Forschungsumsetzungen und er festige die US-amerikanischen Monopole (Schwerk et al. 2018, S. 5).

Explorative Datenanalysen, die personenbezogene Daten einbeziehen, sind wegen möglicher nachträglicher Zweckänderungen aus datenschutzrechtlicher Sicht grundsätzlich unzulässig (Hornung und Herfurth 2018, S. 167 ff.). Die Begrenzung des Sammelns und Verarbeitens von Daten auf das für einen spezifischen Zweck Erforderliche ist aber mit der Praxis von Big Data nicht oder nur sehr begrenzt zu vereinbaren. Maschinelles Lernen benötigt Daten, um den Computer für bestimmte Situationen und Entscheidungen zu trainieren, die nicht im Voraus bestimmt, aus den Ursprungsdaten abgeleitet oder auch danach nicht erklärt werden können, kritisiert Anthropologie- und Informatikprofessorin Alison Cool (2018). Der Branchenverband Bitkom fordert deshalb, die beiden Prinzipien der Datensparsamkeit und Zweckbindung durch die Prinzipien der Datenvielfalt und des Datenreichtums zu ersetzen.

Der Deutsche Ethikrat nennt weitere uneinlösbare Vorgaben der DSGVO, insbesondere

- dass der Datengeber Bedeutung und Tragweite der Datenverwendung bei der Einwilligung verstehen muss,
- dass der Datengeber bei jeder weiteren Verwendung erneut einwilligen muss,
- das Anonymisierungs- beziehungsweise Pseudonymisierungsgebot, da die Verknüpfung vielfältiger Daten die Gefahr der Re-Identifizierung erhöht,
- das Recht auf Auskunft, Berichtigung, Löschung und Sperrung personenbezogener Daten, was angesichts der vielfältigen Verarbeitungen und Anwendungen immer nur unvollständig sein kann (Deutscher Ethikrat 2017).

Fazit Das bisherige Konzept des Datenschutzes, also die Vorstellung, durch (detaillierte) rechtliche Normen die Bürger vor dem Missbrauch ihrer Daten zu schützen, selbst wenn sie als Nutzer sorglos damit umgehen, stößt sichtbar an seine Grenzen. Denn das Recht kann die politischen Versprechen von Transparenz, Anonymität oder Zweckbindung in Bezug auf Big Data nur begrenzt einlösen, und zwar ganz gleich, aus welcher der beiden genannten Perspektiven

heraus argumentiert wird. Es stellt sich die Frage, ob Recht bzw. Rechtsetzung im Kontext einer sich dynamisch entwickelnden Technologie damit nicht grundsätzlich überfordert ist. Angesichts vergleichsweise einfacher Möglichkeiten des Profilings bzw. der De-Anonymisierung muss vielmehr davon ausgegangen werden, dass sämtliche Daten als personenbezogen gelten müssen (siehe auch Sachverständigenrat für Verbraucherfragen 2018, S. 68 f).

Über die geschilderten rechtstechnischen Herausforderungen einer Gesetzgebung hinaus, die in eine sich rasant verändernde Technologie einzugreifen versucht, erschweren in diesem Fall auch noch basale normative Konzepte des politischen und ökonomischen Handelns bzw. tradierte Menschenbilder die Suche nach einer wirkungsvollen Regulierung. Wie im Folgenden gezeigt wird, sind althergebrachte Narrative, wie die vom informierten Verbraucher und rationalen Konsumenten nicht gerade hilfreich, um die genannten Paradoxien aufzulösen oder wenigstens sicher durch sie durch zu navigieren. Trotzdem bilden diese tradierten Idealtypen nach wie den Ausgangspunkt für die Suche nach einem sinnvollen Umgang mit Big Data.

1.4 Vom Heldenbild des rationalen, souveränen Nutzers: Narrationen im politischen Diskurs

Begleitet wird die öffentliche Auseinandersetzung um die Frage, ob und wie der Schutz der persönlichen Daten durch Regulierungen des Gesetzgebers zu realisieren ist, von der fortgesetzten Erzählung traditioneller Geschichten über den Nutzer bzw. den Bürger, der als Akteur bzw. Aktant dieser Erzählungen auftritt. Während der öffentliche Diskurs von Erzählungen rund um Risiken und dystopischen Erwartungen dominiert wird, ist der politische Diskurs nach wie vor von tradierten Vorstellungen bzw. Leitbildern vom kritischen Verbraucher, informierten Kunden und rationalen Homo oeconomicus geprägt. Alle diese Idealtypen sind als Komplementäre der demokratischen Leitidee des mündigen Bürgers zu sehen, der – so die Erzählung – eigenverantwortlich, selbstbestimmt und unabhängig entscheidet, und zwar nicht zuletzt über seine (personenbezogenen) Daten.

Doch diese Idealtypen der Aufklärung, insbesondere die Vorstellung von rationalem, nutzenmaximierendem Verhalten, mit denen weite Teile von Wirtschaft und Gesellschaft erklärt werden und die in so starkem Kontrast zu den furchterregenden Narrativen zu Big Data stehen, haben Risse, und das schon seit Jahrzehnten. So ist vielfach untersucht, dass Risiken mit geringer Wahrscheinlichkeit und hohem Schadenpotenzial deutlich stärker wahrgenommen werden als Risiken mit hoher Wahrscheinlichkeit und geringerem Schadenpotenzial

(vgl. auch Müller-Peters und Gatzert 2016). Mit Big Data werden diese Risse jedoch unübersehbar. Ein besonders prägnantes Beispiel zeigt eine Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI): Die Risiken im Zusammenhang mit Terrorangriffen werden viel höher eingeschätzt als die Alltagsrisiken des Hackings (Bundesamt für die Sicherheit in der Informationstechnik 2011). Das BSI warnt regelmäßig vor Desinteresse, Überforderung und sorglosem Handeln in der digitalen Welt (www.bsi.bund.de).

1.4.1 Von rationaler Ignoranz und anderen Paradoxien: Nutzerverhalten jenseits der Idealtypen

Die Geschichte stand zuerst in der New York Times (Duhigg 2012): Ein Vater beschwerte sich wütend beim Manager eines Supermarkts der Target-Kette in der Nähe von Minneapolis. Target habe seiner Tochter Coupons für Schwangerschaftskleidung und Babyprodukte zugeschickt, seine Tochter gehe aber noch zur High-School, ‚wollen Sie sie ermutigen, schwanger zu werden?'Aber tatsächlich erwartete seine Tochter ein Kind, wie er kurze Zeit später einräumen musste. Target hatte das allein aus dem jüngsten Einkauf der Tochter geschlossen. Denn darunter waren einige Artikel, die auf der Liste von 25 Produkten standen, die Target als Basis für ein ‚Schwangerschaftsvorhersage-Modell' dienen. Das sind jeweils für sich unverdächtige Artikel, aber wenn eine Frau auf einmal beginnt, größere Mengen unparfümierter Seife oder Watte zu kaufen oder Nahrungsergänzungen wie Kalzium, Magnesium und Zink, errechnet eine Software von Target daraus die Wahrscheinlichkeit einer Schwangerschaft und das Datum der Niederkunft – Daten, die für das Marketing wichtig sind, weil in dieser Phase die Bereitschaft der Kundinnen, neue Produkte zu nutzen, zunimmt.

Ein Fall, der beispielhaft steht für Predictive Analytics mittels Big Data. Durch ihr alltägliches Verhalten, also Einkaufen, Kommunikation mit Familienangehörigen oder Freunden, Lesen von Nachrichten oder E-Books, Hören von Musik, Tanken, E-Mails, Teilen von Fotos in den Sozialen Medien, geben die Menschen persönliche Informationen freiwillig bewusst oder unbewusst preis. Sie sprechen quasi über alles mit Sprachassistenten wie Alexa, deren Anthropomorphismus so dosiert ist, dass die Vermenschlichung als angenehm und nicht bedrohlich empfunden wird. „Sie kontrollieren zwar selbst den Informationsfluss, aber realisieren nicht, dass sich aufgrund der Verarbeitung dieser persönlichen Informationen neue Informationen ergeben, die sie nicht kontrollieren können" (Mai 2016, S. 192).

Viele Nutzer haben zudem inzwischen den Überblick verloren, welche persönlichen Daten sie wem preisgegeben haben, oder sie nehmen die vorgefundene Datenpraxis hin. In einer Umfrage von PwC nach dem Cambridge-Analytica-Skandal äußerten 43 %, sie hätten daraufhin nichts in Bezug auf Datenschutz unternommen, 13 % hatten den Skandal sogar überhaupt nicht mitbekommen (PwC 2017). Viele Nutzer gehen sorglos mit den eigenen Daten und persönlichen Informationen um und verraten freiwillig Vorlieben und Gewohnheiten, wenn ihnen kleine Vorteile, wie die Teilnahme an Gewinnspielen oder Rabatte, versprochen werden. Sogar Apps mit Persönlichkeitstests werden massenhaft ausgefüllt (Farnadi et al. S. 3). Auch wenn die Akzeptanz von Super-Scores nach chinesischem Muster in Deutschland insgesamt nur gering ist, so findet die Idee bei immerhin fast jedem Zehnten der Befragten Zustimmung (Sachverständigenrat für Verbraucherfragen 2018, S. 102). Alle Furchtappelle, die von den dystopischen Narrativen ausgehen, haben nicht dazu geführt, dass sich mehrheitlich ein vorsichtiger Umgang mit Spuren bzw. Daten im Netz durchgesetzt hätte.

Die Vorstellung darüber, wie aus einzelnen Informationsschnipseln Persönlichkeitseigenschaften erschlossen werden können, fällt schwer. So haben Wissenschaftler der Universität Cambridge und von Microsoft anhand der Daten von 58.000 freiwilligen US-Amerikanern gezeigt, dass sich aus den Facebook-Likes mit einer Wahrscheinlichkeit von 88 % ableiten lässt, ob jemand homo- oder heterosexuell ist (Kosinski et al. 2013). Anhand von standardisierten Modellen wie dem „Big Five Personality Model“ (Youyou et al. 2015, S. 2; Farnadi et al. 2014, S. 2 ff.) werden ebenfalls aus Facebook-Likes spezifische Persönlichkeitsprofile von Nutzern ermittelt. Diese Ergebnisse sind sogar besser als die im Umfeld der Personen direkt per Fragebogen ermittelten Einschätzungen (Youyou et al. 2015). Viele Nutzer glauben fälschlicherweise auch, dass Online-Daten keine Rückschlüsse auf die Identität zulassen. Was nicht stimmt: So konnten drei Wissenschaftler aus London mithilfe von Systemen maschinellen Lernens anhand der Metadaten bei 10.000 Twitter-Nutzern jeden mit einer Wahrscheinlichkeit von 96,7 % identifizieren – ein Ergebnis, das nach Angaben der Wissenschaftler auch bei ähnlichen Plattformen wie Facebook erreicht worden wäre (Borgböhmer 2018).

Informationelle Selbstbestimmung setzt jedoch voraus, dass die Menschen bewusst, rational und selbstständig entscheiden, welche persönlichen Informationen sie offenbaren und wie mit ihren Daten verfahren wird. Das wird unter den Bedingungen von Big Data immer schwieriger, wenn nicht unmöglich. Viele geben ihr Einverständnis zur Verarbeitung persönlicher Daten, ohne viel nachzudenken, ohne die Einverständniserklärung ganz oder auch nur in Teilen gelesen zu haben. Der Anspruch informationeller Selbstbestimmung im Sinne einer

bewussten individuellen Wahlhandlung überfordert heute häufig die Fähigkeit, aber auch den Willen der Individuen zu solchen Entscheidungen. Die Annahme, dass allein die Transparenz von Datenschutz- bzw. Nutzungsbestimmungen, die Offenlegung von Algorithmen, ja selbst die Transparenz von Datenmissbrauch dazu führt, dass Verhaltensänderungen im normativ gewünschten Sinne stattfinden, ist schon in sich nicht schlüssig. Denn jede Transparenz stellt sich nur durch Kommunikation ein, d. h. sie nützt nur so viel, wie sie vom Nutzer auch tatsächlich für sein Online-Verhalten herangezogen wird (Knorre 2018).

Das lässt sich erneut exemplarisch bei Facebook und Google zeigen. Das Geschäftsmodell beider besteht darin4, eine Plattform für personalisierte Werbung zu bieten. Die eigentlichen Kunden sind nicht die User, sondern die Werbetreibenden in Wirtschaft, Verbänden oder Parteien. Und je besser Facebook und Google ihre User kennen, desto zielgenauer können sie Werbeplätze verkaufen. Facebook teilt die Nutzer dazu in zahlreiche, sehr kleinteilig definierte Zielgruppen ein. Von Facebook sind 1300 Merkmale bekannt, anhand derer die Nutzer für die Werbung klassifiziert werden.

Wer bei Facebook Mitglied ist, muss damit rechnen, dass zumindest sein Name, seine Kontakte und sein Profilbild im Internet frei zugänglich sind. Das Sichern persönlicher Daten ist, möglicherweise nicht ohne Absicht, bei beiden Plattformen kompliziert und für den normalen User nicht leicht zu durchschauen. Zudem haben Facebook und Google die Privatsphäre-Voreinstellung immer wieder geändert, und vielen Nutzern ist deshalb nicht bewusst, welche Daten sie offenbaren. Das Gefühl der Machtlosigkeit und den Internetkonzernen ausgeliefert zu sein, überwiegt. In den USA gaben 72 % der Bevölkerung an, ihre Daten nur widerwillig mit den Unternehmen zu teilen, und in Deutschland sagen 56 %, dass sie persönliche Informationen in E-Mails vermeiden (Mooy De 2017, S. 21).

Doch obwohl ihnen der Schutz der eigenen Daten wichtig ist, so möchten viele User andererseits nicht auf die Vorteile und den Komfort verzichten, den diese Plattformen bieten. Entstanden ist deshalb das Paradoxon, dass einerseits die Big Brother-Erzählungen die öffentliche Diskussion beherrschen, andererseits aber das individuelle Nutzerverhalten diese Ängste nicht widerspiegelt. Vergleichbare Beobachtungen beschreibt das ‚Digital Privacy Paradox' (Athey et al. 2018). Forscher an der Stanford University fanden in Erhebungen auf dem Campus heraus, dass Menschen schon für eine kleine Vergünstigung bereit sind, private Daten weiterzugeben, obwohl sie auf der anderen Seite die Vertraulichkeit von persönlichen Daten für sehr wichtig halten. So waren die befragten Studierenden schnell bereit, die Namen ihrer besten Freunde weiterzugeben, wenn ihnen dafür eine Pizza versprochen wurde. Die Social Media- und Suchmaschinenplattformen kalkulieren kühl ein Phänomen ein, das in den Wirtschaftswissenschaften

als ‚rationale Ignoranz' bekannt ist. „Sobald der Aufwand, der benötigt wird, um alle relevanten Zusammenhänge zu verstehen, größer ist als der daraus folgende Nutzen, ist Ignoranz rational" (Sandfuchs 2015, S. 13).

Diese Logik zeigt sich auch in einem ebenfalls bekannten Paradoxon: So wünschen sich 74 % der Deutschen ein Angebot von Suchmaschinen oder sozialen Medien, das über nicht-personalisierte Werbung finanziert wird und keine Daten verkauft. Aber sie wünschen sich auch ein kostenloses Angebot. Und im Zweifel überwiegt der zweite Wunsch: Im Austausch für die kostenlose Nutzung dieser Plattformen geben sie ihre privaten Daten preis – selbst wenn ihnen dabei unwohl ist. Und solange die meisten Nutzer bereit sind, ihre Daten Facebook kostenlos zu überlassen, macht die Forderung, Facebook solle dafür zahlen, wenig Sinn (Haucap zitiert in Budras 2018).

Wohl wissend um diese psychische Anfälligkeit der Nutzer kontert Facebook-Geschäftsführerin Sheryl Sandberg auch den Vorwurf, Facebook würde ein Geschäft mit den personalisierten Daten seiner User machen, dass Facebook ja ein Gebührenmodell für diejenigen User einführen könne, die ihre Daten nicht für Werbezwecke verarbeitet wissen wollen (Haucap zitiert in Budras 2018). Dass die Nutzer nicht nur sorglos mit ihren persönlichen Informationen umgehen, sondern sich auch über den Wert ihrer Daten nicht bewusst sind, zeigt schon der immense Gewinn, den Facebook mit personalisierter Werbung daraus erzielt: Im vergangenen Jahr waren das 15,934 Mrd. US$ bei einem Umsatz von 40,653 Mrd. US$ (Facebook 2017). Das ergibt eine Umsatzrendite von knapp 40 %, eine Marge, von der klassische Industrien nur träumen können und die ein Indiz für eine marktbeherrschende Stellung und mangelnden Wettbewerb sein kann.

Bisher hatten User keine Chance, die Einverständniserklärungen der Plattformen zu verweigern, wenn sie deren Dienste in Anspruch nehmen wollten. Denn wenn sie deren Datenschutzbedingungen ablehnten, wurden sie von der Verwendung dieser Dienste ausgeschlossen. Ob das Kopplungsverbot in der EU-Datenschutzgrundverordnung daran etwas ändert, ist umstritten. Während Datenschützer darauf bestehen, dass diese Plattformen ihre Dienste auch denjenigen zur Verfügung stellen müssen, die ihre Datenschutzerklärung nicht akzeptieren, versucht Facebook alles, damit sein Geschäftsmodell, der Tausch von Daten gegen eine kostenlose Leistung, vom Kopplungsverbot ausgenommen wird. Google gibt den Schwarzen Peter an seine Werbekunden weiter, die nun dafür Sorge tragen sollen, dass die User eine Einwilligung zur Datenverarbeitung für Werbezwecke geben.

Diese Strategie kann aufgehen. Denn die Annahme eines eigenverantwortlichen, rationalen, seine persönlichen Daten schützenden Nutzers, der die Preisgabe seiner Daten begrenzen oder kontrollieren wird, wenn dafür nur mittels

Gesetzgebung die Voraussetzungen geschaffen sind, ist angesichts der täglich zu bewältigenden Informationsflut, der dynamischen Entwicklung und der realen Machtstrukturen in der Internetgesellschaft genauso unrealistisch wie das Modell des Homo oeconomicus in der klassischen Ökonomie.

1.4.2 Vom Datenschutz zur Datensouveränität: Mit persönlichen Daten eigenverantwortlich umgehen

In diesem Zusammenhang ist ein Blick auf ein neues Leitbild zu werfen: Datensouveränität. Kritiker unter den Daten- und Verbraucherschützern denunzieren den Begriff gern als ‚Euphemismus' oder ‚Lobbybegriff' den die Datenindustrie den Politikern verkauft habe, so der Gründer von Netzpolitik.org, Markus Beckedahl (zitiert in Krempl 2018). Immer öfter werde damit das Recht auf informationelle Selbstbestimmung infrage gestellt, moniert in diesem Zusammenhang die nieder-sächsische Datenschutzbeauftragte Barbara Thiel (zitiert in Krempl 2018).

Tatsächlich ist der Begriff in einem etwas umfassenderen Kontext entstanden: Ausgangspunkt war die Erkenntnis, dass angesichts der hiesigen Rückständigkeit in digitaler Technologie, der Vorherrschaft der großen amerikanischen Internetunternehmen bei Big Data und der Speicherung der meisten Nutzerdaten im außereuropäischen Ausland Deutschland und Europa die Kontrolle über einen wichtigen Wirtschaftsbereich zu verlieren drohen und wieder ‚digitale Souveränität' erreichen sollen. Diese definierte der Branchenverband Bitkom beispielsweise als die Fähigkeit, „Geschäftsgeheimnisse der Unternehmen und Forschungseinrichtungen bestmöglich zu schützen" (Bitkom 2015). Auch der Aufsatz „Datensouveränität: Fortschritt und Verantwortung" (Schwerk et al. 2018), der mit Unterstützung des Bundesministeriums für Wirtschaft entstanden ist, verwendet den Begriff im Kontext des europäisch-amerikanischen Digitalwettbewerbs.

Inzwischen wird Datensouveränität auch als individuelles Recht verstanden. Individuelle Datensouveränität meint aber nicht das juristische Eigentum an Daten, auch wenn in der Politik der Begriff „Dateneigentum"[6] gelegentlich verwendet wird. Der juristische Eigentumsbegriff gilt für Sachen, greift aber nicht bei Daten, weil diese i. d. R. durch Beziehungen begründet sind. „Wenn ich tanke, gehört die Information über meine Käufe mir und der Tankstelle."

[6]So etwa sprach Angela Merkel von „Datenschutz, Dateneigentum und neuen Produktmöglichkeiten" (Merkel 2015).

(Mai 2016, S. 195) Ob und wie der Eigentumsbegriff überhaupt auf Daten anzuwenden ist, welche Verfügungsrechte sich ergeben und wie ein Eigentumsrecht ggf. technisch umgesetzt werden kann, bleibt in widersprüchlichen Diskussionsbeiträgen stecken (Jentzsch 2018).

Der Deutsche Ethikrat interpretiert Datensouveränität deshalb im Sinne von Datenhoheit. Der Datengeber soll die Möglichkeit haben, auf Basis persönlicher Präferenzen effektiv in den Strom persönlich relevanter Daten eingreifen zu können. Reichlich kompliziert und nebulös heißt es in der dazu veröffentlichten Presseerklärung: „Die mit dem Begriff der Datensouveränität umschriebene verantwortliche informationelle Freiheitsgestaltung versteht er [der Deutsche Ethikrat, d. V.] in Weiterentwicklung der informationellen Selbstbestimmung als interaktive Persönlichkeitsentfaltung unter Wahrung von Privatheit in einer vernetzten Welt“ (Deutscher Ethikrat 2017).

Datensouveränität ist nicht als bloßes Abwehrrecht vor Übergriffen von staatlichen oder privatwirtschaftlichen Organisationen zu verstehen, wie es die bestehenden Datenschutz-Gesetze in Bezug auf personenbezogene Daten vorsehen. Datensouveränität verschiebt den Fokus schon rein begrifflich weiter in die Richtung des Akteurs, des vermeintlich souveränen Nutzers. Hier entsteht eine weitere Variante der Homo oeconomicus-Erzählung, nämlich die des Datensouveräns, des Nutzers mit Datenhoheit, zu der er – und dieser Akzent wird immer wichtiger – allerdings erst noch befähigt werden muss.

Im Fokus steht das – neudeutsch Empowerment oder, in diesem Zusammenhang noch passender, Boosting – des Nutzers. Aus einem Abwehrmechanismus, nämlich einen rechtlichen Schutzbereich für den Nutzer zu schaffen, wird ein Gestaltungsanspruch in einem Hoheitsgebiet, auf dem er dank exzellent designter Bildungsangebote an der Weitergabe seiner Daten aktiv mitwirkt. Dies ist so gesehen eine Weiterentwicklung des Heldenbilds des rationalen Verbrauchers, der die ihm gegebenen Möglichkeiten im Sinne einer kritisch-reflektierten Entscheidung auch tatsächlich nutzt. Allerdings sieht das Konzept der Datensouveränität noch flankierende Elemente vor, um das tradierte Leitbild aufrechterhalten zu können.

Demnach müssen drei Ebenen von Verantwortung ineinandergreifen, damit die Nutzer einen souveränen Umgang mit ihren Daten praktizieren. Die Individuen selbst tragen weiterhin Verantwortung für die Nutzung ihrer Daten, aber dazu muss zunächst einmal – wie eben erwähnt – ihre Kompetenz im Umgang mit den Daten frühzeitig gefördert werden. Zweitens liegt die Verantwortung bei den mit dem Handling der Daten befassten Unternehmen und Institutionen, die die Rahmenbedingungen für die informationelle Freiheitsgestaltung der Datengeber

zu gewährleisten haben. Schließlich muss der Staat regulierend und sanktionierend immer dann eingreifen, wenn Unternehmen und Institutionen keine technischen und administrativen Möglichkeiten bereitstellen, die dem Einzelnen den kontrollierten Umgang mit seinen Daten ermöglichen. Ähnlich sieht das Konzept der Bertelsmann-Studie die Verteilung der Verantwortung auf diesen drei Ebenen angesiedelt (Bertelsmann Stiftung 2017). Diese Grundelemente, mit denen der Begriff der Datensouveränität gefüllt wird, finden sich dann auch in den Überlegungen zur Datenethik wieder, die im folgenden Kapitel skizziert werden.

1.5 Datenethik als neues Paradigma? Handlungsangebote jenseits der Regulierung

Erstmals überhaupt finden sich bereits in einem Koalitionsvertrag Äußerungen zum Potenzial von Big Data und Künstlicher Intelligenz für den Standort Deutschland. Unter der Überschrift „Daten – Rohstoff und sensibles Gut“ (Bundesregierung 2018) führt der Koalitionsvertrag vom 12. März 2018 auf knapp 40 Zeilen einige Ziele und geplante Maßnahmen auf. Am 18. Juli 2018 publizierte die Bundesregierung dann ihren Masterplan zur Künstlichen Intelligenz (Bundesministerium für Bildung und Forschung 2018), in dem sie angesichts der Dominanz der amerikanischen Internetkonzerne und der riesigen Investitionssummen in China etwas großspurig die Absicht bekundete:

„Deutschland soll zum weltweit führenden Standort für KI werden“ (S. 1). Die Bundesregierung wolle die Forschung, Entwicklung und vor allem die Anwendung von Künstlicher Intelligenz fördern. So sollen unter anderem Datenbestände der öffentlichen Hand im Sinne einer Open-Data-Strategie nutzbar gemacht, die Infrastruktur zur Echtzeit-Datenübertragung ausgebaut, wissenschaftlichen Kompetenzzentren die Möglichkeit zur Unternehmensausgründung gegeben und ein Tech-Growth-Fund gegründet werden.

Das Zwölf-Seiten-Papier erhielt zwar viel prinzipielle Zustimmung für den guten Willen, den die Bundesregierung damit zeigt, aber auch Kritik. Wie Deutschland an die Weltspitze vorstoßen wolle, diese Frage beantworte die Bundesregierung angesichts eines Etats für diesen Bereich in Höhe von geschätzt 200 Mio. EUR nicht. Frankreich investiere dafür jährlich das Zehnfache, ganz zu schweigen von den immensen Geldsummen, die die USA und China in Big Data steckten (Armbruster 2018a). Auch bleibt nach Ansicht von Kritikern die Frage unbeantwortet, warum Deutschland auf diesem Gebiet in der Forschung zwar gar nicht mal so schlecht abschneidet, es aber an der praktischen Anwendung mangelt. So hat ein Wagniskapitalgeber analysiert, dass 40 % der relevanten

KI-Unternehmen in den USA beheimatet sind, jeweils 11 % in China und Israel, und dann folgen, mit deutlichem Abstand, Großbritannien, Deutschland und Frankreich (Armbruster 2018b).

Schon während ihrer vorherigen Amtsperiode erklärte Bundeskanzlerin Angela Merkel auf einer Konferenz mit IT-Fachleuten, dass Deutschland den Datenschutz nicht wieder so restriktiv handhaben dürfe, dass „das Big-Data-Management dann doch nicht möglich wird" (Merkel zitiert in Beckedahl 2016). Als Beispiel nannte sie damals das Prinzip der Datensparsamkeit, das nicht die generelle Leitschnur sein könne für die Entwicklung neuer Produkte. Dass nunmehr die Bundesregierung hier Handlungsbedarf sieht, lässt sich an zwei Hinweisen im Masterplan ablesen: Zum einen stellt die Bundesregierung in Aussicht, gegebenenfalls den Rechtsrahmen für die Nutzung von Daten, insbesondere die Klärung der Rechtsbeziehung zwischen den Beteiligten, anzupassen. Zum anderen will sie untersuchen, ob und wie gegebenenfalls der Zugang zu und die Nutzung von Daten sektorenspezifisch geregelt werden soll.

Mit der Ausgestaltung dieser Richtungsentscheidung betraut die Bundesregierung die sogenannte Datenethik-Kommission, die innerhalb eines Jahres einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen und künstlicher Intelligenz vorschlagen soll, um Legitimität und Akzeptanz in der Bevölkerung zu erreichen. Airbus-Chef Tom Enders graut es schon bei dem Gedanken daran, dass Entscheidungen durch die zähen politischen Abstimmungsprozesse auf die lange Bank geschoben werden: „Politik und Wirtschaft müssen rasch handeln. Was wir nicht brauchen, ist ein neues ‚Gesamtkonzept' und einen Ethikrat für KI. Stattdessen müssen wir in der Industrie experimentieren, lernen und korrigieren" (Enders zitiert in Schubert 2018).

Der Deutsche Ethikrat (2017) fordert seinerseits „flexible, innovationsoffene Regelungen", um die Potenziale von Big Data für die medizinische Forschung, die klinische Anwendung und das individuelle Gesundheitsverhalten realisieren zu können.

Unter anderem schlägt er folgende Maßnahmen vor:

- Für die Grundlagenforschung rechtliche Möglichkeiten zu einer umfassenden Datennutzung ohne enge Zweckbindung (Datenspende).
- Software-Werkzeuge (‚Datenagenten'), die die Daten nach den Vorstellungen der Datengeber kontrollieren, auch bei der Datenweitergabe.
- Technische Grundeinstellungen, die von vorneherein einen Schutz der Privatsphäre gewährleisten (privacy by design, privacy by default).
- Aufklärung der Datengeber über die Datenakkumulation und die verwendeten Algorithmen in einer auch für Laien verständlichen Sprache.

- Stärkung der Datenschutzbeauftragten und Neujustierung ihres Aufgabenfelds unter Berücksichtigung von Big Data.
- Einführung von Treuhandmodellen für Datenbestände, um Interessenkollisionen entgegenzuwirken, auch für internationale Datenverwender wie Google, Facebook, Apple, Microsoft oder Amazon.
- Einführung von Gütesiegeln und Zertifizierungen, um Mindeststandards zu gewährleisten.
- Frühzeitige Ausbildung der Datengeber zu mehr Kompetenz im Umgang mit Big Data.

Bis auf den Hinweis auf die Datenschutzbeauftragten, der wie ein Relikt aus vergangenen Zeiten wirkt, ist hier bereits der Paradigmenwechsel zu erkennen, um den es geht: Anstelle eines umfassenden Regulierungsansatzes durch den Gesetzgeber, der im Zweifelsfall Bürger und Nutzer vor sich selber bzw. ihrem leichtfertigen Umgang mit Big Data schützen soll, tritt ein normativer, aber flexibler Handlungsrahmen, der sowohl für die Nutzer als auch die Big Data-Verwender Orientierung in einem grundsätzlich unübersichtlichen Feld gibt und im Sinne einer Selbstverpflichtung wirkt. Im Mittelpunkt steht nicht mehr die zu kontrollierende Erfassung von (bereits gesammelten) Daten, sondern deren ethisch zu vertretende Verarbeitung: Die Herausforderung besteht darin zu entscheiden, wann und wie es ethisch zu verantworten ist, Informationen zu analysieren, was in den Daten zu suchen ist, welche Fragen an die Daten zu stellen sind, und das Ausmaß festzulegen, in dem Vorhersagen über zukünftiges Geschehen und Handeln basierend auf diesen Daten vernünftig sind (Mai 2016, S. 194).

Wie bereits unter dem Begriff Datensouveränität gezeigt wurde, bleibt es bei der Leitidee des souveränen, informierten und eigenverantwortlich handelnden Datengebers bzw. Nutzers, der aber jenseits seines rechtlichen Schutzbereiches auf vielfältige Weise dabei unterstützt wird, souverän mit seinen Daten umzugehen. Dabei sollen ihm wiederum Algorithmen (‚privacy bots') helfen, wenn dies effektiver ist, als auf das eigene Tun zu vertrauen. Aus Sicht der Datenethik kann es aufgrund der Zwecksetzung sogar geboten sein, dass der Nutzer aktiv seine Daten zur Verfügung stellt und sie gerade nicht verweigert. Wenn 90 % aller Unfälle im Straßenverkehr durch menschliches Versagen bedingt sind, wenn im vergangenen Jahr in Deutschland allein 3177 Verkehrstote zu beklagen waren und diese Zahlen durch autonomes Fahren drastisch reduziert werden können, dann wäre es im Zweifelsfall ethisch geboten, sowohl seitens des Datengebers als auch des Datennehmers diese Option zu nutzen.

Datenethik fordert aber vor allem erheblich mehr Eigenverantwortung von jenen, die Daten sammeln, verarbeiten und eventuell weitergeben. Nach dem Subsidiaritätsprinzip soll die Selbstregulierung von Branchen bzw. Anwendungsbereichen innerhalb staatlich vorgegebener Rahmenbedingungen Priorität haben. Ziel ist die Erarbeitung von verbindlichen Kodizes, die, differenziert nach Branchen bzw. Sektoren, Grundregeln für den Umgang mit Daten aller Art aufstellen, in denen sich sowohl Nutzer als auch Datenverwender bewegen können, um die gewünschten Anwendungen, z. B. in der Medizin, zu ermöglichen. Einige Unternehmen wie Salesforce oder SAP haben inzwischen Ethik-Beiräte eingesetzt, die beraten sollen, wie ein ethisch verantwortungsvoller Umgang mit Daten aussehen muss. Ziel ist es, aus Künstlicher Intelligenz eine Technologie zu machen, die es Menschen ermöglicht, „an anderer Stelle ihre typischen Fähigkeiten wie Kreativität oder Empathie einzubringen“ (SAP 2018).

Hervorzuheben sind in diesem Zusammenhang die Denkanstöße, die nicht auf neue Regulierungen hinauslaufen, sondern an bestehendes Soft Law und bekannte Reporting-Mechanismen anknüpfen. Unter dem Stichwort Corporate Digital Responsibility wird beispielsweise über eine Ergänzung der bisherigen Corporate Social Responsibility (CSR)-Konzepte nachgedacht (Smart-Data-Begleitforschung 2018). Ähnlich gelagert ist die Option, den bestehenden Corporate Governance Kodex entsprechend zu erweitern. Verbindliche Standards, deren Einhaltung in den Jahresabschlüssen testiert werden muss und die mit Berichtspflichten belegt sind, könnten die ethischen Betrachtungen konkret umsetzen. Der vergleichende Blick auf die USA zeigt eine ähnliche Diskussion über die ‚Treuhänder‘-Rolle von Online-Unternehmen sowie die sich daraus ergebenden Sorgfalts- und Gemeinwohlpflichten im Umgang mit Big Data (Zittrain 2018).

Der Deutsche Ethikrat plädiert in diesem Zusammenhang dafür, stärker als bislang „die kontextabhängig wandelbare Sensibilität von Daten zu berücksichtigen“. Vorbild solcher branchen- oder themenspezifischen Regeln könnten die Ausarbeitungen des Deutschen Ethikrates für den Gesundheitsbereich sowie der Bericht der Ethik-Kommission „Automatisiertes und vernetztes Fahren“ beim Bundesministerium für Verkehr und digitale Infrastruktur (Bundesministerium für Verkehr und digitale Infrastruktur 2017) sein. Der entscheidende Unterschied zwischen allen eben genannten datenethisch begründeten Ansätzen und dem bisher vorherrschenden Datenschutzparadigma besteht darin, dass hier die Unternehmen nicht nur Compliance mit den Schutz- bzw. Abwehrrechten der Nutzer nachweisen müssen. Vielmehr sind sie gefordert, Big Data für begründete und akzeptierte Zwecke zu nutzen und dies darzulegen.

Dass allerdings auch dieser anwendungsbezogene datenethische Ansatz zu ganz schwierigen und kontroversen Debatten führt, ließ sich im Januar 2018 in den Medien nachverfolgen. Der Direktor des Freiburger Cochrane-Zentrums, Gerd Antes, hatte am 02.01.2018 in der FAZ unter der Überschrift „Medizin im Datenrausch" den Sinn von Big Data in der Medizin infrage gestellt und dafür heftige Repliken erhalten. Seitdem wird gestritten, ob zukünftig das „Korrelations-Bingo" (Antes 2018) die evidenzbasierte Medizin ersetzt oder wir eine neue Interpretation von evidenzbasiert brauchen.

1.6 Ordnungspolitik und Big Data: Den fairen Zugang sichern

Ergänzend zum überwiegend nicht-regulatorischen Datenethik-Ansatz, der vor allem den datengebenden Bürger und die datenverarbeitenden Unternehmen in die Pflicht nimmt, sind abschließend ordnungspolitisch motivierte Gestaltungsmaßnahmen zu erwähnen. Wie es die genannte dritte Verantwortungsebene im Konzept der Datensouveränität vorsieht, geht es hier um die Flankierung eines neuen, chancenorientierteren Umgangs mit Big Data durch den Gesetzgeber.

Skaleneffekte, Netzwerkeffekt und die systematische Verwertung der Kunden- und Nutzerdaten haben zur Herausbildung von oligopolistischen Strukturen geführt. Die ‚Frightful 5' haben eine historisch beispiellose globale Monopolstellung erreicht und dominieren den globalen Werbemarkt beziehungsweise den globalen E-Commerce. Der Technologie- und Marktvorsprung der dominierenden Internetkonzerne erhöht die Markteintrittsbarrieren für neue Anbieter und beschränkt so die Möglichkeiten zu Innovationen. Ihre Herrschaft über die Daten schützt die Internetkonzerne vor Wettbewerbern. Mit ihren Datenerfassungssystemen haben sie den Überblick über die Märkte und auch die potenziellen Konkurrenten: Google weiß, was die Leute suchen, Facebook weiß, mit wem die Leute ihre Informationen teilen, Apple weiß, wo sie sind, Amazon weiß, was sie kaufen.

Wenn Start-ups eine neue Anwendung oder ein neues Produkt entwickeln, können die ‚Fürchterlichen 5' diese schnell kopieren oder aufkaufen, um neue Konkurrenten vom Markt zu halten. Dass Facebook die Fotoplattform Instagram oder den Messenger-Dienst WhatsApp und Google den Online-Karten-Anbieters Waze übernehmen konnten, zeigt den grundsätzlichen kartellrechtlichen Handlungsbedarf. Auch wenn die EU im Juni 2018 Google mit Milliardenbußen belegt hat, so ist doch symptomatisch, dass die Behörde dabei nicht auf die marktbeherrschende Stellung, also den Marktanteil, zielt, sondern lediglich auf das – marktverzerrende – Verhalten des Suchmaschinenbetreibers.

Unter Wettbewerbsgesichtspunkten ist auch die Expansion der großen Internetkonzerne in andere Bereiche von Big-Data-Anwendungen als problematisch anzusehen. Google, Facebook, Amazon und Apple investieren Milliardenbeträge ihrer üppigen Gewinne in Medizin, Biotech, autonomes Fahren und Smart-Home-Technik. Die Internet-Plattformen drohen zu riesigen, unkontrollierbaren Internet-Konglomeraten auszuwachsen und sich über die ganze Wirtschaft zu legen. „Das Problem der Regulierungsbehörden besteht darin, dass standardisierte Antimonopolsysteme nicht gelten in einer Welt, in der die Kosten für die Verbraucher hauptsächlich in Form von Daten und Privatsphäre völlig intransparent sind", analysiert Harvard-Professor Kenneth Rogoff (2018). Auch der liberale Economist (2017) sieht „Grund zur Sorge: Die Kontrolle der Daten durch die Internetgiganten gibt ihnen enorme Macht. Die alten Wege, Wettbewerb zu erfassen, sehen überholt aus in der Datenökonomie".

Diese Erfahrung musste auch das Bundeskartellamt machen. Als Facebook 2014 den Messenger-Dienst WhatsApp für 19 Mrd. US$ kaufte, durfte die Behörde diese Übernahme nicht einmal untersuchen, weil sie unterhalb der Umsatz-Schwellenwerte der Fusionskontrolle lag. Inzwischen hat der Gesetzgeber reagiert. Die neunte Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) vom Juni 2017 ermöglicht nun auch eine Fusionskontrolle, wenn der Transaktionswert 400 Mio. EUR überschreitet (Bundeskartellamt 2016). Darüber hinaus wurden noch zwei weitere Paragrafen geändert, die ebenfalls auf digitale Plattformen und Märkte zielen. Zum einen stellt die neunte GWB-Novelle klar, dass Märkte auch dann angenommen werden können, wenn dort Leistungen unentgeltlich erbracht werden, weil Nutzer beispielsweise mit ihren Daten ‚bezahlen' (Haucap und Heimeshof 2017, S. 34 ff.). Zum anderen wurden in § 18 Abs. 3a GWB fünf neue Kriterien aufgenommen, die für die Beurteilung von Marktmacht herangezogen werden, wie sie insbesondere von Netzwerken und Plattformen ausgeübt werden kann. Eines dieser Kriterien betrifft den Zugang zu wettbewerbsrelevanten Daten.

Zweifelsohne konkretisieren und ergänzen diese Neuerungen das kartellrechtliche Instrumentarium im Hinblick auf die Besonderheiten von digitalen Märkten. Kritik richtet sich aber weiterhin darauf, dass die genannte Transaktionsschwelle immer noch im Vergleich beispielsweise mit den USA viel zu hoch liegt (Haucap und Heimeshof 2017, S. 36). Auch die in der 9. GWB-Novelle ergänzten direkten und indirekten Netzwerkeffekte, die Einfluss auf die Marktstellung eines Unternehmens haben können, erweisen sich in der Umsetzung als schwierig. So prüft das Bundeskartellamt seit gut zweieinhalb Jahren die Praxis von Facebook, die Nutzerdaten aus Drittquellen wie etwa den Töchtern WhatsApp und Instagram auf dem Facebook-Konto zusammenzuführen und zu nutzen. Das Kartellamt

vermutet hier einen Konditionenmissbrauch, weil Facebook seine Marktmacht dazu nutze, den Teilnehmern am Netzwerk solche Bedingungen vorzuschreiben (Bundeskartellamt 2017). Ähnlich gelagert ist der Fall von Amazon. Da Amazon nicht nur selbst als Händler auftritt, sondern seine Plattform auch anderen Händlern anbietet, untersucht das Bundeskartellamt nun auf Beschwerden einzelner Händler hin, ob Amazon seine Stellung nutzt, um andere Händler auf seiner Plattform zu behindern (Bünder und Koch 2018).

Darüber hinaus wird bemängelt, dass der Datenzugang zwar als Kriterium für Marktmacht gelten kann, daraus aber kein weiteres Datenzugangsrecht für Dritte abgeleitet wird (Schweitzer et al. 2018). Lösungen versprechen da nicht zuletzt Konzepte jenseits des klassischen Wettbewerbsrechts. Diese Reformvorschläge gehen weitgehend konform mit den Zielen der Open-Data-Bewegung, die alle Daten beispielsweise mittels freier Lizenzen verfügbar machen will, die nicht unter das Datenschutzrecht fallen bzw. keine personenbezogenen Daten sind. Open Data ist im Grunde nichts Anderes als eine Wiederbelebung des Gedankens der Allmende (‚commons'). Es geht nicht um die Offenlegung von Algorithmen, die vor allem im Datenschutz-Paradigma und von Aufsichtsbehörden diskutiert wird, sondern um den weitestgehend freien Zugang zu Big Data, um möglichst viele im Wettbewerb stehende Algorithmen zu generieren und die Chancen von Big Data zu realisieren.

Der Fokus liegt dabei zunächst auf Daten, die von der öffentlichen Hand erhoben werden. Über das reine Veröffentlichen von Daten und Informationen hinaus sollen Datenbestände öffentlicher Stellen in maschinenlesbaren und offenen Formaten zur freien Weiterverwendung durch externe Dritte wie z. B. Bürger und Wirtschaft verfügbar gemacht werden. Es war eine der ersten Amtshandlungen von US-Präsident Barack Obama, die Datenbestände der Regierung frei zugänglich zu machen. In Deutschland trat mit der Änderung des E-Government-Gesetzes im Sommer 2017 das „Open-Data-Gesetz" in Kraft. Es verpflichtet die Behörden der unmittelbaren Bundesverwaltung, strukturierte Rohdaten, die sie zur Erfüllung ihrer Aufgaben erhoben haben, zu veröffentlichen. Unter der Webadresse www.govdata.de stehen derzeit zu 13 Themenfeldern strukturierte Daten von Bundesbehörden für die Nutzung durch andere Behörden, Bürgern, Wirtschaft und Wissenschaftlern zur Verfügung. Ähnlich gelagert ist der Aufbau einer nationalen Forschungsdateninfrastruktur, wie ihn die Gemeinsame Wissenschaftskonferenz von Bund und Ländern im November 2018 beschlossen hat (www.forschungsdaten.org).

Von dem Internet-Kritiker Evgeny Morozov (2015) stammt der Vorschlag, Daten zu begreifen als entscheidender Bestandteil einer Infrastruktur, die allen gehören sollte. Unternehmen sollten Daten benutzen können, aber dafür bezahlen. Daten

und künstliche Intelligenz, die auf ihnen aufbaut, müssen öffentlicher Besitz bleiben (Morozov 2015). In der Tat weisen Infrastruktur und Daten gemeinsame Merkmale auf. Für Daten gilt genauso wie etwa für Verkehrs- oder Kommunikationsnetze, dass sie mehrfach benutzt werden können, ohne dass sie dadurch verbraucht werden. „Daten werden zu einem universalen Enabler: allgemeine Zweckbestimmung, große Mengen, hohe Fixkosten, keine variablen Kosten. Wie Straßen oder Telekommunikation werden sie Infrastruktur" (Evans 2018, S. 141).

Andere Autoren kommen zu ähnlichen Schlussfolgerungen, indem sie Massendaten mit öffentlichen Gütern vergleichen, die nicht in Konkurrenz zu anderen stehen, von deren Gebrauch niemand ausgeschlossen werden kann und die von mehreren Nutzern gleichzeitig gebraucht werden können. Auch hier spielt der Gesetzgeber bzw. der Staat eine entscheidende Rolle: Zu seinen Aufgaben könne es gehören, den „diskriminierungsfreien Zugang aller Menschen zu geregelten Bedingungen sicherzustellen und den Markt ordnungspolitisch zu rahmen" (Schlüter 2017, S. 2). Damit wird der Datenzugang, vielleicht sogar die Sicherung der Datenqualität, zu einem Teil der Daseinsvorsorge des Staates definiert wie Bildungswesen, Sicherheitsbehörden, Wasser- und Energieversorgung oder das Gesundheitswesen. Wie bei den Netzen der Energie und Telekommunikation müssten private Datenbanken dann nach definierten Regeln auch anderen Marktteilnehmern zur Verfügung stehen, selbst wenn sie dort selbst keine Daten eingestellt haben.

Eine private Lösung, aber mit Umverteilungscharakter, schlägt demgegenüber Oxford-Professor Mayer-Schönberger vor. Um neuen Anbietern einen Marktzugang gegenüber den großen Playern und damit mehr Wettbewerb zu ermöglichen, sollen Letztere einen Teil ihrer Daten mit Wettbewerbern teilen müssen. Bei Erreichen eines Marktanteils von beispielsweise zehn Prozent müssen sie einen bestimmten Anteil ihrer zufällig ausgewählten Daten anderen Wettbewerbern zur Verfügung stellen. Dieses Data-Sharing soll progressiv wie bei der Einkommensteuer in Relation zum erreichten Marktanteil gestaltet werden (Mayer-Schönberger und Ramge 2018). Interessanterweise greift auch eine Kommission um den Düsseldorfer Wettbewerbsökonomen Justus Haucap diesen Vorschlag einer Daten-Sharing-Pflicht in einem Gutachten für das Bundeswirtschaftsministerium auf (Schweitzer et al. 2018). Erste Praxisbeispiele sehen die Befürworter dieses Modells bereits in der Versicherungsbranche und verweisen darauf, dass große Versicherungen kleineren Marktteilnehmern Hinweise geben müssen, wie sie ihre Tarife sinnvoll schneiden können (Thomas 2017).

Zweifelsohne ließe sich auch eine Kombination aus beiden Konzepten vorstellen, zum Beispiel, indem Massendaten aus bereits bestehenden öffentlichen Infrastruktureinrichtungen den Grundstock für eine neuartige Big Data-Infrastruktur

bilden, die dann im Rahmen von Data-Sharing weiter befüllt wird. Auch wenn dies nicht unmittelbar realisierungsfähig scheint, ist allein die ernsthafte Diskussion darüber ein Indiz dafür, dass in der neuen Datenökonomie neue Regeln für einen offenen Um- und Zugang mit Big Data ebenso gefordert sind wie eine weitere Konkretisierung und Ergänzung des Kartellrechts, dessen Möglichkeiten noch nicht ausgeschöpft scheinen. So gesehen sollte die 2018 eingesetzte Regierungskommission „Wettbewerbsrecht 4.0“ eine Reihe von relevanten Vorschlägen entwickeln können, wie die bisherigen Wettbewerbsregeln auf das Digitalzeitalter weiter anzupassen sind (Bundesministerium für Wirtschaft und Energie 2018). Ergänzend sei darüber hinaus auf rein privatwirtschaftliche Lösungen wie das Modell „Industrial Data Space“ (Fraunhofer 2016) verwiesen, das auf einen Datenaustausch zwischen Club-Mitgliedern in einer sicheren, geprüften Austausch-Architektur setzt.

Erleichtert wird der öffentliche Diskurs an dieser Stelle dadurch, dass diese Konzepte eines diskriminierungsfreien offenen Zugangs zu Big Data auf bekannte Konstrukte wie die der Allmende, der öffentlichen Infrastruktur oder öffentlichen Güter Bezug nehmen. Dies kann nicht nur die politische Verständigung über ein solches Vorgehen befördern, sondern passt auch zu der neuen Rolle des Nutzers als souveräner Datengeber, der weniger geschützt als vielmehr zur aktiven Mitarbeit zum Aufbau der Infrastruktur aufgefordert ist.

1.6.1 Propositionen: Wie der öffentliche Diskurs zu Nutzen und Schutz von Daten des souveränen Bürgers gestaltet werden kann

Aus alledem lässt sich schlussfolgern, dass ein politisch relevantes Handlungskonzept zum Nutzen und Schutz von Daten des souveränen Bürgers gleich mehrere Merkmale aufweisen muss, die kumulativ zu verstehen sind. Denn ein solches Konzept muss nicht nur die Leitplanken von Nutzen einerseits und Schutz andererseits ausgewogen berücksichtigen, um den damit begrenzten Zielkorridor kollisionsfrei begehbar zu machen. Es muss zugleich realistischere, d. h. weniger von normativen Idealen geprägte Annahmen in Bezug auf die bereits existierenden Bedingungen von Big Data treffen. Denn schließlich muss ein solches Konzept flexibel und schnell umsetzbar sein und nicht zuletzt die inhaltlichen wie kommunikativen.

Voraussetzungen erfüllen, um einen breiten Konsens zu ermöglichen bzw. mehrheitsfähig zu sein.

Der dafür erforderliche Paradigmenwechsel im (politischen) Umgang mit Big Data, wie er sich aktuell abzeichnet, ist wie in Tab. 1.1 zusammenzufassen.

Tab. 1.1 Erforderlicher Paradigmenwechsel im (politischen) Umgang mit Big Data

Bisheriger Fokus	Neuer Fokus	Gestaltungsmerkmale
Big Data	Künstliche Intelligenz	Anwendungsorientiert, themenspezifisch
Datenschutz	Datensouveränität	Handlungsorientiert, offensiv
Regulierung	Ethik	Beziehungsorientiert, vertrauensbasiert
Wettbewerbsrecht	Open Data-Modelle, Daten-Sharing, Dateninfrastruktur	Kompetitiv, diskriminierungsfrei

Darüber hinaus lassen sich aus den hier zugrunde gelegten Darstellungen einige logische Feststellungen (Propositionen) bilden, die ihrerseits dafür genutzt werden können, um Hypothesen für die weitere empirische Arbeit zu bilden.

1. Der öffentliche, insbesondere in den Medien ausgetragene Diskurs zum Umgang mit Datenmassen, mithin zur Frage, wie viel Nutzen wir uns versprechen können und wie viel Schutz wir umgekehrt vor Big Data brauchen, ist von Erzählungen geprägt, die um Konflikte und Kollisionen zwischen den handelnden Akteuren kreisen und nicht über diese hinauskommen. Sie sind als Varianten des Big-Brother-Narrativs einzuordnen und haben überwiegend den Charakter von Dystopien.
2. Umso auffälliger ist es, dass die Nutzer kaum auf diese Furchtappelle reagieren. Sie blicken einerseits skeptisch auf Big Data und konsumieren ausgiebig dystopische Big-Brother-Geschichten, andererseits gehen sie sorglos oder fatalistisch mit ihren Daten um und nehmen angebotene bzw. gesetzlich vorgeschriebene Informations- oder Schutzmöglichkeiten nicht oder nur begrenzt wahr. Diese Beobachtung lässt sich als User-Paradoxon bezeichnen.
3. Der politische Diskurs, insbesondere im Kontext der Gesetzgebung, ist demgegenüber von tradierten Idealtypen geprägt, die einerseits auf das Aufklärungsideal des mündigen Bürgers, andererseits auf das Menschenbild des Homo oeconomicus, des rationalen Akteurs, zurückgreifen. Während der mediale bzw. öffentliche Diskurs also eher von einer pessimistischen Grundstimmung geprägt ist, geht der politische Diskurs im engeren Sinne weiterhin von optimistischen, ja idealistischen, Grundannahmen aus, denen mit geeigneten Maßnahmen, nicht zuletzt einer detaillierten Rechtsetzung, Geltung verschafft werden könne.

4. Die Nutzer glauben weder der einen noch der anderen Erzählung. Das User-Paradoxon weist nämlich nicht nur darauf hin, dass die Nutzer in ihrem individuellen Nutzungsverhalten die Risiken von Big Data zugunsten des subjektiven Nutzens vernachlässigen. Sondern das User-Paradox lässt zugleich vermuten, dass auch die optimistischen Erzählungen der Politik, wonach Nutzer sich sinnvoll vor unkontrollierter Datensammlung und deren ungewünschten Auswertungen schützen können, wenn sie nur aufgeklärt und informiert handeln, wenig überzeugend sind bzw. nicht dem Selbstbild der Nutzer entsprechen.
5. So herrscht schließlich auf kollektiver Ebene weitgehende Orientierungslosigkeit darüber vor, wie sich die Risiken von Big Data beherrschen lassen, ohne deren Chancen unangemessen zu reduzieren. Der von dystopischen Erzählungen beherrschte öffentliche Diskurs führt zwar nicht zu einem entsprechenden individuellen Nutzerverhalten, bestimmt aber dennoch das öffentliche Meinungsbild mit seiner überwiegend skeptischen Sicht auf Big Data und Künstliche Intelligenz. Die geradezu konträren öffentlichen und politischen, insbesondere datenschutzrechtlichen Narrative – Dystopie hier, aufgeklärter User da – verhindern es, dass die eigentliche Funktion von Narrationen bzw. Narrativen, nämlich über die Reduktion von Komplexität mehrheitsfähige Verständigungen möglich zu machen, im Falle von Big Data greifen kann.
6. Gleichzeitig erweist sich der bisherige Lösungsansatz von Datenschutzpolitik bzw. -recht, nämlich den aufgeklärten Nutzer, den Bürger im Netz, vor Datenmissbrauch schützen zu wollen, als wenig aussichtsreich, um das User-Paradoxon aufzulösen. Dazu tragen nicht zuletzt einige grundsätzliche Unvereinbarkeiten zwischen Datenschutz und den Chancen von Big Data bei, insbesondere die Frage der Datensparsamkeit und Zweckbindung. Überhaupt stößt eine detaillierte Rechtsetzung bzw. Regulierung im Kontext einer dynamischen Digitalisierung an ihre Grenzen. Allein die Differenzierung zwischen personenbezogenen und nicht-personenbezogenen Daten ist angesichts der explodierenden Datengenerierung und den Mitteln der Re-Anonymisierung de facto nicht mehr möglich und hat als Entscheidungskriterium nur noch begrenzte Relevanz.
7. Die lähmenden Paradoxien lassen sich rein logisch sowohl in die eine als auch die andere Richtung auflösen. Zum einen wäre es dadurch möglich, dass sich öffentliche Erzählungen mit glücklichem Ausgang über gezähmte Datenkraken und eingedämmte Datenfluten herausbilden, die als wirkmächtige Narrative eine breit getragene Verständigung über den Nutzen von Big Data begründen können. Diese Option muss angesichts der dominierenden dystopischen Big

Brother-Erzählungen als wenig realistisch angesehen werden, zumindest auf absehbare Zeit. Es erscheint deshalb sinnvoll, das Feld der Datenschutzdiskussion zu verlassen und einen alternativen Erzählstrang zu entwickeln.

8. Denn die andere logische Alternative, die beschriebenen Paradoxien aufzulösen, besteht darin, das tradierte Leitbild des aufgeklärt-kritischen Nutzers mit neuen bzw. neu zu konstruierenden Narrationen zu revitalisieren, die sich unter den Bedingungen von Big Data und Künstlicher Intelligenz als wirksam erweisen können, weil sie die Denkschablonen des bisherigen Datenschutzrechts aufbrechen. In diesem Zusammenhang bietet das Konzept der Datensouveränität bzw. weiterführend der Datenethik geeignete Anregungen. Das politische Narrativ des souveränen Nutzers wird im Datenethik-Ansatz weiter gestärkt, allerdings sieht es für ihn eine neue, realistischere Rolle vor, die ihn in seinem augenblicklichen, eher unkontrollierten Nutzerverhalten abholt. Es geht nunmehr weniger darum, den Bürger und seine Daten zu schützen, sondern ihn dabei zu unterstützen, dass er seine Daten gezielt zu den von ihm gewünschten Zwecken weitergibt. Der Bürger in seiner Rolle als Nutzer digitaler Technologien ist nicht mehr ein Schutzobjekt, sondern wird zum aktiven Datengeber, Datenspender oder gar Datenhändler.
9. Ordnungspolitisch motivierte Konzepte, die die Rolle des souverän mit seinen Daten agierenden Nutzers unterstützen, bieten auf der Makro-Ebene relevante Handlungsansätze, um die Konzepte von Datensouveränität und Datenethik zu flankieren. Sie bieten zugleich Stoff für zusätzliche Narrative, die zur eben erwähnten neuen Rolle des Bürgers als souveränen Datengebers passen. Eine Daten-Allmende (‚Open Data‘), in der Massendaten nach definierten Regeln der Nachhaltigkeit zwischen Organisationen aller Art geteilt werden, ist so ein Stoff für gesellschaftlich und politisch relevante Erzählungen. Das gilt auch für eine Erzählung von der Zerschlagung der Daten-Oligopolisten, die gezwungen werden, ihre Daten mit anderen zu teilen. Noch weitergehend ist der Gedanke einer nach ethisch verantwortbaren Zwecken differenzierten Daten-Infrastruktur, die den fairen Zugang zu Big Data ermöglicht. Der Bürger als digitaler Datengeber hinterlässt seine persönlichen Daten gezielt für diese Daten-Infrastruktur, die Unternehmen sind wie schon der öffentliche Sektor im Obligo, die Datenbanken zu füllen. Beide Konzepte sichern Wettbewerb der Algorithmen statt Wettbewerb der Datenkraken – auch dieser Gedanke hat das Zeug für eine neues politisches Narrativ, das nicht in Konflikten und Kollisionen hängen bleibt.
10. Datenethik setzt insgesamt darauf, dass Vertrauensbeziehungen zwischen den Akteuren unter bestimmten Bedingungen möglich gemacht werden. Deshalb sind für Unternehmen und andere Organisationen, deren Geschäftsmodelle

auf dem Sammeln, Analysieren und Auswerten von Daten beruhen, zusätzliche Konstrukte der ‚verbindlichen Selbstverpflichtung' erforderlich, z. B. in Form von Kodizes, Selbstverpflichtungen oder Treuhänderstatuten. Mit dem Perspektivenwechsel hin zur Datenethik geht es aber dabei nicht mehr vorrangig um Compliance mit den Datenschutzgesetzen. Im Mittelpunkt steht vielmehr der positive Beitrag für gesellschaftlich relevante Zwecke, der mithilfe von Big Data geleistet werden kann. Einige Akteure werden deshalb die Chancen von Big Data bzw. Künstlicher Intelligenz besser nutzen können als andere. Das gilt insbesondere für Unternehmen, die über einen Vertrauensvorsprung verfügen, weil ihr Umgang mit von ihnen gesammelten und genutzten Daten auf klaren ethischen Handlungsgrundsätzen beruht.

11. Die bisherigen, vom Datenschutzziel geprägten Regulierungen bieten keine ausreichenden Perspektiven für einen ausgewogeneren Umgang mit Big Data, der neben den Risiken auch die Chancen des digitalen Zeitalters angemessen berücksichtigt. Nicht zuletzt die bisher herrschende dystopische Tradition der Big-Brother-Narrative steht dem entgegen. Deshalb ist ein Paradigmenwechsel in dem eben beschriebenen Sinne nötig, der nicht nur nach dem Schutz, sondern auch nach dem Nutzen von Big Data fragt. Er umfasst eine neue, aktive Rolle des souveränen Nutzers, verbindliche Selbstverpflichtungen der Online-Unternehmen und den Gedanken einer wettbewerbskonformen Dateninfrastruktur oder eines fairen Daten-Sharings gleichermaßen und gleichzeitig. Dieser Paradigmenwechsel wird umso erfolgreicher sein, je besser es gelingt, ihn mit wirksamen öffentlichen und politischen Narrationen zu verbinden, die die Komplexität des Themenfelds im Sinne einer konsensfähigen Sinnstiftung und breiten Verständigung reduzieren. Genau dafür eignen sich sowohl Überlegungen der Datenethik als auch der offenen Dateninfrastruktur grundsätzlich gut, denn sie bieten Stoff für neue Erzählungen bzw. die Revitalisierung tradierter Narrative bzw. Leitbilder. Diese konstruktivistische Perspektive mag gerade in Deutschland ungewohnt sein, sie ist aber notwendig, um einen gesellschaftlichen und politischen Mehrheitskonsens über den Umgang mit Big Data zu finden.

Um diese narrativ-diskursiven Handlungskonzepte weiter zu konkretisieren, bedarf es einer Betrachtung von konkreten (digitalen) Lebenswelten, die sozusagen als neues Spielfeld für die Konstruktion von gesellschaftspolitisch relevanten Erzählungen genutzt werden können. Konkrete Lebenswelten, die sich zu Erzählungen über einen positiv wirkenden Einsatz von Big Data verdichten lassen, helfen das Unbekannte und deshalb.

Furcht einflößende von Big Data zu dechiffrieren. Zugleich lässt sich an konkreten Lebenswelten zeigen, welche neuen (ordnungspolitischen) Regeln kontextabhängig eingesetzt werden können, um Nutzen und Schutz eines souveränen Nutzers, sprich Datengebers, gleichzeitig und ausgewogen zu realisieren.

Literatur

Altrogge, G., & Schade, M. (2018). „Die alte Garde ist am Ende, und zwar überall". Interview mit Mathias Döpfner. https://meedia.de/2018/07/18/die-alte-garde-ist-am-ende-und-zwar-ueberall-springer-ceo-mathias-doepfner-ueber-die-aufloesung-von-leadership-modellen-in-politik-und-medien/. Zugegriffen: 28. Aug. 2018.

Aly, G., & Roth, K. H. (1984). *Die restlose Erfassung. Volkszählen, Identifizieren, Aussondern im Nationalsozialismus*. Berlin: Rotbuch.

Amazon. (2018). Suchergebnisse zu Büchern über Big Data. https://www.amazon.de/s?k=big+data&i=stripbooks&__mk_de_DE=%C3%85M%C3%85%C5%BD%C3%95%C3%91&ref=nb_sb_noss_2. Zugegriffen: 28. Aug. 2018.

Antes, G. (2. Januar 2018). Die Medizin im Datenrausch. Frankfurter Allgemeine Zeitung. https://edition.faz.net/faz-edition/feuilleton/2018-01-02/9b583344667f696c3b3aabbc13b7424f/. Zugegriffen: 28. Aug. 2018

Armbruster, A. (2018a). Der deutsche KI-Weg. http://www.faz.net/aktuell/wirtschaft/diginomics/kuenstliche-intelligenz-made-in-germany-kommentar-15706427.html. Zugegriffen: 28. Aug. 2018.

Armbruster, A. (2018b). Künstliche Intelligenz. Große Gefahr, übertriebene Angst – Was denn nun? http://www.faz.net/aktuell/wirtschaft/kuenstliche-intelligenz/computer-assistenten-machen-der-werbung-den-garaus-15595402.html. Zugegriffen: 28. Aug. 2018.

Athey, S., Catalini, C., & Tucker, C. (2018). The digital privacy paradox: Small money, small costs, small talk. https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141392.pdf. Zugegriffen: 27. Nov. 2018.

Atwood, M. (2013). When privacy is theft. The New York review of books. https://www.nybooks.com/articles/2013/11/21/eggers-circle-when-privacy-is-theft/. Zugegriffen: 10. Okt. 2018.

Beckedahl, M. (2016). Datensouveränität. https://netzpolitik.org/2016/angela-merkel-hat-gehoert-dass-sie-datenschutz-jetzt-datensouveraenitaet-nennen-soll/. Zugegriffen: 28. Aug. 2018.

Bernard, A. (2014). Dave Eggers' ‚Der Circle'. Der dritte Kreis der Hölle. http://www.faz.net/aktuell/feuilleton/buecher/der-dritte-kreis-der-hoelle-dave-eggers-der-circle-im-vergleich-mit-huxley-und-orwell-13089429.html. Zugegriffen: 12. Sept. 2018.

Bertelsmann Stiftung. (Hrsg.). (2017). Rethinking privacy self-management And data sovereignty in the age of big data. Considerations for future policy regimes in the United States and the European Union 2017. https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/rethinking-privacy-self-management-and-data-sovereignty-in-the-age-of-big-data/. Zugegriffen: 28. Aug. 2018.

Bild. (2016). Wahlkampf-Hilfe für Donald Trump: Vorsicht! Diese Firma weiß, wie SIE denken. https://www.bild.de/politik/ausland/us-wahl-inside/trump-online-wahlkampf-49063290.bild.html. Zugegriffen: 5. Sept. 2018.

Bitkom. (2015). Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/05-Mai/BITKOM-Position-Digitale-Souveraenitaet1.pdf. Zugegriffen: 28. Aug. 2018.

Bitkom. (2018). Große Mehrheit für Künstliche Intelligenz in der Polizeiarbeit. https://www.bitkom.org/Presse/Presseinformation/Grosse-Mehrheit-fuer-Kuenstliche-Intelligenz-in-der-Polizeiarbeit. Zugegriffen: 28. Aug. 2018.

Blatter, J., Langer, P. C., & Wagemann, C. (2017). Qualitative Methoden in der Politikwissenschaft, Grundwissen Politik. https://doi.org/10.1007/978-3-658-14955-0_2.

Blumtritt, J. (2015). Big data. http://www.digitalwiki.de/big-data/. Zugegriffen: 28. Aug. 2018.

Borgböhmer, T. (2018). Twitter weiß, wann du schlafen gehst. Wie Algorithmen aus 144 Metadaten die Identität der Nutzer ermitteln. https://meedia.de/2018/07/10/twitter-weiss-wann-du-schlafen-gehst-wie-algorithmen-aus-144-metadaten-die-identitaet-der-nutzer-ermitteln/. Zugegriffen: 28. Aug. 2018.

Brecht, B. (1981). *Der aufhaltsame Aufstieg des Arturo Ui*. London: Methuen.

Brown, R. (2018). 1984, Cambridge analytica and what others know of our selves. http://www.publicaddress.net/hardnews/1984-cambridge-analytica-and-what-others/. Zugegriffen: 5. Sept. 2018.

Budras, C. (8. April 2018). Vom Wert unserer Facebook-Daten. *Frankfurter Allgemeine Sonntagszeitung,* 21.

Bünder, H., & Koch, B. (2018). Jetzt hat das Kartellamt Amazon im Visier. http://www.faz.net/aktuell/wirtschaft/andreas-mundt-endspiel-um-die-telekommunikation-15725311.html. Zugegriffen: 13. Okt. 2018.

Bundesamt für die Sicherheit in der Informationstechnik BSI. (2011). BSI-Bürgerumfrage zur Internetsicherheit. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2011/BSI-Buergerumfrage-Internetsicherheit_11022011.html. Zugegriffen: 5. März 2018.

Bundeskartellamt. (2016). Arbeitspapier Marktmacht von Plattformen und Netzwerken. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.pdf?__blob=publicationFile&v=2. Zugegriffen: 23. Sept. 2018.

Bundeskartellamt. (2017). Hintergrundinformationen zum Facebook-Verfahren des Bundeskartellamtes. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Diskussions_Hintergrundpapier/Hintergrundpapier_Facebook.pdf?__blob=publicationFile&v=5. Zugegriffen: 1. Okt. 2018.

Bundesministerium der Justiz und für Verbraucherschutz. (2018). Datenschutz-Grundverordnung. https://www.bmjv.de/DE/Themen/FokusThemen/DSGVO/DSVGO_node.html. Zugegriffen: 10. Okt. 2018.

Bundesministerium für Bildung und Forschung. (2018). Eckpunkte der Bundesregierung für eine Strategie künstliche Intelligenz. https://www.bmbf.de/files/180718%20Eckpunkte_KI-Strategie%20final%20Layout.pdf. Zugegriffen: 28. Aug. 2018.

Bundesministerium für Verkehr und digitale Infrastruktur. (2017). Ethik-Kommission, Automatisiertes und Vernetztes Fahren. https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?blob=publicationFile. Zugegriffen: 28. Aug. 2018.

Bundesministerium für Wirtschaft und Energie. (2018). https://www.bmwi.de/Redaktion/DE/Artikel/Wirtschaft/kommission-wettbewerbsrecht-4-0.html. Zugegriffen: 28. Aug. 2018.
Bundesregierung. (2018). Koalitionsvertrag zwischen CDU, CSU und SPD. https://www.bundesregierung.de/resource/blob/975226/847984/5b8bc23590d4cb2892b31c987ad672b7/2018-03-14-koalitionsvertrag-data.pdf?download=1. Zugegriffen: 10. Okt. 2018.
Bunk, P., & Goldschmidt, P. (2016). Big Data und die Dual-Use Problematik am Beispiel öffentlicher Daten. *Datenschutz und Datensicherheit, 40*(7), 463–467. https://doi.org/10.1007/s11623-016-0637-3.
Burchardt, A. (2018). So schnell schafft der Mensch sich nicht ab! Die digitale Zukunft. Auslandsinformationen der Konrad-Adenauer-Stiftung, 1(2018), 10–17.
Busch, R. (20. Juli 2018). Jobkiller? Nein, Jobmotor! *Wirtschaftswoche,* 10.
Cool, A. (2018). Europe's data protection law is a big, confusing mess. https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html. Zugegriffen: 11. Okt. 2018.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. (2018). Eingriffe in das Recht auf informationelle Selbstbestimmung nur auf Grundlage eines Gesetzes, das auch dem Datenschutz Rechnung trägt. Volkszählungsurteil. https://www.bfdi.bund.de/DE/Datenschutz/Themen/Melderecht_Statistiken/VolkszaehlungArtikel/151283_VolkszaehlungsUrteil.html. Zugegriffen: 28. Aug. 2018.
Der Spiegel (1/1983). Die neue Welt von 1984. http://www.spiegel.de/spiegel/print/d-14017938.html. Zugegriffen: 28. Aug. 2018.
Deutscher Ethikrat. (2017). Ethikrat fordert eine an Datensouveränität orientierte Gestaltung von Big Data im Gesundheitsbereich. https://www.ethikrat.org/fileadmin/PDF-Dateien/Pressemitteilungen/pressemitteilung-08-2017.pdf. Zugegriffen: 28. Aug. 2018.
Duhigg, C. (16. Februar 2012). How companies learn your secrets. New York Times Magazine. www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Zugegriffen: 28. Aug. 2018.
Duparc, A., & Hourdeaux, J. (2018). Cambridge Analytica, le Big Brother électoral de Donald Trump. www.mediapart.fr/journal/international/190318/cambridge-analytica-le-big-brother-electoral-de-donald-trump?onglet=full. Zugegriffen: 5. Sept. 2018.
Economist. (2016). Big data, meet big brother. China invents the digital totalitarian state. https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state. Zugegriffen: 28. Aug. 2018.
Economist. (2017). The world's most valuable resource is no longer oil, but data. Regulating the internet giants. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Zugegriffen: 28. Aug. 2018.
Eggers, D. (2013). *The circle*. New York: Random House.
Evans, P. (2018). Harnessing big data: A tsunami of transformation. In J. Wanna & S. Vincent (Hrsg.), *Opening government: Transparency and engagement in the information age* (S. 137–144). Acton: ANU Press.
Facebook. (2017). Annual report. https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2017_FINAL.pdf. Zugegriffen: 28. Aug. 2018.
Farnadi, G., Sitaraman, G., Rohani, M., Kosinski, M., Stillwell, D., Moens, M.-F., Da-valos, S., & De Cock, M. (2014). How are you doing? Emotions and personality in Facebook. http://ceur-ws.org/Vol1181/empire2014_paper_05.pdf. Zugegriffen: 1. Okt. 2018.
Fischer, S., & Petersen, T. (2018). Was Deutschland über Algorithmen weiß und denkt. Ergebnisse einer repräsentativen Bevölkerungsumfrage. Güterseloh: Bertelsmann-Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/

GrauePublikationen/Was_die_Deutschen_ueber_Algorithmen_denken.pdf. Zugegriffen: 28. Aug. 2018.

Fraunhofer-Gesellschaft. (2016). Industrial data space. Digitale Souveränität über Daten. https://www.fraunhofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/Industrial-Data-Space_whitepaper.pdf. Zugegriffen: 26. Nov. 2018.

Gadinger, F., Jarzebski, S., & Yildiz, T. (2014). Politische Narrative. Konturen einer politikwissenschaftlichen Erzähltheorie. In F. Gadinger, S. Jarzebski, & T. Yildiz (Hrsg.), *Politische Narrative* (S. 3–38). Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-658-02581-6_1.

GfK. (2018). Künstliche Intelligenz (KI). Meinungsumfrage im Auftrag des Bundesverbandes deutscher Banken. https://bankenverband.de/media/files/Umfrage_Kuenstliche_Intelligenz.pdf. Zugegriffen: 28. Aug. 2018.

Grassegger, J., & Krogerus, M. (2016). Diese Firma weiß, was Sie denken. https://www.tagesanzeiger.ch/ausland/amerika/Diese-Firma-weiss-was-Sie-denken/story/25805157. Zugegriffen: 28. Aug. 2018.

Groth, O., Nitzberg, M., & Esposito, M. (2018). Regeln für Roboter. Die digitale Zukunft. Auslandsinformationen der Konrad-Adenauer-Stiftung, 1(2018), 18–31.

Hajek, S. (2018). Der Spion in meiner App. *Wirtschaftswoche, 27,* 56.

Harris, S., & Castelao, L. (2014). The social laboratory. *Foreign Policy, 207,* 64–71.

Haucap, J., & Heimeshof, U. (2017). Ordnungspolitik in der digitalen Welt. Ordnungspolitische Perspektiven Nr. 90. http://www.dice.hhu.de/fileadmin/redaktion/Fakultaeten/Wirtschaftswissenschaftliche_Fakultaet/DICE/Ordnungspolitische_Perspektiven/090_OP_Haucap_Heimeshoff.pdf. Zugegriffen: 2. Okt. 2018.

Hornung, G., & Herfurth, C. (2018). Datenschutz bei Big Data Rechtliche und politische Implikationen. In C. König, J. Schröder, & E. Wiegand (Hrsg.), *Big Data. Schriftenreihe der ASI – Arbeitsgemeinschaft Sozialwissenschaftlicher Institute*. https://doi.org/10.1007/978-3-658-20083-1_11.

Institut für Demoskopie Allensbach. (2013). Sicherheitsreport. https://www.ifd-allensbach.de/uploads/tx_studies/Sicherheitsreport_2013_01.pdf. Zugegriffen: 12. Okt. 2018.

Jentzsch, N (2018). Dateneigentum – Eine gute Idee für die Datenökonomie? https://www.stiftung-nv.de/sites/default/files/nicola_jentzsch_dateneigentum.pdf. Zugegriffen: 10. Okt. 2018.

Kehlmann, D. (2017). Im Gespräch mit V. Balzer. George Orwell ist plötzlich richtig wirkungsmächtig geworden. http://www.deutschlandfunkkultur.de/daniel-kehlmann-ueber-1984-als-geistige-waffe-george-orwell.1013.de.html?dram:article_id=389022. Zugegriffen: 14. Sept. 2018.

Knop, C. (2018). Hat der Mensch die Technik noch im Griff? https://www.faz.net/aktuell/wirtschaft/cebit/hat-der-mensch-die-technik-noch-im-griff-15622975.html. Zugegriffen: 1. Okt. 2018.

Knorre, S. (2018). Mehr Transparenz wagen – Bitte nicht! http://www.consulting.de/=hintergruende/kolumne/einzelansicht/mehr-transparenz-wagen-bitte-nicht/. Zugegriffen: 12. Sept. 2018.

Knüwer, T. (2016). Big Data für Donald Trump. Fake News für die Intelligenzija. http://www.indiskretionehrensache.de/2016/12/cambridge-analytica/. Zugegriffen: 12. Okt. 2018.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behaviour. PNAS Proceedings of the National

Academy of Sciences of the United States of America, 11. März 2013. http://www.pnas.org/content/110/15/5802. Zugegriffen: 28. Aug. 2018.
Kostka, G. (2018). China's social credit systems and public opinion: Explaining high levels of approval. https://papers.ssrn.com/sol3/papers.cfm?%20abstract_id=3215138. Zugegriffen: 10. Okt. 2018.
Krempl, S. (2018). Datensouveränität. Die Säge am informationellen Selbstbestimmungsrecht. https://www.heise.de/newsticker/meldung/Datensouveraenitaet-Die-Saege-am-informationellen-Selbstbestimmungsrecht-3953776.html. Zugegriffen: 28. Aug. 2018.
Kröger, F. (2015). Das automatisierte Fahren im gesellschaftsgeschichtlichen und kulturwissenschaftlichen Kontext. In M. Maurer, J. C. Gerdes, B. Lenz, & H.Winner (Hrsg.), *Autonomes Fahren. Technische, rechtliche und gesellschaftliche Aspekte* (S. 41–67). Wiesbaden: Springer VS.
Lindner, R. (2017). Darum wird „1984" plötzlich wieder zum Bestseller. http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/george-orwells-roman-1984-wird-wieder-bestseller-14771376.html. Zugegriffen: 28. Aug. 2018.
Madden, M. (2014). Public perceptions of privacy and security in the post-Snowden era. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions. Zugegriffen: 28. Aug. 2018.
Mai, J.-E. (2016). Big Data privacy. The datafication of personal information. *The Information Society, 32,* 192–199. https://doi.org/10.1080/01972243.2016.1153010.
Mayer-Schönberger, V., & Ramge, T. (2018). *Reinventing capitalism in the age of big data*. New York: Hachette.
Mazur, P. (2018). Inside China's dystopian dreams. A. I., shame and lots of cameras. www.nytimes.com/2018/07/08/business/china-surveillance-technology.html. Zugegriffen: 28. Aug. 2018.
McKinsey Global Institute. (2018). Notes from the AI Frontier. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/notes%20from%20the%20ai%20frontier%20applications%20and%20value%20of%20deep%20learning/mgi_notes-from-ai-frontier_discussion-paper.ashx. Zugegriffen: 28. Aug. 2018.
Merkel, A. (2015). Rede von Bundeskanzlerin Merkel bei der Deutsch-Französischen Digitalen Konferenz am 27.Oktober 2015. https://www.bundeskanzlerin.de/bkin-de/aktuelles/rede-von-bundeskanzlerin-merkel-bei-der-deutsch-franzoesischen-digitalen-konferenz-am-27-oktober-2015-370546. Zugegriffen: 28. Aug. 2018.
Mooy De, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data. Considerations for future policy regimes in the United States and the European Union. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/RethinkingPrivacy_2017_final.pdf. Zugegriffen: 28. Aug. 2018
Morozov, E. (2015). Socialize the data centres! *New Left Review 91*. https://newleftreview.org/II/91/evgeny-morozov-socialize-the-data-centres. Zugegriffen: 28. Aug. 2018.
Müller-Peters, H., & Gatzert, N. (2016). Todsicher: Die Wahrnehmung und Fehlwahrnehmung von Alltagsrisiken in der Öffentlichkeit. *Schriftenreihe Forschung am IVW Köln, Bd. 12*.
Neuerer, D. (2018). Können wir künstlicher Intelligenz vertrauen? https://www.handelsblatt.com/politik/deutschland/bitkom-umfrage-koennen-wir-kuenstlicher-intelligenz-vertrauen/20930352.html?ticket=ST-3309346-0XRTohfAJ0uZ4xq2RpEW-ap4. Zugegriffen: 28. Aug. 2018.

Neuroth, B. (2014). „The Specter of Orwell". Narrative nach Nineteen Eighty-Four in US-amerikanischen Privacy-Debatten der 1960er und 1970er Jahre. In W. Hofmann, J. Renner, & K. Teich (Hrsg.), *Narrative Formen der Politik* (S. 73–92). Wiesbaden: Springer VS.

Orwell, G. (1949). *Nineteen eighty-four*. London: Secker & Warburg.

Osterhammel, J. (2009). *Die Verwandlung der Welt*. München: Beck.

PwC. (2017). Bevölkerungsbefragung Künstliche Intelligenz. https://www.pwc.de/de/consulting/bevoelkerungsbefragung-kuenstliche-intelligenz-2017.pdf. Zugegriffen: 28. Aug. 2018.

Reinhold, F., & Schnack, T. (2016). US-Wahl und Daten-Ingenieure. Ich ganz allein habe Trump ins Amt gebracht. http://www.spiegel.de/netzwelt/netzpolitik/donald-trump-und-die-daten-ingenieure-endlich-eine-erklaerung-mit-der-alles-sinn-ergibt-a-1124439.html. Zugegriffen: 12. Sept. 2018.

Rogoff, K. (2018). Big tech is a big problem. https://www.project-syndicate.org/commentary/regulating-big-tech-companies-by-kenneth-rogoff-2018-07. Zugegriffen: 28. Aug. 2018.

Saal, M. (2017). Zenith-Prognose. Digital wächst weiter – doch nur Google und Facebook profitieren. https://www.horizont.net/medien/nachrichten/Zenith-Prognose-Digital-waechst-weiter—doch-nur-Google-und-Facebook-profitieren-163161. Zugegriffen: 11. Okt. 2018.

Sachverständigenrat für Verbraucherfragen. (2018). Verbrauchergerechtes Scoring. http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Verbrauchergerechtes_Scoring.pdf. Zugegriffen: 24. Nov. 2018.

Sandfuchs, B. (2015). *Privatheit wider Willen? Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht*. Tübingen: Mohr Siebeck.

SAP. (2018). SAP gründet Ethik Beirat für Künstliche Intelligenz. https://news.sap.com/germany/2018/09/ethik-beirat-fuer-kuenstliche-intelligenz/. Zugegriffen: 19. Sept. 2018.

Schaar, P. (2017a). Verbraucherdatenschutz in der Digitalisierung. http://library.fes.de/pdf-files/wiso/13497.pdf. Zugegriffen: 19. Sept. 2018.

Schaar, P. (2017b). Wie die Digitalisierung unsere Gesellschaft verändert. In M. Schröder, & A. Schwanebeck (Hrsg.), *Big Data. In den Fängen der Datenkraken. Die (un-)heimliche Macht der Algorithmen* (S. 105–122). Baden-Baden: Nomos.

Schlüter, B. (2017). Digitale Plattformen. Ein neues Handlungsfeld für die Daseinsverantwortung des Staates? http://library.fes.de/pdf-files/wiso/13402.pdf. Zugegriffen: 19. Sept. 2018.

Schubert, C. (15. Juni 2018). Europa muss seine Bürger besser schützen. Interview mit Tom Enders (Airbus) und Charles-Édouard Bouée. *Frankfurter Allgemeine Sonntagszeitung,* 26.

Schulz-Ojala, J. (2013). Der große Bruder greift dich an. https://www.tagesspiegel.de/kultur/erschreckend-aktuell-george-orwells-1984-unheimliche-verwandtschaft-zwischen-der-nsa-und-dem-grossen-bruder/8555434.html. Zugegriffen: 28. Aug. 2018.

Schweitzer, H., Haucap, J., Kerber, W., & Welker, R. (2018). Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen. Endbericht. Projekt im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi). Projekt Nr. 66/17. https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-miss-

brauchsaufsicht-fuer-marktmaechtige-unternehmen.pdf?__blob=publicationFile&v=15. Zugegriffen: 1. Okt. 2018.
Schwerk, A., Thoms, J., Rabl, T., & Markl, V. (2018). Datensouveränität. Fortschritt und Verantwortung. https://smartdataforum.de/wp-content/uploads/2018/04/Final-Datensouveränität.pdf. Zugegriffen: 28. Aug. 2018.
Shiller, R. J. (2017). Narrative economics. http://www.cowles.yale.edu/sites/default/files/files/pub/d20/d2069.pdf. Zugegriffen: 14. Aug. 2018.
Smart-Data-Begleitforschung. (2018). Corporate digital responsibility. https://www.digitale-technolo-gien.de/DT/Redaktion/DE/Downloads/Publikation/2018_02_smartdata_corporate_digital_responsibility.pdf?__blob=publicationFile&v=8. Zugegriffen: 26. Nov. 2018.
Srinivasan, C. R. (2018). Sicherheitsrisiken der Digitalisierung. https://www.security-insider.de/sicherheitsrisiken-der-digitalisierung-a-732737/. Zugegriffen: 28. Aug. 2018.
Steltzner, H. (7. Januar 2018). Chinas Weg zur Weltherrschaft. *Frankfurter Allgemeine Sonntagszeitung,* 19–20.
Szidzek, C., & Bolsinger H. J. (2018). Datensouveränität und Vertrauen. Der „Amazon-Fall". *FHWS Science Journal 2018, 1,* 22–36.
The Guardian. (17. März 2018). Revealed. 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Zugegriffen: 1. Okt. 2018.
Thomas, J. (2017). Kultur- und Kreativschaffende sind künftig im Vorteil. Interview mit Thomas Ramge. https://www.creative-city-berlin.de/de/ccb-magazin/2017/12/11/interview-thomas-ramge-das-digital/. Zugegriffen: 12. Sept. 2018.
Welt. (2018). Facebook verliert Nutzer in Europa. Aktie stürzt ins Bodenlose. https://www.welt.de/wirtschaft/article179980142/150-Milliarden-Dollar-weg-Facebook-verliert-Nutzer-in-Europa-Aktie-stuerzt-ins-Bodenlose.html. Zugegriffen: 12. Sept. 2018.
Witzeck, E. (2. Mai 2018). Der Skandal um Cambridge Analytica ist eine Inszenierung. Gespräch mit Lorena Jaume-Palasi. *Frankfurter Allgemeine Zeitung*, S. 15.
YouGov. (2018). Künstliche Intelligenz. Deutsche sehen eher die Risiken als den Nutzen. https://yougov.de/news/2018/09/11/kunstliche-intelligenz-deutsche-sehen-eher-die-ris/. Zugegriffen: 10. Okt. 2018.
Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *PNAS January 2015, 112*(4), 1036–1040. https://doi.org/10.1073/pnas.1418680112.
Zittrain, J. (2018). How to exercise the power you didn't ask for. https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for. Zugegriffen: 26. Nov. 2018.