

RESEARCH

Susanne Knorre
Horst Müller-Peters
Fred Wagner

Die Big- Data-Debatte

Chancen und Risiken
der digital vernetzten Gesellschaft

OPEN



Springer Gabler

Die Big-Data-Debatte

Susanne Knorre · Horst Müller-Peters ·
Fred Wagner

Die Big-Data-Debatte

Chancen und Risiken der digital
vernetzten Gesellschaft

OPEN

 **Springer** Gabler

Susanne Knorre
Institut für Kommunikations-
management, Hochschule Osnabrück
Osnabrück, Deutschland

Horst Müller-Peters
Institut für Versicherungswesen
Technische Hochschule Köln
Köln, Deutschland

Fred Wagner
Institut für Versicherungslehre
Universität Leipzig
Leipzig, Deutschland



ISBN 978-3-658-27257-9 ISBN 978-3-658-27258-6 (eBook)
<https://doi.org/10.1007/978-3-658-27258-6>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Gabler

© Der/die Herausgeber bzw. der/die Autor(en) 2020. Dieses Buch ist eine Open-Access-Publikation. **Open Access** Dieses Buch wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Buch enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Je rascher die Digitalisierung voranschreitet, desto intensiver wird darüber diskutiert, dass Deutschland in vielerlei Hinsicht den Anschluss an die führenden Länder dieser globalen Transformation verliert. Dabei geht es nicht nur ganz konkret um die offensichtlichen Mängel in der Netzinfrastruktur, um zu kleine Forschungsbudgets, eine unterentwickelte Start-up-Kultur oder den gravierenden Mangel an IT-Fachkräften, sondern auch um Fragen zur digitalen Innovationsfähigkeit von Wirtschaft und Gesellschaft ganz allgemein. Ob Deutschland tatsächlich die Digitalisierung verschläft, hängt nicht zuletzt vom Umgang mit Big Data ab, also der Frage, in welchem Umfang und unter welchen Bedingungen Massendaten erhoben und ausgewertet werden. Aus vielen Befragungen ist festzustellen, dass eine allgemeine Orientierungslosigkeit darüber herrscht, wie die Chancen und Risiken von Big Data und deren Nutzung für die Entwicklung von Künstlicher Intelligenz einzuordnen sind.

Am deutlichsten wird diese Orientierungslosigkeit beim Thema Datensicherheit bzw. Datenschutz. Hier verhalten sich die Bundesbürger in hohem Maße ambivalent: Einerseits sorgen sie sich, dass ihre persönlichen Daten missbraucht werden könnten und sprechen dem Datenschutz hohe Bedeutung zu. Andererseits gehen sie im Alltag ausgesprochen sorglos mit privaten Daten um. Die Situation ist paradox: Die Nutzer als Bürger sind skeptisch, schutzbedürftig und kulturpessimistisch, als Verbraucher sind sie sorglos, bequem und pragmatisch. In der öffentlichen Wahrnehmung überwiegen deutlich die mit Big Data verbundenen Risiken, während sich das Verhalten der Nutzer deutlich stärker an den Chancen von Big Data ausrichtet.

Wie aber lässt sich vor diesem Hintergrund Orientierung geben, welche Signale und welche Leuchttürme braucht es, damit ein Kurs gefunden werden kann, der Chancen und Risiken von Big Data ausgewogen berücksichtigt? Diese Frage

steht im Mittelpunkt der vorliegenden Studie, die hypothesenbasiert und auf Basis unterschiedlicher Methoden durchgeführt und in iterativer Arbeitsweise finalisiert wurde. Um sie zu beantworten, wird in einem ersten Schritt von Susanne Knorre analysiert, welche Narrative die öffentliche Diskussion dominieren und welche Schlussfolgerungen sich daraus für aktuelle rechtliche und politische Lösungsangebote ergeben. In einem zweiten Schritt zeigen Fred Wagner und Theresa Jost anhand der Lebensbereiche Wohnen, Gesundheit und Mobilität exemplarisch auf, wie die Chancen der Digitalisierung konkret aussehen und wie sich Smart Services und datengetriebene Geschäftsmodelle entwickeln. Letzteres wird mit bereits real existierenden Angeboten in anderen Ländern (u. a. USA und China) sowie am Beispiel der Versicherungen dargestellt. Schließlich überprüft Horst Müller-Peters anhand einer repräsentativen Erhebung, inwieweit all diese Überlegungen beim Bürger im Netz ‚angekommen‘ sind. Im Schlusskapitel werden die Ergebnisse und Handlungshinweise für Entscheider in Politik und Wirtschaft zusammengefasst und Big Data in seiner Ambivalenz als Bürgerschreck und Hoffnungsträger abschließend bewertet.

Zunächst wird deutlich, dass der öffentliche, in den Medien ausgetragene Diskurs zum Umgang mit Big Data von Erzählungen dominiert ist, die um Konflikte und Kollisionen kreisen und nicht über diese hinauskommen. In der Medienanalyse sind sie als Varianten des ‚Big-Brother‘-Narrativs einzuordnen und haben ganz überwiegend den Charakter von Dystopien, also negativer Zukunftsszenarien. Es kann angenommen werden, dass allenfalls eine neue, ebenso starke Erzählung dazu beitragen kann, die geschilderten paradoxen Verhältnisse aufzulösen. Es müssten deshalb andere, weniger dystopische Erzählungen konstruiert werden, die mit neuen Rollenbildern für den digitalen Bürger einhergehen. Tatsächlich zeigt sich, dass die Bürger den Mehrwert, den Smart Services ihnen bieten können, durchaus wertschätzen. Die Grundskepsis gegenüber Big Data kippt, wenn konkrete, nutzenstiftende Anwendungen genannt werden.

Insgesamt kann die Vorstellung eines Paradigmenwechsels im Umgang mit Big Data zur Orientierung im öffentlichen Diskurs dienen. Dieser Paradigmenwechsel beinhaltet im Kern, den Datenschutz nicht mehr ausschließlich als Abwehrrecht zu betrachten, sondern ihn in ein aktivierendes Handlungskonzept zu integrieren. Der Bürger soll in seiner Rolle als Nutzer digitaler Technologien so unterstützt werden, dass er seine Daten gezielt und sicher zu den von ihm gewünschten Zwecken weitergeben kann. Das Zielbild sind Bürger als selbstbewusste und souveräne Nutzer, die sich nicht mehr primär als Schutzobjekt verstehen, sondern als Datengeber, Datenspender oder gar Datenhändler.

Dies erfordert auch ein anderes Rollenverständnis in der Wirtschaft. Zukünftig reicht es nicht mehr aus, die Compliance mit den Datenschutzgesetzen zu garantieren. Vielmehr sind gerade die Unternehmen mit digitalen Geschäftsmodellen aufgefordert, mithilfe von Big Data positive Beiträge für gesellschaftlich relevante Zwecke zu ermöglichen. Unternehmen würden dementsprechend ethisch verpflichtet, die Chancen von Big Data bzw. Künstlicher Intelligenz proaktiv für Zwecke des Gemeinwohls („social good“) zu nutzen. Das ist der Stoff, aus dem neue Erzählungen entstehen, die Big Data aus der Big-Brother-Umklammerung befreien können.

Die Ergebnisse dieser Studie wurden anlässlich des Verkehrsgerichtstages 2019 in einer Podiumsdiskussion erörtert. Das Thema braucht den öffentlichen Diskurs, damit Deutschland dem digitalen Wandel nicht hinterherläuft, sondern ihn mit einer ausgewogenen Betrachtung von Chancen und Risiken aktiv gestaltet. Wir bedanken uns bei Theresa Jost, Geschäftsführerin der V.E.R.S. Leipzig GmbH, für ihren Beitrag zu den digitalen Lebenswelten, bei Anne Wrede für ihre Unterstützung in der Vorbereitung und Auswertung der empirischen Studie sowie beim Goslar Institut, das diese Studie ermöglicht und vielfältige tatkräftige Unterstützung geleistet hat.

Hannover
Köln
Leipzig
im März 2019

Susanne Knorre
Horst Müller-Peters
Fred Wagner

Inhaltsverzeichnis

| | | |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 1 | Big Data im öffentlichen Diskurs: Hindernisse und Lösungsangebote für eine Verständigung über den Umgang mit Massendaten | 1 |
| 1.1 | Big Data und Datenschutz im politischen Diskurs: Einführung und Bestandsaufnahme | 1 |
| 1.1.1 | Nutzen und Schutz von Daten: Überlegungen zur Analyse eines politischen Diskurses | 2 |
| 1.1.2 | Big Data, Künstliche Intelligenz und Algorithmen: Begriffe und Konzepte in der Diskussion | 4 |
| 1.1.3 | Arten, Herkunft und Nutzer von Daten: Annäherung an eine Dual-Use Technologie | 7 |
| 1.1.4 | Diffuses Bild: Was bislang über die öffentliche Einschätzung von Datennutzung erhoben wurde. | 12 |
| 1.2 | Von Konflikten und Kollisionen: Big Data als Gegenstand öffentlicher Narrationen. | 15 |
| 1.2.1 | Ein Narrativ wird entdeckt: ‚Big Brother‘ in der Kampagne gegen die Volkszählung 1983 | 16 |
| 1.2.2 | ‚Big Brother‘ reloaded: Die Erzählung von Edward Snowden. | 18 |
| 1.2.3 | Die Manipulation: Die Erzählung von der Beeinflussung des US-Wahlkampfs 2016 | 20 |
| 1.2.4 | Spione im Kinderzimmer: Die Erzählung vom Verlust der Privatsphäre | 22 |
| 1.2.5 | Die Apokalypse: Die Erzählung vom digitaltotalitären Staat | 23 |
| 1.2.6 | Die Verselbstständigung der Maschine: Die Erzählung vom unkontrollierbaren Auto. | 25 |

| | | |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 1.2.7 | Die globale Gier: Die Erzählung von der Weltherrschaft der ‚Frightful 5‘ | 26 |
| 1.3 | Nutzen und Schutz von Daten des Bürgers im politischen Diskurs | 28 |
| 1.3.1 | Datenschutz im Fokus der Gesetzgebung: Rechtliche Regelungen für den Umgang mit personenbezogenen Daten | 30 |
| 1.3.2 | Kritik von allen Seiten: Daten- und Verbraucherschützer versus Innovationstreiber | 32 |
| 1.4 | Vom Heldenbild des rationalen, souveränen Nutzers: Narrationen im politischen Diskurs | 35 |
| 1.4.1 | Von rationaler Ignoranz und anderen Paradoxien: Nutzerverhalten jenseits der Idealtypen | 36 |
| 1.4.2 | Vom Datenschutz zur Datensouveränität: Mit persönlichen Daten eigenverantwortlich umgehen | 40 |
| 1.5 | Datenethik als neues Paradigma? Handlungsangebote jenseits der Regulierung | 42 |
| 1.6 | Ordnungspolitik und Big Data: Den fairen Zugang sichern | 46 |
| 1.6.1 | Propositionen: Wie der öffentliche Diskurs zu Nutzen und Schutz von Daten des souveränen Bürgers gestaltet werden kann | 50 |
| | Literatur | 55 |
| 2 | Big Data, Data Analytics und Smart Services rund um Wohnen, Gesundheit und Mobilität: Bürgerschreck und Hoffnungsträger in privaten Lebenswelten | 63 |
| 2.1 | Grundlagen zum Konzept der Lebenswelten | 63 |
| 2.1.1 | Begriff der Lebenswelten | 63 |
| 2.1.2 | Tatsächliche Lebenswelten aus Sicht von Bürgern | 64 |
| 2.1.3 | Big Data und Data Analytics in den Lebenswelten | 66 |
| 2.1.4 | Smart Services und Geschäftsmodellentwicklungen in zentralen Lebenswelten | 69 |
| 2.2 | Lebenswelt Wohnen | 73 |
| 2.2.1 | Smart Services im Überblick | 73 |
| 2.2.2 | Ausgewählte Geschäftsmodelle innerhalb der Smart Services | 77 |
| 2.2.3 | Spannungsfeld Datennutzung und Datenschutz | 82 |
| 2.2.4 | Rolle der Versicherer | 86 |

| | | |
|----------|-----------------------------------------------------------------------------------------------------------------------------|------------|
| 2.3 | Lebenswelt Gesundheit | 90 |
| 2.3.1 | Smart Services im Überblick | 90 |
| 2.3.2 | Ausgewählte Geschäftsmodelle innerhalb der Smart Services | 94 |
| 2.3.3 | Spannungsfeld Datennutzung und Datenschutz. | 100 |
| 2.3.4 | Rolle der Versicherer | 102 |
| 2.4 | Lebenswelt Mobilität | 105 |
| 2.4.1 | Smart Services im Überblick | 105 |
| 2.4.2 | Ausgewählte Geschäftsmodelle innerhalb der Smart Services | 109 |
| 2.4.3 | Spannungsfeld Datennutzung und Datenschutz. | 115 |
| 2.4.4 | Rolle der Versicherer | 119 |
| 2.5 | Utopien und Dystopien | 123 |
| 2.5.1 | Utopien: Möglichkeiten und gesellschaftlicher Nutzen | 123 |
| 2.5.2 | Dystopien: Grenzen und gesellschaftliche Risiken | 126 |
| | Literatur. | 130 |
| 3 | Big Data: Chancen und Risiken aus Sicht der Bürger | 137 |
| 3.1 | Einleitung. | 137 |
| 3.2 | Datenwissen. | 140 |
| 3.3 | Handlungsfreiheit. | 143 |
| 3.4 | Folgeabschätzungen, Bewertung von Anwendungsfeldern und Einstellungen zu Datenschutz und Technologie („Wollen“). | 146 |
| 3.4.1 | Folgeabschätzungen. | 146 |
| 3.4.2 | Bewertung von Anwendungsfeldern | 154 |
| 3.4.3 | Einstellungen zu Datenschutz und Technologien | 158 |
| 3.5 | Verhalten („Handeln“) | 160 |
| 3.5.1 | Umfang der Online-Nutzung | 160 |
| 3.5.2 | Selbst- und Fremdeinschätzung | 162 |
| 3.5.3 | Maßnahmen zum Datenschutz. | 163 |
| 3.6 | Datenpolitik und Datenethik („Neue Paradigmen“) | 169 |
| 3.6.1 | Datenpolitik aus Sicht der Bevölkerung | 169 |
| 3.6.2 | Fairness als Mindestanforderung an Big Data | 170 |
| 3.6.3 | Bewertung von Paradigmen in der Datenpolitik | 172 |
| 3.6.4 | „Rohstoff“ Daten. | 175 |
| 3.7 | Alte und neue Narrative | 176 |
| 3.8 | Neue Rollen am Beispiel der Versicherungswirtschaft | 179 |
| 3.8.1 | Anwendungsfelder von Big Data | 179 |
| 3.8.2 | Akzeptanz neuer Rollen. | 180 |

| | | |
|----------|-----------------------------------------------------------------------------------------------------------------------|-----|
| 3.9 | Fazit | 187 |
| 3.9.1 | Wissen – Können – Wollen – Handeln | 187 |
| 3.9.2 | Neue Paradigmen für Politik, Wirtschaft und Gesellschaft? | 189 |
| 3.9.3 | Rollenwandel für die Versicherungswirtschaft? | 190 |
| 3.9.4 | Conclusio | 191 |
| | Literatur. | 191 |
| 4 | Big Data: Bürgerschreck und Hoffnungsträger! | |
| | Zusammenfassung und Fazit | 195 |
| 4.1 | Zur Gestaltung des öffentlichen Diskurses über Chancen und Risiken von Big Data: Die Ergebnisse im Überblick | 196 |
| 4.2 | Zum Nutzen von Big Data in konkreten Lebenswelten: Die Ergebnisse im Überblick | 201 |
| | Anhang | 207 |

Über die Autoren

Prof. Dr. Susanne Knorre arbeitet als Unternehmensberaterin mit den Schwerpunkten Kommunikation und Management sowie Strategie- und Organisationsentwicklung. Sie verfügt über langjährige Aufsichtsratserfahrung und hat derzeit fünf Mandate inne. Nach Studium der Politischen Wissenschaften und Volkswirtschaftslehre sowie dem Staatsexamen für den höheren allgemeinen Verwaltungsdienst war sie im Wirtschaftsministerium in Rheinland-Pfalz u. a. als Leiterin des Ministerbüros tätig. Sie promovierte in der Zeit über die Entwicklung der deutschen Tarifautonomie. Danach wechselte sie zur Preussag AG und übernahm 1998 die Leitung der Konzernkommunikation. Von 2000 bis 2003 war sie Wirtschafts- und Verkehrsministerin in Niedersachsen. Susanne Knorre ist seit 2007 nebenberufliche Professorin am Institut für Kommunikationsmanagement der Hochschule Osnabrück.

Horst Müller-Peters ist Professor für Betriebswirtschaftslehre, Marketing und Wirtschaftspsychologie am Institut für Versicherungswesen der Technischen Hochschule Köln und Leiter der dortigen Forschungsstelle Versicherungsmarkt. Daneben ist er Dozent in mehreren versicherungs- und finanzwirtschaftlichen Studiengängen, unter anderem an der Universität Leipzig. Er war Mitgründer und langjähriger Vorstandsvorsitzender des Marktforschungs- und Beratungsunternehmens psychonomics AG (heute YouGov Deutschland) und hat zahlreiche Beiträge zu Marktforschung, Marketing und zum Versicherungsmarkt publiziert. Er ist Mitglied verschiedener Beiräte und Gremien sowie Herausgeber der Branchenportale marktforschung.de, dataanalyst.eu und consulting.de. Ein besonderer Forschungsschwerpunkt liegt im Bereich Risikopsychologie, Behavioral Insurance sowie in der Analyse des Kundenverhaltens im Kontext der Digitalisierung.

Fred Wagner, Prof., Dr. rer. pol., Dipl.-Kfm. Bankkaufmann. Studium der Betriebswirtschaftslehre in Köln bis 1987. Wissenschaftlicher Mitarbeiter an der Universität zu Köln bis 1992. Promotion 1991 (Thema der Dissertation: Sovabilitätspolitik von Kompositversicherungsunternehmen). Habilitation 1997 (Thema der Habilitationsschrift: Risk Management im Erstversicherungsunternehmen). Seit 1996 Direktor des Instituts für Versicherungslehre, Universität Leipzig. Vorstand im Institut für Versicherungswissenschaften e. V. an der Universität Leipzig. Mitglied im Verwaltungsrat der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und im Deutschen Rechnungslegungs-Standards-Committee, AG Versicherungen. Forschungsschwerpunkte: Versicherungsmarkt; Versicherungsvertrieb; Rechnungslegung nach HGB und IFRS; „Solvency II“, Risikomanagement und Wertorientierte Unternehmenssteuerung; Lebensversicherung und betriebliche Altersversorgung; Asset Management; innovative Geschäftsmodelle, Insur-Techs und Digitalisierung in der Versicherungswirtschaft.

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

1

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 enthielt 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

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, permanently 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 Neu-erfindung 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 erlauben 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](https://www.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 Demoskopien 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 %) (Bitcom 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 Bitcom-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 Bitcom-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

¹Dass 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

²Hier 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 Parteilite 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 Auf-
lagenentwicklung gezeigt, sprang er zwischen 1982 und 1984 auf die Bestseller-
liste 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 Welt-
erfolg 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 harret 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, wengleich 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-Wahlkampfes 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 Treppenvitz der Geschichte, dass Trump oft über die Wissenschaft schimpfte, aber wohl dank ihr die Wahl gewann“ (Grassegger und Krogerus 2016). Dass Steve Bannon,

³Mehr 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 (Witzeck 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 Verteidigung 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 Cambridge-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 Horrervision 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

⁴Erkennbar 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 übergreifenden 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

⁵Facebook 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 wettet 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 Scorerwerten, 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 oder 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 Profiling 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 [Krempf 2018](#)). Immer öfter werde damit das Recht auf informationelle Selbstbestimmung infrage gestellt, moniert in diesem Zusammenhang die nieder-sächsische Datenschutzbeauftragte Barbara Thiel (zitiert in [Krempf 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.“

⁶So 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 Datenehmers 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 ‚Treuhand‘-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 Antimonopolssysteme 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 Paragraphen 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 Wettbewerbsökonom 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/2018-01-02/9b583344667f696c3b3aabb31b7424f/>. 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/eggert-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-eggert-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.bmjuv.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.bmw.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., Davalos, 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. Gütersloh: Bertelsmann-Stiftung. <https://www.bertelsmann-stiftung.de/fileadmin/files/BS/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., & Castela, 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.
- Krempel, 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/BSI/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-verwandschaft-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-Daten-souveraenitaet.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-technologie.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.
- Witzcek, 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.

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.



Big Data, Data Analytics und Smart Services rund um Wohnen, Gesundheit und Mobilität: Bürgerschreck und Hoffnungsträger in privaten Lebenswelten

2

2.1 Grundlagen zum Konzept der Lebenswelten

2.1.1 Begriff der Lebenswelten

Jeder Mensch befindet sich und handelt in verschiedenen Lebenswelten. Eine erste einfache Definition gibt der Duden und beschreibt eine Lebenswelt als „persönliches Umfeld; Welt, in der sich jemandes Leben abspielt“ (Duden 2019). Seine Wurzeln hat der Begriff ‚Lebenswelt‘ in der philosophischen Strömung der Phänomenologie und er wurde insbesondere durch den Philosophen Edmund Husserl geprägt. Nach seiner Definition umfassen Lebenswelten den menschlichen Wirklichkeitsbereich und dessen ökologische Beziehung zur Umwelt. Es ist das Erleben einer Welt, die von Anderen mit vergleichbarer Haltung und Erfahrungsschatz gleichartig empfunden wird (Spektrum 2001). Eine Lebenswelt erklärt das Umfeld, das ein Subjekt (oder eine Gruppe) im Alltag wahrnimmt und in dem es sich bewegt. Diese Wahrnehmung wird zum Bestandteil seiner subjektiven Lebenswelt (Mamerow 2012, S. 7).

Die Subjektivität führt dazu, dass Lebenswelten von jedem Menschen anders wahrgenommen werden und daher nicht objektiv abgegrenzt werden können. Eine Lebenswelt kann für eine einzelne Person über eine Spannweite bestimmt sein, die sich von übergeordneten Themen (wie Wohnen, Gesundheit und Mobilität) bis hin zu kleinsten Erlebnisbereichen erstrecken kann. Auf der Definition von Husserl aufbauend, beschreiben Schütz und Luckmann die Lebenswelt als „Wirklichkeit, an der der Mensch in unausweichlicher, regelmäßiger Wiederkehr teilnimmt“ (Schütz/Luckmann 2017, S. 29). Die Verwendung des Ideenansatzes

Dieses Kapitel wurde von Fred Wagner und Theresa Jost verfasst.

der Lebenswelten eröffnet in vielerlei Hinsicht Chancen. Theoriekonzepte sowie praktische Vorgehensweisen, die auf Lebenswelten basieren, haben den Vorteil, ganzheitlich angelegt zu sein.

Lebenswelten berühren aus der Sicht von Bürgern alle möglichen Themenfelder des alltäglichen Lebens und unterscheiden sich in ihrer Komplexität und Tiefe. Allgemeiner berühren Lebenswelten den Handlungsraum, das Umfeld oder die Denkweise, in denen sich Bürger täglich bewegen. Sie lassen sich nach ihrer Identität, ihrer Struktur und ihrem räumlichen Bezug unterscheiden. Meist werden Lebenswelten im privaten und geschäftlichen Kontext differenziert. Jedoch überschneiden sich Lebenswelten oft und können, je nach Situation oder Perspektive, ineinander übergehen. Daher haben Lebenswelten eine gewisse Unschärfe. Viele Lebenswelten von Bürgern können einer bestimmten Klientel zugeordnet werden, spiegeln eine bestimmte Orientierung wider und können Aufschluss über ‚die Lebensweise‘ geben. Damit geben Lebenswelten teilweise auch Einsichten in die physische und psychische Kondition eines Bürgers (Kraus 2006). Auch daraus ergibt sich, dass Lebenswelten nicht konstant sind, sondern sich im Verlauf des Lebens je nach aktueller Lebenssituation und Umweltfaktoren dynamisch verändern. Ein wichtiger Einflussfaktor sind dabei gesellschaftspolitische Entwicklungen und der technologische Fortschritt, der sich auf die Lebenswelten auswirkt, in denen Bevölkerungsgruppen zu Hause sind.

2.1.2 Tatsächliche Lebenswelten aus Sicht von Bürgern

Lebenswelten können von großen Themenkomplexen geprägt, aber auch sehr fein untergliedert sein. Eine objektive und pauschale Kategorisierung ist nicht möglich, vielmehr sind subjektive und standpunktabhängige Kriterien hinzuzuziehen. Zudem weichen die Auffassungen über die Relevanz und Abgrenzung bestimmter Lebenswelten in verschiedenen Ländern stark voneinander ab. Aus Sicht von Bürgern ist damit die Einteilung der Lebenswelten nicht immer trennscharf und für alle Milieus gleichermaßen umsetzbar, da je nach Kontext, sozio-ökonomischen und kulturellen Unterschieden Lebenswelten sehr differenziert wahrgenommen werden. Es ist allerdings zweckmäßig, den Lebenswelten einen geeigneten Rahmen zu geben und zentrale Lebenswelten voneinander abzugrenzen, um in theoretischen Rahmenbedingungen arbeiten zu können, aber auch um in der Praxis gesamtheitlich nach Lösungen bestimmter Probleme suchen zu können. Generell stellt sich die Frage, ob sich für die Einordnung von Lebenswelten ein allgemeingültiges Schema aufstellen lässt oder diese nur in einem bestimmten Kontext zu sehen sind, in dem sie interpretiert werden können. Dies wird unterschiedlich

gehandhabt. Beispielsweise unterteilt die Gesellschaft für Konsum-, Markt- und Absatzforschung e. V. die für die Marktforschung relevanten Lebenswelten zum einen in eine biografische, um die persönliche Lebensumwelt einer Person zu erfassen, und zum anderen in eine familiäre Lebenswelt, um auch private Haushalte einzuschließen. Lebenswelten lassen sich dann feiner nach Erwerbssituation, kulturellem Kontext, demografischen Faktoren (insbesondere Alter), monetären oder sozialen Rahmenbedingungen sowie familiären Strukturen und Verhaltensweisen differenzieren (Corthier et al. 2011, S. 5).

Für die vorliegende Arbeit wurde den Lebenswelten ebenfalls ein vorgegebener Rahmen gesetzt. Der Fokus lag dabei allerdings weniger auf persönlichen, individuellen Umständen, unter denen die Menschen leben. Stattdessen wurde schwerpunktmäßig auf Lebensbereiche abgestellt, in denen sich die Menschen bewegen, mit denen sie sich beschäftigen und die sie für sich gestalten wollen. Das ist z. B. die Wohnung, in der sich der Bürger privat aufhält und zu Hause fühlt, und die mit der ‚Lebenswelt Wohnen‘ abgedeckt wird. Ein zentrales Thema für die meisten Menschen ist das körperliche, geistige und seelische Wohlbefinden, mit dem die ‚Lebenswelt Gesundheit‘ angesprochen ist. Die Möglichkeiten, sich räumlich von A nach B zu bewegen, führen die ‚Lebenswelt Mobilität‘ zusammen. Interessen und Aktivitäten im beruflichen Umfeld bilden die Lebenswelt Arbeit, das Zusammenleben in der häuslichen Gemeinschaft die Lebenswelt Familie usw. Zentrale Lebenswelten, die für gewöhnlich hohe Relevanz für die meisten Menschen besitzen, sind ohne Anspruch auf Vollständigkeit, trennscharfe Strukturierung und Priorisierung (da diese letztlich subjektiv geprägt, s. o.) z. B. folgende:

1. Wohnen
2. Gesundheit
3. Mobilität
4. Arbeit
5. Familie
6. Freizeit
7. Sport
8. Urlaub
9. Kommunikation
10. Recht
11. Finanzen
12. Altersvorsorge

Innerhalb einer Lebenswelt kann weiter differenziert werden. In Freizeit und Sport (die sich vielfach überlappen) können etwa die Lebenswelten des Fußballs und des Motorrads unterschieden werden. Unter den Motorradfahrern grenzen sich viele Harley Davidson-Fahrer vermutlich mit dem Empfinden einer eigenen Lebenswelt ab. Zugleich verschwimmen Lebenswelten, wenn z. B. Arbeit und Freizeit räumlich und zeitlich nicht mehr strikt getrennt werden. Die Orientierung, in der eine Lebenswelt wahrgenommen wird, ist also ebenfalls ein wichtiger Faktor, um die richtigen Schlüsse zu ziehen.

Aus den übergeordneten Lebenswelten stechen Wohnen, Gesundheit und Mobilität aus dem Grund besonders hervor, weil der Bürger mit ihnen permanent konfrontiert wird. Zudem betreffen diese Lebenswelten nicht nur einzelne Gruppen, sondern jeder Bürger ist von ihnen betroffen. Darüber hinaus stehen die Lebenswelten Wohnen und Gesundheit für sehr persönliche Themen und müssen daher – gerade im Hinblick auf die Nutzung von Daten – besonders sensibel gehandhabt werden. Auch die Mobilität ist sensibel, soweit aus entsprechenden Daten Bewegungsprofile abgeleitet werden können. In der vorliegenden Arbeit, die das Spannungsfeld zwischen ‚Datennutzung‘ und ‚Datenschutz‘ beleuchtet, werden daher Smart Services und verschiedene Geschäftsmodelle in gerade diesen drei Lebenswelten exemplarisch analysiert.

Da es in den drei Lebenswelten Wohnen, Gesundheit und Mobilität Überschneidungen gibt, sind nicht alle für eine Lebenswelt vorgenommenen Analysen trennscharf zu denen einer anderen Lebenswelt. So sind beispielsweise smarte Assistenz-systeme für immobile Personen sowohl der Lebenswelt Wohnen als auch Gesundheit zuzuordnen.

2.1.3 Big Data und Data Analytics in den Lebenswelten

2.1.3.1 Big Data

‚Big Data‘ steht für die Verfügbarkeit großer digitaler Datenmengen und deren technologische Auswertungsmöglichkeiten. Der Trend zu ‚Big Data‘ wird durch die zunehmenden Speicherkapazitäten und die steigende Verarbeitungsgeschwindigkeit neuer Computertechnologien getrieben und beschleunigt. Zur Charakterisierung von ‚Big Data‘ können vier Dimensionen von Kriterien herangezogen werden: *Volume*, *Velocity*, *Variety* und *Value* (IBM 2019).

Volume beschreibt ‚Big Data‘ mit der verfügbaren Datenmenge und der Maßgröße ‚Byte‘. Die jährlich generierte Datenmenge wird vor allem in den nächsten Jahren rasant wachsen. Wurden 2016 16,1 ZetaByte¹ an digitalen Daten weltweit generiert, soll sich diese Zahl bis zum Jahr 2025 verzehnfachen (siehe hierzu Statista 2019). Das Kriterium *Velocity* steht für die Geschwindigkeit der Datenerzeugung und Verarbeitung.

Die Datenvielfalt ist Gegenstand des Kriteriums *Variety*. Damit sind nicht lediglich unterschiedliche Dateiformate (z. B. Bilder, E-Mails, PDF, Word-Dateien, Videos etc.) gemeint, sondern auch ihr Strukturierungsgrad. Daten sind unstrukturiert, wenn sie keiner formalisierten Ordnung entsprechen. Dies ist i. d. R. bei Bildern und E-Mails der Fall. Semistrukturierte Daten weisen entweder keine fest typisierte, sondern lediglich eine versteckte Struktur auf oder sind insgesamt unterschiedlich strukturiert. Mit der Struktur sind neben den Dateiformaten, die mit der Unternehmensdatenbank kompatibel sein müssen, auch die Strukturen des Feldtypen gemeint, die eine Datei in einer Datenbank näher beschreibt (Deutsches Institut für Vertrauen und Sicherheit im Internet 2016, S. 26). Eine weitere Einteilung differenziert in statische und dynamische Daten. Statische Daten werden einmal erfasst und liegen dann unverändert vor.

Dagegen lassen sich die Merkmale von dynamischen Daten verändern und neue Informationen hinzufügen (Denkena et al. 2017, S. 299). Nach den Bezugsgrößen können Personendaten, Objektdaten und Prozessdaten unterteilt werden.² Je nach Datentyp lassen sich Datenanalysen zur Generierung mehrwertiger Informationen mehr oder weniger effektiv und effizient umsetzen (Sobe 2018, S. 6). Die Investitionen von Unternehmen in Informationstechnologien zur Speicherung und Verarbeitung von ‚Big Data‘ sollen sich selbst-verständlich amortisieren und den Unternehmenswert steigern. Anders ist die Sammlung, Speicherung und Auswertung von ‚Big Data‘ aus unternehmerischen Gesichtspunkten nicht sinnvoll. Diese Zielsetzung ist im Kriterium *Value* enthalten (Fasel/Maier 2016, S. 6).

Für die folgende Arbeit sind insbesondere maschinelle Daten relevant, die digitale Informationen enthalten. Erzeugt werden die Maschinendaten von immobilien oder mobilen und möglichst vernetzten Endgeräten, Computern und eingebetteten Systemen (Roussem 2017).

¹1 Zetabyte entspricht ca. 10²¹ Byte.

²Eine ähnliche Unterteilung, die allerdings Schnittmengen aufweist, differenziert Personendaten, Haushaltsdaten, Gebäudedaten, Objektdaten, Gewerbedaten und Device-Daten (Beenken et al. 2018).

2.1.3.2 Data Analytics in den Lebenswelten

Data Analytics bezeichnet Verfahren, bei denen Daten aus verschiedenen Datenquellen extrahiert und auf bestimmte Fragestellungen hin untersucht werden. Dabei sollen Schlussfolgerungen gezogen werden, die in einem bestimmten Zusammenhang zu den analysierten Daten stehen. Häufig taucht Data Analytics im Zusammenhang mit Data Mining auf. Beim Data Mining geht es darum, neue und noch unbekannte Zusammenhänge aus Daten herzustellen (Bardmann 2019, S. 579).

Durch die Datenerhebung und -auswertung können und sollen Mehrwerte für die Bürger in ihren Lebenswelten entstehen. Dafür werden im Rahmen der Datenanalyse zunächst Einstellungen, Verhaltensweisen und sonstige Merkmale der Bürger erfasst, um daraus ihre Bedürfnisse abzuleiten. Auf Basis der Erkenntnisse sollen Angebote ermöglicht werden, mit denen diese Bedürfnisse erfüllbar sind – und dies immer individueller. Zudem soll mithilfe von Data Analytics die Zukunft vorhersehbarer werden. Beispielsweise können zugunsten der ‚Lebenswelt Gesundheit‘ nicht nur bereits eingetretenen Krankheiten frühzeitig erkannt und schneller und damit erfolgreicher therapiert werden, sondern es eröffnen sich auch Möglichkeiten, drohende Krankheiten aufzudecken, um sie mit präventiven Maßnahmen noch abzuwenden.³

Generell bieten Data Analytics auch in der Forschung und Entwicklung über nahezu alle Wissenschaftsdisziplinen hinweg Potenziale zur Verbesserung der Lebensqualität. Big Data und deren Analyse haben damit die Wirkungsfähigkeit, die Lebenssituation jedes einzelnen Bürgers zu verbessern. Allerdings sind gleichzeitig die Risiken, vor allem durch fehlende Datensicherheit, nicht zu unterschätzen. Besonders die ausdrücklich vom Bürger nicht gewollte Verwendung von persönlichen Daten durch Dritte muss reguliert werden. So ist möglichst zu verhindern, dass Daten ohne Einverständnis der betroffenen Personen erfasst, individuell ausgewertet und für Eigeninteressen von Unternehmen oder beispielsweise zur politischen Beeinflussung der Bürger verwendet werden.

³Mithilfe der Apple Watch und damit erhobener Vitaldaten ihrer Träger ist es amerikanischen Forschern bereits gelungen, unter Nutzung von Data Analytics und Backtesting-Verfahren typische Muster zu erkennen, die Patienten mit Herzvorhof-Flimmern bereits vor Eintritt der Krankheit aufwiesen. Umgekehrt soll es damit schon heute möglich sein, mit den entsprechenden Mustererkennungen von Echtzeitdaten mit einer Treffsicherheit von über 95 % vorherzusagen, dass ein bestimmter Träger der Apple-Watch unter sonst gleichbleibenden Umständen in Zukunft Herzvorhof-Flimmern erleiden wird. Mit geeigneten Präventivmaßnahmen kann dies aber häufig noch verhindert werden.

Um möglichst viele Chancen für mehrwertige Erkenntnisse zu schaffen, ist es hilfreich, Daten unbegrenzt sammeln und auswerten zu können. Oft ergeben sich die Anwendungsfelder erst nach Mustererkennungen in Big Data, die mithilfe von Data Analytics hervorgebracht wurden und an die zuvor überhaupt nicht gedacht worden war. Eine getrennte Erhebung der Daten, beispielsweise nach Lebenswelten, ist von daher gar nicht zweckmäßig. Die größten Chancen bieten Datenpools über die Grenzen der verschiedenen Datentypen und Lebenswelten hinweg. Allerdings sieht der Datenschutz – verständlicherweise – gerade diese Form der Datenerhebung und Datenauswertung als besonders problematisch an. Insbesondere die EU-DSGVO mit den Erfordernissen der Datenminimierung⁴ gem. Art. 5 Abs. 1 c EU-DSGVO, Speicherbegrenzung⁵ gem. Art. 5 Abs. 1 e EU-DSGVO und Zweckbindung⁶ gem. Art. 5 Abs. 1 b EU-DSGVO beschränken die faktischen Einsatzmöglichkeiten von Big Data und Data Analytics. Mangels bislang klar abgesteckter Regelungen besteht die Herausforderung in der Praxis derzeit schon allein darin, den rechtlich zulässigen Spielraum für die Nutzung von verfügbaren Daten und deren Analyse auszuloten.

2.1.4 Smart Services und Geschäftsmodellentwicklungen in zentralen Lebenswelten

Smart Services verknüpfen Produkte, Dienstleistungen und Prozesse, die dem Kunden als individualisiertes Gesamtangebot und ‚as a service‘ zur Verfügung stehen (Acatech 2018). Damit sind Smart Services intelligente, digitalisierte Angebote, die durch die Erhebung, Bündelung und Auswertung gesammelter Daten ermöglicht werden. Gebündelt und ausgewertet werden die Daten meist auf digitalen Plattformen, die ortsunabhängig einen übergreifenden Zugang zu den Informationen gewähren und auf denen Anbieter und Nachfrager zusammenkommen (Arbeitskreis Smart Services Welt 2015, S. 21 f.). Durch den datenzentrierten Plattform-Ansatz wird zudem das Andocken weiterer Dienste

⁴Die erhobenen Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

⁵Die Identifizierung der jeweiligen Person darf nur so lange möglich sein, wie es für den Zweck der Datenerhebung notwendig ist.

⁶Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

ermöglicht, die aufgrund der intelligenten Datenanalyse individualisiert und damit auf die Situation und den Bedarf des Kunden angepasst werden können.

Im Mittelpunkt der Smart Services steht der Bürger mit seinen Wünschen und Bedürfnissen, die oftmals nicht durch einzelne Anbieter und deren Produkte erfüllt werden können. Zentral für nutzenstiftende Angebote in den Lebenswelten der Bürger ist daher der ganzheitliche Ansatz digitaler Ökosysteme, das sind branchenübergreifende Netzwerke von digital miteinander verbundenen Produktherstellern und Dienstleistern, die gemeinsam Smart Services generieren (Bundesministerium für Wirtschaft und Energie 2017a, S. 4). Der Plattformansatz liefert hierfür die notwendige Infrastruktur und ermöglicht die Kooperationen und vernetzten Systeme. Voraussetzungen für jede Teilnahme als Zulieferer in einem solchen Netzwerk sind standardisierte, schlanke Prozesse, die Bildung von fachlichen und technischen Schnittstellen zu den Ökosystempartnern und letztlich die Akzeptanz der eigenen Austauschbarkeit, weil sich die Netzwerke der Zukunft vermutlich nicht von den Leistungen und Effizienzpositionen bestimmter Zulieferer abhängig machen wollen. Beispiele für Smart Services, die die Bürger in ihren jeweiligen Lebenswelten unterstützen, sind die innovativen datengetriebenen Angebote rund um Smart Home (Lebenswelt Wohnen), Smart Health (Lebenswelt Gesundheit) und Connected Mobility (Lebenswelt Mobilität).

Im Rahmen der Verwertung solcher Smart Services auf Märkten entstehen zunehmend neue **Geschäftsmodelle**. Dabei ist ein Geschäftsmodell als ein Konzept unternehmerischen Handelns zu verstehen, nach dem mit einem Angebot Mehrwerte für den Kunden und ein Gewinn für den Anbieter realisiert werden können (Grösser 2018). Gegenüber analogen Geschäftsmodellen zeichnen sich digitale Geschäftsmodelle durch eine schnelle Bereitstellung von Lösungen und eine deutlich gesteigerte Umsetzungsgeschwindigkeit aus (Bundesministerium für Wirtschaft und Energie 2017b, S. 18). Das heißt, dass auch Änderungen dem Kunden zeitnah bereitstehen. Als Rückkopplung bieten der einfache Kundenzugang und verbesserte Kundeninformationen wertvolles Potenzial für neue Smart Services. Geschäftsmodelle werden durch die Digitalisierung immer stärker skalierbar und sind dynamisch anpassungsfähig (Seiberth und Gründinger 2018, S. 8). Parallel steigt auch die Geschwindigkeit der Generierung neuer nutzenstiftender Produkte und immer kundenfreundlicherer Prozesse, was wiederum den Wettbewerb erhöht und die Kundenansprüche anwachsen lässt. Die Erwartungen der Kunden an individuelle Lösungen für ihre Wünsche (für die wiederum eine geeignete Datenbasis erforderlich ist) und an eine attraktive ‚Customer Journey‘ passen sich also den Entwicklungen an und erhöhen ihrerseits zunehmend den Entwicklungsdruck. Am Rande sei hier auf das Paradoxon hingewiesen, dass die Kunden immer stärker individualisierte Angebote bekommen

und erwarten, wofür einerseits die Preisgabe und Nutzung von Daten erforderlich ist, andererseits aber der Datenschutz ein hohes gesellschaftliches Gewicht hat und von den Kunden ebenfalls erwartet wird.

Zurück zu den Geschäftsmodellen: Eine gute Methode, um Geschäftsmodelle zu analysieren, bietet das Businessmodell Canvas. Das Business Model Canvas ist ein vom Schweizer Alexander Osterwalder entwickeltes Konzept, das zur Visualisierung und Strukturierung von Geschäftsmodellen dient. Durch den einfachen grafischen Aufbau dient es als Werkzeug, die wesentlichen Charakteristika von Geschäftsmodellen darzustellen. Es kann insbesondere dazu genutzt werden, innovative Geschäftsmodelle zu beschreiben (Osterwalder und Pigneur 2010). Der Vorteil des Business Model Canvas liegt darin, dass es universell einsetzbar und damit nicht auf einzelne Branchen oder Geschäftsbereiche beschränkt ist.

Zur Erfassung und Darstellung eines Geschäftsmodells zieht das Business Model Canvas neun Kernelemente heran (siehe Tab. 2.1), deren Ausprägungen und Wechselwirkungen das Geschäftsmodell charakterisieren.

Im Mittelpunkt des Business Model Canvas steht das zentrale **Wertangebot** an die Kunden. Es beantwortet die Frage, auf welchen Produkten und Services das Geschäftsmodell basiert, um zum einen die Wünsche und Bedürfnisse der Kunden zu befriedigen und sich auf der anderen Seite vom Wettbewerb abzuheben. Aufbauend auf dem Wertangebot werden dazu passende **Kunden-segmente** angesprochen, die sich insbesondere in Endkunden (B2C) und Firmenkunden (B2B) unterscheiden. Darunter können jeweils auch spezielle, weiter differenzierte Kundengruppen adressiert werden. In Abhängigkeit von den Zielkunden sind die **Kanäle** zu wählen, die für die Kommunikation mit den Kunden und zum Absatz der Leistungen dienen. Auf deren Basis wird die **Kunden-beziehung** ausgestaltet, die persönlich oder automatisiert gestaltet sein kann. Da das Geschäftsmodell oftmals nicht alleine vollständig umgesetzt werden kann, ist die Zusammenarbeit mit **Schlüsselpartnern**, wie Lieferanten oder anderen Dienstleistern, notwendig. Mit dem Absatz der Leistungen entstehen **Einnahme-quellen**, die wiederum je nach Produkt und Service verschiedenartig sind. Die **Kostenstruktur** ist außer durch die Partnerbeziehungen und deren Einnahmeerwartungen insbesondere durch die eigenen **Schlüsselaktivitäten** und die dafür benötigten **Schlüsselressourcen** geprägt, zu denen bspw. Personal, Sachmittel und eine Datenbasis gehören. Gerade die Datenbasis ist bei den innovativen digitalen Geschäftsmodellen meistens die zentrale Ressource für die Wertangebote gegenüber den Kunden.

Die nachfolgend diskutierten Geschäftsmodelle rund um die Lebenswelten Wohnen, Gesundheit und Mobilität werden nach einer jeweils grundlegenden

Tab. 2.1 Business Model Canvas

| | | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <p>Schlüsselpartner Netzwerk von Partnern & Lieferanten Strategische Allianzen/Joint Ventures/ Käufer-Anbieter-Beziehungen</p> | <p>Schlüsselaktivitäten wichtigste Handlungen eines Unternehmens Schaffen & Unterbreiten des Wertangebot/erreichen die Märkte/Aufbau & Pflege der Kundenbeziehungen</p> | <p>Wertangebote Paket von Nutzen, das ein Unternehmen seinen Kunden anbietet verschiedene Produkte & Dienstleistungen qualitativer oder quantitativer Natur Neuheiten/ Leistungsoptimierung/Marke/Design/ Arbeitserleichterung</p> | <p>Kundenbeziehungen Arten von Beziehungen persönliche Unterstützung/ Selbstbedienung/ automatisierte Dienstleistungen/ Communities/Mitbeteiligung</p> | <p>Kundensegmente Segmentierung nach Bedürfnissen/ Verhaltensweisen/ Merkmale/Finanzkraft/bevorzugte Kanäle/etc</p> |
| <p>Kostenstruktur Fixkosten & variable Kosten die zwei Extreme: kostenorientierte & wertorientierte Geschäftsmodelle</p> | <p>Schlüsselressourcen können physischer, finanzieller, intellektueller, menschlicher Natur sein</p> | <p>Kanäle Kundenberührungspunkte alle Kommunikations- & Verkaufskanäle</p> | | |
| | | <p>Einnahmequellen aus Verkauf von Wirtschaftsgütern/Nutzungsgebühren/Mitgliedsbeiträgen/Verleih, Vermietung, Leasing/Lizenzen, Maklergebühren/Werbung</p> | | |

Beschreibung anhand des Business Models Canvas näher analysiert. Auch dabei wird sich zeigen, dass alle diese Geschäftsmodelle als Schlüsselressource auf eine digitale Datenbasis setzen, die für die zentralen Wertangebote benötigt wird.

2.2 Lebenswelt Wohnen

2.2.1 Smart Services im Überblick

Die Lebenswelt Wohnen umfasst alle Verhältnisse und Aktivitäten innerhalb des häuslichen Umfelds von Bürgern. Darin inbegriffen sind damit die Beschaffenheit (Dach, Fenster etc.), die Ausstattung (Möbel, Haushaltsgeräte etc.) von Haus bzw. Wohnung sowie dessen/deren unmittelbares Umfeld (Garage, Garten etc.). Der Lebenswelt Wohnen können darüber hinaus alle Tätigkeiten zugeordnet werden, die typischer- oder notwendigerweise im Haus oder in der Wohnung durchgeführt werden (bspw. kochen, waschen, bügeln, schlafen, ...). Damit ergibt sich eine Reihe von Anknüpfungspunkten für die Bereitstellung von Smart Services, die im Wohnumfeld zur Steigerung der Lebensqualität eingesetzt werden können (Bundesministerium für Wirtschaft und Energie 2014, S. 13). Ein übergeordneter Begriff für unterschiedliche digitalisierte Angebote in der Lebenswelt Wohnen ist ‚Smart Home‘, also die intelligente Vernetzung des eigenen Zuhauses. Dabei gibt es unterschiedliche Entwicklungsstufen, wobei nicht eindeutig definiert ist, ab wann es sich um ein Smart Home handelt. In der letzten Entwicklungsstufe sind alle Geräte, Gegenstände, Materialien etc. miteinander vernetzt, sammeln Daten, werten sie aus und nutzen diese selbstständig mittels Künstlicher Intelligenz zur Optimierung der Wohnumgebung. Durch die intelligente Vernetzung und Auswertung der Daten können zudem Mehrwerte für die Bewohner entwickelt werden. Im Mittelpunkt der Bedürfnisse der Bewohner stehen dabei.

1. die Erhöhung von Lebensqualität durch mehr Komfort,
2. eine erhöhte Sicherheit innerhalb des Hauses sowie der Schutz nach außen und
3. eine möglichst hohe Effizienz bei der Nutzung eingesetzter Ressourcen (Bendel 2018a).

In diese drei Bedürfniskategorien lassen sich auch die Smart Services kategorisieren, wobei eine trennscharfe Abgrenzung nicht immer möglich ist und der größte Mehrwert in der Verknüpfung der verschiedenen Mehrwerte und damit in der Befriedigung aller drei Bedürfniskategorien liegt.

Smart Services im Bereich **Komfort** sollen den Bewohner von Alltagsaufgaben entlasten, das Leben in der Wohnung oder im Haus einfacher machen und eine komfortable und gemütliche Wohnatmosphäre schaffen. Anknüpfungspunkte sind z. B. die Regulierung von Luft, Licht und Temperatur, des Zutritts zur Wohnung, der Fensteröffnungen sowie die bequeme, ggf. auch automatisierte Steuerung verschiedener Komponenten und Gegenstände. So ist bei vielen Beleuchtungssystemen mittlerweile eine per App steuerbare Veränderung der Helligkeit und der Lichtfarbe möglich, inkl. des An- und Abschaltens des Lichts aus der Ferne. Ein weiteres Beispiel ist die intelligente Steuerung der Heizung, wie sie mittlerweile von einer ganzen Reihe von Herstellern angeboten wird. Dabei kann die Raumtemperatur wiederum entweder manuell per App oder Sprachsteuerung geregelt werden, oder aber die Einstellung erfolgt automatisiert, indem Daten per Funk, über Wandsensoren, durch Geofencing oder mittels Einsatzes einer Künstlichen Intelligenz weitergeleitet und für die Steuerung eingesetzt werden. Das Geofencing sammelt Standort- und Bewegungsdaten über GPS und erkennt, wenn die Bewohner zu Hause sind und wo sie sich aufhalten; demnach wird die Temperatur in den entsprechenden Heizzonen angepasst. Verlassen die Bewohner das Haus, wird die Temperatur automatisch abgesenkt. Befinden sie sich auf dem Heimweg, springen die Thermostate an und adjustieren die Heizung (Innogy 2017). Dabei kann zusätzlich über eine App oder andere Steuerungsmechanismen nachgeregelt werden. Wird zudem eine Künstliche Intelligenz verwendet, können Daten über die Gewohnheiten der Bewohner gesammelt und die Temperaturregelung selbstlernend angepasst werden. Ergänzend können auch weitere Sensoren zum Einsatz kommen, die zu hohe Luftfeuchtigkeit registrieren und z. B. mit einem Schimmelwarnungssystem ausgestattet sind.

Wie sich zeigt, erhöht diese den Komfort adressierende Lösung zudem die **Ressourceneffizienz**, indem die Energienutzung optimiert und z. B. vermieden wird, dass die Heizung im Fall einer längeren Abwesenheit der Bewohner unnötig viel Öl, Gas oder Strom verbraucht. Durch die Vernetzung und den Datenaustausch mit Fenster- und Türsensoren kann zudem ein Energieverlust beim Lüften verhindert werden. Darüber hinaus können zahlreiche weitere Daten gesammelt werden, die wertvolle Informationen über den Energieverbrauch bieten und Verbesserungspotenziale aufzeigen. Insbesondere sog. ‚Smart Meter‘ (intelligente Zähler) können den Bewohnern in einem Smart Home entsprechende Mehrwerte schaffen. So wird etwa ein intelligenter Stromzähler mit den verschiedenen Geräten, die an das Stromnetz angeschlossen sind, vernetzt und über ein Gateway zur Datenübertragung dazu befähigt, alle Verbrauchsdaten nicht nur gesamthaft, sondern auch differenziert nach den Einzelgeräten auszulesen und zu analysieren.

Der Nutzer erhält sodann über seine Smart-Home-App ausgewertete und visuell aufbereitete Informationen über seinen Stromverbrauch. Ähnlich differenziert kann über Smart Meter auch der Öl-, Gas- und Wasserverbrauch analysiert werden. Im Ergebnis lassen sich verbrauchsintensive Einrichtungen wie bspw. wiederum die Heizung oder eine Bewässerungsanlage im Garten optimiert steuern. Auch die automatische Deaktivierung von Elektronikgeräten in den Stand-by-Modus hilft, Betriebskosten zu senken und kommt damit überdies dem ökologischen Umgang mit Energieressourcen entgegen.

Ein weiterer Smart Service entsteht durch die Nutzung von Fotovoltaik-Anlagen: Der Nutzer wird über den aktuellen Stand der Stromerzeugung seiner Anlage informiert. Wird bei entsprechendem Wetter gerade ausreichend Strom produziert, kann er z. B. ad hoc kostengünstig seine Wäsche waschen (Strom Magazin 2018). Dieses Konzept verfolgt beispielsweise der Smart Meter-Hersteller Discovery über die Kooperation mit der Smart Home-App iHaus: Ein Ampelsystem zeigt dem Kunden auf dem Smartphone an, wann Strom besonders günstig bereitsteht. Außerdem kann der Nutzer ‚Wenn-dann-Regeln‘ aufstellen. Damit steuert er seine Geräte über ihre Beziehungen untereinander. Beispielsweise wird zunächst das Elektroauto bis zur gewünschten Kapazität aufgeladen und der Geschirrspüler nur dann gestartet, sollte noch genügend günstige Energie verfügbar sein (Discovery 2018). Gleichmaßen kann das vernetzte Smart Home an den Energieversorger zum Datenaustausch angebunden werden. Dadurch können Energieflüsse besser prognostiziert und die Versorgungssicherheit gesteigert werden.

Im Bereich der **Sicherheit** decken Smart Services vorrangig den Einbruchschutz und die haus- bzw. wohnungsinterne Schadensprävention ab. Neben kamerabasierten Zugangskontrollen und Überwachungssystemen innerhalb und außerhalb des Wohnraums sind es WLAN-Schlösser, die sich per App öffnen und schließen lassen, sowie Alarmsysteme, die mit direkten Dienstleistungen gekoppelt sind. Auch die oben beschriebenen Lichtsysteme lassen sich zum Schutz vor Einbrechern einsetzen. Dies kann insbesondere durch sog. Anwesenheitssimulatoren geschehen, die das Verhalten der Bewohner erlernen und bei deren Abwesenheit das Licht analog der üblichen Gewohnheiten steuern.

Ein Anwendungssystem für Smart Services im Bereich der Schadenprävention sind sensorbasierte Angebote zur frühzeitigen Aufdeckung von Wasserschäden. So können Sensoren in den Wohnräumen installiert werden, die ungewöhnliche Nässe melden und durch ein Abschalten der Wasserversorgung vor Durchfeuchtung oder Überschwemmung schützen. Zudem bietet bspw. Grohe ein System an, das bereits in den Wasserrohren Mikroleckagen erkennt und so frühzeitige Präventionsmaßnahmen ermöglicht (Grohe 2018).

Neben klassischen Smart Home-Anwendungen, die im privaten Wohnraum allen möglichen Nutzern zugutekommen, können auch intelligente Assistenzsysteme (Ambient Assisted Living) zu den Smart Services in der Lebenswelt Wohnen gezählt werden, die insbesondere für Senioren und pflegebedürftige Menschen entwickelt wurden. Dabei geht es um Anwendungen, die diese Zielgruppen im Haushalt unterstützen und ein selbstbestimmtes Leben im gewohnten und vertrauten Umfeld gewährleisten sollen (SmartHome Initiative Deutschland und mm1 o. J., S. 5 f.). Die Angebote reichen dabei von Notrufmelde-systemen über elektronische Gesundheitsdienste bis hin zu Pflegerobotern. Der Übergang zur Lebenswelt Gesundheit ist an dieser Stelle fließend (Siepermann 2018).

Eine wichtige technologische Entwicklung, die in vielen Lebenswelten Anwendung findet, ist die Sprachsteuerung: Im Bereich Wohnen sind es Sprachassistenten wie Google Home und Amazon Alexa, die die Bedienbarkeit des vernetzten Zuhauses erleichtern und für den Nutzer komfortabler gestalten. Allerdings ist es in den meisten Fällen weiterhin erforderlich, dass Anweisungen und Vorgaben durch den Menschen vorgenommen werden. Die zukünftigen Entwicklungen im Smart Home-Bereich forcieren jedoch zunehmend die eigenständige Kommunikation der Komponenten untereinander, sodass sich das Smart Home eigenständig und automatisiert steuert und menschliches Zutun nicht mehr erforderlich ist. Dazu ist es notwendig, Daten aller Geräte und Komponenten kontinuierlich zu sammeln und über eine gemeinsame Plattform geeigneten Anwendungsdiensten zur Verfügung zu stellen. Nur so kann eine intelligente Regulierung z. B. der Heizungswärme oder des Einsatzes der Waschmaschine mit Strom aus der Fotovoltaikanlage automatisiert auf Basis vorhandener Wetterdaten erfolgen. Ziel ist es, dass die smarten Systeme aus vergangenen Ereignissen lernen und entsprechende Handlungsweisen daraus selbstständig ableiten – und nach und nach optimieren. Bereits heute können regelmäßig wiederkehrende Aktionen einzelner Einrichtungen im Haushalt automatisiert gesteuert werden (z. B. zentrale Heizungsanlagen mit Zeitschaltuhren oder Temperaturfühlern). Jedoch ist es aktuell noch nicht möglich, verkettete Systeme ereignisbasiert handeln zu lassen, da nach aktuellem Stand die Datenquellen und Geräte bzw. Einrichtungen noch nicht ausreichend miteinander verknüpft sind. Zudem existieren bislang noch kaum hinreichend intelligente Dienste, um die Daten entsprechend auszuwerten und daraus Handlungsweisen ableiten zu können.

Im Folgenden werden zwei bereits real existierende Geschäftsmodelle beschrieben, die sich in Smart Services rund um die Lebenswelt Wohnen eingliedern. Dabei steht der Nutzen der Daten im Vordergrund, auf deren Basis Wertangebote für die Bewohner in einem ‚Smart Home‘ erzeugt werden.

2.2.2 Ausgewählte Geschäftsmodelle innerhalb der Smart Services

2.2.2.1 Amazon Key

1. Beschreibung des Geschäftsmodells

Mit dem Service „Amazon Key“ bietet Amazon ein schlüsselloses Zugangssystem zu Wohnungen/Häusern an, durch das der Nutzer dritten Personen aus der Ferne die eigenen Räumlichkeiten öffnen kann. Damit kann zum einen der Zutritt für Familienangehörige und Freunde, zum anderen das Erbringen von Dienstleistungen in den Räumlichkeiten der Nutzer ohne deren Anwesenheit ermöglicht werden (Heise online 2017). Für diesen Zweck wird die Haustür mit einem smarten Türriegel versehen, der sich mittels der zugehörigen Amazon Key-App programmieren lässt. Zusätzlich enthält das Angebot eine ebenfalls per App steuerbare Überwachungskamera, mithilfe derer der Eingangsbereich bei jeder Türöffnung aufgezeichnet wird. So kann der Nutzer z. B. der Haushaltshilfe, dem Dogsitter oder einem Handwerker temporären Zugang zu seinem Wohnraum verschaffen. Über die Amazon-Key-App stellt der Nutzer der entsprechenden Person einen Code zur Verfügung, mit dem die Tür innerhalb eines bestimmten Zeitraums geöffnet werden kann. Wenn der Zugang erfolgt, bekommt der Hausbewohner eine Benachrichtigung auf sein Handy. Eine Kontrolle ist dann durch Einsicht in die Aufzeichnung des Eingangsbereichs ohne Weiteres möglich.

Amazon selbst schafft sich mit Amazon Key die Voraussetzungen und die Möglichkeit einer ‚in-home‘-Paketlieferung, die Amazon-Prime-Kunden exklusiv angeboten wird. Der Paketbote erhält dafür bei Auslieferung eine Authentifizierung, kann hiermit das smarte Türschloss öffnen und das Paket in der Wohnung des Nutzers abstellen. Der Nutzer kann mit diesem Service nicht mehr nur den Lieferstand ‚tracken‘, sondern sich zudem die Lieferung selbst über das aufgezeichnete Video ansehen (Amazon 2018).

Die erhobenen Daten rund um Amazon Key umfassen Verhaltens- inkl. Konsuminformationen über die Bewohner, indem übermittelt wird, wann der Nutzer zu Hause ist, wann er Besuch empfängt und welche Produkte und Dienstleistungen er bei welchen Anbietern in Anspruch nimmt. Basierend darauf lassen sich weitere Mehrwertdienste anbieten, die sich in das Angebot von Amazon Key integrieren lassen. Daneben werden Videodaten der Überwachungskamera gesammelt, die bei Amazon gespeichert werden, um dem Nutzer bei Bedarf zur Verfügung zu stehen.

Überdies kann Amazon Key ein massives Kostenproblem für Paketzustelldienste lösen, denen Mehrfachanfahrten oder Zusatzwege zu alternativen

Lieferungsorten erspart werden. Alternativ kommt es in der Realität immer wieder vor, dass Pakete bei Abwesenheit der Bewohner von den Zustellern einfach vor die Tür gestellt werden und dann abhandenkommen. Auch das wird durch Amazon Key verhindert – und erhöht die Sicherheit des Paketerhalts bzw. vermeidet Verlustschäden. Indem die Türöffnungsfunktion auch für andere Zusteller jenseits von Amazon-Lieferanten nutzbar werden soll, erhält Amazon auch Daten über die Bestellung bei Drittanbietern und über deren Zustellmodalitäten, damit also ggf. auch von Konkurrenten.

Bis auf Weiteres ist Amazon Key eine singuläre Smart Home-Anwendung, ohne Vernetzung mit anderen Funktionen, die zu gesamtheitlichen Lösungen führen könnten. Amazon Key bietet aber wichtige Ansatzpunkte und Informationen auf dem Weg dorthin und kann mit der Möglichkeit zur Verknüpfung der gewonnenen Daten mit weiteren Daten aus der Wohneinheit einen Meilenstein zu einem ganzheitlich vernetzten Smart Home darstellen.

2. Geschäftsmodellanalyse nach dem Business Model Canvas

Das **Wertangebot** von Amazon Key ist die App-basierte Zugangskontrolle für dritte Personen zum eigenen Wohnraum. Dadurch können Dienstleistungen flexibler in Anspruch genommen und Zeiten effizienter genutzt werden. Ziel des Angebots ist es, Familienmitgliedern, Freunden und Nachbarn sowie Dienstleistern jederzeit und aus der Ferne kontrollierten Zugang zu ermöglichen und den Wohnraum während des temporären Zugangs Dritter zu überwachen. Durch die jederzeitige Lieferung der bestellten Ware in den eigenen Wohnbereich kommt es nicht mehr zur Paketzustellung an andere Orte, wie dem Nachbarn oder einem nahegelegenen Shop, sodass dies zu Convenience und Zeitersparnis bei den Kunden führt. Im **Kundensegment** ist Amazon Key auf den B2C-Bereich fokussiert, da das Angebot primär auf den Privathaushalt zugeschnitten ist. Was den Lieferservice betrifft, sind die Zielgruppe in erster Linie Personen mit Affinität zum Onlinehandel (Amazon 2018). Als **Distributionskanal** bedient sich Amazon Key verschiedener Medien wie einer App, der Homepage, dem Telefon und der E-Mail. Die **Kundenbeziehung** ist durch eine hohe Standardisierung und zudem technisch geprägt, da die Anwendung mithilfe der App gesteuert wird. Es gibt zudem kaum einen direkten Kundenkontakt. Bei einer Bestellung im Amazon Store sind die üblichen Self-Service-Optionen integriert, die um die Option der Inhouse-Lieferung erweitert sind. **Einnahmequellen** ergeben sich zunächst aus den einmaligen Gebühren für die Anschaffung von Amazon Key in Höhe von derzeit 212 EUR. Darin enthalten sind neben der für die Nutzung erforderlichen App die Kamera und das smarte Türschloss (Ignor 2018). Da Amazon Key zunächst nur für Prime-Mitglieder verfügbar ist, sind zusätzlich Mitgliedsgebühren mit

dem Angebot verknüpft. Ebenfalls können sich die Kundenzahl im herkömmlichen Online-Handelsgeschäft und die Bestellintensität bei Amazon durch die angebotenen Mehrwerte erhöhen, sodass weitere Einnahmen erschlossen werden.

Die **Schlüsselaktivitäten** zur Umsetzung des Geschäftsmodells liegen in der Bereitstellung der technischen Geräte sowie der App und in den damit geschaffenen Zugangs- und Kontrollfunktionen. Es ist zwingend notwendig, dass das smarte Türschloss und die Kamera einwandfrei arbeiten. Ebenfalls ist die Absicherung gegen mögliche Einbrüche aufgrund digitaler Sicherheitslücken essenziell. Dafür sind ggf. laufende Updates erforderlich, wenn Schwachstellen erkannt werden. Des Weiteren können die erfassten Verhaltens- und Konsumdaten der Bewohner genutzt werden, um über die eigentliche Funktionalität von Amazon Key hinaus weitere Mehrwertleistungen anbieten zu können. Zu den **Schlüsselpartnern** zählen die Hersteller der smarten Türschlösser, bei denen der Nutzer zwischen Schlage, Yale oder Kwikset wählen kann. Ebenfalls sind Paketdienstleister, über die eigene Produkte ausgeliefert werden, Partner. Ergänzend arbeitet Amazon mit ca. 1300 Servicepartnern zusammen, das sind u. a. Hundesitter, Handwerker oder Reinigungsunternehmen (Kapalschinski 2017). **Schlüsselressourcen** sind neben dem smarten Türschloss und der Überwachungskamera vor allem die gesammelten Daten über die Nutzer und deren Anwesenheitsverhalten, Besucher- und Dienstleisterbeziehungen sowie Konsummerkmale. Diese Daten und die damit generierten Informationen ermöglichen es Amazon, das Angebot für die Kunden stetig zu verbessern und immer individueller auszugestalten (Siethoff 2017). Soweit Amazon auch in die interne Lebenswelt Wohnen, bspw. über Alexa, Einblick erhält, ist die Kombination dieser Informationen mit denen aus Amazon Key zentral, um künftig noch umfassendere Offerten kreieren zu können. Damit schließt sich wiederum der Kreis zu möglichen neuen **Wertangeboten**.

2.2.2.2 Ubtech Robotics Lynx

1. Beschreibung des Geschäftsmodells

„Lynx“ ist der Roboter des chinesischen Robotic-Herstellers Ubtech, der seit 2017 auf dem Markt angeboten wird. Der datengesteuerte Roboter ist ca. 40 cm groß, kann über eingebaute Mikrofone und Lautsprecher hören und sprechen und sich selbstständig fortbewegen. Ubtech arbeitet mit Amazon zusammen und verwendet die von Amazon entwickelte Sprachsteuerungsfunktion Alexa. Dadurch kann Lynx automatisch Sprache erkennen und anhand seiner Verständnisfunktion antworten (Wollaston 2017). Zudem ist der Kopf des Roboters mit einer Kamera ausgestattet, die sich mithilfe von Gelenkmotoren drehen, senken und erhöhen lässt und dadurch Bildmaterial aus der Umgebung vollständig erfassen und

aufnehmen kann (Ubtech 2018). In Kombination mit der integrierten Gesichtserkennungsfunktion kann Lynx ausmachen, wer sich in der Wohnung befindet, bekannte Personen mit Namen ansprechen und mit diesen in Interaktion treten. Im Aktivitätsmodus kann der Roboter selbstständig die Kommunikation aufnehmen, er kann aber auch per App dazu aufgefordert werden, mit den Personen seines Umfelds Kontakt aufzunehmen. Dies erfolgt mittels einer Avatar-Funktion, die den Roboter als Übertragungsschnittstelle nutzt und eine Zweizeitkommunikation⁷ ermöglicht. So kann der Anwender des Roboters auch Kontakt mit Personen aufnehmen, die sich im gleichen Raum mit Lynx befinden, ohne dass er selbst anwesend sein muss. Neben der Sprachkommunikation kann auch Bildmaterial ausgetauscht werden. Des Weiteren sind im Brustbereich Infrarotsensoren eingebaut, mittels derer Bewegungsdaten gesammelt und ausgewertet werden können (Ubtech 2018).

Durch die Schnittstelle zur Alexa-Sprachsteuerung lassen sich unterschiedliche Aktivitäten innerhalb des Smart Home steuern. So kann Lynx – ebenso wie Alexa auch – nach Aufforderung die Rollos nach unten fahren, Musik abspielen und Tätigkeiten wie Terminvereinbarungen, Schreiben von E-Mails und Berechnungen von optimalen Verkehrsrouten übernehmen. Ebenfalls ist der Roboter mit einer Künstlichen Intelligenz ausgestattet, durch die er ständig dazulernen und seine Funktionen verbessern kann (Lacace 2017). Außer rein sprachlich kann Lynx auch körperlich mit seinem Umfeld in Interaktion treten. Bspw. kann er im Bereich Ambient Assisted Living (AAL) ältere oder in ihrer Bewegungsfreiheit eingeschränkte Menschen im Alltag unterstützen oder zur Unterhaltung oder für verschiedene Aktivitäten eingesetzt werden. Damit wird Lynx zu einem umfassenden (Smart Home-)Assistenten.

Jenseits der physischen Funktionen kann er auch für geistiges Training, bspw. für an Demenz erkrankte Personen, genutzt werden. Ein wichtiges Anwendungsfeld ist zudem die Unterstützung beim Einbruchschutz und die Erhöhung der Sicherheit zu Hause. So kann sich Lynx eigenständig in festgelegten Bereichen des Hauses bewegen und über die integrierten Infrarotsensoren Bewegungen innerhalb des Hauses erkennen, diese seinem Nutzer melden und sofort Bildmaterial der auffälligen Umgebung übermitteln. Auf diese Weise kann der Roboter als mobile Überwachung der Wohnung eingesetzt werden. Neben der

⁷Zweizeitkommunikation meint die Kommunikation, bei der eine Botschaft nicht nur vom Sender zum Empfänger, sondern ebenso vom Empfänger zum Sender übertragen werden kann (zweiseitige, bilaterale Kommunikation).

Sicherheit dient Lynx vor allem dem Komfort: Er unterstützt seinen Anwender bei einfachen und alltäglichen Aufgaben zu Hause, unterhält ihn und dient als Steuerungszentrale des Smart Home (Business Panorama 2017).

2. Geschäftsmodellanalyse nach dem Business Model Canvas

Das **Wertangebot** von Lynx besteht in der Unterstützung bei verschiedenen Tätigkeiten in der erweiterten Lebenswelt Wohnen: Abläufe im Alltag werden vereinfacht und beschleunigt, es sind Unterhaltungsfunktionen enthalten und im Überwachungsmodus ist eine bewegungs- und videodatenbasierte Überwachung möglich, im Rahmen derer sich der Roboter auch aus der Ferne steuern lässt. Es handelt sich bei Lynx damit um einen smarten Assistenten, der nicht nur das Smart Home steuert, sondern das Leben zu Hause erleichtert. Durch die Kombination von Robotertechnik und digitaler Sprachassistenten-Funktionen wird eine persönliche Schnittstelle zwischen Mensch und Maschine geschaffen. Die Serviceleistungen von Lynx richten sich an das B2C-, aber durchaus auch an das **B2B-Kundensegment**, da Lynx sowohl im privaten Zuhause als auch in sonstigen Umgebungen einsetzbar ist. Im B2B-Bereich kann Lynx bspw. in Altenheimen oder Kindergärten genutzt oder zur Überwachung von Bürogebäuden oder Industrieanlagen eingesetzt werden. Der **Distributionskanal** ist vor allem der Online-Verkauf. Bei Amazon ist Lynx für 800 US\$ bestellbar. Aktuell wird der Roboter nur in den USA verkauft; weitere Länder sollen aber zeitnah folgen. Die zugehörige App ist im Google Playstore und im App Store von Apple kostenfrei erhältlich (Ubtech 2018). Die **Kundenbeziehung** ist vor allem durch die persönliche Interaktion mit Lynx gekennzeichnet. Außerdem kann der Kunde über die App mit dem Hersteller in Verbindung treten. Daneben ist der Kundenservice per E-Mail und Telefon erreichbar. Nicht nur Ubtech, sondern auch Amazon steht mit dem Kunden in enger Beziehung. Alle Daten, die im Zusammenhang mit der Alexa-Nutzung entstehen, laufen über das Rechenzentrum von Amazon und dienen dem Unternehmen als Kundenschnittstelle. Primäre **Einnahmequelle** ist zunächst der (jeweils einmalige) Verkaufspreis des Roboters. Jedoch steht derzeit die Monetarisierung von Lynx nicht im alleinigen Fokus. Insbesondere geht es darum, den Markt zu erobern, Wettbewerbsvorteile zu erzielen und die Robotertechnik sowie die enthaltene Künstliche Intelligenz zu verbessern. Mit steigenden Nutzerzahlen werden nicht nur höhere Einnahmen generiert, sondern es können vor allem auch mehr Daten gesammelt und ausgewertet werden, die zu einer Verbesserung der Leistungen nutzbar sind.

Durch die Datensammlung sind sowohl Amazon als auch Ubtech in der Lage, die Kommunikation, das Wohn- und Kaufverhalten, die Mediennutzung etc. jedes Nutzers besser zu verstehen. Mittels entsprechender Datenanalyse können

somit über passende Kaufempfehlungen mehr Umsatz generiert und die Möglichkeit verbessert werden, neue Mehrwerte zu erzeugen. **Schlüsselaktivitäten** sind die (Weiter-)Entwicklung von Robotics und der Künstlichen Intelligenz. Dies geschieht durch die Sammlung und Auswertung aller Nutzerdaten, die über die Interaktion mit Lynx anfallen und im Rahmen der Kundenprofilanalyse analysiert werden. Lynx liefert damit umfassende Daten über das Verhalten und die Bedürfnisse seiner Nutzer und generiert damit ein umfangreiches Kundenverständnis, auf Basis dessen immer weitere Services angeboten werden können. Neben dem **Schlüsselpartner** Amazon arbeitet Ubtech mit verschiedenen Universitäten und Forschungseinrichtungen zusammen (Industriepraxis 2018). Die gewonnenen Kunden-, Umgebungs- und Kommunikationsdaten stellen die **Schlüsselressourcen** dar. Gerade in Bezug auf den Überwachungsmodus sind zudem die Bewegungsdaten und Videoaufzeichnungen essenziell. Die möglichst umfassende Kenntnis der Lebensumstände und der Präferenzen seiner Anwender ist die Grundlage für das **Wertangebot** von Lynx und dessen weitere Entfaltung.

2.2.3 Spannungsfeld Datennutzung und Datenschutz

Services in den Bereichen Smart Home und Ambient Assisted Living unterstützen das Leben im häuslichen Umfeld mit dem Ziel, ein höheres Maß an Sicherheit, Komfort und Effizienz für die Bewohner herzustellen. Dies geschieht beispielsweise durch Automatisierung von Warnungen, Arbeitsabläufen und physischer Hilfe. Dabei entfaltet das vernetzte Zuhause sein volles Potenzial erst dann, wenn möglichst viele Daten über die Einrichtungen, Geräte und deren Nutzer ausgelesen und analysiert werden. Erst dadurch entsteht ein umfassendes Bild über den Menschen in seinem Zuhause und können individuell passende (Unterstützungs-)Leistungen angeboten bzw. in Anspruch genommen werden.

Die Lebens- und Wohnqualität kann insbesondere für ältere Menschen gesteigert werden. Mit dem Eintritt in den Massenmarkt können Smart Home-Komponenten das sichere und altersgerechte Wohnen fördern (Nationaler IT-Gipfel 2015). Das häufig wichtigste Ziel älterer Menschen, so lange wie irgend möglich selbstständig und selbstbestimmt zu leben (Bundesinstitut für Bevölkerungsforschung 1996), wird dadurch gefördert. Insgesamt hilft das Smart Home, die gesellschaftliche Entwicklung eines möglichst individualisierten Wohnangebots je nach persönlichen Vorlieben in Bezug auf Wohnumgebung und Verfügbarkeiten von Assistenzsystemen umzusetzen (Hartmut et al. 2010, S. 11).

Neben allgemeinen Daten zur Person, wie Alter, Geschlecht, Authentifizierungs- und Kontaktdaten, die in aller Regel bereits bei der Anmeldung zu Smart

Services preisgegeben werden, sind es im Wohnbereich vor allem Verhaltens- und Nutzungsdaten sowie Überwachungsdaten (Bild und Ton), die erhoben und ausgewertet werden. Aber auch Standort- und Bewegungsdaten werden in der Lebenswelt genutzt, um Sicherheit (bewegt sich etwas im Haus, obwohl der Bewohner nicht daheim ist?), Komfort (die Heizung schaltet sich ein, wenn sich der Bewohner auf dem Nachhauseweg befindet) und Effizienz (alle Lampen schalten sich aus, wenn der Bewohner das Haus verlässt) zu generieren. Essenziell für Smart Services, die im Bereich Wohnen das Bedürfnis nach Sicherheit adressieren, sind die Überwachungs- und insbesondere Videodaten. Durch Aufzeichnung der Überwachungsdaten (Bild und Ton) mittels verschiedener Systeme, wie Kameras und Bewegungssensoren, können Auffälligkeiten erkannt, analysiert bzw. verifiziert und weiterverarbeitet werden. In Kombination mit der Möglichkeit, Daten automatisiert auszuwerten und im Notfall weitere Schritte einzuleiten, liegt eine effektive Hilfestellung für die Betroffenen vor, insbesondere indem Maßnahmen in Akutfällen auch ohne deren aktives Eingreifen eingeleitet werden können.

Zudem kann die Sicherheit präventiv durch die Analyse von Verhaltens- und Nutzungsdaten gesteigert werden, indem die Erkenntnisse bspw. zur automatisierten Anwesenheitssimulation dienen. Auch unter Komfort- und Effizienzerwägungen sind gerade die Verhaltens- und Nutzungsdaten interessant. Je umfangreicher Informationen über Gewohnheiten der Bewohner eines Smart Home vorliegen, desto genauer können Leistungsangebote auf deren Bedürfnisse zugeschnitten werden. Erst das Wissen über die Uhrzeit des Aufstehens (auch in Echtzeit, z. B. durch Konnektivität mit einem smarten Wecker) ermöglicht das rechtzeitige Erwärmen des Badezimmers und die automatisierte Inangsetzung der Kaffeemaschine und des Toasters. Benötigt werden dafür fast ausschließlich sensible personenbezogene Daten (Akoto 2018), die besonderen Datenschutzbestimmungen unterliegen. Jedoch sind gerade diese Daten aufgrund des engen Bezugs zu den Gewohnheiten und Bedürfnissen der Menschen von besonderem Interesse für die Entwicklung smarter Geschäftsmodelle. Damit handelt es sich auch um Daten und Informationen, die eben nicht frei zugänglich sind, sondern einen direkten Zugang zum Nutzer und dessen Einverständnis zur Erhebung voraussetzen, um ein hinreichend treffendes Bild über das Privatleben zu gewinnen. Durch die Analyse dieser Daten können Geschäftsmodelle nutzerzentriert weiterentwickelt und neue Angebote und Services konzipiert werden.

Aufgrund des Umfangs und der Sensibilität der im Wohnbereich erhobenen Daten gibt es verschiedene Gesetze, die aus Daten- und Verbraucherschutzgründen für den Bereich Smart Home Anwendung finden und damit auch Anwendungsrestriktionen setzen. Dazu zählen u. a. das Telekommunikationsgesetz (TKG), das

Telemediengesetz (TMG), das Energiewirtschaftsgesetz (EnWG) und das Gesetz zur Digitalisierung der Energiewende. Des Weiteren stellt die seit 2018 gültige Europäische Datenschutzgrundverordnung (EU-DSGVO) persönliche Daten unter einen strengen und komplexen Schutz. Die neue EU-DSGVO regelt Vorschriften für die Erhebung und Verwertung personenbezogener Daten, die auch für das Smart Home umfassend Gültigkeit besitzen (Bundesverband Digitale Wirtschaft 2018a, S. 6 f.). Mit der EU-DSGVO drohen empfindliche Bußgelder, wenn Unternehmen gegen gültige Datenschutzbestimmungen verstoßen. Dabei gelten die folgenden Grundsätze:

- Die Erhebung personenbezogener Daten bedarf einer Legitimation durch einen gesetzlichen Erlaubnistatbestand oder durch Einwilligung des Nutzers.
- Die Einwilligung muss freiwillig erfolgen, d. h. die Nutzung eines Geräts darf nicht an die Einwilligung gekoppelt sein. Das fällt bei vernetzten Smart Home-Geräten in der Praxis schwer, da sie ja faktisch nur genutzt werden können, wenn sie Daten erheben.
- Der Einwilligende muss umfassend über die Datenerhebung informiert werden.
- Die Datennutzung darf nur in den Grenzen der Einwilligung erfolgen. Das Sammeln von Daten ‚auf Vorrat‘ ohne Zweckbindung ist damit untersagt.
- Der Grundsatz der Datenminimierung steht im Vordergrund der EU-DSGVO. Damit dürfen nur Daten erhoben werden, die für einen definierten Zweck erforderlich sind.
- Alle Geräte und Anwendungen müssen so konzipiert (‚Privacy by Design‘) und voreingestellt (‚Privacy by Default‘) sein, dass möglichst wenig personenbezogene Daten erhoben werden. Ein Ausweg besteht nur über die Anonymisierung der Daten (Verordnung des Europäischen Parlaments und des Rates 2016/679 2018).

Eine Herausforderung im Zusammenhang mit dem Smart Home besteht darin, dass Nutzer oftmals nicht sicher sind und sein können, welche Daten über die verwendeten Geräte aufgezeichnet werden und wofür diese tatsächlich genutzt werden. Ein Beispiel ist das Sprachsteuerungssystem Alexa, das laut Hersteller-Angaben Audiodateien erst dann aufzeichnet, wenn der Nutzer Alexa anspricht. Um Alexa zu verstehen, muss jedoch eine gewisse Aktivität des Geräts zu jedem Zeitpunkt sichergestellt sein. Ähnlich verhält es sich mit Überwachungssystemen, die Audio- oder auch Videodaten aufzeichnen. Über die Netzwerkanbindung können solche Daten direkt von den angebotenen Unternehmen verwertet werden. Vor diesem Hintergrund haben viele Bürger nach wie

vor eine hohe Skepsis gegenüber einer umfassenden Datenpreisgabe und Datenauswertung in der sehr privaten Lebenswelt Wohnen. Verstärkt wird die Sorge dadurch, dass insbesondere die datengetriebenen ‚BigTechs‘, die mit ihren individuellen Smart Services weltweit führend sind, außerhalb der EU in den USA (Amazon, Apple, Facebook, Google) und China (Baidu, Alibaba, Tencent) sitzen, wo andere, viel liberalere Datenschutzregeln gelten. Das Datenschutzklima und der rechtlich fixierte Datenschutz dürften von daher eine größere Verbreitung der Smart Home-Technologien in Deutschland und Europa bislang bremsen (Deloitte 2018, S. 25 ff.).

Ansätze zur Lösung und zur Fortentwicklung von Smart Services in der Lebenswelt Wohnen liegen in der Sicherung der Systeme und der Hoheitsrechte über sensible personenbezogene Daten. Gerade vernetzte Haussysteme, die Sicherheits- und deshalb Überwachungssysteme beinhalten, müssen zudem ausreichend Schutz gegen Hackerangriffe bieten und manipulationssicher sein. Es ist unerlässlich, dass die Geräte über verschlüsselte Netzwerke miteinander kommunizieren und immer automatisch die neuesten Updates aufgespielt werden, um entstehende Sicherheitslücken möglichst unverzüglich zu schließen. Auch die Datenübertragung nach außen, zum Server bzw. in die Cloud (und wieder zurück), muss verschlüsselt und entsprechend gesichert erfolgen. Was die Hoheitsrechte anbetrifft, ist rechtlich sicherzustellen, dass der Bürger selbst als Nutzer von Smart Services entscheidet, welche Daten von ihm und seinem Wohnumfeld erhoben werden und welche Teile davon er wem für welche Zwecke zur Verfügung stellt – aber dafür muss er auch die Möglichkeit entsprechender Wahlhandlungen bekommen, unabhängig vom Hersteller der vernetzten Geräte oder vom Plattformbetreiber.

Herausforderungen entstehen ferner durch das Tempo, mit dem Internetkonzerne und Start-ups datengetriebene Services auf den Markt bringen. Oftmals können Politik und Regulierung mit dieser Geschwindigkeit nicht schritthalten (Heide 2018). Um umfassende Smart Services in den Lebenswelten bieten zu können, müssen das Verständnis aufseiten der Bürger erhöht und Risiken möglichst minimiert werden, um auch die Chancen zu wahren und zu realisieren. Die Chancenwahrung wiederum steht durchaus im Widerspruch zu einem aktuell sehr restriktiv regulierten Markt mit insbesondere sehr hohen (und anscheinenden immer noch weiter steigenden) Datenschutzstandards, die den technologischen Möglichkeiten der Vernetzung und der Datengenerierung, -analyse und -übertragung vielfach nicht gerecht werden.

Schon heute sind zahlreiche Smart Services und innovative Geschäftsmodelle in der Lebenswelt Wohnen vorzufinden, die sich in den kommenden Jahren weltweit voraussichtlich rasant weiterentwickeln und verbreiten werden. Die

Potenziale liegen gerade in Deutschland jedoch bislang noch weitgehend brach. Dabei ist der Nutzen, den die Datensteuerung im intelligenten Zuhause liefert, zu großen Teilen bekannt, zugehörige Geschäftsmodelle entwickeln sich heute und Märkte werden international jetzt erschlossen und verteilt. Folglich sollte die Abwägung zwischen notwendigem Datenschutz und den möglichen Mehrwerten der datengetriebenen Geschäftsmodelle nicht einseitig geführt werden. Hier gilt es, die Balance unter Berücksichtigung aller Aspekte zu wahren, denn auch für Unternehmen stehen der Kundennutzen und das Kundeninteresse im Fokus ihrer Geschäftsmodelle (Bundesverband Digitale Wirtschaft 2018a, S. 3 f.).

2.2.4 Rolle der Versicherer

Datengetriebene Smart Services werden die Lebenswelt Wohnen in naher Zukunft nachhaltig verändern. Insbesondere gilt das für den Privatkundensektor, an den sich ein Großteil der Angebote richtet. Damit einher gehen das Eintreten neuer Marktteilnehmer, eine Neuverteilung bestehender Rollen sowie die Notwendigkeit, (branchenübergreifende) Kooperationen im Umfeld Wohnen einzugehen. In der jüngeren Vergangenheit ließen sich bereits einige Allianzen beobachten, und es zeigt sich eine langsam zunehmende Bereitschaft, Schnittstellen zur Verfügung zu stellen (Versicherungsbote 2018). Jedoch ist gerade der Smart Home-Markt nach wie vor sehr stark zersplittert. Zahlreiche Anbieter wie Hersteller von Haustechnik, Energielieferanten und Telekommunikationsunternehmen versuchen, den direkten Zugang zum Kunden zu gewinnen und sich mit ihren Lösungen am Markt zu positionieren.

Für die Kunden entsteht dadurch die Herausforderung zahlreicher unterschiedlicher Angebote, die teils überschneidende Services bieten und oft untereinander nicht kompatibel sind – insbesondere auch, was die Kommunikation der Geräte und den Datenaustausch untereinander angeht. Gerade durch die fehlende Kompatibilität der Geräte und Anwendungen untereinander ergeben sich Hemmnisse bei der Nutzung von Smart-Home-Technologien. Mehr und mehr wird deutlich, dass der Kunde kein Verständnis für separate und voneinander losgelöste Services hat, die einzeln installiert werden müssen und keine vollständige Lösung aufweisen (Deloitte 2018, S. 29). Vor diesem Hintergrund kristallisieren sich zunehmend Netzwerke heraus, die gemeinschaftlich an umfassenden, kundenzentrierten Smart Services arbeiten. Beispielhaft kann an dieser Stelle das Netzwerk ‚Connected Living‘ genannt werden, an dem zahlreiche namhafte Industrie- und Softwareunternehmen, Dienstleister sowie Versicherer mitwirken

(Connected Living 2018). Häufig dienen diese Zusammenschlüsse jedoch vorrangig dem Austausch und weniger der Entwicklung konkreter Lösungen, die umfassende Mehrwerte für die Bürger mit sich bringen. Bei der gemeinschaftlichen Entwicklung konkreter Leistungen überwiegen nach wie vor meist der Wunsch, das eigene Unternehmen und die damit verbundene Marke zu positionieren, sowie die Angst vor Konkurrenz und dem Verlust von Marktanteilen.

Mit den o. a. Entwicklungen in der Lebenswelt Wohnen wird sich auch das Geschäftsmodell der Versicherer verändern und werden neue Herausforderungen und Chancen entstehen. Mit den neuen Smart Services ändern sich zunächst die Kommunikationswege mit den Kunden und die Kontaktpunkte zu ihnen erheblich. Digitale Assistenten in den Wohnräumen schaffen eine völlig neue Form des Austauschs und bringen neue Touchpoints mit sich (Krohn 2018). Sie begleiten den Kunden in seinem privatesten Umfeld und schaffen dadurch eine genaue Kenntnis über seine Lebenssituation und Gewohnheiten. Mittels Datenanalyse können darüber hinaus Wünsche und Bedarfe der Kunden abgeleitet, passgenaue Leistungen individuell und bedarfsgerecht erstellt und über die intelligenten Interaktionsschnittstellen empfohlen und abgeschlossen werden. Das gilt auch für die Versicherungsprodukte rund ums Wohnen, die bei intelligenter Auswertung der Wohnausstattung und der damit verbundenen Sach- und Haftpflichtrisiken zielgenau, mit der treffenden Deckungshöhe und gesamthaft zugeschnitten angeboten werden können. Im Umkehrschluss kann ein smarter Helfer auch überflüssige oder nicht mehr notwendige Versicherungen aufdecken und kündigen. Außerdem kann er dem Kunden bei intelligenter Analyse den günstigsten Tarif vorschlagen und ihm bei neuen Angeboten einen Wechsel empfehlen. Ob es in Zukunft zudem noch derart zersplitterte Produktlandschaften geben wird, wie heute üblich, mit Wohngebäudeversicherungen zum ‚Versicherungswert 1914‘, Hausratversicherungen nach dem ‚Vollwertprinzip‘ und Gewässerschadenhaftpflichtversicherungen für den Öltank im Vorgarten, die kein normaler Bürger versteht, kann hinterfragt werden.

Die Entwicklungen lassen auch eine weitere Konsolidierung des Versicherungsmarkts erwarten. Wenn in größeren Netzwerken künftig ganzheitliche Lösungen für das Smart Home des Kunden angeboten werden, könnte es ausreichen, daran jeweils nur einen Versicherer exklusiv zu beteiligen. Auch die personalen Versicherungsvermittler werden nicht wie bisher zum Einsatz kommen, wenn die digitalen Analysemöglichkeiten und die automatisierten Prozesse vermehrt zum Tragen kommen. Einerseits müssen sich die Versicherungsvertreter und -makler die digitalen Anwendungen selbst zunutze machen, andererseits werden die Entwicklungen aber auch zu einer Substitution ihrer bisherigen Arbeit führen.

Außer für eine stärker kundenzentrierte Produktgestaltung können die in der Lebenswelt Wohnen gewonnenen Daten unter Nutzung von Methoden des Data Mining und Künstlicher Intelligenz zur Prognose, Früherkennung und Prävention von Schäden verwendet werden, was ebenfalls erhebliche Auswirkungen auf das Geschäftsmodell der Versicherer mit sich bringt. Durch Sensoren in den Rohrleitungen werden Wasserschäden verhindert, smarte Schließ- und Überwachungssysteme beugen Einbrüchen vor, und auch Schäden durch Unwetter und Feuer können durch Wettersensoren, intelligente Rauchmelder u. ä. reduziert werden. Die bislang hohen Schadenssummen, die besonders bei Gebäudeschäden im Zusammenhang mit Wasser und Feuer auftreten, können dadurch signifikant sinken (Munich Rr 2017). Kommt es dennoch zum Schadenfall, werden Schadenabwicklung und -regulierung durch eine intelligente Datenanalyse grundlegend vereinfacht, da der Versicherer für seine Aufgaben der Schadenprüfung viele relevante Daten in Echtzeit einsehen und verarbeiten kann. Mit der einhergehenden Ursachenanalyse könnten die lernenden Systeme zudem wiederkehrende Schäden immer besser vermeiden. Dadurch werden die Risiken in der Hausrat- und Wohngebäudeversicherung gemindert, und in der Folge sinkt auch schlicht die Bedeutung klassischer Versicherungsprodukte. Dadurch ist eine Neuausrichtung des Geschäftsmodells unausweichlich.

Allerdings kommen im Smart Home auch neue Risiken auf, die einer Absicherung bedürfen. So scheint es im Hinblick auf die wachsende Bedeutung von Daten- und Prozesssicherheit angezeigt, eventuelle Ausfälle des Smart Home-Systems oder Hackerangriffe abzusichern sowie bspw. bei möglichem Fehlalarm für die entstandenen Kosten aufzukommen. Um sich langfristig in der Lebenswelt Wohnen zu etablieren, ist die strategische Positionierung im Ökosystem Wohnen erforderlich. Von großer Bedeutung sind dabei branchenübergreifende Kooperationen und die Eingliederung in einem umfassenden Netzwerk – sei es als Orchestrator oder Zulieferer von Komponenten rund um Lösungen im Smart Home.

Einen Schritt hin zu strategischen Partnerschaften haben viele Versicherer in den letzten Monaten und Jahren bereits getan. Ein Beispiel dafür ist ein Produkt der ERGO, die in Kooperation mit der Deutschen Telekom einen Smart-Home-Schutzbrief anbietet. Löst ein Magenta-Smart-Home-Gerät (Rauchmelder, Wassersensor, Alarmanlage) einen Alarm aus, wird der abwesende Bewohner über sein Smartphone informiert und über die ERGO werden entsprechende Notfallmaßnahmen eingeleitet. Der Versicherer ergänzt damit die technologischen Komponenten der Telekom um tatsächliche Hilfeleistungen im Schadenfall. Darüber hinaus übernimmt die ERGO im Rahmen der Kooperation auch die

Schadendeckung und die Kosten für eine nachfolgende Bewachung bei eingeschlagenen Fenstern und Reparaturen bis zu einer Höhe von 3000 EUR.

Analog funktioniert die Zusammenarbeit zwischen dem Elektronikhersteller Gigaset und der AXA. Registriert die Alarmanlage von Gigaset einen Einbruch, wird der Kunde per Smartphone informiert und kann über das Überwachungssystem prüfen, ob es zu einem Einbruch gekommen ist. Im gegebenen Fall hat er die Möglichkeit, den angeschlossenen AXA-Sicherheitsdienst zu informieren, der sich um die weiteren erforderlichen Maßnahmen kümmert. Durch die konkrete Hilfeleistung durch den Versicherer wird der Service für den Kunden besser greifbar und Installationshemmnisse gegenüber einem Smart Home können abgebaut werden.

Einen ähnlichen Ansatz verfolgen Allianz und Panasonic mit ihrer Kooperation (Allianz Assist Versicherung), die u. a. einen kostenlosen Schlüsseldienst, eine Sicherheitskontrolle vor Ort und die Anbindung verschiedener Handwerkspartner organisieren. Auf der einen Seite zeigt sich, dass durch derartige Partnerschaften neue Absatzkanäle sowie über die Smart Home-Geräte zusätzliche Kontaktpunkte zum Kunden erschlossen werden können (Müller 2018). Auf der anderen Seite verdeutlichen die Beispiele, dass sich die Kooperationen aktuell nur auf bilaterale Partnerbeziehungen beschränken und mit verschiedenen Anbietern und Versicherern sehr ähnliche bis deckungsgleiche Services angeboten werden. Dadurch und mit den vorrangig singulären Smart Home-Produkten konnten bislang kaum Alleinstellungsmerkmale realisiert werden.

Damit eine umfassende Lösung für die Lebenswelt Wohnen angeboten werden kann, sind statt bilateraler Partnerschaften auf Produktebene übergreifende Kooperationen mit Akteuren aus mehreren relevanten Branchen erforderlich. In der Lebenswelt Wohnen überwiegt das Bedürfnis nach Sicherheit gegenüber dem Wunsch nach Innovationen und neuesten Technologien. Zudem wird ein großer Teil Privatsphäre berührt, wodurch Vertrauen und Zuverlässigkeit für viele Menschen eine wichtige Rolle bei der Wahl des Anbieters spielt. Dadurch entstehen für Versicherer Chancen der Positionierung, denn sie sind schon seit Langem dafür bekannt und akzeptiert, sensible Daten über ihre Kunden zu verarbeiten und sorgsam zu nutzen. Verschiedene Studien schreiben daher den Versicherern auch ein deutlich größeres Vertrauen beim Datenschutz zu als internationalen Großkonzernen wie Amazon oder Google. Dieses Potenzial könnte genutzt werden, um sich als ‚Enabler‘ oder Orchestrator eines umfassenden Netzwerks in Stellung zu bringen. Zudem haben Versicherer mit dem Ziel geringer Schäden ein den Kunden ähnliches Anliegen.

Das hohe Vertrauen der Kunden und die ähnlichen Interessen bei der Absicherung der eigenen vier Wände, verbunden mit den Potenzialen, die nach

wie vor mit den Beratungs- und Betreuungskapazitäten einer breiten Vermittlerschaft verbunden sind, schaffen auch gute Voraussetzungen für den Kundenzugang. Damit könnte es einem Versicherer gelingen, Unternehmen aus anderen Branchen und deren Smart Services an das eigene Angebot anzukoppeln und das Netzwerk damit im Interesse des Kunden zu steuern. Der Versicherungsschutz muss dabei nicht im Mittelpunkt stehen. Vielmehr kann und sollte ggf. der Versicherer als umfassender Dienstleister auftreten, der sich im Interesse des Kunden um die Absicherung seiner Wohnumgebung kümmert, zugleich im Netzwerk Wohnkomfort und Ressourceneffizienz fördert und zudem bei Bedarf unkompliziert Versicherungsschutz und im Schadenfall auch Assistenzleistungen beisteuert (Müller 2018).

2.3 Lebenswelt Gesundheit

2.3.1 Smart Services im Überblick

Die Gesundheit zählt zu den höchsten Gütern der Menschen. Die Entwicklungen im Gesundheitssektor und der medizinische Fortschritt sind vor diesem Hintergrund in der Breite der Bevölkerung von großem Interesse. Ohne Übertreibung stellt die eigene Gesundheit per se eine ‚Lebenswelt‘ für die Menschen dar. Die Entwicklung des Gesundheitswesens ist im Grunde so alt wie die Menschheit selbst, und die Technologieverwendung geht weit in die Vergangenheit zurück. Vor allem im letzten Jahrhundert sind die technischen Anwendungen im Gesundheitssektor immer schneller vorangeschritten. Im Zusammenspiel mit der zunehmend besser werdenden medizinischen Versorgung sowie der stärkeren Aufklärung über die verschiedenen Krankheitsrisiken und Präventionsmöglichkeiten werden die Menschen immer älter und bleiben länger gesund. Seit einiger Zeit hat sich zudem die ‚Quantified Self‘-Bewegung als bedeutender Trend entwickelt, der sich durch einen großen Teil verschiedener Altersstufen und durch breite Bevölkerungsgruppen zieht. Dieser Trend, zu dem neben der Selbstvermessung auch die Selbstoptimierung gehört, hat bedeutende Auswirkungen auf die Lebenswelt Gesundheit (Heyen 2016, S. 2). Viele der Verhaltensweisen und Einfluss nehmenden Faktoren, wie bspw. der Grad der sportlichen Betätigung oder die Ernährung, sind allerdings stark subjektiv geprägt und nicht ohne Weiteres kontrollierbar. Dafür rücken Alltagshelfer und Tracking-Systeme, die beim Aufzeichnen des eigenen Lebensstils helfen, immer stärker in den Fokus.

Einen starken Einfluss auf die Medizin, namentlich auf die Diagnostik und Therapie, haben Daten. Die Flut an Daten, die inzwischen gesammelt werden

kann, führt zu besseren und genaueren Analysen und – insbesondere auch im Zusammenhang mit Künstlicher Intelligenz – zu besseren Vorhersagemöglichkeiten. Damit können nicht nur die Effizienz (schnellere Diagnose) und der Komfort (automatische Erhebung) medizinischer Leistungen gesteigert werden, sondern vor allem auch deren Qualität.

Eine Besonderheit der in der Lebenswelt Gesundheit erhobenen Daten liegt in dem hohen Grad der Sensibilität: Bei Gesundheitsdaten handelt es sich um personenbezogene Daten, die nach Art. 4 Nr. 15 der Europäischen Datenschutzgrundverordnung (EU-DSGVO, siehe hierzu auch Abschn. 2.2.3) besonders schutzbedürftig sind und daher einem ausgeprägten Datenschutz unterliegen. Gerade die sensiblen Personendaten sind aber in einem hohen Detaillierungsgrad notwendig, um die Bürger in der Lebenswelt Gesundheit unterstützen zu können und ihnen Mehrwerte zu bieten. Daher ergibt sich in besonderem Maße ein Spannungsfeld, das immer wieder stark in der gesellschaftspolitischen Diskussion steht.

Neben den Daten sind verschiedene Technologien, wie die Sensorik, die zunehmende Vernetzung im Rahmen des Internet of Things (IoT) oder die Künstliche Intelligenz (KI), essenzielle Bestandteile der Smart Services in der Lebenswelt Gesundheit. Dabei können die Smart Services wie folgt gegliedert werden:

Datensammlung

Ausgangspunkt und zugleich erstes mehrwertiges Ergebnis ist die Sammlung von Körpermessdaten. Zunehmend ermöglichen es technische Geräte, beispielsweise Smart Watches, smarte Waagen, intelligente Laufbänder oder andere Wearables, Körperdaten wie den Pulsschlag, die Körpertemperatur, die Sauerstoffsättigung, das Gewicht, die Muskelmasse, den Fett- und Wasseranteil zu messen. Angereichert werden können diese Informationen durch Daten wie die Blutgruppe, Allergien oder Vorerkrankungen. Zusätzlich können Arztberichte und Befunde die Auswertungen ergänzen, sodass die Zielsetzung und das Ergebnis ein Datenpool ist, der ein umfassendes Bild über den Gesundheitszustand eines Menschen liefert. Aus diesem Datenpool können unterschiedliche Akteure verschiedene Nutzen ziehen. So kann die messende Person selbst den eigenen Lebensstil analysieren und optimieren und mit anderen teilen – etwa um sich so in ihrer Peergroup zu vergleichen.

Im Zusammenspiel zwischen Patient und Arzt können mit einer qualifizierten Datenbasis und den Auswertungsmöglichkeiten Krankheiten und körperliche Beeinträchtigungen besser behandelt werden. Und die Forschung kann die Medizin durch Einbeziehung umfassenderer Datengrundlagen und verbessertem Zusammenhangswissen substanziell weiterentwickeln (Heyn 2016, S. 4 f.).

Diagnoseunterstützung

Auf Basis der gesammelten Daten ergeben sich Smart Services, die Mehrwerte für die Diagnoseunterstützung bieten. Dabei gibt es verschiedene Anwendungsmöglichkeiten: So können Daten, die gewisse Anomalien signalisieren, eine automatische Meldung an den Nutzer mit dem Hinweis auslösen, einen bestimmten Arzt aufzusuchen. Digitale Fotos einer auffälligen Hautstelle können durch eine Analysesoftware über eine Datenbank gespielt und im Sinne einer Ersteinschätzung automatisch ausgewertet werden. Zusammen mit dem übermittelten Analyseergebnis kann gegebenenfalls zugleich ein geeigneter Facharzt zur näheren Begutachtung und anschließenden Therapie empfohlen werden. Auch mit Röntgenbildern, CT's und MRT's, ferner mit Blutwerten, EKG's und allen sonstigen möglichen Analysewerten lassen sich solche Datenbanken füllen und nutzen.

Unter Einbeziehung einer Künstlichen Intelligenz kann das System von den Ergebnissen nachfolgender Untersuchungen lernen und dadurch im Gleichschritt mit der Nutzungshäufigkeit verbessert werden. Systeme mit Künstlicher Intelligenz können über die Zeit immer ausgefeiltere Verknüpfungen von Gesundheitsdaten interpretieren und sich selbstlernend verbessern, d. h. Krankheitssymptome immer zuverlässiger automatisch erkennen und zielführende Therapien vorschlagen. Schon heute gibt es Künstliche Intelligenzen, die mittels bildgebender Verfahren, etwa der sog. Positronen-Emissions-Tomografie (PET), Demenzerkrankungen deutlich früher erkennen können als Ärzte. Das Ziel ist es, durch eine ausreichend große Zahl an Daten, die mithilfe vorangegangener und gespeicherter Untersuchungsergebnisse generiert wird, Befunde automatisch und damit sowohl schneller als auch präziser als von Menschen möglich zu erstellen (PwC 2017, S. 7 f.).

Therapieunterstützung

Die technischen Hilfsmittel zur Diagnoseunterstützung gehen Hand in Hand mit Mehrwerten, die Smart Services im Bereich des Monitorings von Heilungsverläufen oder im Rahmen der Unterstützung bei körperlichen Beeinträchtigungen im Alltag bieten. Nach Feststellung einer Erkrankung bieten digitale Anwendungen die Möglichkeit, den Therapieverlauf 24/7 für den Arzt abzubilden. Dieser erhält beispielsweise über die beim Patienten aufgezeichneten Daten Einblick in dessen Gesundheitszustand und empfängt zusätzlich eine Meldung, sobald ein bestimmter Wert abseits der Toleranz liegt. Mit einer dann erfolgten frühzeitigen Intervention kann der Heilungsverlauf schneller und effizienter weitergeführt werden. Wenn der Patient zusätzlich die Einnahme der Medikamente in die Anwendung einpflegt, kann der behandelnde Arzt schneller Ursachen für eine falsche Entwicklung der Genesung finden. Über cloud-

basierte Kommunikationsplattformen kann das Zusammenspiel der verschiedenen Akteure, also Patient, Arzt, Krankenhaus, Pflegekraft, Krankenversicherer etc., erheblich verbessert werden und Doppel- und Mehrfachuntersuchungen können vermieden werden. Auch können das Internet of Things (IoT), also die Vernetzung z. B. von medizinischem Gerät, und der Austausch über Informations- und Kommunikationsplattformen wichtige Hilfestellungen für die Zusammenarbeit der verschiedenen Parteien geben.

Ambient Assisted Living

Ambient-Assisted-Living-(AAL)-Technologien können auch im Krankheitsfall oder bei körperlichen Beeinträchtigungen ein selbstbestimmtes Leben ermöglichen. AAL-Technologien beinhalten Produkte, Dienstleistungen und Konzepte, die die Lebensqualität vor allem älterer Menschen in allen Lebenslagen erhöhen sollen. Beispielsweise können Sensoren die Bewegungsabläufe in der Wohnumgebung messen und einen Notdienst alarmieren, wenn eine auffällige Bewegungsunterbrechung vorliegt. Viele solcher Systeme haben sich aufgrund der Scheu vor Technik, von Überwachungsängsten oder zu hohen Kosten noch nicht durchgesetzt. Einzig der Hausnotruf, bei dem ein Alarmknopf am Körper getragen wird, ist bereits weit verbreitet (Ambient Assisted Living Deutschland Acatech 2018).

Transhumanismus

Die Entwicklungen zeigen, dass es eine immer stärkere Verschmelzung von Mensch und Maschine gibt. Im Rahmen von Testversuchen werden bereits Technologien entwickelt, bei denen Chips oder Sensoren direkt unter die Haut des Menschen gelegt werden. Das enge Zusammenspiel zwischen der Digitaltechnik und dem Menschen kann zu einem ganzheitlichen Ansatz der Gesundheitsbegleitung führen, der einerseits die verfügbaren Datengrundlagen nochmals exponentiell ausweitet, andererseits die Potenziale für eine schnellere und zuverlässigere Diagnose und Therapie ebenso nochmals steigert.

Die verschiedenen Entwicklungen können eine Fülle von Problemen lösen, denen Patienten Ärzte, Pfleger und weitere Beteiligte gegenüberstehen. Die Zeitrestriktionen der Ärzte werden durch die Diagnosemöglichkeiten und Therapieempfehlungen mittels Technologie entschärft, die Behandlung der Patienten durch die Überwachung während der Genesung verbessert, umständliche Vorgehensweisen beispielsweise beim Arztwechsel durch die erleichterte Kommunikation zwischen den Parteien vereinfacht und effizientere und zielgerichtetere Pflegeleistungen auf Basis der AAL-Technologien werden ermöglicht. Immobilen Personen und Personen, die in einem Gebiet mit schlechter Arztdeckung woh-

nen, können durch die Technologie viele Wege sparen. In die Diagnose und Therapieempfehlung können Computersysteme eine große Zahl an Parametern einbeziehen und damit deutlich zuverlässigere und zudem noch schnellere Ergebnisse liefern.

Es zeigt sich, dass Smart Services in der Lebenswelt Gesundheit die Anwendungsfelder Prävention, Diagnostik, Therapie, Überwachung von Krankheitsverläufen, Pflegeunterstützung und nicht zuletzt Fitness/Freizeit/Lebensstil beinhalten. Diese Anwendungsfelder basieren auf der Erhebung von Daten, deren Auswertung zunehmend mit Künstlicher Intelligenz vorgenommen wird. Im Folgenden werden drei ausgewählte Geschäftsmodelle betrachtet, die bereits auf Märkten existieren und aus den zuvor beschriebenen Entwicklungen hervorgegangen sind. Dabei liegt der Fokus auf der Beschreibung und Würdigung der Nutzenversprechen, die mit diesen Geschäftsmodellen verbunden sind.

2.3.2 Ausgewählte Geschäftsmodelle innerhalb der Smart Services

2.3.2.1 Apple Health

1. Beschreibung des Geschäftsmodells

Nach den Anwendungsfeldern der Smart Services lässt sich das Geschäftsmodell von Apple Health in die Bereiche Datengenerierung, Prävention, Diagnostik, Therapie, Überwachung von Krankheitsverläufen und Fitness/Freizeit/Lebensstil einordnen. Apple Health ist eine Anwendung, mittels derer Gesundheitsdaten gesammelt, aufbereitet und ausgewertet werden können. Sie ist als App auf dem iPhone vorinstalliert und in die vier Gruppen ‚Aktivität‘, ‚Achtsamkeit‘, ‚Schlaf‘ und ‚Ernährung‘ eingeteilt. Da das Smartphone selbst nur begrenzt Gesundheitsdaten erheben kann, sind zusätzliche Gadgets wie die Apple Watch oder kleine Adapter zur Messung der Blutwerte für eine umfassende Nutzung und Datenerhebung unabdingbar. Auch mit Geräten aus dem Haushalt, wie der digitalen Körperwaage oder einer intelligenten Zahnbürste, kann die Anwendung gekoppelt und mit Daten angereichert werden. Als kompatibles Hauptgerät von Apple misst die Apple Watch u. a. die Herzfrequenz. Bei besonders hohen oder niedrigen Frequenzen löst sie eine Warnung aus und gibt unter Umständen einen Hinweis, zum Arzt zu gehen (Stanford Medicine 2018).

Zum anderen ist in die Apple Watch ein sogenannter Beschleunigungs- und Gyrosensor eingebaut, der einen möglichen Sturz des Trägers erkennt. Nach einem Sturz kann mit einem Klick ein Notruf gesendet werden. Wenn der Gestürzte allerdings 60 s nicht reagiert, wird der Notruf automatisch ausgelöst.

Über GPS wird den Rettungskräften bei Ausruf des Notfalls unmittelbar der Standort der gestürzten Person angezeigt, ohne dass sich der Nutzer zunächst orientieren muss. Durch die einfache und direkte Kommunikation über die Anwendung werden Fehler vermieden und die Effizienz gesteigert. Daneben erfasst die Apple Watch Freizeitaktivitäten und kann als eine Art Trainer im Sport agieren (Apple 2018a). Für Anwender der Freizeitfunktionen bietet Apple einige Gadgets zur Kopplung mit dem iPhone an. Dazu zählen u. a. ein smarterer Fahrradhelm, ein smartes Fahrradsystem für Licht, Navigation, Diebstahlsicherung und Fitness Tracking, ein Springseil, ein Tennisschläger und weitere Geräte zur Messung von Körperdaten, wie Blutdruck- und Blutzuckermessgeräte und andere Überwachungssensoren (Apple 2018b).

Wegen der Notwendigkeit und des Angebots, weitere Geräte und Anwendungen zu nutzen, ist eine standardisierte Schnittstelle erforderlich, um den Datenaustausch zwischen den verschiedenen Geräten zu organisieren. Apple stellt mit ‚CareKit‘ ein Open Source Software Framework zur Verfügung, mit dessen Hilfe Entwickler Apps generieren können, die beim Umgang mit Krankheiten helfen, indem sie die individuelle Behandlung unterstützen (bspw. Festhalten von Symptomen oder der Medikation). Ein ähnliches Software Framework stellt das ‚ResearchKit‘ dar, das die medizinische Forschung adressiert und bei der Durchführung medizinischer Studien hilft, indem bspw. Teilnehmer registriert werden können (Apple 2018c). Damit werden zwei Funktionen angeboten, mit denen andere Entwickler Gesundheitsapps erstellen können, die auf die gesammelten Daten von Apple Health zugreifen und mit der Anwendung interagieren. Apple setzt also ausdrücklich den Anreiz, dass weitere Gesundheitsapps programmiert werden, und stellt gleichzeitig sicher, dass sie mit Apple Health, das weiterhin als Zentrum für alle Daten fungiert, kompatibel sind. Ebenfalls unterstützt Apple medizinische Studien, die mittels App Gesundheitsdaten auswerten (Apple 2018c).

Apple Health fungiert also als eine Art Zentrale, die über verschiedene Geräte mit Daten ‚gefüttert‘ wird. Folgende Gesundheitsdaten können dabei u. a. ausgewertet werden:

- Atemfrequenz
- Blutdruck und -gruppe
- Body-Mass-Index
- Herzfrequenz
- Kalorienverbrauch
- Körpergewicht und -größe
- Körpertemperatur

- Sauerstoffsättigung
- Schlafverhalten
- Schritte inkl. Treppenstufen bzw. Höhenmeter
- Stürze

Seit Einführung des Betriebssystems iOS12 ist für iPhone-Besitzer auch die elektronische Patientenakte ‚Medisafe‘ verfügbar. Diese beinhaltet schon bislang die Möglichkeit der Eingabe von Medikamentierungen, verbunden mit der Funktion, vor Wechselwirkungen verschiedener Medikamente zu warnen. Ebenfalls wird ein Notfallpass angeboten, der einen besonderen Nutzen entfaltet: Im Sperrbildschirm werden relevante Gesundheitsdaten angezeigt, auf die im Notfall der Rettungssanitäter oder Notarzt direkt zugreifen kann, um dem Patienten zielgerichteter zu helfen. Die Möglichkeit, an einem Ort alle Daten zu sammeln, schafft die Voraussetzung, weitere Leistungen anzuknüpfen, die das Gesundheitssystem im Ganzen optimieren.

2. Geschäftsmodellanalyse nach Canvas

Apple Health adressiert als **Kundensegment** vorrangig die Endverbraucher und kann damit als B2C-Lösung klassifiziert werden. Die Funktionen von ‚CareKit‘ und ‚ResearchKit‘ richten sich allerdings eher an Unternehmen, wodurch auch eine B2B-Komponente vorliegt. Unter den Endkunden werden speziell iPhone-Besitzer adressiert, die technisch affin sind, Gesundheitsbewusstsein aufweisen und deshalb entweder ihre Werte beobachten, präventiv sportliche Aktivitäten ‚tracken‘ oder den Umgang mit vorliegenden Krankheiten optimieren wollen. Für diese Zwecke und als weiteres **Wertangebot** bietet Apple Health eine Basis für eine umfassende Datensammlung, um damit einen Überblick über die eigene Lebensweise und Gesundheit bereitzustellen. Insbesondere liegen die Daten für ihre Nutzer nicht mehr nur an verschiedenen Stellen, wie z. B. Apps, getrennt vor, sondern sind in Apple Health zusammengefasst und damit komfortabel zugreifbar. Zudem bieten die Auswertungen der Daten eine Hilfestellung, Krankheiten frühzeitig zu erkennen und in die Behandlung einzutreten. Mithilfe des Notfallpasses gibt es eine weitere Absicherung bei Unfällen. Sozioökonomisch führen die Anwendungen zu einer möglichen Einsparung von Kosten, da durch die allgemeine Gesundheitsförderung und frühzeitigere Aufdeckung von Krankheiten weniger Arztbesuche notwendig sind und der Heilungsverlauf besser abgebildet und unterstützt werden kann, was ihn beschleunigt. Kundennutzen erzeugt auch die Transparenz, mit der der Nutzer über die eigene Lebensweise und seine Aktivitäten informiert wird. Dazu werden die Daten dem Nutzer

auch grafisch aufbereitet. Ein weiteres Wertangebot liefert die Integration von Self-Service-Optionen. Neben der automatischen Datenerhebung sind weitere manuelle Eingaben, wie z. B. die Blutgruppe, vorliegende Allergien und Erkrankungen möglich. Durch die Zentralisierung der Daten in einer Anwendung steigt der Komfort für den Nutzer, und die Datenpflege wird erleichtert. Apple hat besonderen Wert auf eine intuitive App gelegt, sodass die Übersichtlichkeit auch beim angestrebten Ausbau der Datenbank und der Anwendungen nicht verloren geht. Der reduzierte Bedarf an Arztbesuchen, die Beschleunigung des Behandlungserfolgs und womöglich auch die Effizienzsteigerung im sportlichen Training führen zu Zeitersparnissen (Apple 2018d).

Als **Kommunikations- und Vertriebskanäle** bedient sich Apple Health der App sowie einer Homepage. Es besteht aber keine direkte Beziehung zwischen Unternehmen und Nutzer, vielmehr stellt die App Hilfsmittel zur Selbstbedienung zur Verfügung. **Einnahmequellen** von Apple Health werden indirekt durch den Verkauf der kompatiblen Geräte generiert, da die App selbst kostenlos ist. Die **Kooperationspartner** von Apple Health können vielfältig sein. Jeder App-Entwickler, der ‚CareKit‘ oder ‚ResearchKit‘ nutzt, aber auch Ärzte, Krankenhäuser, Apotheken und Pfleger können eingebunden werden (Apple 2018e). Zudem sind sowohl Kranken- als auch Unfall- und Berufsunfähigkeitsversicherer als mögliche Kooperationspartner prädestiniert – und damit Versicherungsanbieter aus allen Sparten des Versicherungsgeschäfts. Als **Schlüsselressourcen** stehen die Daten über den Nutzer und seine Gesundheit im Vordergrund. Des Weiteren wird medizinisches Know-how als intellektuelle Ressource eingesetzt, das zudem mit sich ständig weiterentwickelndem Zusammenhangswissen sowohl auf der Unternehmensseite als auch auf der Seite der Nutzer kontinuierlich gesteigert wird. Infolge der Datengenerierung, des Datenpooling und der Datenanalyse unter Verknüpfung vieler gesundheits- bzw. krankheitsrelevanter Parameter kann auch das medizinische Wissen insgesamt in der Gesellschaft erweitert werden – was wiederum ein besonderes **Wertangebot** darstellt.

2.3.2.2 Digitale Krankenversicherer am Beispiel Oscar und Clover

Ein digitaler Krankenversicherer nutzt für sein Geschäftsmodell im Kern neue Technologien, insbesondere für seine Produkte und Services („Smart Services“) sowie für die innerbetrieblichen und nach außen gerichteten Abläufe. Sie verwenden Daten aus Anwendungen wie beispielsweise Apple Health. Die Kommunikation erfolgt so weit wie möglich digital. Oscar und Clover, zwei Versicherer aus den USA, bieten auf diese Weise neue Möglichkeiten.

1. *Beschreibung der Geschäftsmodelle*

Oscar ermöglicht den vollkommen digitalen und transparenten Abschluss einer Versicherungspolice. Dabei werden folgende Leistungen angeboten: Über ein Suchfeld in der Smartphone-Applikation kann der Versicherte seine Symptome eintragen, und er erhält daraufhin erste Hinweise über eine mögliche Erkrankung. Nach Anwählen einer Rückruf-Funktion meldet sich innerhalb kürzester Zeit ein Arzt oder eine Krankenschwester und berät den Kunden. Zusätzlich steht dem Anwender ein persönliches Concierge-Team zur Verfügung, das z. B. Arzttermine bzw. Rückrufe vereinbart, Krankenhausaufenthalte organisiert und Schreiarbeiten nach einem Krankenhausaufenthalt übernimmt. Außerdem unterstützt Oscar den Kunden dabei, einen gesünderen Lebensstil zu führen: Beispielsweise lässt das Unternehmen dem Versicherungsnehmer bei Erreichen einer vorgegebenen Schrittzahl, die über die App gemessen wird, einen Amazon-Gutschein zukommen (Hioscar 2018).

Clover sammelt Patienteninformationen zur datenbasierten Erstellung klinischer Profile der versicherten Personen. Dabei greift das Unternehmen auf ein Netzwerk aus Ärzten, Arzthelfern, Krankenhäusern und (Online-)Apotheken zurück, deren Daten von Clover zusammengeführt und ausgewertet werden. So nutzt Clover z. B. Informationen zur Krankheitsgeschichte eines Versicherten, um ihn bei der Genesung zielgerichtet unterstützen zu können. Wird einem Patienten ein Medikament verschrieben, das regelmäßig einzunehmen ist, wird dies von Clover getrackt: Wird keine diesbezügliche Abrechnung eingereicht, schaltet sich Clover ein, erinnert den Patienten und informiert über die ‚Einnahmehinweise‘. Falls Arzttermine versäumt wurden, erhält der Patient ggf. Hausbesuche von Mitgliedern des Clover-Health-Teams, dazu gehören z. B. Krankenschwestern, Krankenpfleger oder Sozialarbeiter. Mit den Präventionsmaßnahmen verfolgt Clover insgesamt das Ziel, den Gesundheitszustand der Versicherten zu verbessern, kostenintensive Gesundheitsleistungen zu vermeiden und damit die allgemeinen Aufwendungen für die Versorgung von Patienten zu senken. Weiterhin gehören zum Leistungs- und Serviceangebot ein digitaler Katalog, der eine Übersicht über die Medikamente gibt, die durch den Versicherungsschutz abgedeckt sind, ein digitaler Apotheken- und Ärztefinder sowie kostenfreie Zusatzleistungen, wie z. B. routinemäßige Augen- oder Zahnuntersuchungen (Cloverhealth 2018).

2. *Geschäftsmodellanalyse nach Canvas*

Beide Unternehmen bieten neue Smart Services im Bereich Gesundheit. Während das **Wertangebot** von Oscar den digitalen und transparenten Abschluss einer Versicherungspolice umfasst und den Versicherungsnehmer beim Erkennen und einer

möglichen Behandlung unterstützt, konzentriert sich Clover auf die präventive Gesundheitsvorsorge, die auf einer softwarebasierten Datenanalyse beruht. Es können individuell zugeschnittene Informationen bereitgestellt, passende Ärzte gefunden, die Medikamenteneinnahme überprüft werden und vieles mehr.

Auch die individuellere Tarifierung auf Basis der erhobenen Daten stellt eine Neuheit dar. Die datenbasierte Risikoermittlung führt dazu, dass der Versicherte in der Krankenversicherung immer näher an seinem wirklichen Schaden-erwartungswert policiert werden kann. Auch dadurch kann sich eine mittelbare Kostenreduktion ergeben. Beispielsweise wird das individuelle Krankheitsrisiko aufgrund der Anreizwirkungen für eine gesündere Lebensweise gesenkt, was sich für die Versicherten auch in niedrigeren Prämien widerspiegeln kann. U. a. durch die Hilfe bei der Suche nach einem passenden Arzt geben die digitalen Krankenversicherer ein Transparenzversprechen ab. Ebenfalls werben sie mit einer äußerst transparenten Kosten- und Leistungsdarstellung. Durch die digitalen Angebote sind eine ortsunabhängige Beratung und Betreuung möglich. Zusätzlich können viele Daten über den persönlichen Gesundheitszustand oder eine vorliegende Krankheit in einem geschützten persönlichen Datenfeld eingetragen werden, wodurch die Integration solcher Self-Service-Optionen stark zur Prozessbeschleunigung beiträgt.

Die **Kundensegmente** von Oscar und Clover liegen sowohl im B2B- als auch im B2C- und B2B2C-Bereich. Neben der eigenen Verbindung zu den Versicherten werden Ärzte, Krankenhäuser, Pfleger und weitere Gesundheitsdienstleister einbezogen. Als Versicherungskunden werden vor allem digital affine Menschen mit Gesundheitsbewusstsein angesprochen, die für finanzielle und medizinische Vorteile bereit sind, ihre Daten an den Versicherer zu geben. Da Clover zum Medicare-Advantage-Programm der USA gehört, stehen die Leistungen nur darin einbezogenen Personen offen.⁸ Im Jahr 2017 lag die Versichertenzahl von Oscar bei etwa 135.000, Clover zählte rund 25.000 Versicherte.

Als **Kommunikations- und Vertriebskanäle** werden diverse Social Media, Apps, Chatfunktionen und die Homepages genutzt. Weiterhin wird den Kunden der Kontakt über (Video-) Telefonie oder E-Mail angeboten, und in Blogs werden sie zudem regelmäßig mit Informationen versorgt. Auch in der **Kundenbeziehung** bietet dieses Geschäftsmodell einen weiten Spielraum. So ist von automatisierten Angeboten und Dienstleistungen über Selbstbedienungen bis hin zur persönlichen und auch individuell persönlichen Unterstützung, also mit

⁸Mindestalter 65 Jahre oder Menschen mit terminaler Nierenkrankheit oder bestimmten Behinderungen.

immer gleichbleibendem Ansprechpartner, alles möglich. **Primäre Einnahmequelle** sind die Versicherungsprämien vonseiten der Kunden. Werden zusätzlich Kooperationen mit Ärzten oder anderen Gesundheitsdienstleistern vereinbart, ergeben sich weitere Einnahmen. So bezahlen etwa Dienstleister einen Preis dafür, in das Netzwerk einzutreten oder den Kunden in bestimmten Fällen vorgeschlagen zu werden. Die **Schlüsselaktivität** ist bei beiden Unternehmen die Bereitstellung von Versicherungsschutz, die Datenanalyse und die Pflege des Netzwerks. Die Mitglieder dieses Netzwerks, Ärzte, Krankenhäusern, Apotheken, Krankenschwestern, Pfleger und weitere Gesundheitsdienstleister, stellen die **Schlüsselpartner** der Unternehmen dar. **Schlüsselressourcen** sind die Kundenstammdaten und die Gesundheitsdaten der Versicherten. Auf Basis der gesammelten Daten aus den geschaffenen Netzwerkstrukturen und der effizienten digitalen Prozesse kann ein ganzheitliches Angebot an Smart Services und damit ein umfassendes **Wertangebot** zur Verfügung gestellt werden.

2.3.3 Spannungsfeld Datennutzung und Datenschutz

Wie gezeigt wurde, kann das Sammeln und die Nutzung von Daten in der Lebenswelt Gesundheit erhebliche Auswirkungen entfalten. So kann nicht nur die Gesundheit des Individuums verbessert, sondern auch eine Optimierung des gesamten Gesundheitswesens vorangetrieben werden. Systeme, die auf Basis von Daten Krankheiten in all ihren Parametern erfassen, künstliche Intelligenzen, die diese auswerten, und Assistenzsysteme, die Ärzte in ihrer täglichen Arbeit unterstützen, gehören zu den großen Chancen, die die Datennutzung mit sich bringt.

Dem gegenüber steht der berechtigte und notwendige Datenschutz, der im Gesundheitswesen auch spezifisch geregelt ist. In Art. 4 Nr. 15 der EU-DSGVO sind Gesundheitsdaten konkret berücksichtigt und abgegrenzt: „Gesundheitsdaten [sind] personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“ (Verordnung des Europäischen Parlaments und des Rates 2016/679 2018, Art. 4 Nr. 15). Nach § 22 des Bundesdatenschutzgesetzes (BDSG) und der EU-DSGVO gehören Gesundheitsdaten zur besonderen Kategorie personenbezogener Daten. Danach gilt für alle Gesundheitsdaten eine besondere Schutzbedürftigkeit. In diesem Zusammenhang besteht ein grundsätzliches Verbot der Verarbeitung von Gesundheitsdaten, das nur unter der Voraussetzung des Art. 9, 2a-j EU-DSGVO etwas aufgeweicht wird (Deutsche Gesellschaft für Qualität 2017). Das Verarbeitungsverbot gilt demnach nicht, wenn die betroffene Person für einen festgelegten Zweck zustimmt, dass ihre

Daten genutzt und verwertet werden. Neben weiteren Erlaubnistatbeständen beziehen sich die Absätze h und i direkt auf Gesundheitsdaten. In Art. 9, 2h EU-DSGVO (Verordnung des Europäischen Parlaments und des Rates 2016/679 [2018](#)) heißt es:

Die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich.

Und in Art. 9, 2i EU-DSGVO (Verordnung des Europäischen Parlaments und des Rates 2016/679 [2018](#)) steht:

Die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich.

Das hohe Niveau des Datenschutzes von Gesundheitsdaten macht die Durchführung einer Datenschutz-Folgeabschätzung notwendig, was zu einem erhöhten Aufwand in Einrichtungen des Gesundheitswesens führt und die Datennutzung erheblich erschwert (Deutsche Gesellschaft für Qualität [2017](#)).

Für das Individuum hat der ausgeprägte Datenschutz den Schutz vor Missbrauch zum Ziel. Dazu gehört nicht nur der Schutz vor Hackerangriffen auf Gesundheitsdaten, die inzwischen häufig vorkommen ([Ärztezeitung 2017](#)). Auch die Weitergabe an Unternehmen, die die Gesundheitsdaten für verschiedene Zwecke verwenden können, wird kritisch gesehen. Die Sorge vor einer Datenweitergabe und vor Missbrauch ist bei den Bürgern jedoch deutlich geringer, wenn es um den Arzt geht, der die Daten verarbeitet, speichert und weitergibt. Laut der Studie „Zukunft der Gesundheitsversorgung“ der pronovaBKK empfinden es 77 % der Befragten als Vorteil, wenn Daten über Diagnosen, Behandlungen, Medikamente, Allergien oder ähnliches zentral gespeichert sind und sich Haus- und Fachärzte jederzeit einen umfassenden Überblick über den Gesundheitszustand eines Patienten verschaffen können. Auch das Durchführen von Video- oder Onlinebehandlungen sowie per Telefon würden 56 % der

Befragten begrüßen (Schlingensiefen 2017). Dies lässt sich damit begründen, dass die eigene Gesundheit für den Bürger ein sehr wertvolles Gut ist und bei besserer Hilfe, beispielsweise weil der Arzt einen guten Überblick über den Gesundheitszustand bekommt, die Risiken schwächer bewertet werden. Ebenso kann davon ausgegangen werden, dass eine Verbesserung der medizinischen Leistung im Interesse aller ist. So beschneidet der starke Datenschutz die Chance und damit den großen Mehrwert, der beispielsweise durch das Fortschreiten der Forschung auf Basis großer Datenmengen erreicht werden kann. Die Forschung und damit das Wissen in der Medizin, die Qualität der Behandlung und letztlich die Gesundheit des Einzelnen werden damit nachhaltig gestört. Dies gilt zumindest in Deutschland und Europa. Die datenbasierte Forschung auch und gerade im Gesundheitswesen wird beispielsweise in den USA und in China stärker vorangetrieben (PwC 2018), was letztlich auch zum komparativen Nachteil von Bürgern und Unternehmen hierzulande führen kann.

Es entsteht daher ein Spannungsfeld, das es nicht nur rechtlich, sondern auch politisch und vor allem im Dialog mit den Bürgern zu lösen gilt. Hierbei muss ein Abwägen zwischen dem Missbrauchsrisiko und der Datennutzung und -auswertung zur Verbesserung der Medizin erfolgen, wobei der Wille und die Wünsche der Bürger im Vordergrund stehen müssen. Der Datenschutz hat in diesem Zusammenhang eine wichtige Funktion, sollte aber möglichst nicht die Potenziale beschneiden, die neue technologische Möglichkeiten heute bieten. Für viele Anwendungen lassen sich die Hürden des Datenschutzes vermutlich durch ausdrückliche Einwilligungserklärungen der Betroffenen zur Datenerhebung, -speicherung, -analyse und -weitergabe überwinden. In Betracht kommen dabei auch ‚Datenspenden‘ an Forschungseinrichtungen o. ä. Das gilt aber nicht für jede Situation. Beispielsweise ist die Voraussetzung zur Einwilligung bei einem Unfall, um gesundheitsrelevante Daten an einen Arzt oder ein Krankenhaus zu übermitteln, damit schneller eine adäquate Hilfe bestimmt und organisiert werden kann, vielfach nicht zweckmäßig oder unerfüllbar (Bass 2017, S. 34 f.). Allzu restriktive Datenschutzbestimmungen sind etwa in einer solchen Situation nicht hilfreich und sind vor allem nicht im Interesse derjenigen, die mit den Regelungen eigentlich geschützt werden sollen.

2.3.4 Rolle der Versicherer

Die Potenziale, die aufgrund der Menge an Daten und neuen Technologien in der Lebenswelt Gesundheit erwachsen, sind vielseitig und bringen viele Chancen, auch für die Versicherer. Wie in Abschn. 2.3.2.2 (Digitale Krankenversicherer am

Beispiel Oscar und Clover) gezeigt wurde, liefern Daten die Grundlage zur Entwicklung neuer kundenorientierter Geschäftsmodelle. Dadurch werden allerdings auch ein Zutritt immer neuer Marktteilnehmer und die Bildung von Netzwerken (Ökosystemen) im Gesundheitssektor begünstigt, was die eigene Positionierung eines traditionellen Versicherers in diesem dynamischen Marktumfeld unabdingbar macht. Im Folgenden wird mit Blick auf das Gesundheitsthema auf traditionelle Krankenversicherer fokussiert. Sie werden heute unzweifelhaft gezwungen, sich die neuen technologischen Möglichkeiten und eine moderne Datenbasis zunutze zu machen, um ihre Aufgabe zu erfüllen, eine bestmögliche Gesundheitsversorgung für ihre Kunden hervorzubringen sowie auch ihre eigene Marktposition zu verteidigen und zu stärken. Dafür sind auch im digitalen Umfeld der Kontakt und der Zugang zum Kunden deutlich zu verbessern und dem Kunden gleichzeitig die relevanten Nutzenversprechen anzubieten. Umgekehrt ergibt sich ein Risikopotenzial, das darin liegt und sich konkretisiert, wenn Entwicklungen verkannt und sich daraus ergebende Chancen nicht genutzt werden.

Die Ausgangslage der Versicherer unter den neuen Entwicklungen ist als grundsätzlich gut einzuschätzen. Ihr Geschäftsmodell basiert seit jeher auf den Daten der Kunden und deren gesundheitlicher Situation. Zudem genießen sie beim Thema (Gesundheits-)Daten ein hohes Vertrauen (siehe dazu Nitschke 2018), was gerade in der sich digitalisierenden Datenwelt von hoher Relevanz ist. Herausforderungen der Versicherer bestehen jedoch in der Reaktions- und Innovationsgeschwindigkeit bei der Nutzung neuer Technologien und damit auch der Befriedigung der konkreten Kundenwünsche. Gerade in der inzwischen sehr dynamischen Lebenswelt Gesundheit ist eine hohe Reaktionsgeschwindigkeit essenziell, um stets die bestmögliche Versorgung zu bieten.

Insbesondere von Versicherungsunternehmen sind jedoch auch ethische und moralische Aspekte in besonderem Maße zu berücksichtigen: So muss geprüft werden, ob Personen, die weniger auf ihre Gesundheit achten, zukünftig etwa bei der Versicherungsprämie benachteiligt werden und inwieweit dies gesellschaftspolitisch vertretbar ist. Ebenfalls sollte der Druck auf die potenziellen Kunden und den Bestand an Versicherten geprüft werden, der mit einem indirekten Zwang einhergeht, die eigenen Daten zur Gesundheit und Lebensweise preiszugeben.

Dass umgekehrt mit einer möglichst umfangreichen Datenbasis allerdings im Endeffekt die allgemeine Gesundheit durch Förderung einer gesunden Lebensweise steigt, Diagnose und Therapie verbessert werden können, die Kosten für die Versicherer und Versicherten auf breiter Front sinken sowie Ärzte und das gesamte Gesundheitssystem entlastet werden, ist im gesellschaftlichen Diskurs ebenfalls zu berücksichtigen. In diesem Spannungsfeld müssen die Versicherer und die gesamte Versicherungswirtschaft ihren Weg finden. Schwierig wird dabei

die Grenzziehung bei der Datenerhebung, -auswertung und -nutzung zwischen einerseits verhaltensgeprägten Gesundheitsdaten, die der Bürger selbst beeinflussen kann (z. B. durch seine Ernährung, Sport, Schlaf oder den Konsum von bzw. Verzicht auf Alkohol, Zigaretten und Drogen) und für die ihm daher auch eine Verantwortung zugeschrieben werden kann, und andererseits schicksalhaften Gesundheitsdaten (z. B. genetische Disposition).

Die weitere Entwicklung kann bei den Krankenversicherern eine grundlegende Änderung des Geschäftsmodells mit sich bringen. Hierbei ist nicht nur an die Möglichkeiten gedacht, Prämienrabatte für bestimmte Lebensweisen zu geben oder Anreize für Präventionsmaßnahmen zu setzen, um mit den damit sinkenden Behandlungskosten die Policen insgesamt günstiger anbieten zu können. Die aktuelle Marktsituation bietet vielmehr auch Ansätze für die Versicherer, sich in den entstehenden Ökosystemen Gesundheit als Orchestrator oder Zulieferer zu positionieren. Auf diese Weise können Kooperationspotenziale genutzt und die Zusammenarbeit mit Ärzten, Krankenhäusern, Pflegern und anderen Gesundheitsdienstleistern gestärkt werden. Möglicherweise haben dabei andere, schon digitaler aufgestellte Unternehmen und Branchen aufgrund einer ausgeprägteren Technologieaffinität, schlankeren Prozessen und einer höheren Agilität und Flexibilität derzeit einige Wettbewerbsvorteile. Umso wichtiger ist es für die Versicherer, sich auf ihre Kompetenzen zu konzentrieren und sich eine passende Rolle zu suchen.

Gerade in der Lebenswelt Gesundheit ist die Rolle des ‚Enablers‘ für den Versicherer gut vorstellbar: Der Kundenzugang und das hohe Kundenvertrauen könnten genutzt werden, um sich stärker als eine Art vermittelnder Akteur zwischen den Parteien Patient, Arzt, Krankenhaus und Pflegedienstleister zu positionieren und somit für das Gesamtsystem die Schlüsselrolle als Orchestrator eines Netzwerks einzunehmen. Die Daten, die dadurch zusätzlich generiert werden können, sind eine wertvolle Ressource. Mit dieser Möglichkeit geht allerdings auch eine sehr große Verantwortung einher. Wenn alle Daten zentral bei einem Versicherer zusammenlaufen, ist er damit in einem hohen Maß im gesamten Ökosystem für die Datensicherheit der Kunden verantwortlich. Das vorher aufgeworfene Paradoxon, die Übersensibilisierung der Datensicherheit einerseits und der Wunsch nach besseren Gesundheitsleistungen andererseits, muss in dieser Rolle auch maßgeblich von den Versicherern gelöst werden.

In Betracht kommt für ein Versicherungsunternehmen natürlich auch die Rolle des Zulieferers in einem Ökosystem Gesundheit. Hier stellt sich die Frage, welche Kernkompetenzen darin eingebracht werden können. Typischerweise wird es sich dabei um die Risikotragung und die Finanzierung von Gesundheitsleistungen handeln. Eine gute Ausgangsposition haben die Versicherer auch mit ihren

historischen Daten über die Gesundheit, Krankheitsverläufe und Behandlungsdaten ihrer Versicherten, die sie einbringen könnten – wobei natürlich der Datenschutz abermals eine zentrale Rolle spielt. Fallweise kommen weitere Kompetenzen infrage, wie z. B. die Kundenberatung und -betreuung, sowie die Übernahme von Backoffice-Funktionen und -Prozessen (Kalkulationsaufgaben, Abrechnungsleistungen, Datenverwaltung).

2.4 Lebenswelt Mobilität

2.4.1 Smart Services im Überblick

Die Digitalisierung des Automobils sowie die zunehmende Vernetzung von Verkehrsmitteln und der Verkehrsinfrastruktur werden in den nächsten Jahren den größten Wandel im Mobilitätssektor mit sich bringen. Der Kampf um den Kunden verschiebt sich dabei von der Fahrzeugebene auf die Ebene smarter Mobilitätsservices (Bratzel und Teller mann 2018, S. 3 f.). Künftig steht z. B. nicht mehr das Automobil selbst, sondern verschiedene Mobilitätsangebote und damit verbundene Dienstleistungen im Vordergrund. Zentral sind dabei a) die jederzeitige Verfügbarkeit von Mobilität, die durch On-Demand-Lösungen sichergestellt wird, b) die erhöhte Sicherheit im Straßenverkehr, die durch Kommunikation der einzelnen Fahrzeuge untereinander sowie den (Daten-)Austausch der Fahrzeuge mit ihrer Umwelt ermöglicht werden, und c) der Komfort für den Bürger, der durch verschiedene angebundene Services von seinen (Fahr-)Aufgaben entlastet wird und zahlreiche Mehrwertleistungen angeboten bekommt, wie z. B. Entertainment-Lösungen, die ihm das Fahrerlebnis so angenehm wie möglich machen. Der Kunde erhält individuelle ‚Smart Mobility‘-Dienstleistungen bedarfsgerecht je nach seinen persönlichen Präferenzen.

1. *Connected Car*

Laut einer PwC-Studie beträgt die jährliche Wachstumsrate vernetzter Fahrzeuge bis zum Jahr 2022 annähernd 25 % (Ahlemann et al. 2016, S. 24 f.). In den nächsten Jahren werden daher nahezu alle neu produzierten Fahrzeuge mit dem Internet verbunden sein. Dadurch können Informationen und Daten mit anderen Verkehrsteilnehmern, Objekten in der Umgebung oder der Cloud ausgetauscht werden. Der Fahrer eines Connected Car wird über Umweltbedingungen, wie bspw. Verkehrsinformationen und Wetterdaten, informiert, erhält Hinweise von verbundenen Ampelsystemen oder Beschilderungen und tauscht Daten zur Position und Geschwindigkeit mit anderen Verkehrsteilnehmern aus. Dadurch können

Wege optimiert und das Ziel schneller erreicht werden. Der Datenaustausch und die Kommunikation mit anderen Verkehrsteilnehmern helfen zudem, den Verkehr sicherer zu machen und Unfällen vorzubeugen. In diesem Zusammenhang wird oft von der Car-to-Car- bzw. der Car-to-Infrastructure-Kommunikation gesprochen (Bratzel und Tellermann 2018, S. 28).

Daneben ist die fahrzeuginterne Kommunikation ein weiterer Anwendungsfall im Rahmen des Connected Car. Durch im Fahrzeug verbaute Sensorik können potenzielle Mängel vom Fahrzeug selbst erkannt werden, und in den gegebenen Fällen erhält der Fahrer eine Benachrichtigung, die mit einer Handlungsempfehlung sowie einem Hinweis auf die nächste Werkstatt verknüpft sein kann. Dadurch können schadenvorbeugende Maßnahmen ergriffen und Reparatur- und Serviceleistungen optimiert werden (Chaudhuri 2018). Zunehmend gehören zu den fahrzeuginternen Daten auch Sensoren, die im Sitz oder im Lenkrad eingebaut sind und die Vitalparameter des Fahrers messen, um Müdigkeit und gesundheitliche Beeinträchtigungen frühzeitig zu erkennen.

Durch die Vernetzung mit der Umwelt und die Ausstattung mit einem Internetzugang wird ein Echtzeit-Daten-Austausch mit anderen Verkehrsteilnehmern und Geräten ermöglicht, und dem Fahrer stehen zahlreiche digitale Services zur Verfügung, die er während der Fahrt nutzen kann. Dazu gehören Navigationssysteme, Fahrassistenzsysteme, Entertainmentdienste und viele mehr. Darüber hinaus sind die gewonnenen Daten und Schnittstellen nicht nur zum Zweck der Verkehrssteuerung, sondern auch zur Strafverfolgung und für Versicherungsunternehmen nutzbar. Auch lassen sich gezielt personalisierte Werbung sowie standort- bzw. kontextspezifische Angebote einspielen. Bspw. können in der Umgebung befindliche Sonderaktionen, Events oder Spritpreise im Fahrzeugdisplay angezeigt werden.

Neben Bewegungsdaten entstehen im Zusammenhang mit dem Connected Car viele weitere Daten, die durch GPS, Kameras und Sensoren erfasst und verarbeitet werden und durch Nutzungs- und Verhaltensdaten des Fahrers angereichert werden können. Damit gibt der Fahrzeugnutzer einen umfangreichen Einblick in sein Fahrverhalten, seine Nutzungsgewohnheiten bis hin zu Konsumpräferenzen. Neben Fahrzeugdaten können Daten zum Fahrverhalten und -stil, zum Musikgeschmack, Kommunikationsdaten sowie Bewegungsprofile ausgelesen und verarbeitet werden (Bundesverband Digitale Wirtschaft 2018b, S. 2). Das Connected Car stellt die Voraussetzung für weitere Smart Services, wie bspw. das Car- oder Ridesharing und das autonome Fahren, dar.

2. *Carsharing und Ridesharing*

Carsharing meint die gemeinschaftliche Nutzung von Fahrzeugen und deren spontane und kurzfristige Anmietung auf Grundlage einer Rahmenvereinbarung (Carsharinggesetz vom 5. Juli 2017 (BGBl. I S. 2230)). Damit wird Carsharing dem Trend der Sharing Economy und der On-Demand-Lösungen gerecht, indem je nach Bedarf spontan und ortsunabhängig Mobilität bereitgestellt wird.

Zur Nutzung von Carsharing stellt der Kunde seine Anmelde- und seinen Standort über eine App zur Verfügung. In der Folge kann er nahegelegene Fahrzeuge der Carsharing-Flotte ausfindig machen und per App reservieren. Die Fahrpreisabrechnung erfolgt nach in Anspruch genommener Leistung, meist minutengenau. Unterhaltskosten und andere Fixkosten sind in die Nutzungsgebühren eingepreist; dadurch zahlt der Fahrer nur, solange er den Service in Anspruch nimmt, und er muss keine gesonderten Sprit- oder Parkkosten aufwenden. Neben der Bereitstellung und Kurzzeit-Vermietung können dem Kunden ergänzende Dienstleistungen vor, während und nach der Fahrt angeboten werden (ADAC 2018). Beispielsweise kann der Kunde während des Supermarkteinkaufs kostenlos parken und dabei Rabatte im Lebensmittelmarkt erhalten. Im Rahmen des Carsharings werden personenbezogene Daten einschließlich der individuellen Bewegungsdaten über GPS, also u. a. Fahrstrecken, Fahrzeiten, Geschwindigkeiten, das Beschleunigungs- und Bremsverhalten, gesammelt, ferner Daten über das benutzte Fahrzeug. Neben Automobilen können im Rahmen des Bikesharings auch Fahrräder zur Kurzzeitmiete angeboten und damit gemeinschaftlich genutzt werden.

Ein anderer, dem Carsharing verwandter Smart Service ist das Ridesharing, bei dem ebenfalls die gemeinsame Nutzung eines Fahrzeugs im Mittelpunkt steht. Im Unterschied zum Carsharing erfolgt die Nutzung des Fahrzeugs jedoch zeitgleich durch verschiedene Personen (Fahrgemeinschaft). Die Organisation des Ridesharings erfolgt über eine Plattform, auf der anderen Nutzern das eigene Auto zur Mitfahrt angeboten oder selbst nach Mitfahrgelegenheiten gesucht werden kann (Randelhoff 2014). Außer im Rahmen von geplanten Fahrten (Bsp. Bla-bla-car) ist auch das spontane Teilen von Fahrdienstleistern möglich (Bsp. Uber). Insbesondere beim spontanen Ridesharing sind Bewegungs- und Standortdaten Grundvoraussetzung für die Bereitstellung des Smart Services.

3. *Autonomes Fahren*

Die Fahrzeugtechnik befindet sich aktuell in der Entwicklungsstufe der Teilautomatisierung: Das teilautonome Fahrzeug kann vorausfahrenden Automobilen auf geraden Strecken folgen, dabei die Spur und den Abstand halten und bei Ver-

kehrsstau Fahraufgaben auch vollständig übernehmen. In Zukunft ist der vollständig autonome Verkehr möglich, bei dem das Automobil in jeder Situation alle Fahrfunktionen übernimmt und die Fahrt zum automatisierten Shuttle Service wird. Die Fahrzeit kann dann für andere Zwecke genutzt werden und das Fahrzeug verwandelt sich in einen Ort für neue Dienstleistungen (Eckstein et al. 2018, S. 4 f.).

Somit wird das Automobil nicht länger ein reines Fortbewegungsmittel sein, sondern es entwickelt sich zum mobilen Arbeitsplatz, Restaurant oder Hotelzimmer. Der Friseur kann seinen Kunden vor der Haustür abholen und ihn während des Haarschnitts zum nächsten Termin bringen. Das autonome Fahren erzeugt damit einen hohen Komfort und Zeitersparnisse. Ein autonomer Transportservice kann zudem im ländlichen Raum lebende Personen oder ältere Menschen mobiler machen. Ermöglicht wird das autonome Fahren durch eine Echtzeit-Datenanalyse, die mittels Sensoren und Aktoren erfasste Daten wie Lichtzeichen, Verkehrsschilder und andere Verkehrsteilnehmer verarbeitet und intelligent verknüpft.

4. Verkehrsüberwachung

Insbesondere in der VR China ist die digitale Verkehrsüberwachung mittels Datenaufzeichnung auf dem Vormarsch. Vernetzte Kameras und Messsysteme erfassen zahlreiche Daten im öffentlichen Raum, die sich mittels Bilderkennung und künstlicher Intelligenz automatisiert auswerten lassen und eine Reihe neuer Geschäftsmodelle hervorbringen (Wired 2018). So lassen sich bspw. Verkehrsflüsse mittels der gesammelten und analysierten Daten steuern: Vernetzte und mit Sensoren versehene Ampelanlagen erfassen Bild- und Audiodaten und optimieren mit einer smarten Signalsteuerung den Verkehrsfluss, um Staus und Unfälle zu vermeiden. Dies zeigt schon heute ein Feldversuch in der Metropole Peking: Auf der Strecke zwischen Flughafen und Innenstadt wurden alle Daten aus Verkehrsleitsystemen, Kameras und Fahrzeugen mittels künstlicher Intelligenz ausgewertet. Dadurch ließ sich das Verkehrsaufkommen in den darauffolgenden 45 min vorhersagen. Anschließend konnte der Verkehr so gesteuert werden, dass es auf dieser Verbindung keinen Stau mehr gab (Rohkamm 2018).

Automatisierte Verkehrsüberwachungssysteme sind damit in der Lage, das Verkehrschaos in der Stadt zu lösen. Die in der Verkehrsüberwachung aufgezeichneten Daten sind Fahrzeugdaten, Bewegungsdaten, Audio- und Bild-daten sowie personenbezogene Daten. Zudem dient die Verkehrsüberwachung dazu, regelwidriges Verhalten zu erkennen und automatisiert Schritte einzuleiten. Fahrzeuge und Personen, die sich verkehrswidrig verhalten, werden über das Nummernschild oder mittels Gesichtserkennung identifiziert, computergesteuert

werden alle weiteren relevanten Daten zusammengetragen, und eine Ahndung des Regelverstößes kann ohne menschliche Interaktion erfolgen. Dabei werden neben fest installierten Kamerasystemen mittlerweile auch Drohnen eingesetzt, die die mobile Verkehrsüberwachung noch flächendeckender ermöglichen.

5. *Connected Mobility*

Die bisher betrachteten Smart Services beruhen vorrangig auf dem Automobil als Mobilitätsträger. Daneben bestehen viele weitere Verkehrsmittel, deren Verknüpfungen weitere Smart Services hervorbringen. Anbieter wie bspw. moovel bündeln das Angebot verschiedener Mobilitätsdienstleister und Verkehrsformen auf einer Plattform und ermöglichen ihren Nutzern damit Informationen über den Zugang zum individuell besten Angebot (moovel 2018). Verknüpft werden im Rahmen solcher Connected-Mobility-Services typischerweise Car- und Ridesharing, öffentliche Verkehrsmittel, wie Busse und Züge, sowie Fahrdienstvermittlungen (Taxi). Der Nutzer gibt hierfür seinen aktuellen Standort oder einen anderen beliebigen Startpunkt sowie seinen Zielort ein und erhält Informationen über die verschiedenen Reisemöglichkeiten. Neben der Verbindung mit öffentlichen Verkehrsmitteln werden auch Leihfahrräder in der Nähe angezeigt, und zusätzlich hat der Nutzer die Möglichkeit, über die Plattform ein Taxi zu bestellen (Bratzel und Tellermann 2018, S. 30 f.). Der Kunde spart dadurch Zeit und kann bequem in nur einer App Reisemöglichkeiten vergleichen und, je nach Anbieter und bestehender Kooperation, die für ihn beste Option direkt über die Plattform buchen. Voraussetzung für das Angebot einer solchen Plattform ist ein umfassender Datenaustausch zwischen den einzelnen angebotenen Mobilitätsdienstleistern. Zugangs- und Kundeninformationsdaten werden nur einmal eingegeben (bzw. aus dem Google- oder Facebook-Konto abgerufen) und stehen für alle weiteren Dienste zur Verfügung.

2.4.2 **Ausgewählte Geschäftsmodelle innerhalb der Smart Services**

2.4.2.1 **ReachNow**

1. *Beschreibung des Geschäftsmodells*

Die Mobilitätsplattform ReachNow wurde 2016 von BMW ins Leben gerufen. Anfangs war ReachNow ausschließlich in Seattle verfügbar, das Angebot wurde dann aber auf andere Bundesstaaten ausgedehnt und ist seit 2017 auch in Chengdu, China, und damit außerhalb der USA nutzbar. ReachNow kombi-

niert auf seiner per Smartphone erreichbaren Mobilitätsplattform verschiedene Mobilitätsangebote miteinander und stellt seinen Kunden damit eine flexible Lösung zur Verfügung, die von überall in Anspruch genommen werden kann. Der Kunde kann dabei zwischen unterschiedlichen Fortbewegungsmöglichkeiten entscheiden und die für ihn beste Option per Knopfdruck auswählen und buchen. Zwar sind darin auch Kooperationen mit dem öffentlichen Nahverkehr enthalten, im Vordergrund steht jedoch – sicher auch mit Blick auf den Mutterkonzern – nach wie vor das Automobil.

ReachNow bietet drei unterschiedliche Services: Erstens enthält das Angebot die klassische Vermietung von Fahrzeugen. Dabei kann der Kunde per interaktiver App sehen, welche Fahrzeuge wo in der Nähe bereitstehen, das Wunschfahrzeug reservieren und für die geplante Fahrt freischalten. Alle Daten zum Standort, zur Verfügbarkeit sowie verschiedene weitere technische Informationen zum Fahrzeug werden zentral auf der Plattform gespeichert und können jederzeit von den Nutzern eingesehen werden. Das Angebot unterscheidet sich damit kaum von anderen Carsharing-Angeboten wie bspw. DriveNow oder Car2Go. Neben dem klassischen Carsharing bietet ReachNow aber zweitens mit dem Chauffeurdienst und drittens mit dem Reservierungs- und Zustellservice weitere Leistungen: Der Chauffeurdienst als Premiumfunktion der App ist ähnlich dem Angebot von Uber oder DiDi, d. h. auch hier werden dem Nutzer verfügbare Fahrzeuge inklusive Fahrer angezeigt, die per App ausgewählt werden können und den Nutzer auf Wunsch innerhalb weniger Minuten von seinem Standort abholen (Schaal 2016). Beide Parteien, also ReachNow-Kunde und der Fahrer, sind dabei miteinander verbunden: Kontakt- und Standortdaten werden geteilt, sodass der Standort des jeweils anderen jederzeit verfügbar ist. Der Kunde erhält in Echtzeit Informationen über die voraussichtliche Ankunftszeit des Fahrers. Das dritte Angebot, der Reservierungs- und Zustellservice, ist die On-Demand-Lösung der Plattform und erinnert eher an eine Bestellung bei Amazon als an die heute in Deutschland verfügbare Autovermietung: Auf Wunsch wird dem Kunden ein Fahrzeug nach Hause oder zu einem beliebigen anderen Ort gebracht. So kann der Nutzer bspw. angeben, am nächsten Tag zu einer bestimmten Uhrzeit ein bestimmtes Fahrzeug für seinen Weg ins Wochenende zu wünschen, das dann pünktlich vor seiner Haustür bereitsteht. Wird das Fahrzeug nicht weiter benötigt, kann es im ReachNow-Gebiet geparkt und damit auf sehr einfache Weise zurückgegeben werden. Die App informiert den Kunden auch über geeignete Parkflächen. Mittelfristig sollen BMW- und Mini-Eigentümer zudem in der Lage sein, ihren Privatwagen über ReachNow zu vermieten (ReachNow 2018).

Bei ReachNow kann der Kunde aus über 1000 Fahrzeugen von BMW und Mini auswählen. Von Automobilen mit klassischen Verbrennungsmotoren über

Hybride bis hin zu Elektrofahrzeugen steht je nach Präferenz ein passendes Fahrzeug zur Verfügung. Dadurch erhält der Kunde Zugang zu aktuellen Fahrzeugmodellen verschiedener Klassen und Antriebsformen. Um dem Kunden weiteren Komfort zu bieten, haben die Fahrer die Möglichkeit, ihr Smartphone mit dem Entertainment-System des Automobils zu verbinden und so die eigene Musik abzuspielen sowie Messengerdienste und (Video-)Telefonie während der Fahrt in Anspruch zu nehmen. Der Nutzer kann somit die Fahrtzeit im fremden Mietwagen individuell gestalten, was ein hohes Maß an Convenience bedeutet. Dem Anbieter eröffnen sich erneut Anknüpfungspunkte zur Datensammlung sowie zur Anbindung weiterer Services.

Gesamtgesellschaftlich betrachtet wird jedes Fahrzeug, das unter einem Geschäftsmodell wie ReachNow betrieben wird, dank der geteilten Nutzung effizienter ausgelastet. In letzter Konsequenz sinken mit den komfortablen Nutzungsmöglichkeiten per App auch die Motivation und Notwendigkeit, überhaupt ein eigenes Fahrzeug zu besitzen, das die meiste Zeit ohnehin nur geparkt am Straßenrand oder in der Garage steht. Auf längere Sicht entstehen damit insbesondere in den Städten, in denen der Raum ohnehin begrenzt ist, viele wieder alternativ nutzbare Flächen, die bislang von massenhaft parkenden Fahrzeugen in Anspruch genommen werden.

2. Geschäftsmodellanalyse nach dem Business Model Canvas

Das **Wertangebot** von ReachNow liegt in der flexiblen und komfortablen Bereitstellung von Mobilität, die von den Kunden einfach und transparent genutzt werden kann. Ziel des Angebots ist es, individuelle Mobilität je nach Standort, Zielort, Zeitplanung, sonstigen Präferenzen und Budget zu ermöglichen. Neben kurzfristigen On-Demand-Lösungen bietet ReachNow auch Langzeitmieten an, die u. a. auch für Nutzer-Communities zur Verfügung stehen. So können bspw. Firmen oder Wohngemeinschaften ein Fahrzeug mieten und die Nutzung des Fahrzeugs untereinander aufteilen. Abgesehen von der Gruppen-Vermietung an Unternehmen (B2B2C) richtet sich das Angebot von ReachNow an das **Kundensegment** der Endverbraucher (B2C) (Schmidt-Lackner 2016). Zwar wird dabei keine spezielle Kundengruppe fokussiert, die Nutzer werden jedoch häufig in urbanen Gegenden zu finden sein und typischerweise kein eigenes Auto besitzen.

Der vorrangig genutzte **Kanal** ist die ReachNow-App. Zwar gibt es auch eine Webseite sowie Aktivitäten auf verschiedenen sozialen Medien, die als Kommunikationskanäle dienen; die eigentliche Nutzung und damit der Distributionskanal des Wertangebots beschränkt sich allerdings auf die ReachNow-App. Die **Kundenbeziehung** ist durch einen hohen Grad an Automatisierung und Individualisierung gekennzeichnet. Es gibt kaum einen persön-

lichen Kontakt, vielmehr enthält die ReachNow-App eine Reihe unterschiedlicher Self-Service-Optionen, über die der Kunde seine individuelle Dienstleistung buchen kann. Aktuell hat ReachNow über 100.000 Kunden, die mit dem ReachNow-Service bislang mehr als 1,2 Mio. km gefahren sind. Die **Einnahmequellen** von ReachNow setzen sich aus einmaligen Mitgliedsgebühren (15 US\$) und Nutzungsgebühren für die verschiedenen Dienstleistungen zusammen. Die Fahrzeugnutzung wird dem Kunden dabei pro Minute oder bei Langzeitmieten als Tagessatz in Rechnung gestellt.

Die **Schlüsselaktivitäten** zur Umsetzung des Geschäftsmodells bestehen im Betrieb der Plattform, der Bereitstellung und Verwaltung/Pflege der Fahrzeuge sowie der Koordination der angebotenen Partner. Neben der Bereitstellung verschiedener Mobilitätslösungen können auch die in der App erfassten Daten über das Nutzungsverhalten und die Fahrgewohnheiten genutzt werden, um dem Kunden weitere individualisierte Angebote zu stellen. Dies kann durch ReachNow selbst oder die angebotenen **Schlüsselpartner** erfolgen: Über verschiedene Kooperationen mit lokalen Regierungen, anderen Mobilitätsanbietern, Parkplatzbetreibern u. a. werden weitere Dienstleistungen angeschlossen, Rabatte gewährt und die Kundenbindung gefördert. Zudem investiert BMW in die städtische Infrastruktur, bspw. durch die Installation von Ladesäulen. Dadurch können wiederum neue Daten zu Ladezeiten und Tarifen gesammelt werden. Es zeigt sich, dass neben den Fahrzeugen die bereitgestellten und gewonnenen Kundendaten eine **Schlüsselressource** des Geschäftsmodells von ReachNow darstellen. Essenziell sind vor allem die Standort-Daten, die mittels GPS von jedem Fahrzeug sowie allen Nutzern jederzeit bereitstehen und abgerufen werden können. Dadurch ist es möglich, den Nutzern Fahrzeuge in der Nähe anzuzeigen und in Echtzeit nachzuverfolgen, wo sich der Nutzer und das Automobil gerade aufhalten. Neben den Standort- und Bewegungsdaten spielen die Nutzungs- und Verfügbarkeitsdaten eine wichtige Rolle. Jede Fahrzeugnutzung wird aufgezeichnet und alle Informationen über den Zustand des Wagens oder bspw. den Ladestatus von Elektrofahrzeugen sind jederzeit präsent. Auch dadurch kann die Ressource ‚Fahrzeuge‘ optimiert werden. Angereichert werden die Nutzungs- und Fahrverhaltensdaten der Kunden durch Daten, die im Rahmen der verschiedenen Kooperationen von ReachNow entstehen.

ReachNow erhält damit u. a. Informationen, wohin der Nutzer mit dem Auto fährt, wie schnell oder vorsichtig dies geschieht, wie oft er dabei telefoniert und welche Entertainment-Angebote genutzt werden. Dies ermöglicht es ReachNow wiederum, den Kunden passgenaue Produkte oder Dienstleistungen anzubieten – womit die Rückkopplung zu den **Wertangeboten** vollzogen wird.

2.4.2.2 Tesla Software Version 9

1. *Beschreibung des Geschäftsmodells*

Die Tesla Software Version 9 ist ein Fahrassistenz-System, das bei Model S, Model X und Model 3 der Automobile von Tesla eingesetzt wird und diese Fahrzeugmodelle zunehmend autonom steuert. Mit jedem weiteren Softwareupdate erhält das System neue Funktionen, die weitere Aufgaben des Fahrers übernehmen und damit dem Ziel des autonomen Fahrens näherkommen. Zwar trägt der Fahrer noch die Verantwortung und muss die Kontrolle über das Fahrzeug und die Verkehrslage behalten, viele Schritte werden aber bereits selbstständig durch das Fahrzeug durchgeführt.

Dazu gehören eine hindernisabhängige Fahrzeuggeschwindigkeit sowie die Kombination aus Lenkassistent und Spurwechselassistent, die den selbstständigen Spurwechsel des Fahrzeugs ermöglicht. Soll die Spur gewechselt werden, reicht ein einfaches Antippen des Blinkers. Mithilfe der am Fahrzeug angebrachten 360-Grad-Kameras beobachtet das Fahrzeug den Verkehr der benachbarten Spuren und wechselt im geeigneten Zeitpunkt auf die angrenzende Fahrbahn. Neben dem Spurwechsel ist damit auch die eigenständige Nutzung von Autobahnausfahrten möglich, wobei das Navigationssystem mittels der bereitgestellten Daten die optimale Route und die passende Ausfahrt selbst auswählt – die mit dem Lenk- und Spurwechselassistenten selbstständig befahren werden kann. Auch Anschlussstellen kann der Autopilot selbstständig ansteuern. Unterstützend wirkt dabei die ebenfalls neu verfügbare Totwinkelwarnung, mit der nun auch die Seite und das Heck des Autos kontrolliert werden und die vor Hindernissen im toten Winkel der Spur warnt, auf die eingeschert werden soll. Radfahrer oder andere Verkehrsteilnehmer werden vollautomatisch registriert und die Geschwindigkeit wird der Gefahrensituationen zur Unfallvermeidung angepasst.

Die Anpassung der Fahrtgeschwindigkeit an den Verkehr erfolgt selbstständig durch das Automobil, ohne dass ein manueller Eingriff erforderlich ist. Über acht außen am Fahrzeug befindliche Kameras zeichnet Tesla Videodaten über die Fahrzeugumgebung auf, die in Echtzeit im Bordcomputer verarbeitet werden. Dabei werden Informationen mit einer Reichweite von bis zu 250 m einbezogen. Die 360-Grad-Visualisierung des Fahrzeugs gewährleistet eine ganzheitliche Überwachung des Verkehrs und unterstützt die Reaktion auf die wahrgenommene Umgebung. Dafür werden durch die Software Version 9 neben Video- auch Ultraschall- und Radarsignaldaten analysiert, sodass auch durch dichten Nebel oder vorausfahrende Fahrzeuge hindurch Daten gesammelt werden können. Die Videodaten können aufgezeichnet und gespeichert werden (Tesla 2018a).

Dadurch soll bspw. bei einem Unfall die Ursache leichter aufgedeckt werden können. Ergänzend werden weitere Funktionen, wie die Parkplatzsuche und das Einparken, autonom vom Fahrzeug durchgeführt. Allein die rechtliche Situation erfordert (noch) das Vorhandensein eines menschlichen Insassen mit Führerschein.

2. Geschäftsmodellanalyse nach dem Business Model Canvas

Bei der Geschäftsmodellanalyse nach dem Business Model Canvas muss zwischen dem Geschäftsmodell Tesla und der Softwareversion 9 unterschieden werden. Einige der Kernelemente des Business Model Canvas können für die Version 9 nicht angewandt werden; insoweit erstreckt sich dann die Analyse auf das Geschäftsmodell von Tesla im Allgemeinen.

Das **Wertangebot** der Tesla Version 9 liegt vornehmlich in der Unterstützung des Fahrers bei seinen Fahraufgaben. Durch teilautonomes Fahren wird der Fahrer entlastet, und er soll künftig in der Lage sein, sich während der Fahrt auf andere Interessen als das Steuern seines Fahrzeugs zu konzentrieren. Zudem sollen Unfälle vermieden und zu einer höheren Verkehrssicherheit beigetragen werden. Soweit dennoch Unfälle eintreten, sollen die Erfassungs- und Beweismöglichkeiten für die Verursachung verbessert werden (Tesla 2018b). Daneben ist der Prestige-Gewinn eines autonom gesteuerten Oberklassefahrzeugs für viele Kunden ein weiteres Kaufargument. Das angesprochene **Kundensegment** von Tesla-Fahrzeugen sind vorrangig Endkunden (B2B), ebenso sind aber auch B2B2C-Lösungen, bspw. über Leasing, möglich. Im B2B-Markt stellt das Fahrzeug besonders für innovative oder ökologisch orientierte Unternehmen eine Alternative zu herkömmlichen Oberklassendienstwagen dar. Als konkrete B2C-Zielgruppe stehen Nutzer höherer Einkommensklassen im Vordergrund, die technologischen Neuerungen gegenüber aufgeschlossen sind. Die **Kundenbeziehung** und -bindung werden über das Fahrzeug selbst gepflegt, indem regelmäßige Updates erscheinen und dadurch der Kontakt zu Tesla fort-dauernd aufrechterhalten wird. Neben dem Fahrzeug selbst sind für Tesla die Flagship-Stores in ausgewählten Städten ein wichtiger **Kanal**, über den mit dem Kunden interagiert und Fahrzeuge abgesetzt werden. Des Weiteren werden unterschiedliche Foren und Communities als Kommunikationskanäle genutzt, über die Tesla Kunden gewinnen und binden möchte.

Primäre **Einnahmequelle** ist der Verkauf von Fahrzeugen. Daneben werden auch durch die Nachrüstung bspw. mit Kamerapaketen sowie über Reparaturen und Wartungsarbeiten Einnahmen generiert. Eine zusätzliche, wenn auch nur kleine Einnahmequelle sind Subventionen der Forschungs- und Entwicklungsarbeit im Bereich autonomer Fortbewegung, die Tesla von unterschiedlichen

Institutionen oder Förderprogrammen erhält. Daneben ermöglichen wiederum Kundendaten das Anbinden zusätzlicher Services, die eine zusätzliche Einnahmequelle darstellen können. Die **Schlüsselaktivitäten**, die zur Umsetzung des Geschäftsmodells notwendig sind, sind die Forschung und Entwicklung sowie die Produktion von Fahrzeugen. Die Software, die die autonome Fortbewegung steuert, bindet keine Kooperationen ein, weshalb es insofern keine **Schlüsselpartner** gibt. Als Grund hierfür nennt Tesla die Gefahr eines Verlusts von Know-how und erhöhter Fehleranfälligkeit bei verteilten Kompetenzen. Kooperationen und Partnerschaften gibt es nur bei Tesla-Komponenten, die keine autonomen Fahrfunktionen steuern (bspw. Partnerschaften im Bereich der Ladestationen und der Batterieentwicklung). Damit umfangreichere Daten generiert werden können, fallen **Kosten** für die Softwareentwicklung an, und die Fahrzeuge müssen entsprechend aufgerüstet und mit Kamerasystemen und Sensoren ausgestattet sein. Außerdem verursachen die Pflege der IT-Systemlandschaft und die Rechenzentren, die von Tesla eingesetzt werden, hohe Kosten. Zu den **Schlüsselressourcen** von Tesla zählen zunächst Rohstoffe und Personal zur Entwicklung und Produktion von Fahrzeugen. Die Schlüsselressource des Systems, das das autonome Fahren ermöglicht, ist die Tesla-Software, die wiederum nur mit den Fahrzeug- und Umgebungsdaten funktioniert – die also letztlich maßgebliche Schlüsselressourcen für das **Wertangebot** von Tesla darstellen.

2.4.3 Spannungsfeld Datennutzung und Datenschutz

Datengetriebene Services in der Lebenswelt Mobilität bieten nicht nur eine höhere Sicherheit im Straßenverkehr,⁹ sie ermöglichen auch eine neue Form der Flexibilität und Bequemlichkeit, bei der zahlreiche unterschiedliche Mobilitätsformen jederzeit und für jeden bereitstehen. Darüber hinaus enthalten Smart Services in der Lebenswelt Mobilität zahlreiche Komponenten, die den Komfort der Bürger erhöhen, wenn sie sich im öffentlichen Raum bewegen. Beispielsweise können bequem verschiedene Transportmittel für eine Reise nach den Präferenzen der Nutzer aufeinander abgestimmt und miteinander verknüpft

⁹Nach wie vor ist der häufigste Grund für Unfälle das Abkommen des Fahrzeugs von der Fahrbahn, oft durch Unachtsamkeit. Durch intelligente Assistenzsysteme, die den Fahrer durch die Auswertung von Videodaten bspw. beim Halten der Spur unterstützen (Spurhalte-systeme), können Unfälle vermieden und die Sicherheit im Straßenverkehr erhöht werden.

werden, bei Autofahrten wird die Parkplatzsuche erleichtert oder obsolet, und die Bezahlung erfolgt einfach per App (Goodwall et al. 2017, S. 114 f.). Ermöglicht wird dies durch das Erkennen und Auswerten der Bedürfnisse und typischen Verhaltensweisen verschiedener Straßenverkehrsteilnehmer, die Bereitstellung verschiedener Mobilitätsformen, ergänzender Services sowie Bezahlsysteme.

Im Hinblick auf die Datenerhebung ergibt sich in der Lebenswelt Mobilität eine Besonderheit: Zum einen geht es um die eigenen Daten, die bspw. ermöglichen, dass jederzeit und von überall auf verschiedene Dienste zugegriffen werden kann (Bsp. Apple CarPlay¹⁰) oder auf Basis persönlicher (Standort-).

Daten nutzerorientierte Empfehlungen abgegeben werden (Bsp. Google Maps). Daneben ist im Bereich der Mobilität auch die Interaktion mit anderen Personen und Objekten erforderlich (z. B. bei Navigationsservices und beim autonomen Fahren), d. h. es müssen auch Daten Dritter verfügbar sein und verarbeitet werden, um smarte Services zum Nutzen aller zu generieren. Dies sei noch etwas näher erläutert:

Moderne Fahrzeugmodelle sammeln mit einer großen Menge eingebauter Sensoren schon heute Daten über die gefahrene Geschwindigkeit, das Beschleunigungs-/Brems- und Kurvenverhalten, die gefahrenen Gänge und Drehzahlen, die Abstimmung des Fahrgestells (z. B. Öko, Komfort, Sport), womöglich auch den eingestellten Radiosender und natürlich die Ausgangs- und Zielorte sowie Routen. Dadurch können relevante Informationen zum Fahrzeug und dessen Nutzung ausgewertet werden. Zugleich werden Verhaltensdaten der Fahrer erfasst, die dazu geeignet sind, Bewegungsprofile zu erstellen, das Fahrverhalten zu analysieren, um auf dieser Grundlage Smart Services anzubieten. So ermöglichen Standort- und Bewegungsdaten überhaupt erst die Lokalisierung einer Person und/oder ihres Fahrzeugs. Dadurch können geeignete Angebote in der Nähe ausfindig gemacht werden (bspw. Tankstellen, Parkplätze, Restaurants, Sehenswürdigkeiten) und in Kombination mit den Standort- und Bewegungsdaten anderer Personen und Fahrzeuge eine Einordnung in das Umfeld sowie ein Gesamtbild der Verkehrssituation erzeugt werden (Goodwall et al. 2017, S. 119 f.). Solcherart Daten werden bspw. von Navigationsgeräten genutzt, um das Verkehrsaufkommen zu analysieren und zu prognostizieren sowie optimale Verkehrsrouten zu bestimmen – und damit zu einer effizienten Verkehrssteuerung (weniger Staus, weniger Unfälle) beizutragen. Zudem ermöglicht der

¹⁰Apple CarPlay ermöglicht die Nutzung aller möglichen Dienste (persönliche Musik hören, navigieren, Nachrichten schreiben) im Auto.

gesamthafte Verkehrsüberblick, akute Gefahrensituationen zu erkennen (z. B. ein brennendes Fahrzeug hinter einer Kurve auf der Landstraße), um daraus Handlungsempfehlungen abzuleiten und die Sicherheit im Straßenverkehr zu erhöhen.

Wie in anderen Lebenswelten auch, ist allerdings der Datenschutz ein resstringierender Faktor, der im Mobilitätssektor verschiedene Aufgaben erfüllen soll. Dazu gehören der Schutz der informationellen Selbstbestimmung sowie der Privatsphäre. Soweit eine Zuordnung von Daten zum polizeilichen Kennzeichen oder der Fahrgestellnummer – bzw. letztlich zum Fahrer oder Halter selbst – erfolgt oder ermöglicht wird, handelt es sich um personenbezogene Mobilitätsdaten, die der Anwendung der EU-DSGVO unterliegen. Hinzu kommt, dass die Datenaufzeichnung nicht – wie in der Lebenswelt Wohnen vorrangig der Fall – freiwillig und im privaten, geschlossenen Umfeld erfolgt, sondern im öffentlichen Raum stattfindet und dadurch der individuelle Bürger wenig bis keine Chancen hat, sich dieser zu entziehen. Dadurch besteht die Gefahr einer Verwendung, die nicht nur Smart Services unterstützt oder vor Verkehrsdelikten und Verkehrsunfällen schützt, sondern auch eine umfassende Überwachung der Bürger ermöglicht. Sowohl Regelungen der Datenhoheit als auch des Datenschutzes sind daher auch im öffentlichen Interesse. Die vertrauensvolle Preisgabe von Informationen durch die Nutzer und ein adäquater Schutzstandard sind daher essenziell für die Entwicklung und die Nutzung smarter Mobilitätsservices.

Damit ist nicht nur der Schutz vor Datenmissbrauch gemeint – wie z. B. dem Missbrauch von Bewegungsprofilen oder einer unter Umständen unfairen Bepreisung von Smart Services in Notlagen (Gründinger 2018, S. 3). Auch durch Hackerangriffe auf sensible Schnittstellen zwischen der Software des Fahrzeugs und anderen vernetzten Verkehrsteilnehmern und mobilitätsrelevanten Infrastruktureinrichtungen (Ampeln, Bahnübergänge, Zugbrücken, Tunnelschranken) können erhebliche Schäden angerichtet werden. Außerdem kann das Connected Car über ein Botnet¹¹ angegriffen werden. Damit bestehen erhebliche Sicherheitsrisiken, dass Hacker die Kontrolle über die vernetzten Fahrzeuge erlangen oder zumindest die Fahrer die Kontrolle über ihre Automobile verlieren. Insbesondere während der Fahrt hätte dies fatale Auswirkungen auf die Verkehrssicherheit: Unfälle könnten herbeigeführt und der Verkehr könnte vollständig gestört oder lahmgelegt werden.

¹¹Ein Botnet oder Botnetz ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots. Die Bots laufen auf vernetzten Rechnern, deren Daten und Netzwerkanbindung ohne Einverständnis des Datensouveräns zur Verfügung stehen.

Wer den Zugang und die Kontrolle über die gesammelten Mobilitätsdaten erhält, wird entscheidend an der Gestaltung und dem Angebot künftiger Fortbewegungsmöglichkeiten mitwirken. Neben Automobilherstellern sind es zunehmend auch neue Wettbewerber, wie Tech-Unternehmen oder Softwareentwickler, die über ihre Plattformen und Apps insbesondere im Bereich Connected Car Einblicke in Fahrzeug- und Verhaltensdaten der Nutzer erhalten (Becker und Pawelke 2015). Die Frage, wem welche Daten gehören, ist dabei oft noch nicht abschließend beantwortet.

Allerdings ist auch eine zu enge Regulierung hinderlich. So warnen z. B. Automobilhersteller in Deutschland und Europa vor zu starken gesetzlichen Einschränkungen und befürchten, dass die Europäische Union im Gegensatz zu Ländern wie China oder den USA zu enge Grenzen für die Nutzung der Mobilitätsdaten setzt. Damit werden nicht nur Smart Services behindert, sondern auch die unternehmerische Wettbewerbsfähigkeit aufs Spiel gesetzt. Unterschiedliche länderspezifische Regelungen und divergierende Rechtsprechungen betreffen z. B. das autonome Fahren: So ist der Fahrassistent von Tesla bislang nur in den USA und (noch) nicht in der EU verfügbar.¹² Aufgrund teilweise deutlich großzügigerer Datenschutzrichtlinien haben Unternehmen außerhalb Europas insgesamt weit größere Spielräume, datenbasierte Mobilitätsdienstleistungen zu erforschen und anzuwenden.

Innovative Smart Services, wie das autonome Fahren und Ride Sharing, werden in jedem Fall kommen und sich weiter ausbreiten – ob die Angebote in den USA, China oder Europa entwickelt werden und in welchen Ländern die Wertschöpfung erfolgt, ist dafür nicht maßgeblich. Und sie werden mittelfristig auch ganze Branchen und Arbeitswelten verändern. Traditionelle Arbeitsplätze werden in Gefahr geraten, die durch eine intelligente und vernetzte Datenverarbeitung sowie datengesteuerte Automatisierung überflüssig werden (Oliver Wyman 2018). Das beste Beispiel ist der Taxifahrer, der zuerst durch Uber und Didi und in nicht allzu ferner Zukunft durch Künstliche Intelligenz ersetzt wird. Automobile werden zu Dienstleistungsorten, in die während der Fahrt Nachrichten übermittelt, in denen bildschirmgestützte Beratungsgespräche geführt und die Haare geschnitten werden können. Autonom gelenkte Fahrzeuge von Flottenanbietern werden zunehmend Privatwagen ersetzen, d. h. die Nachfrage nach einem eigenen Fahrzeug sinkt (Bratzel und Tellermann 2018, S. 13).

¹²In den USA hat der Kongress bereits ein Gesetz für autonom fahrende Fahrzeuge erlassen, in der EU sind viele Punkte noch offen.

Dies wird auch Druck auf politische Rahmenbedingungen erzeugen. Diesbezüglich steht Deutschland, ein Land, dessen Wirtschaft besonders stark vom Automobil abhängt (Herstellung, Finanzierung, Versicherung), im besonderen Fokus, Lösungsvorschläge anzubieten. Und dies wiederum erfordert auch die Kooperation von Politik und Gesetzgebung mit den betroffenen Branchen und Verbraucherschutzeinrichtungen, ein ausgewogenes Verhältnis zwischen den Möglichkeiten der Datennutzung und den Notwendigkeiten des Datenschutzes rund um smarte Mobilitätsdienstleistungen herzustellen.

2.4.4 Rolle der Versicherer

Die Lebenswelt Mobilität ist seit jeher von einer großer Veränderungsdynamik geprägt. Die Fortbewegung spielt für die Menschen immer eine große Rolle, und die Wichtigkeit einer schnellen und komfortablen Fortbewegung von A nach B gewinnt in einer zunehmend globalisierten Welt fortwährend an Bedeutung: Mehr als eine Billion Euro investieren private EU-Haushalte pro Jahr, um mobil zu sein. In Deutschland fließt jeder siebte Euro in Mobilitätsangebote, und es entstehen immer neue Mobilitätsformen (ADAC 2017, S. 6). Der Mobilitätssektor ist daher von einer hohen Aufmerksamkeit geprägt, die mit einem intensiven Wettbewerb einhergeht.

Nach wie vor ist das Automobil das wichtigste Verkehrsmittel, jedoch verändert sich seine Bedeutung rasant und es vollzieht sich eine Entwicklung, bei der das Auto immer weniger Symbol der Freiheit und des Status ist. Nicht nur aufgrund überfüllter Straßen verliert das eigene Fahrzeug langsam an Attraktivität und Bedeutung und wird zunehmend durch neue Mobilitätsangebote abgelöst. Auch der Einstellungswechsel weg vom ‚Eigentum‘ hin zur ‚Nutzung‘, der mit den aufkommenden Sharing-Konzepten einhergeht, verschiebt die Gewichtungen. Mit der Etablierung verschiedener Smart Services verlegt sich der Fokus von der Ingenieurstechnik und der Hardware auf agile und komfortable Lösungen. Der veränderte Markt, der bisher von Automobilherstellern und Verkehrsbetrieben geprägt war, bringt zusätzlich neue Wettbewerber mit sich. Mit den beschriebenen Smart Services in der Lebenswelt Mobilität verändert sich auch das Geschäftsmodell der Versicherer.

Die zunehmende Vernetzung im Zusammenhang mit dem Connected Car bringt für die Assekuranz sowohl Potenziale als auch Herausforderungen mit sich. Durch die mit zahlreichen Sensoren ausgestatteten Automobile können Unfälle verhindert, Unfallhergänge rekonstruiert und eingetretene Schäden durch das Fahrzeug selbst gemeldet, automatisiert erfasst und begutachtet wer-

den. Die Schadensabwicklung kann damit deutlich schneller und reibungsloser erfolgen, wozu auch neue Technologien wie Chatbots und – in der Logistik – Drohnen beitragen. Damit werden die Prozesse der Versicherer effizienter, und auch für die Kunden werden die Abläufe deutlich vereinfacht und komfortabler gestaltet. Die Abrechnung erfolgt objektiver und damit grundsätzlich fairer, Versicherungsbetrug wird eingedämmt, und nicht nur der Verwaltungsaufwand für die Versicherer sinkt durch die datengetriebenen Services, vermutlich reduziert sich auch das Streitpotenzial bei der Schadenregulierung, was im Ergebnis auch Gelassenheit und Zufriedenheit auf der Kundenseite erhöhen könnten. Jedoch ist der Zugang zu den relevanten Daten für die Versicherer erschwert. Die Daten werden von Systemen generiert, die im Fahrzeug verbaut sind, oder von Kommunikationsmedien, wie dem Smartphone. Damit sind es zunächst die Autohersteller, Telekommunikationsanbieter bzw. Tech-Konzerne, die mit dem Connected Car wertvolle Mobilitätsinformationen einschließlich Informationen über das Fahrverhalten bekommen.

Schon für die Entwicklung und Etablierung von Telematik-Tarifen benötigt aber auch der Versicherer solche Verhaltensdaten, zu denen auch Zugang gewonnen werden kann, wenn der Nutzer die Informationen ausdrücklich mit dem Versicherer teilt. Während Automobilhersteller oder Tech-Unternehmen aber den Vorteil haben, anhand der ausgewerteten Daten tatsächliche Mehrwerteleistungen und neue Smart Services anbieten zu können, sind die Anwendungen der Versicherer bislang noch weitestgehend auf die Kalkulation der versicherungstechnisch richtigen Prämienhöhe und damit auf eine Prämien-differenzierung reduziert, die naturgemäß nur den ‚guten Risiken‘ nützt, also den Risiken mit unterdurchschnittlichen Schadenerwartungswerten. Nach den Regeln der Statistik ist aber immer auch rund die Hälfte der Risiken mit überdurchschnittlichen Schadenerwartungswerten unterwegs, für die Telematik-Tarife eher nachteilig wären. Abgesehen davon, dass allerdings die Korrelationen zwischen dem Fahrverhalten und der Schadenträchtigkeit noch keineswegs hinreichend sicher ermittelt sind und deshalb Telematik-Tarife noch in Kinderschuhen eines Versuchsstadiums stecken, sind damit die unmittelbaren Nutzenpotenziale auf bestimmte Kundengruppen eingeschränkt. Nur wenn es den Versicherern gelingt, über gesellschaftlich hoch akzeptierte Anreiz- und Sanktionsmechanismen die Motivation für ein ‚besseres‘ Fahrverhalten auf breiter Front zu erhöhen, ist damit ein Nutzen für die gesamte Kundschaft in der Kfz-Versicherung generierbar – bis hin zu einem Beitrag für den gesamtgesellschaftlichen Nutzen einer reduzierten Zahl von Unfällen mit Sachschäden, Verletzten und Toten. Insgesamt liegt die große Herausforderung der Versicherungswirtschaft darin, mit den neu gewonnen Mobilitätsdaten echte Mehrwerte für die Kunden und Nutzenpotenziale auch

jenseits einer für einzelne Zielgruppen günstigeren Tarifierung und Prämieeinstufung zu erzeugen.

Die Rolle der Versicherer ändert sich des Weiteren durch das Car- und Ridesharing als immer mehr aufkommende Smart Services. Damit sind zunächst Herausforderungen verbunden, weil mit den Sharing-Konzepten zum einen der Gesamtbestand zu versichernder Fahrzeuge zurückgeht und sich zum anderen die klassischen Deckungskonzepte nicht mehr ohne Weiteres anwenden lassen. Zur Fortbewegung mit dem Auto ist der Bürger nicht mehr länger vom Vorhandensein eines eigenen Fahrzeugs abhängig. Damit sinkt die Nachfrage nach dem eigenen Automobil und damit auch nach privaten Kfz-Versicherungen (Jäckel 2017). Der Nutzer eines Carsharing-Dienstes möchte lediglich die Möglichkeit einer flexiblen Mobilität in Anspruch nehmen, wird sich darüber hinaus jedoch mit dem Fahrzeug – das er nur für kurze Zeit nutzt – nicht weiter beschäftigen. Wichtig sind ihm lediglich die Sicherheit, der Komfort und die Effizienz der Mobilität, also die Erhältlichkeit und Funktionstüchtigkeit des Fahrzeugs, die eigene Fahr-sicherheit sowie die Absicherung, falls doch etwas passiert ... und das Ganze zu einem günstigen Preis.

Der Versicherungsschutz muss in diesem Paket bereits enthalten sein, und der Nutzer möchte sich für seine flexibel und fallweise gewählten Fahrten nicht damit auseinandersetzen. Ein naheliegendes Szenario ist also, dass die Fahrzeuge künftig viel häufiger von einem OEM oder Mobilitätsanbieter und nicht vom Bürger selbst versichert werden. Die private Kfz-Versicherung dürfte damit auf Sicht immer mehr durch Policen für Fahrzeugflotten und Poolfahrzeuge abgelöst werden (Thiele und Schmidt-Jochmann 2015, S. 29). Damit verändert sich nicht nur die Tarifierung, sondern auch der Zugang zum Endkunden geht für den Versicherer zunehmend verloren. Einen noch größeren Einfluss auf die Kfz-Versicherung nimmt das autonome Fahren. Es ist zu erwarten, dass das Unfallrisiko mit autonomen Fahrzeugen erheblich sinkt und einzelne Fahrzeugversicherungen für Privatpersonen und vermutlich auch Flottenversicherungen für Geschäftskunden entbehrlich werden könnten. Ohne einen Fahrzeugführer – und wenn das Fahrzeug noch nicht einmal mehr ein Lenkrad aufweist, über das in die Steuerung eingegriffen werden könnte – wird dem Nutzer des Fahrzeugs auch kein Verschulden mehr für einen Unfall zugewiesen werden können und wird folglich auch kein individueller Versicherungsschutz mehr für den Fahrzeuglenker erforderlich sein. Die Verschiebung der Risikosituation liegt damit auf der Hand: Die Eintrittswahrscheinlichkeit eines Schadens sinkt, dafür erhöhen sich die Schadenssummen angesichts der eingesetzten Technologie und möglicher Kumulationen. Für Unfälle kann kein Fahrer mehr, sondern muss der Hersteller oder müssen Komponentenlieferanten haftbar gemacht werden.

Der Fokus verschiebt sich damit von der Absicherung menschlicher Fehler auf die Absicherung technischer Ausfälle oder Manipulationen. Bereits kurz- bis mittelfristig wird die fortschreitende Entwicklung der autonomen Fortbewegung das Portfolio der Versicherer weiter verändern. Neuere, zunehmend digital vernetzte Kraftfahrzeuge mit vermehrten Assistenzfunktionen bis hin zu weitgehender oder vollkommener Autonomie haben im Gegensatz zu älteren, noch im Großen und Ganzen analogen, Fahrzeugen eine geringere Unfallwahrscheinlichkeit, und die Insassen sind besser geschützt – mit allen Konsequenzen für die Begleitung der Veränderungen durch die Versicherungswirtschaft mit Korrelationsforschungen und der Entwicklung passender Deckungskonzepte und Tarifierungssysteme.

Ein weiterer, besonders wichtiger Trend in der Lebenswelt Mobilität ist die Intermodalität, also die Kombination verschiedener Verkehrsmittel. Zwar kommen die einzelnen Verkehrsmittel nach wie vor typischerweise von verschiedenen Anbietern – neue Mobilitätsformen/-angebote oftmals sogar von ganz neuen Unternehmen, wie Busanbietern (z. B. FlixBus) oder Plattformbetreibern für Car- und Ridesharing, es lassen sich aber zunehmend Konsolidierungen beobachten. Automobilkonzerne entwickeln eigene Sharing-Dienste und kaufen Mobilitäts-Start-ups auf. So hat z. B. Daimler mittlerweile u. a. den Mitfahr-Pionier flinc, das Taxi-Start-up myTaxi und auch den Carsharing-Dienst car2go übernommen. Die Zahl der relevanten Marktakteure scheint also zu sinken, und dem Kunden stehen immer mehr Angebote aus einer Hand zur Verfügung.

Für den Bürger entstehen damit Vorteile: mit der moovel¹³-App können verschiedene Verkehrsmittel für eine bestimmte Route ausgewählt, reserviert, gebucht sowie bezahlt werden und die urbane Mobilität wird für ihre Nutzer vereinfacht. Aufgrund der großen Bedeutung einer einfachen und flexiblen Kombinierbarkeit einzelner Angebote ist gerade in der Lebenswelt Mobilität die Rolle des Orchestrators von herausragender Bedeutung und als Voraussetzung für die intermodale Mobilität anzusehen. Diese Rolle wird von Versicherern schwer einzunehmen sein, da sie im Vergleich zu den Automobilherstellern über eine geringere Größe, weniger Ressourcen – inkl. des Pools an smarten Daten – und meist einen deutlich schlechteren Zugang zum Kunden verfügen. Es muss daher eher eine andere Rolle gefunden werden, sich in dieser Lebenswelt zu positionieren.

Im Zusammenhang mit der Intermodalität könnte das Angebot einer Mobilitätsversicherung einen Lösungsansatz bieten. Die Versicherungspolice könnte

¹³100 %ige Tochter der Daimler AG.

sich damit an ein Ökosystem der vernetzten Mobilität andocken und neben Schäden bei der Nutzung einzelner Fortbewegungsmittel auch die Nichtverfügbarkeit eines Carsharing-Fahrzeugs, die Verspätung eines öffentlichen Verkehrsmittels oder den Ausfall von weitergehenden Services bzw. Mehrwertdiensten abdecken, die rund um die Mobilität von den Anbietern versprochen wurden. Mit der Absicherung von Kfz-Schäden allein wird sich im Rahmen vernetzter Fahrzeuge nicht mehr lange ein Alleinstellungsmerkmal aufrechterhalten lassen. Durch die immer seltener werdenden Schäden, die sich immer besser prognostizieren lassen, ist damit zu rechnen, dass die verbleibenden Schäden künftig auch von den Automobilherstellern selbst übernommen werden (wie beispielsweise bei Tesla). Eine Neuausrichtung ist für die Versicherer daher unumgänglich.

2.5 Utopien und Dystopien

2.5.1 Utopien: Möglichkeiten und gesellschaftlicher Nutzen

Die Beschreibung der Smart Services und die Analyse bestehender Geschäftsmodelle in den Lebenswelten Wohnen, Gesundheit und Mobilität haben gezeigt, dass die Analysen von Daten – auch von personenbezogenen Daten – für die Entwicklung neuer, umfassender Mehrwerte für die Bürger genutzt werden können. Die Sicherheit der Menschen kann durch smarte Lösungen erhöht, der Komfort kann gesteigert und Ressourcen können effizienter eingesetzt werden.

Schon heute besteht z. B. die Möglichkeit, einen Großteil der Wohnumgebung so zu steuern, dass alltägliche Arbeit und Aufgaben des Bewohners entfallen und durch datenbasierte Systeme übernommen werden können. Durch den Einsatz smarter Sensoren können Risiken wie Feuer (smarte Rauchmelder) und Feuchtigkeit (Leckage-Sensoren) nicht nur frühzeitig erkannt werden, vielmehr können sensorgesteuert auch präventive Maßnahmen ergriffen und Schäden von vornherein verhindert werden. Ergänzend können z. B. smarte Thermostate und Lichtsysteme die Wohnumgebung per App oder Sprachsteuerung auf die individuellen Bedürfnisse des Bewohners anpassen und damit den Lebenskomfort erhöhen und die Energieeffizienz steigern.

Doch gerade in der Lebenswelt Wohnen stecken die Smart Services noch in den Kinderschuhen; vieles ist zwar theoretisch schon möglich, kommt aber – gerade in Deutschland – bislang kaum zum Einsatz. Die Gründe dafür sind vielfältig und reichen von einer teils noch komplizierten Handhabung (Stichworte: Installation und Konnektivität) bis hin zu Sicherheits- und Datenschutzbedenken

der potenziellen Nutzer. Während aktuell noch ein gewisser Grad an technischer Versiertheit als Grundvoraussetzung für die Nutzung von Smart Home-Technologien gilt, die eher bei den jüngeren ‚Digital Natives‘ anzutreffen ist (die vielfach noch gar keine eigene Wohnung besitzen), adressieren die Angebote künftig mehr und mehr auch Familien und ältere Menschen, die ohne nennenswerte Technologieaffinität und mittels einer immer intuitiveren Bedienbarkeit die Nutzenpotenziale der Smart Home-Lösungen erkennen. Durch smarte Assistenten wie Amazon Alexa oder Lingxi Voice Assistant¹⁴ können die Funktionen auch allein über die Sprache gesteuert werden. Der nächste Entwicklungsschritt nach der Sprachsteuerung ist die Gestensteuerung. Statt Alexa zu bitten, die Musik etwas leiser zu stellen, reichen dann einfache Handbewegungen, mit der die Lautstärke reguliert (wie bereits bei den AirPods, den Bluetooth-Kopfhörern von Apple, möglich), die Tür geöffnet oder das Rollo nach unten gefahren werden können.

Die Kombination von Touchscreens, Sprach- und Gestensteuerung in allen Lebenswelten stellt fast den Höhepunkt an Komfort für die Nutzer dar, die nur noch durch direkte Gedankensteuerung übertroffen werden kann (was inzwischen als Ergebnis neurologischer Forschungen auch nicht mehr unmöglich scheint). Und in der Lebenswelt Gesundheit entstehen dadurch Potenziale für eine effiziente computergesteuerte Unterstützung und Versorgung eingeschränkter Menschen z. B. mittels Roboter und Künstlicher Intelligenz. Noch weitergehend ist gar an die heute noch utopisch anmutende Möglichkeit zu denken, querschnittsgelähmten Menschen über Gehirnsignale, die unter Überbrückung der geschädigten Wirbelsäule über einen externen Sensor an die Nerven in den Beinen weitergeleitet werden, wieder zum Gehen zu verhelfen. Voraussetzung dafür sind weitere Forschungen über die Zusammenhänge von Gedanken und Gehirnströmen, die in datengesteuerte Systeme zu übersetzen sind.

Gerade die Skepsis, die der Technologie entgegengebracht wird, hemmt aber die Entstehung umfassender Mehrwerte und den gesellschaftlichen Nutzen. Datenanalyse und Künstliche Intelligenz sind auf Big Data angewiesen. Bspw. können in der Lebenswelt Wohnen zwar die individuellen Gewohnheiten und Routinen eines Nutzers analysiert werden, und das smarte Home kann sich auf die Bewohner einstellen. Allgemeingültige Regeln können bisher jedoch nur thesenbasiert aufgestellt und nicht vom System selbst erlernt werden, da die Datenbasis zu gering ist. Wäre jedes Haus ein Smart Home und jedes Auto-

¹⁴Chinas Pendant zu Amazon Alexa.

mobil ein Connected Car, könnten alle Wohnungen, Gebäude, Fahrzeuge sowie ganze Städte und Infrastrukturen miteinander kommunizieren, Daten kombiniert und ausgewertet werden. Mit immer mehr Datenquellen entstünden immer mehr nutzenstiftende Anwendungspotenziale. Sogenannte Smart Cities verknüpfen alle in der vernetzten Stadt vorhandenen Daten. Luft-, Wasser- und Energieverbrauch der verschiedenen Gebäude, Bewegungsdaten der in der Stadt befindlichen Menschen und Informationen über die Verkehrssituation werden zentral zusammengefasst und ausgewertet. Dadurch wird eine gesamthafte Analyse der Verhältnisse in der smarten Stadt ermöglicht, zahlreiche Risiken werden erkannt, Verkehrsflüsse optimiert und der Energieverbrauch maximal effizient gestaltet. Schon heute gibt es in China solche Smart Cities (Weltspiegel 2018), in denen vielerlei Daten zusammengeführt und ausgewertet werden. Dabei ist eine Ausweitung der Nutzung über Zwecke der Stadtverwaltung hinaus für geschäftliche und auch soziale Zwecke denkbar. So können akute Engpässe oder Hilfebedarfe frühzeitig erkannt und gedeckt werden – z. B. der Bedarf nach zusätzlicher (Mobilitäts-) Kapazität bei hoher Auslastungsrate der Fahrzeuge in einem bestimmten Gebiet oder nach zusätzlicher ärztlicher (Gesundheits-)Versorgung im Fall einer beginnenden Pandemie.

Was die Mobilität angeht, wird nach dem autonomen Fahren das autonome Fliegen den nächsten Entwicklungsschritt darstellen. Autonom fliegende Drohnen können z. B. die medizinische Versorgung in ländlichen Gebieten sicherstellen, und zwar mit datenbasierten Echtzeitanalysen ebenfalls auch in Akutsituationen. Dasselbe gilt für weitere Arten von Rettungseinsätzen, z. B. bei der Feuerbekämpfung oder Lawinenbergung, wenn Sensoren selbsttätig autonome Fluggeräte (Löschflugzeuge oder Bergungsdrohnen mit Robotics-Ausstattung) anfordern und effizient steuern. Auch die mobile Alltagssicherheit kann durch eine intelligente datenbasierte Steuerung erheblich gesteigert werden. Eine smarte Verkehrsüberwachung und -lenkung verhilft dazu, Ordnungswidrigkeiten aufzudecken bzw. präventiv zu vermeiden, Verkehrsflüsse zu optimieren und Unfallzahlen massiv zu senken. Straftaten können mithilfe der Gesichtserkennung und Abgleich mit einem großen Datensatz schnell aufgeklärt und mit Aussicht darauf ebenfalls von vornherein vermieden werden. Die Polizei kann dorthin geschickt werden, wo das Risiko von Übergriffen oder öffentlicher Unruhen nach aktueller Datenlage am größten ist. Dies alles führt nicht nur im Bereich Mobilität/Verkehr zu mehr Sicherheit, sondern im gesamten öffentlichen Leben.

Zudem führt die umfassende Datenerhebung in allen Lebenswelten der Bürger zu einem umfassenderen Verständnis individueller Wünsche und Bedürfnisse. Damit können Produkte, Dienstleistungen und Prozesse optimiert und auf die jeweiligen Bedürfnisse ausgerichtet werden. Im smarten Supermarkt (online oder

offline) werden dem Kunden nur noch Produkte angeboten bzw. hervorgehoben angezeigt, die für ihn relevant sind. Tiernahrung wird nur Tierbesitzern präsentiert, Vegetarier erhalten nur fleischlose Rezeptvorschläge und gegenüber Allergikern werden die für sie ungeeigneten Produkte markiert. Denkbar ist auch ein digitaler Assistent, der die Finanzen und Versicherungsbedarfe überwacht, analysiert und sich selbstständig um die individuell besten Lösungen kümmert.

Dies alles beschreibt eine Welt, in der sich die Bürger sicherer fühlen können, in der sie von Alltagsaufgaben entlastet sind, viele Annehmlichkeiten den Lebenskomfort erhöhen und dabei ressourceneffizient noch Zeit und Geld gespart werden können. Alles in allem ist die Utopie ein merklich erhöhtes Maß an Freiheit der Menschen, ihr Leben nach den eigenen Vorstellungen und Wünschen zu gestalten.

2.5.2 Dystopien: Grenzen und gesellschaftliche Risiken

Bei allen Utopien über Nutzenpotenziale, die Big Data, Data Analytics und die künstliche Intelligenz mit sich bringen, stellt sich jedoch die Frage, wer über den Einsatz der Daten entscheidet und wer damit auch bestimmt, was damit angefangen wird. Je nachdem ergibt sich auch ein Spannungsfeld, ob mit den Anwendungen eine Verbesserung oder möglicherweise auch eine Verschlechterung der Lebenssituation von Bürgern in einer Gesellschaft verbunden ist.

Als Ausgangsfrage ist zunächst zu erörtern, wem die Daten über Verhaltensweisen und Vorlieben der Menschen gehören. Die Diskussion darüber zieht sich bereits heute durch Politik, Gesellschaft und sämtliche Branchen. Einigkeit herrscht oft darüber, dass die Datenhoheit bei den Bürgern selbst liegen sollte, deren Verhältnisse und Verhaltensweisen damit repräsentiert werden. Das heißt, die Bürger selbst sollen individuell entscheiden und steuern können, welche Daten wem und für welche Zweck preisgegeben werden. Doch was bedeutet das konkret? Und steht diese Anforderung nicht gerade im Widerspruch zu den Potenzialen einer umfassenden, zunächst noch nicht zweckgebundenen Auswertung durch Behörden und Anbieter verschiedener Smart Services, um neue Anwendungsfelder überhaupt erst zu identifizieren?

Der potenzielle Nutzen einer Datenanalyse wird naturgemäß umso größer, je mehr Daten (Big Data) miteinander verknüpft und kombiniert ausgewertet werden. Voraussetzung dafür ist wiederum, dass die Daten möglichst an einer Stelle zusammenlaufen und gepoolt werden. Dadurch bilden sich jedoch Monopolisten, bei denen die Daten nicht nur erfasst, gespeichert und ausgewertet werden,

sondern die auch die Einsatzfelder kontrollieren können. Mit der Kontrolle aller möglichen Daten geht auch die Kontrolle über die Bürger selbst einher. Von daher ist die Frage zu stellen, wem die Datenverantwortung obliegen darf und ob und inwiefern Kontrollmechanismen etabliert werden können, um den Missbrauch der Daten zu verhindern. In breiten Kreisen der Bevölkerung herrschen inzwischen erhebliche Skepsis, ein steigendes Unwohlsein und sich verstärkende Kontrollängste vor der zunehmenden Macht der großen amerikanischen Datengiganten, wie insbesondere Amazon, Apple, Facebook und Google.

Beispielsweise gewinnt Amazon durch zahlreiche Schnittstellen zwischen Alexa und Hausgeräten, Smartwatches sowie Überwachungssystemen aller Art Informationen über persönliche Aktivitäten, Gewohnheiten und intime Bedürfnisse, die zusammenlaufen und ausgewertet werden können. Mit vielen weiteren Smart Services erhält Amazon schon heute Zugang zu verschiedensten Informationen: Durch Amazon Video oder Amazon Music kennt das Unternehmen den Musik- und Filmgeschmack seiner Nutzer, durch Amazon Marketplace das Einkaufsverhalten, durch Amazon Pay das Zahlungsverhalten und die Bonität und dank Amazon Fresh und Amazon Go sind die Essgewohnheiten des Nutzers bekannt. Daneben liefern Amazon Dash¹⁵, Amazon Smile¹⁶, Amazon Publishing¹⁷, der Amazon App Store und viele weitere Amazon-Services wertvolle Informationen über die Interessen, das Konsumverhalten und die Bedürfnisse der Nutzer, die durch Kombination ein umfassendes Persönlichkeitsprofil des Bürgers ergeben. Dadurch kann Amazon jedem Nutzer die individuell passenden Produkte empfehlen und mit dem eigenen Kurierdienst (Amazon Logistik) in die Amazon Packstation oder dank Amazon Key direkt in dessen Wohnung bringen. Heute wählt der Kunde diese Produkte und den Anbieter noch selbst aus und startet nach eigenem Wunsch den Bestellvorgang. Weitergedacht entstehen durch die Datenmonopolisierung und die Perfektionierung von individuellen Offerten auch Monopole von Anbietern. Und wenn der Anbieter mithilfe künstlicher Intelligenz womöglich noch vor dem Nutzer selbst weiß, welche Produkte dieser braucht

¹⁵Mit dem Amazon Dash Button können Amazon Prime Kunden verschiedene Produkte per Knopfdruck bestellen. Dabei wird der mit WLAN verbundene Knopf bspw. an die Waschmaschine angebracht; nach dem Drücken des Knopfes wird innerhalb von 24 h neues Waschmittel geliefert.

¹⁶Bei Amazon Smile wählen Kunden vor dem Einkauf aus einer Liste eine von Tausenden sozialen Organisationen aus und Amazon überweist 0,5 % der Kaufsumme an die Einrichtung.

¹⁷Eigener Verlag, der Nutzern auch das Verlegen eigener Texte ermöglicht.

und wie die Dienstleistungen für ihn ausgestaltet sein müssen, wird letzten Endes auch die Mündigkeit des Konsumenten immer weiter eingeschränkt.

Schon heute steuert auch Google Maps das Verhalten seiner Nutzer – nicht nur durch die vorgeschlagene Reiseroute und das Angebot besonders gut passender Verkehrsmittel, sondern auch z. B. durch individuelle Vorschläge eines nah gelegenen Restaurants oder sonstige Dienstleistungen. Der Streamingdienst Netflix wertet genau aus, welche Filme sich die Nutzer zu welcher Tageszeit anschauen, welche Genres sie präferieren, an welchen Stellen abgeschaltet wird, bis hin zur konkreten Aufmerksamkeit, die der Zuschauer einzelnen Szenen schenkt. Basierend auf diesen Erkenntnissen produziert Netflix mit großem Erfolg eigene Filme und Serien, die den Kunden individuell empfohlen werden. Im Ergebnis entscheidet der Nutzer kaum noch selbst, welche Filme er sieht.

Ähnlich zu Amazon verfügt auch das chinesische Pendant Alibaba über verschiedene Smart Services, wie einen Online-Markplatz und ein eigenes Bezahlsystem (Alipay). Alibaba kombiniert dabei die Daten, die innerhalb der verschiedenen Services gewonnen werden, und generiert daraus einen Scoring-Wert. In diesem Scoring-Wert werden das Konsum- und Zahlungsverhalten des Nutzers bewertet. Parallel lassen sich Punkte sammeln, die z. B. zum Entfall der Kaution bei Anmietung eines Fahrzeugs oder einer Wohnung genutzt werden können. Darüber hinaus könn(t)en zahlreiche weitere Daten in den Scoring-Wert integriert werden: der Bildungsgrad, der Beruf, das Konsum- und Zahlungsverhalten von Familienmitgliedern, Freizeitbeschäftigungen oder die politische Gesinnung. Neben einem System von Belohnungen durch Entfall von Kautionen oder z. B. vergünstigten Kreditkonditionen ist ebenso ein Bestrafungssystem denkbar. Beispielsweise könnten Kunden von bestimmten Produkten oder Smart Services ausgeschlossen werden, wenn sie für das Unternehmen einen bestimmten Mindestumsatz nicht überschreiten oder Kerndienste nicht in Anspruch nehmen.

Mit der Macht der Anbieter entsteht die Gefahr, dass die Nutzer manipuliert und selbstbestimmtes Verhalten beschnitten werden. Diese Gefahr steigt mit der immer größeren Bereitschaft breiter Bevölkerungskreise, trotz aller Datenschutzskeptis persönliche Daten freizugeben, um günstigere Angebote oder mehr Komfort zu erhalten, und mit der Tendenz zu oligopolistischen Datenpools oder sogar eines Datenmonopols. Schon heute verfügen nur wenige Unternehmen nahezu monopolartig über äußerst große Datensätze. Diese Konzentration der Daten bei wenigen Unternehmen resultiert in einer gewaltigen Macht, die zu einer Verletzung der Persönlichkeitsrechte der Bürger, einem Verlust von Freiheit, Demokratie und sozialen Bindungen führen könnte.

Nicht nur Wirtschaftsunternehmen, sondern auch Behörden und staatliche Einrichtungen können die Daten und Informationen über ihre Bürger missbrauchen. Die Sozialkreditberichte, wie sie aktuell in China bereits getestet werden, sind ein Beispiel dafür. Hier ist es der Staat, der Daten sammelt, wer sich wohin bewegt hat, mit welchem Verkehrsmittel, wer dabei zu schnell gefahren ist oder bei Rot die Straße überquert hat. Übersetzt wird das ebenfalls in einen Punktestand („Social Scoring“), der bei der Vergabe von Jobs herangezogen wird, die Festlegung von Kreditkonditionen bestimmen und auf Dating-Plattformen angegeben werden kann. Zudem kommen Konzepte in Betracht, die Bürger bei unerwünschtem Verhalten zu bestrafen, indem ihnen z. B. der Kauf von Luxusgütern oder Auslandsaufenthalte verboten werden. Aber wie erfolgt die Bewertung der Daten und damit die Übersetzung in ein Punktesystem? Während dies bei Verkehrsverstößen noch relativ objektiv möglich ist, wird es schwierig, wenn auch andere Datenquellen herangezogen und ausgewertet werden – z. B. wer wie lange das Licht anhat, wer sich mit wem getroffen, welche Filme geschaut, welche Produkte gekauft, an welchen Veranstaltungen teilgenommen oder welche Partei gewählt hat. Auch daran könnten wieder Belohnungs- aber auch Bestrafungssysteme geknüpft werden. So könnten z. B. das Anmieten einer Wohnung, der Zugang zu Verkehrsmitteln, bestimmte Sozialleistungen usw. eingeschränkt oder gänzlich unterbunden werden.

Die informationelle Überwachung und digitale Bevormundung können im Zuge von Big Data und Data Analytics zu einer starken Einflussnahme auf die Gesellschaft und zu einer Verschiebung ihrer Strukturen führen (Bendel 2018b). Es drohen der ‚Gläserne Bürger‘, d. h. der Verlust von Privatsphäre und die Manipulation von Denken und Handeln der Menschen mittels gezielter Anreiz- und Bestrafungsmechanismen. Alles in allem ist die Dystopie ein merklich eingeschränktes Maß an Freiheit der Menschen, ihr Leben nach den eigenen Vorstellungen und Wünschen zu gestalten.¹⁸

¹⁸Daneben besteht bei jedem vernetzten und datenbasierten System das Risiko von Fehlern, Hackerangriffen und Datendiebstahl. So wurde z. B. in China ein auf einem Bus angebrachtes Werbegesicht vom System als Fußgänger wahrgenommen, und die betreffende Person wurde in der Folge beschuldigt, eine rote Fußgängerampel überquert zu haben. Die Konsequenz war eine Aufforderung zur Strafzahlung. Was in diesem Fall eher humorvoll zu nehmen ist und ohne schwerwiegende Folgen blieb, kann grundsätzlich für den Bürger gravierende Auswirkungen haben, wenn datenbasierte Systeme auf Basis nicht mehr nachvollziehbarer Algorithmen automatisierte Folgehandlungen einleiten. Darüber hinaus können Hackerangriffe einzelne Anwendungen oder ganze Systeme lahmlegen.

Literatur

- Acatech. (2018). Smart Service Welt. Internetbasierte Dienste für die Wirtschaft. <https://www.acatech.de/Projekt/smart-service-welt/>. Zugegriffen: 19. Dez. 2018.
- ADAC. (2017). Die Evolution der Mobilität. https://www.zukunftsinstitut.de/fileadmin/user_upload/Publikationen/Auftragsstudien/ADAC_Mobilitaet2040_Zukunftsinstitut.pdf. Zugegriffen: 11. Okt. 2018.
- ADAC. (2018). Carsharing. https://www.adac.de/_mmm/pdf/fi_carsharing_sp_58306.pdf. Zugegriffen: 19. Dez. 2018.
- Ahlemann, D., Koster, A., Crusius, D., & Kerstan, H. (2016). Growth in a commoditizing market. In R. Vierreckl, A. Koster, E. Hirsh, & D. Ahlemann (Hrsg.), *Connected car report 2016: Opportunities, risk, and turmoil on the road to autonomous vehicles* (S. 23–30). <https://www.strategyand.pwc.com/media/file/Connected-car-report-2016.pdf>. Zugegriffen: 19. Dez. 2018.
- Akoto, P. (2018). Studie bemängelt Datenschutz bei Smart-Home-Technik. <https://www.energategate-messenger.de/news/183318/-studie-bemaengelt-datenschutz-bei-smart-home-technik>. Zugegriffen: 19. Dez. 2018.
- Amazon. (2018). Amazon key smart lock kit. <https://www.amazon.com/b?ie=UTF8&node=1>. Zugegriffen: 10. Okt. 2018.
- Ambient Assisted Living Deutschland. Technik die unser Leben vereinfacht. <http://www.aal-deutschland.de/>. Zugegriffen: 11. Okt. 2018.
- Apple. (2018a). Die Health-App auf Ihrem iPhone oder iPod touch verwenden. <https://www.apple.com/de/apple-watch-series-4/health/>. Zugegriffen: 11. Okt. 2018.
- Apple. (2018b). Gesundheit & Fitness. <https://www.apple.com/de/shop/iphone/iphone-accessories/health-fitness>. Zugegriffen: 13. Dez. 2018.
- Apple. (2018c). Mehr Möglichkeiten für Forschung, Ärzte und dich. <https://www.apple.com/de/researchkit/>. Zugegriffen: 11. Dez. 2018.
- Apple. (2018d). So hast du noch nie auf deine Gesundheit geachtet. <https://www.apple.com/de/ios/health/>. Zugegriffen: 13. Dez. 2018.
- Apple. (2018e). Doctors put patients in charge with Apple’s health records feature. <https://www.apple.com/newsroom/2018/03/doctors-put-patients-in-charge-with-apples-health-records-feature/>. Zugegriffen: 13. Dez. 2018.
- Arbeitskreis Smart Services Welt. (2015). Smart Service Welt: Umsetzungsempfehlungen für das Zukunftsprojekt internetbasierte Dienste für die Wirtschaft. https://www.acatech.de/wp-content/uploads/2015/03/BerichtSmartService2015_mitUmschlag_bf.pdf. Zugegriffen: 19. Dez. 2018.

Während in einem solchen Fall bspw. die Manipulation von Thermostaten in der Lebenswelt Wohnen nur zu einem Ausfall der Heizungen führt, können etwa in der Lebenswelt Mobilität autonome Fahrzeuge oder in der Lebenswelt Gesundheit medizinische Geräte fehlgesteuert werden, was unmittelbar Menschenleben gefährdet. Solcherart technische Risiken automatisierter datengetriebener Systeme waren allerdings nicht im Fokus der vorliegenden Studie.

- Ärztzeitung. (2017). AGES. Online-Umfrage zu Gesundheitsrisiken. <http://www.aerztezeitung.at/archiv/oeaez-2017/oeaez-3-10022017/elga-datenmissbrauch-hacker-gesundheitsdaten.html>. Zugegriffen: 13. Dez. 2018.
- Bardmann, M. (2019). Grundlagen der Allgemeinen Betriebswirtschaftslehre. Geschichte – Konzepte – Digitalisierung. Wiesbaden, Springer Fachmedien.
- Bass J. (2017): Chancen der Digitalisierung aus Sicht der Krankenkassen, in: Digital-Gipfel Plattform Innovative Digitalisierung der Wirtschaft Fokusgruppe Intelligente Vernetzung (Hrsg.): Deutschland intelligent vernetzt. Digitale Gesundheit 2017. DIV Report Spezial, Juni 2017, S. 33–34. https://deutschland-intelligent-vernetzt.org/app/uploads/2017/06/DIV_Report_Spezial_Gesundheit2017.pdf
- Becker, D., & Pawelke, M. (2015). Automotive. Blechbieger oder Grid Master? Die Automobilindustrie an der Weggabelung in ein hochdigitalisiertes Zeitalter. <https://assets.kpmg/content/dam/kpmg/pdf/2015/11/blechbieger-oder-grid-master.PDF>. Zugegriffen: 13. Dez. 2018.
- Beenken, M., Knörrer, D., Moormann, J., & Schmidt, D. (Hrsg.). (2018). *Digital Insurance: Strategien, Geschäftsmodelle, Daten*. Frankfurt a. M.: Frankfurt School.
- Bendel, O. (2018a). Smart home. <https://wirtschaftslexikon.gabler.de/definition/smart-home-54137>. Zugegriffen: 10. Okt. 2018.
- Bendel, O. (2018b). Big data. <https://wirtschaftslexikon.gabler.de/definition/big-data-54101>. Zugegriffen: 11. Dez. 2018.
- Bratzel, M., & Tellermann, R. (2018). Finanzierung und Absicherung neuer Mobilitätskonzepte. https://auto-institut.de/index_html_files/Finanzierung_und_Absicherung_neuer_Mobilitaetskonzepte.pdf. Zugegriffen: 10. Okt. 2018.
- Bundesinstitut für Bevölkerungsforschung. (1996). *Bundesinstitut für Bevölkerungsforschung. Die Lebenssituation älterer Menschen. Expertise für die Kölnische Rückversicherungsgesellschaft*. Köln: o. V.
- Bundesministerium für Wirtschaft und Energie. (2014). Entwicklung digitaler Technologien. Die Zukunft der Wirtschaft ist digital. https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/entwicklung-konvergenter-ikt.pdf?__blob=publicationFile&v=5. Zugegriffen: 19. Dez. 2018.
- Bundesministerium für Wirtschaft und Energie (2017a). Smart Service Welt- Internetbasierte Dienste für die Wirtschaft. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/smart-service-welt-internetbasierte-dienste-fuer-die-wirtschaft.pdf?__blob=publicationFile&v=9. Zugegriffen: 19. Dez. 2018.
- Bundesministerium für Wirtschaft und Energie. (2017b). Digitale Geschäftsmodelle. https://www.bmwi.de/Redaktion/DE/Publikationen/Mittelstand/mittelstand-digital-digitale-geschaeftsmodelle.pdf?__blob=publicationFile&v=15. Zugegriffen: 19. Dez. 2018.
- Bundesverband Digitale Wirtschaft. (2018a). Wie smart ist das Recht im Smart Home. https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/RZ_BVDW_LF_Recht_im_SmartHome_web_20180611.pdf. Zugegriffen: 10. Okt. 2018.
- Bundesverband Digitale Wirtschaft. (2018b). Wem „gehören“ die Daten im Connected Car? https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/connected_mobility/BVDW_Daten-im-Connected-Car_final.pdf. Zugegriffen: 10. Okt. 2018.

- Business Panorama. (2017). UBTECH Robotics präsentiert Lynx, den interaktiven humanoiden Roboter mit Amazon Alexa. <http://business-panorama.de/news.php?newsid=404118>. Zugegriffen: 11. Dez. 2018.
- Chaudhuri, A. (2018). Predictive maintenance for industrial iot of vehicle fleets using hierarchical modified fuzzy support vector machine. <https://arxiv.org/ftp/arxiv/papers/1806/1806.09612.pdf>. Zugegriffen: 19. Dez. 2018.
- Cloverhealth. (2018). Clover is a medicare plan done differently. <https://www.cloverhealth.com/en/plans>. Zugegriffen: 13. Dez. 2018.
- Connected Living. (2018). Unsere Mitglieder. <https://connected-living.org/organisation>. Zugegriffen: 19. Dez. 2018.
- Corthier, J., Kreuter, V., & Klingholz, R. (2011). *Lebenswelten 2015. Wie sich die Struktur der Konsumenten in den Regionen verändert*. Nürnberg: GfK.
- Deloitte. (2018). Smart Home Consumer Survey 2018. Ausgewählte Ergebnisse für den deutschen Markt. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/Deloitte_TMT_Smart_Home_Studie_18.pdf. Zugegriffen: 17. Dez. 2018.
- Denkena, B., Dittrich, M.-A., Uhlich, F., Maibaum, L., & Mörke, T. (2017). Das genteligte Werkstück. In G. Reinhart (Hrsg.), *Handbuch Industrie 4.0: Geschäftsmodelle, Prozesse, Technik* (S. 239–321). München: Hanser.
- Deutsche Gesellschaft für Qualität. (2017). Datenschutz und die EU-DSGVO im Gesundheitswesen. <http://blog.dgq.de/datenschutz-und-die-eu-dsgvo-im-gesundheitswesen/>. Zugegriffen: 13. Dez. 2018.
- Deutsches Institut für Vertrauen und Sicherheit im Internet. (2016). Big data. <https://www.divisi.de/wp-content/uploads/2016/01/Big-Data.pdf>. Zugegriffen: 19. Dez. 2018.
- Discovergy. (2018). Discovering the Smart Home. Mit Discovergy und iHaus. <https://discovergy.com/smart-home-ihaus>. Zugegriffen: 17. Dez. 2018.
- Duden. (2019). Lebenswelt. <https://www.duden.de/suchen/dudenonline/lebenswelt>. Zugegriffen: 10. Okt. 2018.
- Eckstein, L., Form, T., & Maurer, M. (2018). Automatisiertes Fahren, VDI-Statusreport Juli 2018. <https://www.trialog-publishers.de/media-online/automatisiertes-Fahren-VDI-Statusreport-Juli-2018.pdf>.
- Fasel, D., & Meier, A. (Hrsg.). (2016). *Big Data – Grundlagen, Systeme und Nutzungspotenziale*. Wiesbaden: Springer Vieweg.
- Gesetz zur Bevorrechtigung des Carsharing. (2017) vom 05.07.2018 (BGBl. I S. 2230) in der Fassung der Bekanntmachung vom 05.07.2018 (BGBl. I S. 2230). https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBI&start=//%5b@attr_id=%27bgbl117s2230.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2230.pdf%27%5D__1555779424306. Zugegriffen: 19. Dez. 2018.
- Goodwall, W., Fishman, T. D., Bornstein, J., & Bronthron, B. (2017). The rise of mobility as a service. *Deloitte Review*, 20, 111–129.
- Grohe. (2018). Smarte Kooperation: Grohe und Qivicon lassen Wasserschäden im intelligenten Zuhause keine Chance. https://www.grohe.com/de/corporate/news/category_news/pressreleases/pressrelease/news_10368.html. Zugegriffen: 18. Dez. 2018.
- Grösser, S. (2018). Geschäftsmodell. <https://wirtschaftslexikon.gabler.de/definition/geschäftsmodell-52275>. Zugegriffen: 10. Okt. 2018.

- Gründinger, W. (2018). Smart Mobility Initiative. Eine diskriminierungsfreie Plattform für multimodale Mobilität. https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/connected_mobility/BVDW_Smart_Mobility_Initiative_konzept-v2.pdf. Zugegriffen: 10. Okt. 2018.
- Hartmut, S., Seidel, U., & Knappe, T. (2010). Smart Home in Deutschland. Institut für Innovation und Technik (iit). In VDI/VDE-IT (Hrsg.).
- Heide, D. (2018). Zu langsam für die Digitalisierung. <https://www.handelsblatt.com/unternehmen/it-medien/gesetze-in-deutschland-zu-langsam-fuer-die-digitalisierung/20828056.html?ticket=ST-208995-U6cCswFE0smKwfrkpyYt-ap5>. Zugegriffen: 19. Dez. 2018.
- Heise online. (2017). Amazon Key. Smartes Türschloss soll Paketboten reinlassen. <https://www.heise.de/newsticker/meldung/Amazon-Key-Smartes-Tuerschloss-soll-Paketboten-reinlassen-3872147.html>. Zugegriffen: 10. Okt. 2018.
- Heyen, N. B. (2016). *Digitale Selbstvermessung und Quantified Self. Potentiale, Risiken und Handlungsoptionen*. Karlsruhe: Frauenhofer ISI.
- Hioscar. (2018). Get more from your health insurance. <https://www.hioscar.com/individuals/ny>. Zugegriffen: 13. Dez. 2018. Hofer, a.a.O (Fn. 3).
- IBM (2019). Infographics & animations: The four V's of big data. <https://www.ibmbigdatahub.com/infographic/four-vs-big-data>. Zugegriffen: 19. Dez. 2018.
- Ignor, S. (2018). Amazon Key. Jetzt kommen die Pakete direkt ins Auto. <https://www.computerbild.de/artikel/cb-News-Vernetztes-Wohnen-Amazon-Key-Paketbote-Wohnung-Auto-19247545.html>. Zugegriffen: 10. Okt. 2018.
- Industriepraxis. (2018). IFA 2017. UBTECH präsentiert Zukunft humanoider Roboter. <http://industriep Praxis.de/ifa-2017-ubtech-praesentiert-zukunft-humanoider-roboter/>. Zugegriffen: 24. Nov. 2018.
- Innogy. (2017). Geofencing mit innogy SmartHome. <https://news.innogy.com/geofencing-mit-innogy-smarhome/>. Zugegriffen: 17. Dez. 2018.
- Jäckel, T. (2017). Sharing Economy. Mobilität der Zukunft. <https://www.versicherungsbote.de/id/4860853/Sharing-Economy-Mobilitaet-der-Zukunft/>. Zugegriffen: 20. Dez. 2018.
- Kapalschinski, C. (2017). Amazons tückisches Türschloss. <https://www.handelsblatt.com/unternehmen/handel-konsumgueter/onlinehandel-amazons-tueckisches-tuerschloss/20501516.html?ticket=ST-870154-3rzc7wvOxNLVhOfFn10i-ap5>. Zugegriffen: 10. Okt. 2018.
- Kraus, B. (2006). Lebenswelt und Lebensorientierung. Eine begriffliche Revision als Angebot an eine systematisch-konstruktivistische Sozialarbeitswissenschaft. *Zeitschrift für systemische Therapie und Familientherapie*, 37(2), 116–129.
- Krohn, P. (2018). Soll die Versicherung das Haus kontrollieren? <https://www.faz.net/aktuell/finanzen/meine-finanzen/versichern-und-schuetzen/smar-te-versicherungen-haben-es-bisher-kaum-in-die-deutschen-haeuser-geschafft-15411803.html>. Zugegriffen: 19. Dez. 2018.
- Lacace, M. (2017). Meet lynx, the walking, talking home robot powered by Amazon Alexa. <https://www.androidcentral.com/meet-lynx-walking-talking-robot-powered-amazon-alexa>. Zugegriffen: 17. Dez. 2018.
- Mamerow, S. (2012). *Entscheiden und Wirtschaften: Eine Analyse des wirtschaftlichen Alltags unter anthropologischem Blickwinkel*. Hamburg: Diplomica.
- Moovel. (2018). Unsere Vision ist eine Welt ohne Staus. <https://www.moovel.com/de>. Zugegriffen: 19. Dez. 2018.

- Müller, R. (2018). Smart-Home-Versicherung. Sinnvoll oder nutzlos? <https://www.connect.de/ratgeber/smart-home-versicherung-sinnvoll-nutzlos-3198396.html>. Zugegriffen: 19. Dez. 2018.
- Munich RE. (2017). Smart Home: Potenziale für die Assekuranz. <https://www.munichre.com/topics-online/de/digitalisation/smart-home-potential-insurers.html>. Zugegriffen: 19. Dez. 2018.
- Nationaler IT-Gipfel. (2015). Smart Home. Ergebnisdokument der Projektgruppe Smart Home. https://plattform-digitale-netze.de/app/uploads/2016/06/151105_PF1_007_FG1_Ergebnisdokument-Projektgruppe-Smart-Home.pdf. Zugegriffen: 19. Dez. 2018.
- Nitschke, T. (2018). BLC Studie Datenschutz 2018. <http://berg-lund.de/publikationen/datenschutz-2018>. Zugegriffen: 19. Dez. 2018.
- Oliver Wyman. (2018). Mitarbeiter der Zukunft: Die Automobilindustrie muss handeln. https://www.oliverwyman.de/content/dam/oliver-wyman/v2-de/media/2018/Pressemitteilungen/Kompetenzwandel-in-der-Automobilindustrie_PM_OliverWyman.pdf. Zugegriffen: 19. Dez. 2018.
- Osterwalder, A., & Pigneur, Y. (2010). *Business model generation. A handbook for visionaries, game changer, and challengers*. New Jersey: Wiley.
- PwC. (2017). Sherlock in health. How artificial intelligence may improve quality and efficiency, whilst reducing healthcare costs in Europe. <https://www.pwc.de/de/gesundheitswesen-und-pharma/studie-sherlock-in-health.pdf>. Zugegriffen: 19. Dez. 2018.
- PwC. (2018). Wie Tech Giganten den Gesundheitsmarkt revolutionieren. <https://www.pwc.de/de/gesundheitswesen-und-pharma/wie-tech-giganten-den-gesundheitsmarkt-revolutionieren.html>. Zugegriffen: 13. Dez. 2018.
- Randelhoff, M. (2014). Definition. UberPop, WunderCar, Lyft & Co. – Ridesharing oder vielmehr Rideselling? <https://www.zukunft-mobilitaet.net/74151/analyse/definition-rides-haring-rideselling-unterschiede-taxi-carpooling/>. Zugegriffen: 19. Dez. 2018.
- ReachNow. (2018). Where to? <https://reachnow.com/en/>. Zugegriffen: 19. Dez. 2018.
- Rohkamm, F. T. (19.11.2018). *Connected, Autonomous, Shared & Electric: Perspektiven für die Mobilität, deren Risiken und Versicherungsdeckungen*. Vortrag auf der InnoVario, Bonn.
- Roussem, M. (2017). Maschinendaten. <https://www.searchenterprisesoftware.de/definition/Maschinendaten>. Zugegriffen: 1. Okt. 2018.
- Schaal, S. (2016). Von der Versuchsküche zum Geschäftsmodell. <https://www.wiwo.de/unternehmen/auto/carsharing-bmw-testet-premium-carsharing-in-den-usa/13450910-2.html>. Zugegriffen: 19. Dez. 2018.
- Schlingensiepen, I. (2017). Digitalisierung. Die meisten Patienten würden Gesundheitsdaten mit Ärzten teilen. https://www.aerztezeitung.de/praxis_wirtschaft/e-health/article/943537/digitalisierung-meisten-patienten-wuerden-gesundheitsdaten-aerzten-teilen.html. Zugegriffen: 13. Dez. 2018.
- Schmidt-Lackner, M. (2016). ReachNow. BMW macht Audi beim Premium-Carsharing Konkurrenz. <https://www.automobilwoche.de/article/20160408/NACHRICHTEN/160409917/reachnow-bmw-macht-audi-beim-premium-carsharing-konkurrenz>. Zugegriffen: 19. Dez. 2018.
- Schütz, A., & Luckmann, T. (2017). *Strukturen der Lebenswelt* (2. Aufl.). Konstanz: UTB.

- Seiberth, G., & Gründinger, W. (2018). Data-driven business models in connected cars, mobility services & beyond. https://www.bvdw.org/fileadmin/user_upload/20180509_bvdw_accenture_studie_datadrivenbusinessmodels.pdf. Zugegriffen: 19. Dez. 2018.
- Siepermann, M. (2018). Ambient assisted living. <https://wirtschaftslexikon.gabler.de/definition/ambient-assisted-living-53583>. Zugegriffen: 17. Dez. 2018.
- Siethoff, P. (2017). Amazon Key. Das bisschen Privatsphäre für ein Plus an Komfort. <https://www.business-punk.com/2017/10/amazon-key-privacy/>. Zugegriffen: 17. Dez. 2018.
- SmartHome Initiative Deutschland und mml (o.J.). Smart Home- und AAL-Technologien in der Immobilien- und Wohnungswirtschaft. https://web.gdw.de/uploads/pdf/studien_gutachten/Studie_Smart_Home_und_AAL_in_der_Wohnungswirtschaft.pdf. Zugegriffen: 8. Okt. 2018.
- Sobe, P. (2018). Datenstrukturen und Speicherstrukturen. https://www2.htw-dresden.de/~sobe/Vorjahre/Vo_InfoMB_Jg11/7_Datenstrukturen.pdf. Zugegriffen: 8. Okt. 2018.
- Spektrum. (2001). Lebenswelt. <https://www.spektrum.de/lexikon/geographie/lebenswelt/4677>. Zugegriffen: 10. Okt. 2018.
- Stanford Medicine. (2018). Apple heart study. <http://med.stanford.edu/appleheartstudy.html>. Zugegriffen: 13. Dez. 2018.
- Statista. (2019). Prognose zum Volumen der jährlich generierten digitalen Datenmenge weltweit in den Jahren 2018 und 2015 (in Zettabyte). <https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/>. Zugegriffen: 19. Dez. 2018.
- Strom Magazin. (2018). Solaranlagen & Smart Home. Eigenverbrauch komfortabel steigern. <https://www.strom-magazin.de/ratgeber/solaranlage-smart-home-eigenverbrauch/>. Zugegriffen: 17. Dez. 2018.
- Tesla. (2018a). Introducing software version 9.0. https://www.tesla.com/de_DE/blog/introducing-software-version-9. Zugegriffen: 19. Dez. 2018.
- Tesla. (2018b). Software-Version 9.0 entdecken. https://www.tesla.com/de_DE/support/software-v9. Zugegriffen: 19. Dez. 2018.
- Thiele, J., & Schmidt-Jochmann, C. (2015). Geschäftsmodell der Kfz-Versicherung im Umbruch. <https://www.rolandberger.com/de/Publications/Gesch%C3%A4ftsmodell-der-Kfz-Versicherung-im-Umbruch.html>. Zugegriffen: 19. Dez. 2018.
- Ubtech. (2018). Lynx. <https://ubtrobot.com/products/lynx>. Zugegriffen: 10. Okt. 2018.
- Verordnung des Europäischen Parlaments und des Rates 2016/679 (2018). Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG. <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679>. Zugegriffen: 19. Dez. 2018.
- Versicherungsbote. (2018). Verbraucher haben Interesse an Versicherungen mit Smart-Home-Technik. <https://www.versicherungsbote.de/id/4869097/Versicherungen-Smart-Home-Technik/>. Zugegriffen: 19. Dez. 2018.
- Weltspiegel. (15. Dezember 2018). *Unsere digitale Zukunft? China und die künstliche Intelligenz*. ARD.

- Wired. (2018). China überwacht Autofahrer jetzt mit Drohnen. <https://www.wired.de/article/china-setzt-drohnen-fuer-die-verkehrsueberwachung-ein>. Zugegriffen: 19. Dez. 2018.
- Wollaston, V. (2017). Meet Lionbot, Lynx and Cruzr, the latest humanoids coming for homes and offices. <https://www.wired.co.uk/article/ubtech-robots-ces-2017>. Zugegriffen: 10. Okt. 2018.

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.



Big Data: Chancen und Risiken aus Sicht der Bürger

3

3.1 Einleitung

Ausgehend von den vorangegangenen Teilen beschreibt dieses Kapitel auf einer Basis von 1000 Befragten das Verhältnis der deutschen Bevölkerung zu *digitaler Vernetzung, Big Data* und *Künstlicher Intelligenz*. Der Aufbau folgt der Logik

- a) vom ‚*Wissen*‘ und ‚*Können*‘ als Randbedingungen souveränen Entscheidens ...
- b) über das ‚*Wollen*‘ in Form von Einstellungen und Bewertungen zu Technikfolgen, Anwendungsfeldern und Datenschutz ...
- c) zum tatsächlichen ‚*Handeln*‘ in Onlinenutzung und Datenschutz.

Aufbauend darauf wird das Potenzial für einen möglichen Paradigmenwandel eruiert – in der Datenpolitik, in den medialen und gesellschaftlichen Narrativen und schließlich – beispielhaft für eine Branche – in der Versicherungswirtschaft.

Vernetzung und Big Data, Künstliche Intelligenz und die damit verbundenen Algorithmen bestimmen zunehmend die Lebenswelt der Bürger, sind bisher aber erst wenig in den Köpfen angekommen. Bisherige Umfragen zeigen einen meist geringen Informationsgrad und eine tendenziell skeptische Haltung, aber zugleich eine umfassende, oft wenig bewusste Nutzung der Potenziale.

Aufbauend auf den vorliegenden Studien, theoretischen Grundüberlegungen sowie den vorangegangenen Ausführungen soll im Folgenden das Verhältnis der deutschen Bevölkerung in Bezug auf Daten und Algorithmen erfasst und analysiert werden. Dabei werden einerseits ‚*Wissen*‘ (Abschn. 3.2) und ‚*Können*‘

Dieses Kapitel wurde von Horst Müller-Peters verfasst.

(Abschn. 3.3) als Voraussetzung souveränen Handels beschrieben. Dies wird in Form von Folgeabschätzungen, die Bewertung von Anwendungsfeldern (mit besonderem Schwerpunkt auf den drei Lebenswelten ‚Mobilität‘, ‚Wohnen‘ und ‚Gesundheit‘) sowie durch die Erfassung von Einstellungen zum Datenschutz das ‚Wollen‘ der Bürger abgebildet (Abschn. 3.4). Dem Wollen, Wissen und Können wird in Abschn. 3.5 das tatsächliche ‚Handeln‘ gegenübergestellt: Wie verhalten sich die Bürger? In welchem Umfang werden Geräte und Dienste genutzt und welche aktiven Maßnahmen zum Schutz der persönlichen Daten werden tatsächlich ergriffen? Anschließend werden die in Kap. 1 thematisierten Paradigmen zu Datenpolitik und Datenethik aus Sicht der Bürger beleuchtet (Abschn. 3.6) sowie die Frage, inwieweit den zu beobachtenden und weitgehend negativ besetzten Narrativen rund um Big Data auch positive ‚Erzählungen‘ gegenüberstehen (Abschn. 3.7). Abschließend werden in Abschn. 3.8 am Beispiel der Versicherungswirtschaft Erwartungen an neue Rollen von Marktteilnehmern dargestellt.

Die Auswertung basiert auf einer Befragung von 1000 Bürgern ab 18 Jahren. Diese Gesamtstichprobe wurde in zwei Teilstichproben mit unterschiedlicher Erhebungsform aufgeteilt (siehe Abb. 3.1). Dieser sogenannte Mixed-Mode-Ansatz hat den Vorteil, dass sowohl Personengruppen, die in Telefoninterviews schwer zu erreichen sind, als auch solche, die durch Online-Erhebungen nicht ansprechbar sind, in der Gesamtstichprobe ausreichend abgebildet sind, und dass sich auch Effekte der Interviewsituation in der Gesamtstichprobe ausgleichen.

Um Reihenfolgeeffekte zu vermeiden, wurden die Items innerhalb einer Frage nach dem Zufallsprinzip rotiert. Zudem wurde ein Teil der Fragen jeweils nur der (zufällig ausgewählten) Hälfte der Befragten gestellt um die Gesamtlänge des Fragebogens zu verkürzen (‚split half‘)¹. Die realisierte Stichprobe wurde auf Basis der aktuellen Verbraucheranalyse „best 4 planning 2018 I“ (best 4 planning 2018) mit der Struktur der deutschen Wohnbevölkerung abgeglichen. Auf eine nachträgliche Gewichtung der Antworten wurde aufgrund der insgesamt hohen Übereinstimmung verzichtet.

¹Bei der gegebenen Stichprobengröße von 1000 Befragten ist bei Anteilswerten und einem Signifikanzniveau von 95 % mit einer zufälligen Fehlerabweichung von ca. ± 3 % zu rechnen. Sofern Teilstichproben von ca. 500 Befragten vorliegen, erhöht sich der Fehlerbereich auf ca. ± 4 %. Die Stichprobengröße ist jeweils bei der Frage angegeben ($n = \dots$).

Methode: 1.000 Befragte als „Multimode“-Erhebung

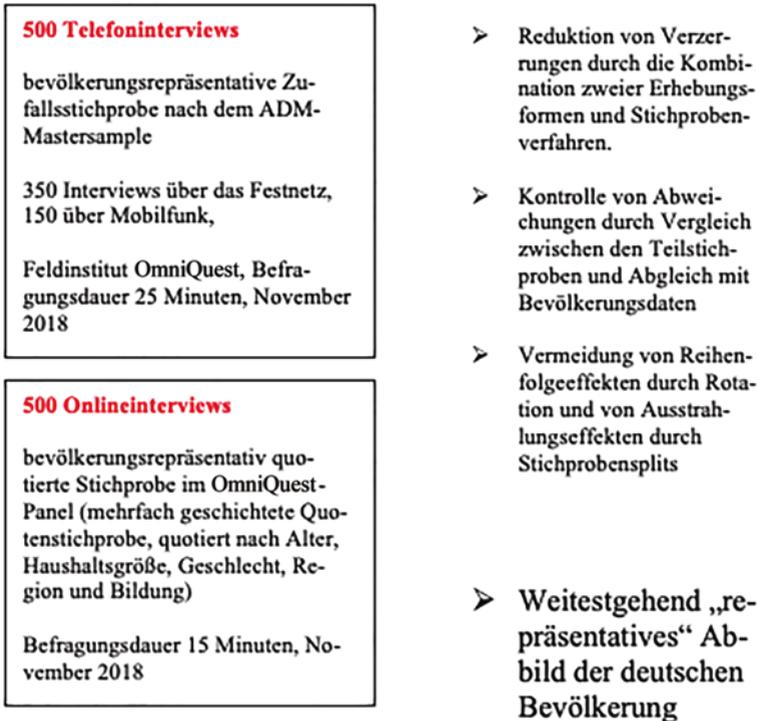


Abb. 3.1 Methodisches Vorgehen

Fazit Im Ergebnis liefert die Erhebung ein weitgehend ‚repräsentatives‘ Abbild der deutschen Bevölkerung beziehungsweise – soweit die Fragen sich nur auf Internetnutzung beziehen, der online-aktiven Bevölkerung².

²Nichtsdestotrotz ist nicht auszuschließen, dass durch Selektionseffekte (Teilnahmebereitschaft an Telefoninterviews einerseits bzw. an einem Online-Panel andererseits) eine gewisse Verzerrung hin zu höherer Datenkompetenz und zu höherer Akzeptanz von Datenaustausch besteht. Zu den grundsätzlichen Grenzen der Repräsentativität von Befragungen siehe Müller-Peters (2012) sowie Müller-Peters (2018).

3.2 Datenwissen

Voraussetzung eines mündigen Umgangs mit den eigenen digitalen Daten ist zuerst einmal eine grundlegende *Kenntnis* des Themas (zur Relevanz von Fähigkeit und Motivation für überlegte Entscheidungen siehe z. B. Petty und Cacioppo 1986). Um das Wissen um Big Data und Künstliche Intelligenz in der Bevölkerung zu erfassen, wurden eine Liste von Begriffen erstellt und die Interviewpartner befragt, inwieweit sie diese einem Bekannten erklären könnten. Die Stichworte umfassten sowohl Fachbegriffe als auch umgangssprachliche Formulierungen zu technischen Grundlagen und deren Anwendungen, zur Gesetzgebung und schließlich zu einigen Daten-Skandalen, die in den Medien breite Aufmerksamkeit erhalten haben.³

Neben dem Wissensstand ist auch die (gefühlte) *Wahlfreiheit* eine Bedingung für Souveränität im Umgang mit Daten. Einerseits haben auf der rechtlichen Seite die EU-Datenschutz-Grundverordnung sowie in Folge das Bundesdatenschutzgesetz weitgehende Schutz- und Verfügungsrechte für die Bürger sowie umfassende Zustimmungspflichten installiert. Andererseits schränken Informationslücken, die Komplexität von Datenschutzerklärungen, digitale Ökosysteme und monopolähnliche Marktstrukturen die faktische Handlungsfreiheit in hohem Maße ein.

Wie die Befragungsergebnisse (siehe Abb. 3.2) zeigen, sind wesentliche Grundbegriffe der Digitalisierung bereits in das *Allgemeinwissen* eingegangen. Das betrifft vor allem weitverbreitete Anwendungen (wie GPS-Ortung oder Cookies) sowie plakative Begriffe aus der öffentlichen Diskussion (wie Selbstfahrendes Auto, Künstliche Intelligenz, aber auch der Name Edward Snowden). Bemerkenswert ist, wie schnell auch neue Angebote den Weg in die Köpfe gefunden haben (wie Smart Home, Smart Watch oder Alexa).

Weitere Begriffe sind zumindest einer *Mehrheit* bekannt, z. B. aktuelle politische Themen wie der Facebook-Datenskandal oder die Europäische Datenschutzgrundverordnung, aber auch Termini wie Tracking oder Algorithmus (was nicht immer auch ein genaueres Verständnis beinhaltet).

³Es liegen bereits eine Reihe aktueller empirischer Studien vor, in denen der Wissensstand zu Big Data, zu Algorithmen oder zu Künstlicher Intelligenz erfasst wurde (siehe zum Beispiel Fisher und Petersen 2018, GfK 2018, Marsden 2017, PWC 2017 oder YouGov 2018, sowie im Überblick Kap. 1 in diesem Band). Dabei wird aber in der Regel nur auf einzelne Begriffe abgezielt, während hier ein breiter definiertes ‚digitales Wissen‘ der Bevölkerung als Voraussetzung souveränen Handelns gemessen werden sollte.

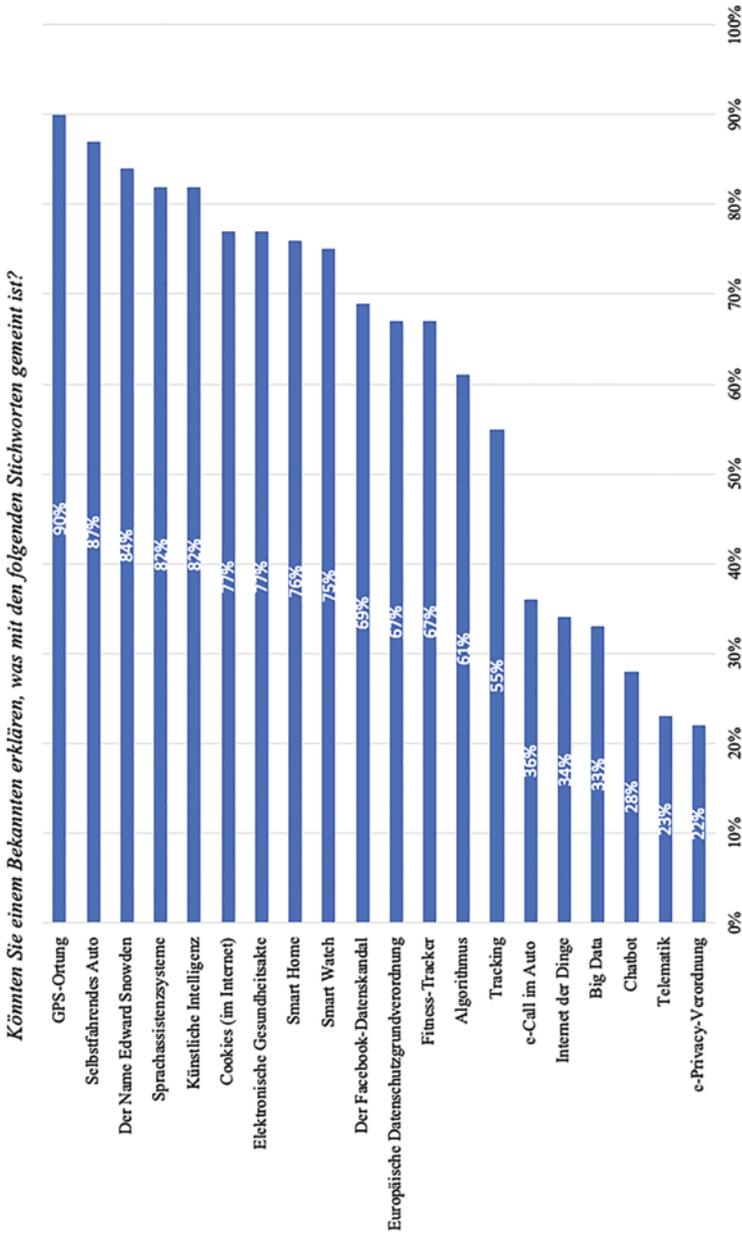


Abb. 3.2 Datenwissen als Bedingung für Souveränität (n = 449–496; alle Befragten [split half])

Könnten Sie einem Bekannten erklären, was mit den folgenden Stichworten gemeint ist?

n=987; alle Befragten
abgebildet ist die Anzahl der laut Selbsteinschätzung erklärbaren Begriffe in Prozent

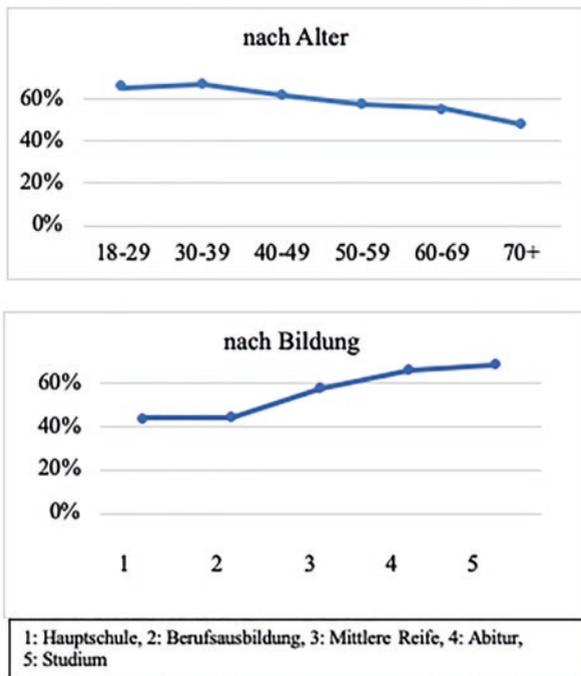


Abb. 3.3 Datenwissen als Bedingung für Souveränität nach Alter und Bildung

Schließlich gibt es Begriffe, die nur einer *Minderheit* vertraut sind. Das sind vor allem Anwendungen, die relativ neu sind (wie Chatbot oder e-Call), aber auch grundlegende Begriffe digitaler Vernetzung, die eher im Hintergrund hinter sicht- und erlebbareren Anwendungen stehen (wie Big Data, Telematik, Internet of Things). Bezüglich des ‚Schlusslichtes‘ *e-Privacy-Verordnung* ist anzumerken, dass sich diese zum Befragungszeitraum politisch noch im Vorbereitungsstadium befand.

Tab. 3.1 Selbsteinschätzung zum Datenwissen (n = 441)

| <i>Ich glaube, ich kenne mich mit dem Internet gut aus</i> | Ja (%) | Teils/teils (%) | Nein (%) |
|------------------------------------------------------------|--------|-----------------|----------|
| | 43 | 47 | 10 |

Entsprechend der Prägung der Generationen durch digitale Techniken ist der Wissensstand der jüngeren Alterskohorte höher, wobei selbst die Gruppe 70+ noch annähernd jeden zweiten Begriff erklären kann. Ebenso steigt das Wissen mit dem Bildungsgrad und ist bei Männern im Durchschnitt etwas höher als bei Frauen (siehe Abb. 3.3 sowie Tab. 3.1).

Fazit Die digitale Welt ist kein ‚Neuland‘ mehr: Grundbegriffe der Digitalisierung sind angekommen, und ein Großteil der Bevölkerung fühlt sich zumindest in Teilen kompetent. Wissensdefizite bestehen aber gerade in Themen, die die Vernetzung von Daten behandeln und damit den souveränen Umgang mit den eigenen Daten besonders tangieren (z. B. Big Data, Telematik, IOT und e-Privacy).

3.3 Handlungsfreiheit

Der empfundene Freiheitsspielraum („Können“) wurde durch eine Reihe von Fragen gemessen, die sowohl objektive als auch subjektive Hürden der Handlungsfreiheit berücksichtigen – denen also sowohl die Marktsituation als auch Grenzen durch Nichtwissen oder Bequemlichkeit der Nutzer zugrunde liegt.

In den Antworten (siehe Abb. 3.4) wird deutlich, dass die Handlungsfreiheit als eher gering eingeschätzt wird, respektive einem wesentlichen Teil der Bevölkerung, der sich den Marktstrukturen ‚ausgeliefert‘ sieht. Ergänzend dazu misstraut eine leichte Mehrheit der Einhaltung von Datenschutzvorschriften durch die Unternehmen. Am ehesten erscheint den Befragten noch die individuelle Datenfreigabe beeinflussbar. Einer Ausschöpfung dieser Spielräume steht allerdings die empfundene Komplexität der jeweiligen Datenschutzbestimmungen entgegen, durch die sich eine Mehrheit überfordert fühlt.

Die Unterschiede nach Geschlecht, Alter und selbst nach Schulbildung sind eher gering: So sind Akademiker genauso der Meinung wie andere Bildungsschichten, dass man „die Datenschutzbedingungen gar nicht alle lesen“ könne, und sehen auch kaum mehr Einflussmöglichkeit auf die eigene Datenspur. Erst mit steigendem *digitalem Wissen* werden tendenziell etwas höhere Handlungsspielräume gesehen (siehe beispielhaft Abb. 3.5).

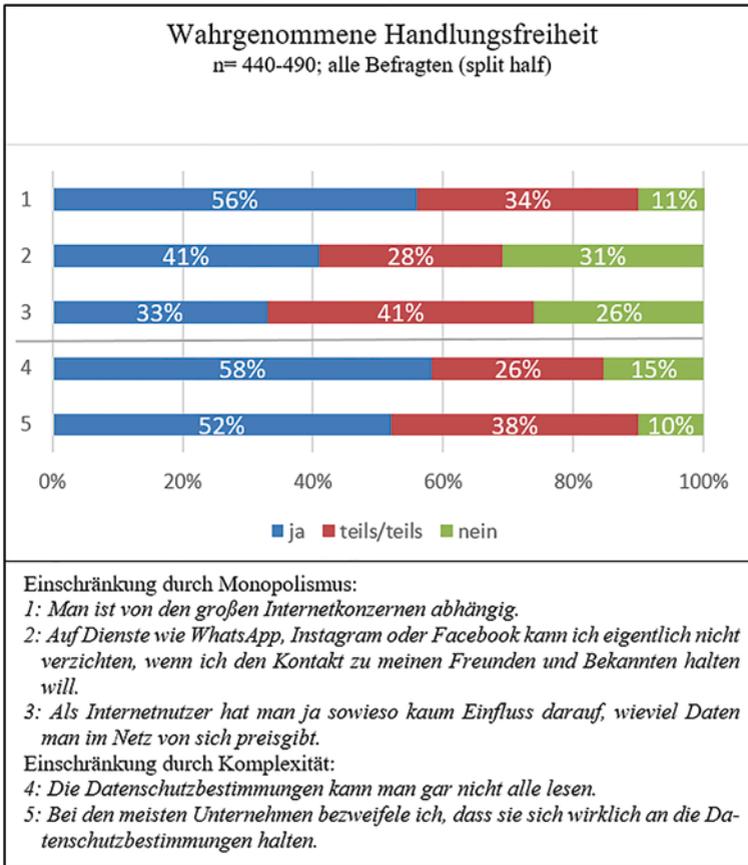


Abb. 3.4 Wahrgenommene Handlungsfreiheit (,Können'): Gesamtbevölkerung

Fazit Es besteht ein hohes Abhängigkeitspotenzial: Die Bürger fühlen sich – quer durch alle Bevölkerungsgruppen – aufgrund von Komplexität und Marktstrukturen nur sehr bedingt handlungsfrei oder souverän. Regelungen wie z. B. aus der Europäischen Datenschutzgrundverordnung, die ausgehend vom Ideal eines mündigen und kritischen Bürgers Verbraucherinteressen über Information- und Zustimmungspflichten sichern wollen (siehe Kap. 1), drohen damit ‚ins Leere‘ zu laufen.

Wahrgenommene Handlungsfreiheit – Internetnutzer

n=934-935, Personen, die zumindest mehrmals im Monat das Internet nutzen

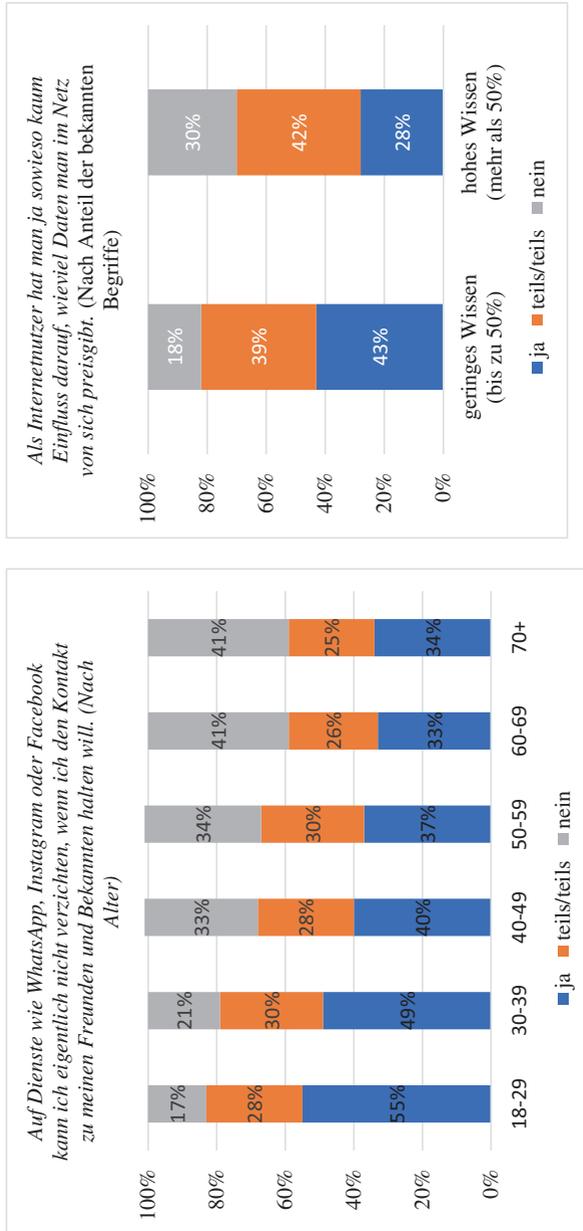


Abb. 3.5 Wahrgenommene Handlungsfreiheit (,Können'): Internetnutzer

3.4 Folgeabschätzungen, Bewertung von Anwendungsfeldern und Einstellungen zu Datenschutz und Technologie (,Wollen‘)

Die affektive Bewertung von Big Data, Vernetzung und Co., also das ,Wollen‘, bezieht sich auf die generelle Einschätzung möglicher Technikfolgen, auf die Bewertung konkreter Anwendungsfelder sowie schließlich auf die generelle Einstellung zu Datenschutz einerseits und neuen Technologien andererseits.

3.4.1 Folgeabschätzungen

Um mögliche positive und negative Folgen von Big Data zu erfassen, wurde betrachtet, welche menschlichen Grundmotive dadurch erfüllt oder gefährdet werden können (zu Grundlagen menschlicher Motivation siehe z. B. McClelland 1985, Heckhausen & Heckhausen 2010). Auf Basis der Motive *Sicherheit, sozialer Zugehörigkeit, Aktivierung, Kontrolle, Komfort* und *Effizienz* wurden Chancen und Risiken für den Einzelnen abgeleitet und durch die Befragten bewertet.

Ergänzend dazu wurden je vier allgemeine Folgeeinschätzungen zum Thema Wirtschaft und Gesellschaft erfasst:

- *Wirtschaft*: Während in der politischen Diskussion derzeit die Frage im Vordergrund steht, wie Daten als ,das neue Öl‘, also als Ressource der Zukunft, ideal zu erschließen und zu nutzen sind, steht in der öffentlichen Diskussion vielfach die Frage nach Arbeitsplätzen im Vordergrund.
- *Medien und Gesellschaft*: Hier werden insbesondere die Wirkung von Vernetzung, Big Data und Künstlicher Intelligenz auf die Aufklärung und die demokratische Grundordnung diskutiert: Einerseits, ob das Wissen der Bürger durch die bessere Verfügbarkeit von Informationen steigt oder durch oberflächliche, falsche, manipulierte oder vorselektierte Informationen (sog. ,Filterblase‘) eher abnimmt. Andererseits, ob infolgedessen die Demokratie eher gefördert oder geschwächt wird.

Auf Basis dieser insgesamt 24 Einschätzungen wurde ein Optimismus-Index gebildet und anhand dessen drei Typen unterschieden. Ergänzend gaben die Befragten eine Gesamteinschätzung an, ob eher die Risiken oder die Chancen von Big Data überwiegen.

Tab. 3.2 Folgeabschätzungen im Überblick: Chancen (n=440–490, die ungekürzten Fragetexte finden sich im Anhang)

| <i>Die Erfassung und automatische Verarbeitung großer Datenmengen über den Einzelnen wird ...</i> | Stimme zu (%) | Teils/teils (%) | Stimme nicht zu (%) |
|---------------------------------------------------------------------------------------------------|---------------|-----------------|---------------------|
| <i>... uns Dinge ermöglichen, von denen wir früher nur zu träumen wagten</i> | 53 | 37 | 10 |
| <i>... uns helfen, Dinge schneller zu erledigen</i> | 51 | 36 | 13 |
| <i>... den Kontakt mit Freunden und Familie erleichtern</i> | 42 | 32 | 26 |
| <i>... dem Einzelnen viele neue Möglichkeiten eröffnen, sein Leben zu gestalten</i> | 41 | 40 | 19 |
| <i>... unser Leben deutlich bequemer machen</i> | 39 | 43 | 18 |
| <i>... uns Spaß und neue Anregungen geben, zum Beispiel durch neue Spiele</i> | 39 | 39 | 22 |
| <i>... den Menschen helfen, besser und günstiger einkaufen zu können</i> | 36 | 41 | 22 |
| <i>... für mehr Wissen und Aufklärung bei den Menschen sorgen</i> | 34 | 43 | 23 |
| <i>.. unser Leben in Zukunft deutlich sicherer machen (z. B. Verkehr, Gesundheit, Eigentum)</i> | 31 | 41 | 28 |
| <i>... uns helfen, Energie zu sparen</i> | 25 | 36 | 38 |
| <i>... auf lange Sicht Geld sparen</i> | 24 | 35 | 41 |
| <i>... die Welt durch mehr Meinungsvielfalt demokratischer machen</i> | 21 | 37 | 42 |
| <i>... insgesamt mehr Wohlstand schaffen</i> | 15 | 37 | 48 |

Überwiegen die Risiken oder die Chancen? Ein erster Blick auf die Verteilungen in Tab. 3.2 und 3.3 (eine genauere Auswertung nach Themenfeldern erfolgt auf den Folgeseiten) zeigt, dass eine recht differenzierte Sicht zu den einzelnen Risiken und Chancen vorliegt – also keinesfalls pauschal Risiken oder Chancen gesehen werden, aber zugleich die Risiken (Tab. 3.3) insgesamt eher bejaht werden als die Chancen (Tab. 3.2).

Die gleiche Tendenz zeigt sich auch in der Gesamtbeurteilung: Unabhängig davon, ob wir die Frage positiv oder negativ formuliert haben, überwiegen jeweils die Risiken gegenüber den Chancen, mit jeweils einem hohen Anteil an ‚neutralen‘ Urteilen (siehe Abb. 3.6).

Tab. 3.3 Folgeabschätzungen im Überblick: Risiken (n=440–490, die ungekürzten Fragetexte finden sich im Anhang)

| <i>Die Erfassung und automatische Verarbeitung großer Datenmengen über den Einzelnen wird ...</i> | Stimme zu (%) | Teils/teils (%) | Stimme nicht zu (%) |
|---------------------------------------------------------------------------------------------------|---------------|-----------------|---------------------|
| <i>... den Schutz unserer Privatsphäre immer schwieriger machen</i> | 80 | 16 | 4 |
| <i>... neue Gefahren schaffen (z. B. durch Fehler in der Technik, Datenmissbrauch ...)</i> | 78 | 19 | 4 |
| <i>... dazu führen, dass manche Menschen aufgrund ihrer Daten ungerecht behandelt werden</i> | 57 | 34 | 9 |
| <i>... uns abhängig machen von Entscheidungen, die ...Computer für uns treffen</i> | 50 | 32 | 18 |
| <i>... das Leben zunehmend stressiger machen</i> | 49 | 34 | 17 |
| <i>... die Menschen immer mehr vereinsamen lassen</i> | 49 | 34 | 17 |
| <i>... dem Einzelnen immer mehr Wahlfreiheit nehmen</i> | 47 | 35 | 19 |
| <i>... dafür sorgen, dass unser Wissen immer oberflächlicher wird</i> | 46 | 32 | 22 |
| <i>... viele Dinge des Alltags noch komplizierter und undurchschaubarer machen</i> | 44 | 36 | 20 |
| <i>... für eine zunehmende Entdemokratisierung sorgen</i> | 35 | 38 | 27 |
| <i>... die Arbeitslosigkeit erhöhen</i> | 30 | 33 | 37 |

Als Zwischenfazit lässt sich festhalten: Chancen und Risiken werden durchaus einzeln und differenziert wahrgenommen, wobei jedoch der Blick auf die Risiken der Digitalisierung und Vernetzung überwiegt (*„Negativitäts-Dominanz“*).

Diese Negativitätsdominanz gilt auch bei der **Betrachtung der einzelnen Motivfelder** (siehe Tab. 3.4) und unterscheidet sich damit vielfach von den optimistischen Erwartungen der Experten (siehe dazu Kap. 2):

- **Sicherheit:** Eine große Mehrheit erwartet neue, digitale Risiken, während nur knapp jeder Dritte glaubt, dass die Welt durch Big Data insgesamt an Sicherheit gewinnt.
- **Soziale Zugehörigkeit:** Hier findet die Befürchtung, dass die Menschen durch die neue Technik weiter vereinsamen, als auch die Chance, dass sich der Kontakt zu Freunden und Familie vereinfacht, moderate Zustimmung. Aber auch in diesem Bereich liegt das Risiko (mit 49 %) vor der Chance (mit 42 %). Noch deutlicher wird die Tendenz bei den Ablehnungen (Risiko 17 %, Chance 26 %).

Folgeabschätzung Gesamteindruck: Mehr Risiken als Chancen

n=462 – 464; alle Befragten (split half)

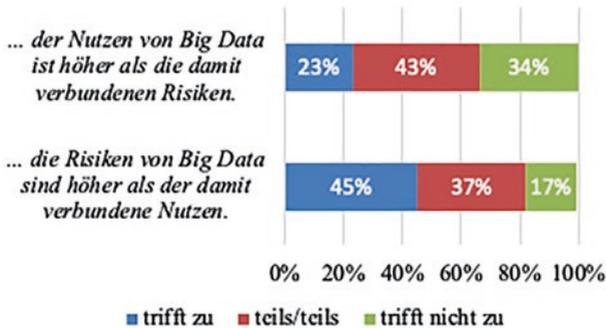


Abb. 3.6 Folgeabschätzung Gesamteindruck („Alles in Allem glaube ich ...“)

- *Aktivierung*: Selbst zu diesem Thema dominiert die Erwartung zusätzlichen Stresses gegenüber der Hoffnung auf „Spaß und neue Anregungen“.
- *Kontrolle*: Dass neue Spielräume und zusätzliche Möglichkeiten der Lebensgestaltung gewonnen werden, wird von immerhin etwa der Hälfte der Befragten bejaht. Dem steht allerdings in gleichem Umfang die Befürchtung entgegen, in Abhängigkeit von computergenerierten Entscheidungen zu geraten und in seinen Wahlfreiheiten beschnitten zu werden. Hinzu kommt – mit der insgesamt höchsten Zustimmungsqute aller Fragen – die Gefährdung der Privatsphäre.

Etwas ausgeglichener ist das Verhältnis von erwarteten Chancen und Risiken in den beiden übrigen Motivfeldern:

- *Komfort*: Hier gleichen sich die Erwartungen eines bequemerem Lebens und die Befürchtung zunehmender Komplexität annähernd aus.
- *Effizienz*: Während eine knappe Mehrheit erwartet, dass „Dinge schneller zu erledigen“ seien, bleiben die Hoffnungen auf finanzielle Einsparungen sowie höhere Energieeffizienz sehr verhalten.

Bezogen auf die Gesellschaft hatten wir bewusst gegensätzliche Formulierungen gesucht und – wie die vorhergehenden Fragen auch – jeweils der Hälfte

Tab. 3.4 Folgeabschätzungen für den Einzelnen, sortiert nach Motivfeldern (n=472–490; alle Befragten [split half]). Die ungekürzten Fragetexte finden sich im Anhang.)

| Motivfeld | <i>Die Erfassung und automatische Verarbeitung großer Datenmengen über den Einzelnen wird ...</i> | Stimme zu (%) | Teils/teils (%) | Stimme nicht zu (%) |
|---------------|-----------------------------------------------------------------------------------------------------|---------------|-----------------|---------------------|
| Sicherheit | <i>... neue Gefahren schaffen (z. B. durch Fehler in der Technik, Datenmissbrauch/-Verlust ...)</i> | 78 | 19 | 4 |
| | <i>... unser Leben in Zukunft deutlich sicherer machen (z. B. Verkehr, Gesundheit, Eigentum)</i> | 31 | 41 | 28 |
| Zugehörigkeit | <i>... die Menschen immer mehr vereinsamen lassen</i> | 49 | 34 | 17 |
| | <i>... den Kontakt mit Freunden und Familie erleichtern</i> | 42 | 32 | 26 |
| Aktivierung | <i>... das Leben zunehmend stressiger machen</i> | 49 | 34 | 17 |
| | <i>... uns Spaß und neue Anregungen geben, z. B. durch neue Spiele oder Unterhaltungsangebote</i> | 39 | 39 | 22 |
| Kontrolle | <i>... den Schutz unserer Privatsphäre immer schwieriger machen</i> | 80 | 16 | 4 |
| | <i>... uns abhängig machen von Entscheidungen, die Maschinen und Computer für uns treffen</i> | 50 | 32 | 18 |
| | <i>... dem Einzelnen immer mehr Wahlfreiheit nehmen</i> | 47 | 35 | 19 |
| | <i>... uns Dinge ermöglichen, von denen wir früher nur zu träumen wagten</i> | 53 | 37 | 10 |
| | <i>... dem Einzelnen viele neue Möglichkeiten eröffnen, sein Leben zu gestalten</i> | 41 | 40 | 19 |
| Komfort | <i>...viele Dinge des Alltags noch komplizierter und undurchschaubarer machen</i> | 44 | 36 | 20 |
| | <i>...unser Leben deutlich bequemer machen</i> | 39 | 43 | 18 |
| Effizienz | <i>... uns helfen, Dinge schneller zu erledigen</i> | 51 | 36 | 13 |
| | <i>... uns helfen, Energie zu sparen</i> | 25 | 36 | 38 |
| | <i>... auf lange Sicht Geld sparen</i> | 24 | 35 | 41 |

Tab. 3.5 Folgeabschätzungen für Wirtschaft und Gesellschaft (n=450–485, alle [split half] Befragten)

| Feld | Risiken/ Chancen | <i>Die Erfassung und automatische Verarbeitung großer Datenmengen über den Einzelnen wird ...</i> | Stimme zu (%) | Teils/teils (%) | Stimme nicht zu (%) |
|--------------|---------------------|---------------------------------------------------------------------------------------------------|---------------|-----------------|---------------------|
| Gesellschaft | Risiken | <i>... dafür sorgen, dass unser Wissen immer oberflächlicher wird</i> | 46 | 32 | 22 |
| | | <i>... für eine zunehmende Entdemokratisierung sorgen</i> | 35 | 38 | 27 |
| | Chancen | <i>... für mehr Wissen und Aufklärung bei den Menschen sorgen</i> | 34 | 43 | 23 |
| | | <i>... die Welt durch mehr Meinungsvielfalt demokratischer machen</i> | 21 | 37 | 42 |
| Wirtschaft | Risiken | <i>... dazu führen, dass manche Menschen aufgrund ihrer Daten ungerecht behandelt werden</i> | 57 | 34 | 9 |
| | | <i>... die Arbeitslosigkeit erhöhen</i> | 30 | 33 | 37 |
| | Chancen | <i>... den Menschen helfen, besser und günstiger einkaufen zu können</i> | 36 | 41 | 22 |
| | | <i>... insgesamt mehr Wohlstand schaffen</i> | 15 | 37 | 48 |

der Stichprobe vorgelegt. In beiden Fällen fällt das Saldo der Antworten leicht pessimistisch aus: also eher *Entdemokratisierung* statt *Demokratiegewinn durch Meinungsvielfalt* sowie *oberflächlicheres Wissen* anstelle von „*mehr Wissen und Aufklärung*“ (siehe Tab. 3.5).

Auch in Bezug auf die Volkswirtschaft erwarten nur 15 % der Befragten positive *Wohlstandseffekte*, doppelt so viele befürchten dagegen einen Anstieg der *Arbeitslosigkeit* (die Wahrnehmung marktwirtschaftlicher Zusammenhänge durch Laien ist in vielen Fällen pessimistisch verzerrt, siehe dazu Caplan 2007 sowie Enste et al. 2009). Daneben sehen deutlich mehr als die Hälfte der Befragten das Risiko der *Diskriminierung* Einzelner, während immerhin 36 % Vorteile für Konsumenten sehen („besser und günstiger einkaufen“).

Auf Basis der Bewertung der von uns vorgegebenen 13 Chancen und 11 Risiken haben wir die Befragten in drei Gruppen klassifiziert (siehe Abb. 3.7):

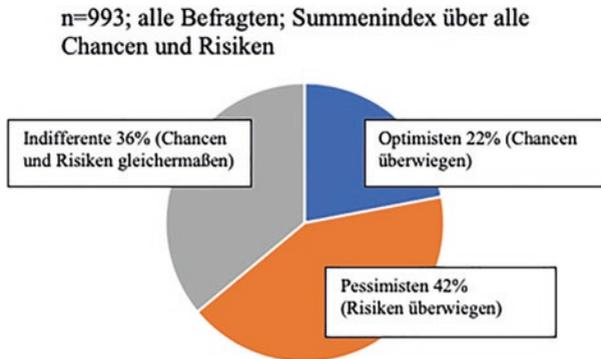


Abb. 3.7 Typen nach Chancen und Risiken

1. ‚Optimisten‘, die primär die Chancen sehen,
2. ‚Indifferente‘, bei denen weder die Chancen noch die Risiken deutlich überwiegen,
3. ‚Pessimisten‘, bei denen die negativen Einschätzungen dominieren.

Als Optimist wurden Befragte klassifiziert, wenn sie bei ihren insgesamt 12 Folgeeinschätzungen mindestens drei Chancen mehr bejahten (oder analog Risiken verneinten) als umgekehrt. Analog wurden Befragte als Pessimist klassifiziert, wenn sie bei ihren insgesamt 12 Folgeeinschätzungen mindestens drei Risiken mehr bejahten (oder analog Chancen verneinten) als umgekehrt.

Chancen, die bei höherem Informationsstand stärker gesehen werden (siehe Abb. 3.8), betreffen vor allem die neuen Möglichkeiten der Lebensgestaltung (Kontrolle) und damit verbunden die zeitliche Effizienz sowie Spaß und Anregung (Aktivierung). Aber auch bei den übrigen Chancen ist tendenziell ein Anstieg zu erkennen.

Sorgen lassen tendenziell mit zunehmender Kenntnis nach (siehe Abb. 3.8). Manche Befürchtungen könnten sich also durchaus als ‚Scheinriesen‘ (im Sinne von Michael Endes bekannter Figur aus dem Kinderbuch „Jim Knopf und Lukas der Lokomotivführer“) erweisen, die bei näherer Betrachtung immer kleiner werden und sich somit durch Aufklärung zumindest in Teilen entkräften lassen. Das betrifft besonders die Sorge vor Verkomplizierung des Alltags, in wirtschaftlicher Hinsicht die Zunahme der Arbeitslosigkeit und aus gesellschaftlicher Perspektive die Gefahr zunehmender Vereinsamung. Einige Erwartungen werden aber nicht durch Aufklärung beeinflusst (z. B. Sorge vor Entdemokratisierung) oder werden sogar durch zusätzliche Informationen noch pessimistischer (z. B. bezüglich Meinungsvielfalt).

Die Erfassung und automatische Verarbeitung großer Datenmengen über den Einzelnen wird ...

Unterschiede nach digitalem Wissen (Beispiele):



Abb. 3.8 Folgeabschätzungen: Typen und Einfluss digitalen Wissens

Fazit Befürchtungen überwiegen. Aufklärung ‚hilft‘, aber einzelne Sorgen nehmen mit zunehmendem digitalen Wissen noch zu.

3.4.2 Bewertung von Anwendungsfeldern

Aufbauend auf der Einschätzung von Nutzen und Risiken haben die Befragten unterschiedliche Einsatzbereiche von Daten, die im Internet oder durch vernetzte Geräte gewonnenen werden, bewertet. Diese wurden untergliedert in

- a) gesamtgesellschaftliche Fragestellungen,
- b) Anwendungsfelder in Marketing und Konsum,
- c) Anwendungen in der Lebenswelt Mobilität,
- d) Anwendungen in der Lebenswelt Wohnen,
- e) Anwendungen in der Lebenswelt Gesundheit⁴.

Bezogen auf Gesellschaft und Konsum wurden einige der verbreitetsten oder der derzeit meistdiskutierten Anwendungen vorgestellt.

Die Ergebnisse (siehe Tab. 3.6 und 3.7) sind eindeutig: Überwachung im Sinne der Strafverfolgung oder öffentlichen Ordnung erfährt weitgehend Zustimmung (die grundgesetzlich bedingten rechtlichen Bedenken hierzu scheinen nicht weit in das Bewusstsein der Bevölkerung vorgedrungen zu sein). Auch spielt die Schwere des Deliktes nur eine nachrangige Rolle: Geht es anstelle von schweren Gewaltverbrechen wie Mord, Totschlag oder Terrorismus nur um Eigentumsdelikte, sinkt die Zustimmung lediglich von 59 % auf 45 %, und die Ablehnenden bleiben deutlich in der Minderheit. Überwiegend negativ werden dagegen die übrigen gesellschaftlichen Anwendungsfelder bewertet. Weder die Vorauswahl von Nachrichten (zur Problematik von ‚Filterblasen‘ siehe Pariser 2011) noch die von Stellenbewerbern findet Zustimmung.

Diese Ablehnung gilt erst recht für das Social Scoring. Ein solches Aufsichtssystem (siehe Kap. 1) findet hierzulande lediglich 10 % Zustimmung. Wenn allerdings berücksichtigt wird, wie weitreichend ein solches Instrument tatsächlich in das Leben eingreift, erscheint dieser Anteil gar nicht mehr wenig, sondern erstaunlich hoch, erst recht, wenn nach Hinzunahme der neutralen Bewertungen immerhin ein Drittel der Bevölkerung ein solches System zumindest nicht ablehnt.

⁴Zu den Lebenswelten siehe Kap. 2.

Tab. 3.6 Anwendungsfelder in der Gesellschaft (n = 461–504, alle Befragten [split half])

| Anwendungsfeld | Das finde ich gut (%) | Neutral (%) | Das finde ich schlecht (%) |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------|----------------------------|
| Überwachung von öffentlichen Plätzen | 60 | 27 | 13 |
| Einleitung einer polizeilichen Überwachung bei Verdacht auf ein schweres Verbrechen (z. B. Mord, Totschlag, Terrorismus) | 59 | 26 | 15 |
| Einleitung einer polizeilichen Überwachung bei Verdacht auf ein Eigentumsdelikt (z. B. Einbruch, Diebstahl, Betrug) | 45 | 34 | 21 |
| Vorauswahl von Nachrichten, die den Interessen des Einzelnen entsprechen | 21 | 33 | 45 |
| Vorauswahl von Bewerbern in Unternehmen | 17 | 30 | 54 |
| „Social Scoring“ ^a | 10 | 22 | 68 |

^aFragetext zu Social Scoring: „Erstellung eines Punktwertes, bei dem die einzelnen Bürger nach ihrer Leistung für die Gesellschaft bewertet werden. Bürger, die viel für die Gemeinschaft leisten, würden beispielsweise bei Wartezeiten in Ämtern oder bei der Wohnungssuche bevorzugt, während andere entsprechend länger warten müssten“

Tab. 3.7 Anwendungsfelder in Marketing/Konsum (n = 461–504, alle Befragten [split half])

| Anwendungsfeld | Das finde ich gut (%) | Neutral (%) | Das finde ich schlecht (%) |
|---------------------------------------------------------------------------------------------------------------|-----------------------|-------------|----------------------------|
| Prüfung der Kreditwürdigkeit | 26 | 35 | 39 |
| Festsetzung von Preisen bei Onlinekäufen, abhängig von der <i>Tageszeit</i> oder <i>Situation</i> des Käufers | 20 | 30 | 50 |
| Bearbeitung von Kundenanfragen durch einen Sprachcomputer | 20 | 30 | 50 |
| Auswahl von Werbung, die zu den Interessen des Einzelnen passt | 18 | 31 | 51 |
| Festsetzung von Preisen bei Onlinekäufen, abhängig von der <i>Person</i> des Käufers | 14 | 25 | 61 |

Eines der Haupteinsatzfelder von Scorings und Künstlicher Intelligenz liegt bereits heute im Bereich des Marketings oder – breiter definiert – des Kundenmanagements von Unternehmen. Auch diesbezüglich überwiegt die Skepsis. Selbst wenn die neutrale Mittelkategorie als Akzeptanz gewertet wird

(schließlich erfährt der Kunde ja meist keinen unmittelbaren Nutzen aus den gewählten Anwendungen), beträgt die Ablehnung 50 % und mehr. Ausnahme ist die Kreditprüfung, bei der die Legitimität des Anbieters, Absicherung zu suchen, auch am ehesten nachzuvollziehen ist. ‚Mikrotargeting‘, ‚Dynamic Pricing‘ (vor allem auf Basis von Personenprofilen) und auch der Einsatz von Sprachcomputern basierend auf Künstlicher Intelligenz (sog. Chatbots) stoßen dagegen auf breite Kritik.

Anhand der Bewertung exemplarischer Anwendungen aus den Lebenswelten (siehe Tab. 3.8, 3.9 und 3.10) sind grundlegende Tendenzen zur Akzeptanz des Einsatzes von Big Data und Algorithmen im Alltag zu erkennen:

Tab. 3.8 Anwendungsfelder in der Lebenswelt Mobilität (n=464–504, alle Befragten [split half])

| Anwendungsfeld | Das finde ich gut (%) | Neutral (%) | Das finde ich schlecht (%) |
|---------------------------------------------------------------------------------------|-----------------------|-------------|----------------------------|
| Verkehrsabhängige Navigation im Auto | 72 | 21 | 7 |
| Bereitstellung von öffentlichen Verkehrsmitteln in Abhängigkeit vom momentanen Bedarf | 62 | 29 | 9 |
| Überwachung der Einhaltung von Verkehrsregeln | 51 | 32 | 17 |
| Steuerung eines selbstfahrenden Autos | 30 | 32 | 38 |

Tab. 3.9 Anwendungsfelder in der Lebenswelt Wohnen (n=464–504, alle Befragten [split half])

| Anwendungsfeld | Das finde ich gut (%) | Neutral (%) | Das finde ich schlecht (%) |
|----------------------------------------------------------------------------------------------------|-----------------------|-------------|----------------------------|
| Überwachung der Wohnung gegen Einbrecher | 53 | 33 | 15 |
| Automatische Übernahme von Tätigkeiten im Haushalt wie Staubsaugen oder Fensterputzen | 49 | 27 | 24 |
| Auf die Gewohnheiten der Bewohner angepasste automatische Steuerung der Wohnungsheizung | 42 | 32 | 26 |
| Auf die Nutzer einer Wohnung angepasste automatische Steuerung der Raumbeleuchtung | 27 | 39 | 33 |
| Intelligenter Kühlschrank, der meldet, wenn etwas fehlt, oder auf Wunsch sogar selbst nachbestellt | 17 | 28 | 55 |

Tab. 3.10 Anwendungsfelder in der Lebenswelt Gesundheit (n = 464–504, alle Befragten [split half])

| Anwendungsfeld | Das finde ich gut (%) | Neutral (%) | Das finde ich schlecht (%) |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------|----------------------------|
| Überprüfung der Medikamenteneinnahme bei älteren Menschen | 62 | 23 | 14 |
| Überwachung von Herzschlag und Blutdruck, um vor einem möglichen Herzinfarkt zu warnen | 62 | 27 | 11 |
| Verbesserte Diagnose/zielgenauere Behandlung von Krankheiten aufgrund der Auswertung aller gesundheitsrelevanten Daten der Bevölkerung | 55 | 30 | 15 |
| Zusammenführung aller Gesundheitsinformationen einer Person für eine bessere Gesundheitsvorsorge | 43 | 36 | 21 |
| Einsatz von Automaten, die einfache Aufgaben in der Altenpflege übernehmen können | 36 | 27 | 37 |
| Überwachung von Bewegung/sportlicher Aktivität, um Empfehlungen für eine gesündere Lebensweise zu geben | 27 | 37 | 36 |
| Überprüfung des Lebensstils, um bei einem gesunden Lebensstil Preisnachlässe in der Krankenversicherung zu erhalten | 24 | 31 | 45 |

- *Hohe Akzeptanz:* Ein Großteil der Befragten kann sich die meisten beschriebenen Anwendungen in allen drei Lebenswelten Mobilität, Wohnen und Gesundheit durchaus vorstellen. **Die zuvor beschriebene Grundskepsis kippt, wenn konkrete, nutzenstiftende Anwendungen genannt werden.**
- *Sicherheit geht vor:* Analog zu den gesellschaftlichen Einsatzfeldern ist die Akzeptanz besonders dann hoch, wenn es um die Abwendung von Gefahren geht – sei es im Feld der Gesundheit, im Einbrecherschutz oder selbst zur Überwachung der Verkehrsregeln.
- *Unterstützung ja, Automatisierung „ja, aber“:* Anwendungsfelder werden in der Tendenz negativer bewertet, je mehr sie den Alltag nicht nur unterstützen, sondern auch gefühlt „die Kontrolle übernehmen“ (vergleiche z. B. die geringe Akzeptanz von intelligenten Kühlschränken, selbstfahrenden Autos oder der automatisierten Raumbeleuchtung).

- *Die Roboter können kommen:* Werden aber keine als wesentlich empfundene Handlungsspielräume eingeschränkt und ist der Nutzen offensichtlich (z. B. beim Staubsaugen, Fensterputzen oder bei der Heizungssteuerung), ist die Akzeptanz automatischer Steuerung hoch. Selbst für sogenannte ‚Pflegeroboter‘ in der Altenpflege finden sich ebenso viele Befürworter wie Ablehner.
- *Wenig Angst vor Überwachung:* Viele der Anwendungen (zum Beispiel im Gesundheitsmonitoring, der Verkehrssteuerung oder auch im Smart Home) erfordern eine weitgehende Überwachung des Einzelnen. In den Antworten lässt sich aber kein klarer Zusammenhang zwischen Überwachungsgrad und Akzeptanz feststellen, vielmehr **scheint alleine der empfundene Nutzen der Anwendung über Befürwortung und Ablehnung zu entscheiden.**

Einige Bewertungen variieren deutlich mit dem Alter der Befragten. So werden Einsätze zu ‚Recht und Ordnung‘ vermehrt von Älteren befürwortet, Smart Home oder das selbstfahrende Auto dagegen deutlich mehr von jüngeren Menschen.

3.4.3 Einstellungen zu Datenschutz und Technologien

Neben Folgeabschätzungen und der Bewertung von Anwendungsfeldern stellt die grundsätzliche *Einstellung zum Datenschutz* einerseits und zum *Umgang neuen Techniken* andererseits ein wesentliches Element der Motivation, also des ‚Wollens‘ von Big Data dar. Um die Einstellung der Befragten gegenüber dem Datenschutz zu erfassen, wurde nach der persönlichen Relevanz gefragt sowie als Gegensatz dazu die Zustimmung zur viel zitierten Meinung, man „habe nichts zu verbergen“. Dies wurde ergänzt um eine Frage zur empfundenen Valenz der Beschäftigung – also der individuellen *Freude an neuen Technologien*.

In den Antworten zur *persönlichen Bedeutung des Datenschutzes* zeigt sich dessen unverändert hoher Stellenwert für die meisten Bürger (siehe Abb. 3.9). Ob der bei den unter 30-Jährigen zu beobachtende ‚Einbruch‘ ein Kohorteneffekt ist (in dem Sinne, dass nachwachsende Generationen weniger Datenschutzbedenken haben) oder lediglich ein Alterseffekt (d. h. junge Menschen haben weniger Erfahrung oder weniger schützenswerte Daten, was sich aber mit zunehmendem Alter wieder ändert), lässt sich durch die vorliegende Studie leider nicht abschließend klären. Umgekehrt findet der viel zitierte Spruch „*ich habe nichts zu verbergen*“ als Argument für einen freizügigen Umfang mit Daten nur bedingte Zustimmung – dies am ehesten noch in der älteren Generation, auch dort zeigt sich also ein tendenziell hohes Datenbewusstsein.

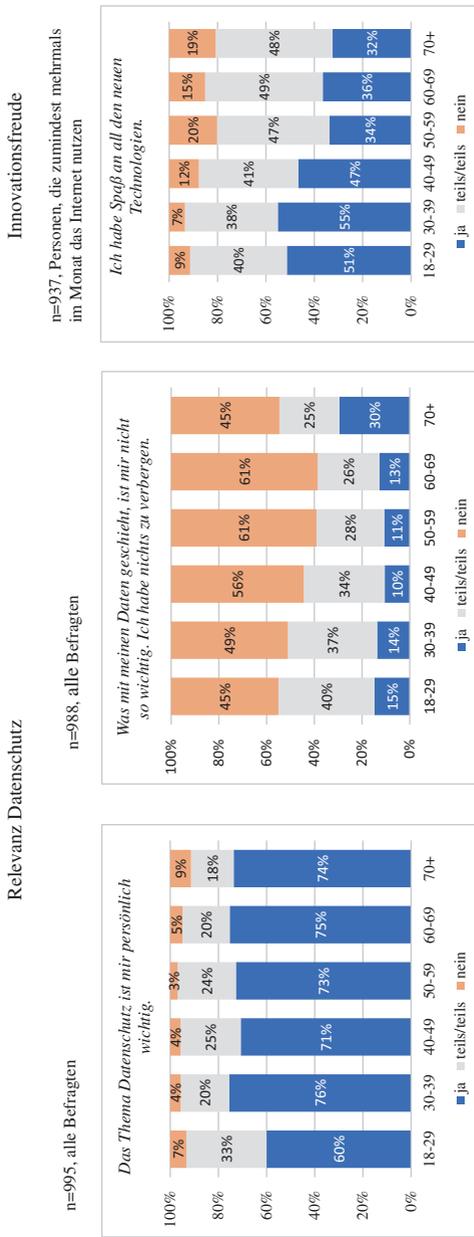


Abb. 3.9 Einstellung zu Datenschutz und Technologien

Ungeachtet möglicher Datenschutzbedenken einerseits und Nutzenversprechen andererseits ist der *Spaß* oder das persönliche ‚*Involvement*‘ ein wesentlicher Faktor, der zur Akzeptanz oder Ablehnung von Innovationen beitragen kann. Dass die neuen Techniken für einen großen Teil der Bevölkerung nicht nur ein notwendiges Übel, sondern – entweder vorrangig oder zumindest auch – eine positive Erfahrung darstellen, zeigt der untere Teil der Abb. 3.9, wobei die Zustimmung erwartungsgemäß in den jüngeren Altersklassen noch höher ist.

3.5 Verhalten („Handeln“)

In den bisherigen Ergebnissen zeigen sich eine Reihe von Konflikten. Die Folgeabschätzungen sind eher negativ, und das Datenschutzbewusstsein ist hoch. Andererseits ist das digitale Wissen rund um Schlüsselbegriffe von Vernetzung und Big Data eher gering und die empfundene Handlungsfreiheit begrenzt. Zudem werden konkrete Anwendungsfelder von Vernetzung und Big Data durchaus als positiv und nutzenstiftend gesehen.

Folgt das Verhalten nun den grundsätzlichen Einstellungen und Befürchtungen oder eher den konkreten Nutzenversprechen? Zu dieser Frage werden im Folgenden sowohl die generelle Onlinenutzung als auch konkrete Maßnahmen der User zum Schutz ihrer Daten erfasst.

3.5.1 Umfang der Online-Nutzung

Die Daten zum Nutzerverhalten (siehe Abb. 3.10) zeigen: Der Alltag der Bevölkerung ist bereits heute in hohem Maße digitalisiert und vernetzt:

- Nicht nur Computer und Smartphone, sondern auch Tablets und internetfähige Fernseher werden von einer Mehrheit genutzt. Autocomputer, Fitnessarmbänder und Homeboxes (wie Alexa) erweitern bereits heute die Vernetzung. Im Schnitt verwenden unsere Befragten 3,6 der aufgeführten ‚Devices‘.
- Ähnlich verbreitet sind führende Onlinedienste: Google, WhatsApp, YouTube und Facebook werden jeweils von einem Großteil der Bevölkerung genutzt. Und auch Dienste wie Amazon Prime, Netflix oder Instagram erreichen bereits wesentliche Teile der Gesellschaft.
- Die große Mehrheit verfügt über einen eigenen Account bei Amazon, Google und eBay (hinzu kommen die oben schon erfassten Social-Media-Dienste WhatsApp und Co.). Ein Drittel der Befragten schätzt, über 20 eigene Accounts zu haben.

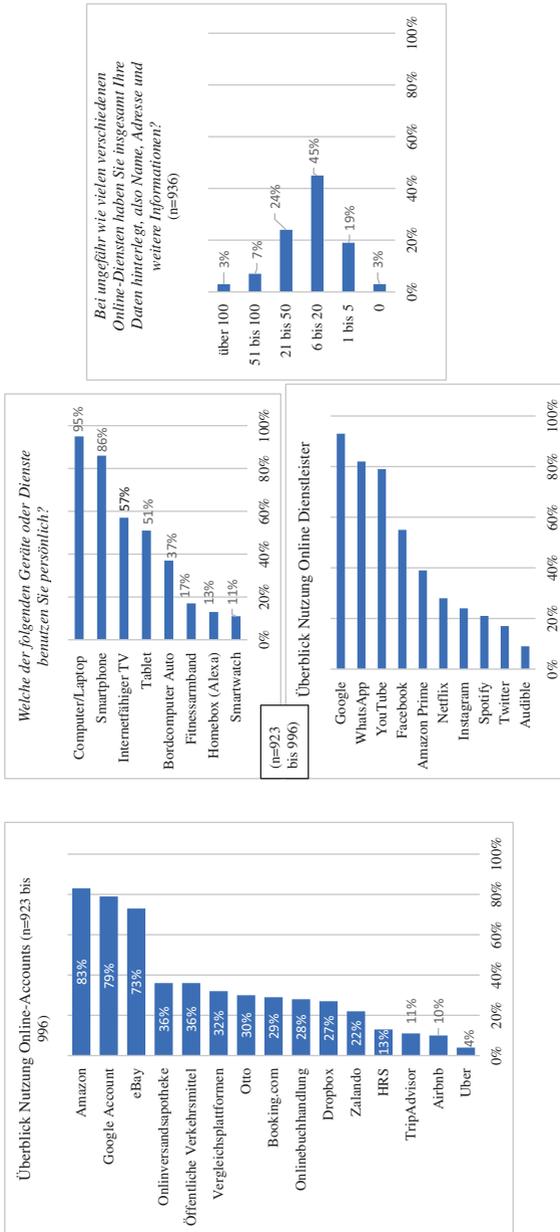


Abb. 3.10 Verhalten: Umfang der Online-Nutzung

- Lediglich die Verbreitung des Internets der Dinge (Internet of Things) hinkt, mit Ausnahme des bereits erwähnten interaktiven TV und des Auto-computers, noch deutlich hinterher. Nur einer von sechs Befragten nutzte zum Befragungszeitpunkt ein vernetztes Gerät aus dem Kontext ‚Smart Home‘.

Fazit Die Bevölkerung ist im Netz, und zwar in doppeltem Sinne: Das Internet wird intensiv und über unterschiedlichste Geräte genutzt. Zugleich sind die Nutzer über zahlreiche Dienste und Geräte ‚im Netz‘ der Dienste und hinterlassen so umfangreiche Datenspuren. Dabei dominieren US-amerikanische Internetgiganten (siehe Kap. 1), die zumindest bis zur Inkraftsetzung der EU-Datenschutzgrundverordnung im Mai 2018 niedrigeren Datenschutzstandards unterlagen als ihre deutschen Wettbewerber. Reichweite und Nutzenumfang der globalen Player dominiert offenbar gegenüber Nähe und Datenschutz, wie auch eine Gegenüberstellung unmittelbarer Wettbewerber wie booking.com versus HRS oder mit gewissen Einschränkungen Amazon versus Otto und Zalando zeigt.

3.5.2 Selbst- und Fremdeinschätzung

Eine Gegenüberstellung der großen Skepsis zum Thema Big Data und der hohen empfundenen Relevanz des Themas Datenschutz auf der einen Seite und der breiten und anscheinend weitgehend unkritischen Nutzung von Diensten und Devices auf der anderen Seite lässt bereits den **tief greifenden Einstellungs-Verhaltenskonflikt rund um den Datenschutz** erkennen: Angebote werden ungeachtet von Werthaltungen und Einstellung genutzt, sofern sich daraus ein unmittelbarer persönlicher Vorteil ergibt. Die meisten der auf der vorhergehenden Seite beschriebenen Verhaltensweisen zeigen dabei kaum einen Zusammenhang mit der persönlichen Bedeutung, die dem Datenschutz zugemessen wird. Das Bewusstsein der Nutzer zu dieser Diskrepanz zeigt Abb. 3.11.

Da Menschen zur Selbstüberschätzung neigen (Kahneman 2011) und bei der Einschätzung ‚anderer‘ Menschen oft objektiver und damit zutreffender urteilen (und dabei oft unbewusst ihr eigenes Verhalten auf die ‚Allgemeinheit‘ projizieren), haben wir die Stichprobe geteilt und die eine Hälfte der Befragten um eine Einschätzung des Verhaltens der ‚meisten Menschen‘ gebeten, die andere Hälfte um eine Selbsteinschätzung.

In der projektiven Frage wird ‚den meisten Menschen‘ ganz überwiegend ein **zu sorgloser Umgang mit den persönlichen Daten** attestiert. Bezogen auf die

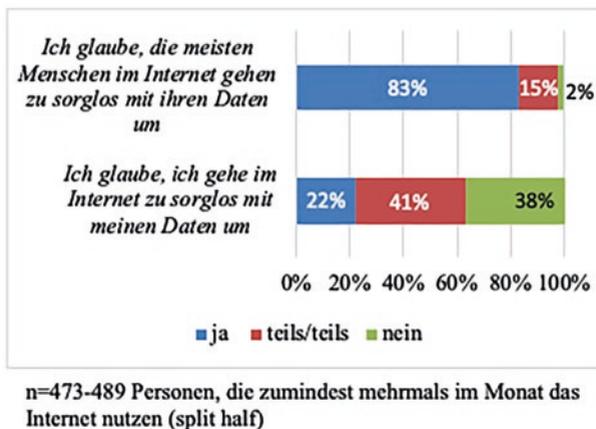


Abb. 3.11 Verhalten: Selbst und Fremdeinschätzung

eigene Person fällt das Urteil erwartungsgemäß deutlich positiver aus: Fast 40 % verneinen dies für sich selbst, aber auch hier gestehen mehr als 60 % zumindest in Teilen Handlungsdefizite ein.

Fazit: Besorgte Bürger, aber sorglose Verbraucher – **das Nutzer-Paradoxon findet weitgehend Bestätigung.** Datenschutzbedenken, generelle Sorge vor Big Data oder auch vor der Übermacht einzelner Anbieter halten die Nutzer kaum davon ab, „nützliche“ oder „notwendige“ Dienste zu nutzen. Die Mehrzahl der Verbraucher ist sich des Konfliktes durchaus bewusst.

3.5.3 Maßnahmen zum Datenschutz

Auch wenn die Dienste und Devices umfassend genutzt werden, hat der Einzelne zahlreiche *Handlungsoptionen zur eigenen Datensicherheit*. Die in den Tab. 3.11 und 3.12 abgebildeten Antworten zeigen, dass durchaus Maßnahmen ergriffen werden, allerdings nicht in dem von Experten immer wieder empfohlenen Umfang (so ändert nur jeder Zweite regelmäßig seine Passwörter).

Da die einzelnen Schutzmaßnahmen nicht unabhängig voneinander sind, sondern gehäuft in bestimmten Kombinationen auftreten, haben wir zur Identifikation *typischer Schutzstrategien* eine Faktorenanalyse durchgeführt und damit

Tab. 3.11 Verhalten: Konkrete Maßnahmen zum Datenschutz – Faktor 1: Passive Abwehr

| Faktor 1: Passive Abwehr | Anteil (%) | Faktorladung ^a |
|-------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------|
| Wenn eine App auf meine Fotos oder Kontakte zugreifen will, lehne ich das meistens ab. | 77 | ,666 |
| Ich habe schon einmal auf die Nutzung einer Webseite oder einer App verzichtet, weil ich dem Datenschutz nicht vertraut habe. | 71 | ,705 |
| (Ich lösche regelmäßig die Cookies von meinen Geräten.) | 68 | (,390) |
| Ich habe schon einmal eine Website verlassen, weil ich den Cookie nicht zulassen wollte. | 66 | ,675 |
| (Ich habe die Kamera an meinem Computer oder Tablet abgeklebt.) | 38 | (,280) |

^aDie Faktorladung gibt an, wie hoch das jeweilige Merkmal mit der jeweiligen Dimension korreliert. Geringe Faktorladungen (in Klammern) zeigen, dass sich ein Merkmal nicht eindeutig einem Faktor zuordnen lässt

die Mehrheit der Maßnahmen auf wenige, dahinterliegende Dimensionen verdichtet:

- *Passive Abwehr* umfasst niederschwellige und damit weitverbreitete Aktivitäten wie das Ablehnen von Zustimmungen oder den Verzicht auf die Nutzung einer Website (siehe Tab. 3.11).
- *Aktiver Datenschutz* umfasst hingegen Handlungen, die eine explizite Entscheidung und einen gewissen Aufwand in der Umsetzung erfordern. Sie werden von einem deutlich geringeren Teil der Nutzer eingesetzt (siehe Tab. 3.12).
- *Laissez-faire* beinhaltet eine weitgehend unreflektierte Übernahme bzw. Akzeptanz von Voreinstellungen oder Abfragen. Die hohen Zustimmungsraten zum Beispiel zum „Überlesen“ von Datenschutzbestimmungen zeigen, dass gesetzlich vorgegebene Regeln zur Aufklärung und Einholung von Zustimmungen zumindest in der derzeitigen Form vielfach ‚ins Leere laufen‘ (siehe Tab. 3.13).

Die Löschung von Cookies und das Abkleben der Kamera liegen an der Grenze zwischen passiver Abwehr (höchste Übereinstimmung) und aktivem Datenschutz und lassen sich den Faktoren daher nicht ganz eindeutig zuordnen.

Eine *Einteilung der Nutzer* nach Zahl der getroffenen Maßnahmen zeigt, dass sich der typische ‚pragmatische‘ Nutzer in ca. der Hälfte der abgefragten

Tab. 3.12 Verhalten: Konkrete Maßnahmen zum Datenschutz – Faktor 2: Aktiver Datenschutz

| Faktor 2: Aktiver Datenschutz | Anteil (%) | Faktorladung |
|---------------------------------------------------------------------------------------|------------|--------------|
| Ich ändere meine Passwörter regelmäßig. | 50 | ,508 |
| Ich verschlüssele meine E-Mails. | 34 | ,564 |
| Ich nutze Funktionen, um im Internet anonym zu bleiben (bspw. einen privaten VPN). | 33 | ,620 |
| Ich nutze eine Suchmaschine, die keine persönlichen Daten sammelt. | 32 | ,491 |
| Ich habe schon einmal ein Unternehmen aufgefordert, meine Daten zu löschen. | 29 | ,447 |
| Ich nutze einen datengeschützten Messenger Dienst, z. B. Threema, Signal oder SIMSme. | 19 | ,570 |

Tab. 3.13 Verhalten: Konkrete Maßnahmen zum Datenschutz – Faktor 3: Laissez Faire

| Faktor 3: Laissez Faire | Anteil (%) | Faktorladung |
|------------------------------------------------------------------------------------------------------------------|------------|--------------|
| Ich habe mindestens eine Payback- oder Kundenkarte, für deren Benutzung ich Rabatte oder andere Vorteile erhalte | 67 | ,479 |
| Ich lese mir die Datenschutzbestimmungen von Websites oder Online-Anbietern eigentlich nie richtig durch | 64 | ,532 |
| Wenn bei einem Kauf das Einverständnis zur Nutzung meiner Daten erfragt wird, stimme ich meist zu | 55 | ,582 |
| Ich akzeptiere Cookies auf Websites, ohne groß darüber nachzudenken | 48 | ,560 |
| Ich nutze die Cloud, um zum Beispiel Fotos, Daten oder Backups zu speichern | 36 | ,538 |
| Die Ortungsfunktion an meinem Handy ist eigentlich immer aktiviert | 34 | ,491 |

Handlungsfelder datenbewusst verhält. Jeder Fünfte verhält sich ‚datenschutzphlegmatisch‘, weniger als jeder Zehnte wirklich konsistent ‚aktiv‘ (Abb. 3.12).

Die in den Tab. 3.14, 3.15 und 3.16 abgebildeten Fragen zeigen den Anteil der Befragten, die die Maßnahmen bejahten, in Abhängigkeit davon, wie ihre Einstellung zum Datenschutz ist. Die gleichen Zahlen finden sich zur Übersicht nochmals in Abb. 3.13.

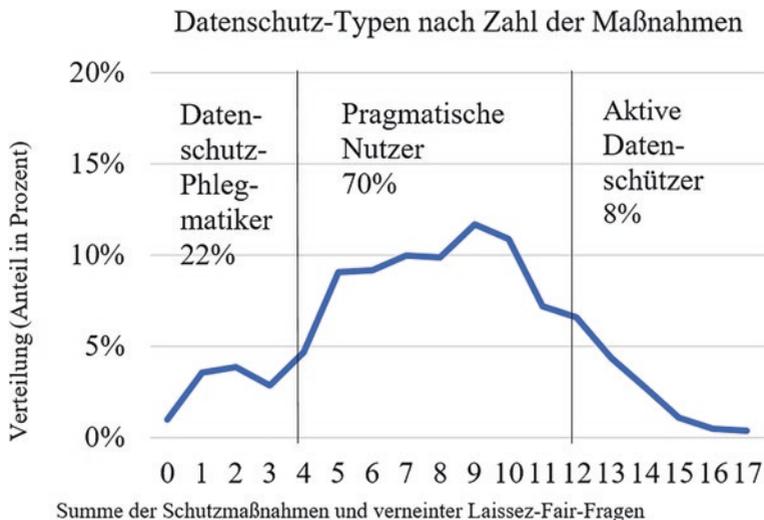


Abb. 3.12 Verhalten: Konkrete Maßnahmen zum Datenschutz

Tab. 3.14 Maßnahmen in Abhängigkeit der Einstellung: Passiver Datenschutz

| | Passiver Datenschutz | „Das Thema Datenschutz ist mir wichtig.“ | | |
|----|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-----------------|----------|
| | | Ja (%) | Teils/teils (%) | Nein (%) |
| P1 | Wenn eine App auf meine Fotos oder Kontakte zugreifen will, lehne ich das meistens ab | 82 ^a | 65 | 78 |
| P2 | Ich habe schon einmal auf die Nutzung einer Webseite oder einer App verzichtet, weil ich dem Datenschutz nicht vertraut habe | 76 | 60 | 41 |
| P3 | Ich lösche regelmäßig die Cookies von meinen Geräten | 71 | 61 | 53 |
| P4 | Ich habe schon einmal eine Website verlassen, weil ich den Cookie nicht zulassen wollte | 73 | 53 | 40 |
| P5 | Ich habe die Kamera an meinem Computer oder Tablet abgeklebt | 42 | 30 | 26 |

^aLesebeispiel: 82 % der Datenschutzbewussten lehnen es meist ab, Fotos den Zugriff auf Fotos oder Kontakte zu gewähren, aber nur 78 % derjenigen, denen der Datenschutz nicht wichtig ist

Tab. 3.15 Maßnahmen in Abhängigkeit der Einstellung: Aktiver Datenschutz

| | Aktiver Datenschutz | „Das Thema Datenschutz ist mir wichtig.“ | | |
|----|--------------------------------------------------------------------------------------|------------------------------------------|-----------------|----------|
| | | Ja (%) | Teils/teils (%) | Nein (%) |
| A1 | Ich ändere meine Passwörter regelmäßig | 55 | 39 | 24 |
| A2 | Ich verschlüssele meine E-Mails | 39 | 25 | 2 |
| A3 | Ich nutze Funktionen, um im Internet anonym zu bleiben (bspw. einen privaten VPN) | 38 | 26 | 12 |
| A4 | Ich nutze eine Suchmaschine, die keine persönlichen Daten sammelt | 36 | 20 | 25 |
| A5 | Ich habe schon einmal ein Unternehmen aufgefordert, meine Daten zu löschen | 31 | 23 | 24 |
| A6 | Ich nutze einen datengeschützten Messenger Dienst, z. B. Threema, Signal oder SIMSme | 21 | 15 | 10 |

Tab. 3.16 Maßnahmen in Abhängigkeit der Einstellung: Laissez Faire

| | Laissez Faire | „Das Thema Datenschutz ist mir wichtig.“ | | |
|-----|------------------------------------------------------------------------------------------------------------------|------------------------------------------|-----------------|----------|
| | | Ja (%) | Teils/teils (%) | Nein (%) |
| LF1 | Ich habe mindestens eine Payback- oder Kundenkarte, für deren Benutzung ich Rabatte oder andere Vorteile erhalte | 65 | 71 | 69 |
| LF2 | Ich lese mir die Datenschutzbestimmungen von Websites oder Online-Anbietern eigentlich nie richtig durch | 60 | 76 | 78 |
| LF3 | Wenn bei einem Kauf das Einverständnis zur Nutzung meiner Daten erfragt wird, stimme ich meist zu | 50 | 67 | 77 |
| LF4 | Ich akzeptiere Cookies auf Websites, ohne groß darüber nachzudenken | 40 | 66 | 68 |
| LF5 | Ich nutze die Cloud, um zum Beispiel Fotos, Daten oder Backups zu speichern | 34 | 44 | 34 |
| LF6 | Die Ortungsfunktion an meinem Handy ist eigentlich immer aktiviert | 33 | 38 | 40 |

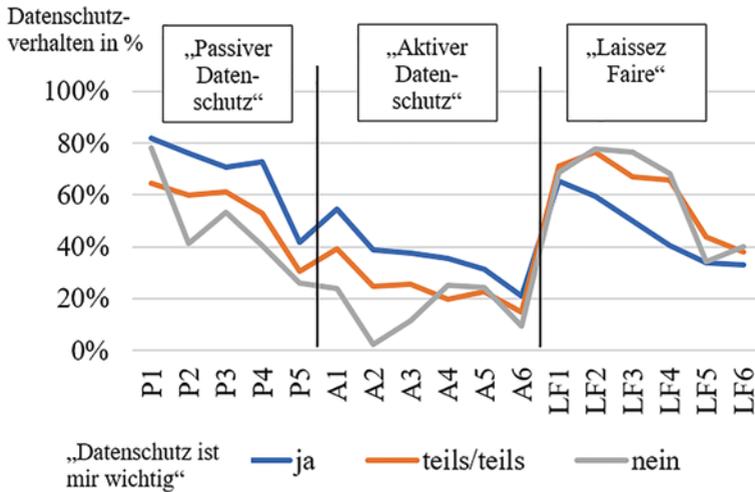


Abb. 3.13 Datenschutz-Verhalten in Abhängigkeit von der Datenschutz-Einstellung

Viele der konkreten Schutzmaßnahmen korrelieren durchaus mit der Einstellung zum Datenschutz – anders, als dies bei der Nutzung der Dienste der Fall war. So geben Menschen, die Datenschutz für wichtig erachten, mehr als doppelt so häufig an, ihre Passwörter regelmäßig zu aktualisieren, als Datenschutzunbewusste (siehe A1 in Tab. 3.15). E-Mail-Verschlüsselung wird von Datenschutzunbewussten sogar so gut wie gar nicht genannt.

Interessant sind dabei wieder die Ausnahmen: Denn die Nutzung einiger essenzieller Funktionen, die die Datenspur erheblich verbreitern, hängt nicht oder nur wenig mit dem Datenschutzbewusstsein zusammen. Dazu gehören insbesondere die Nutzung einer *Cloud* sowie in der ‚analogen‘ Welt der Besitz von *Rabatt- oder Kundenkarten*. Aber auch die datenschutzrechtlich besonders sensible *Freigabe von Fotos oder Adressen* in Apps sowie die Daueraktivierung der *Ortungsfunktion* unterscheidet sich nur wenig zwischen den beiden Gruppen.

Fazit Die in der Bevölkerung weitverbreiteten Datenschutzbedenken haben wenig Einfluss auf den Umfang und die Inhalte der Onlinenutzung. Dennoch beeinflussen sie das Verhalten im Kleinen – in Form konkreter Schutzmaßnahmen, die jeder einzelne Nutzer vornehmen kann. Aber auch dabei ist nur eine kleine Minderheit wirklich konsequent.

3.6 Datenpolitik und Datenethik („Neue Paradigmen“)

Wie die bisherigen Auswertungen zeigen, befürchtet eine Mehrheit der Bürger negative Auswirkungen einer vernetzten ‚Datengesellschaft‘, befürwortet Datenschutz und ist sich dabei der Divergenz der eigenen Ansprüche und des eigenen Verhaltens im (digitalen) Alltag sehr wohl bewusst. Im ersten Kapitel dieses Buches wurden bereits Lösungsansätze diskutiert, wie die Gesellschaft dem nicht zuletzt daraus resultierenden Konflikt zwischen Datennutzen und Datenschutz, zwischen Wettbewerb und zunehmend monopolistischen Marktstrukturen und schließlich zwischen (langsamer) Gesetzgebung und (rasanter) Entwicklung in Technik und Wirtschaft begegnen kann.

Im Folgenden werden einige wesentliche Punkte dieser Diskussion aus Sicht der Bürger beleuchtet, nämlich

- a) Grundannahmen zum Daten-Eigentum, zu computergenerierten Entscheidungen und zur Wettbewerbsfähigkeit,
- b) der Rolle von Fairness bei der Verwendung von Big Data für Scorings und automatisierte Entscheidungen,
- c) ein möglicher Paradigmenwechsel in der Datenpolitik und damit verbunden
- d) die gezielte Bereitstellung persönlicher Daten gegen Vorteile, gegen Bezahlung oder im Sinne des Gemeinwohls.

3.6.1 Datenpolitik aus Sicht der Bevölkerung

Ein wesentlicher Punkt in der öffentlichen Diskussion ist das mögliche *Eigentum an den Daten*: Gehören die Daten dem Nutzer (also bspw. dem Autofahrer oder dem Mitglied eines sozialen Mediums) oder aber dem Anbieter des jeweiligen Dienstes (also z. B. BMW oder Facebook)? Ungeachtet der offenen rechtlichen Problematik (siehe Kap. 1) geben die Befragten ein klares Plädoyer, indem sie die Daten mit großer Mehrheit dem Nutzer zusprechen (siehe Tab. 3.17).

Eine Frage, die mit der zunehmenden Verbreitung von Künstlicher Intelligenz noch wesentlich an Bedeutung gewinnen wird, ist die nach *automatisierten Entscheidungen*, die auf Basis von Big Data und (zunehmend selbstlernenden) Algorithmen durch ‚den Computer‘ getroffen werden. In welchem Maß können wir diesen Entscheidungen *vertrauen*? Auch wenn es mittlerweile eine umfassende psychologische Forschung zur Fehleranfälligkeit menschlichen Urteilens und

Tab. 3.17 Datenpolitik: Bewertungen aus Sicht der Bevölkerung (n=469–481; alle Befragten [split half])

| Diskussionspunkt | These | Zustimmung der Bevölkerung | | |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------|----------|
| | | Ja (%) | Teils/teils (%) | Nein (%) |
| Dateneigentum | <i>Personenbezogene Daten, die im Internet anfallen, sollten dem jeweiligen Nutzer gehören</i> | 86 | 9 | 5 |
| Vertrauen | <i>Entscheidungen sind gerechter, wenn sie von einem Computer getroffen werden als wenn Sie von einem Menschen getroffen werden</i> | 10 | 32 | 58 |
| Wettbewerbsfähigkeit | <i>Damit Deutschland im internationalen Wettbewerb nicht zurückfällt, ist es wichtig, dass es keine zu strengen Datenschutzregeln gibt</i> | 17 | 34 | 50 |

Entscheidens gibt (von persönlichen Interessen menschlicher Entscheider ganz abgesehen): Das Urteil der Befragten fällt hier deutlich zugunsten des Menschen und contra ‚Computer‘ aus (siehe Tab. 3.17).

Schließlich spielt die *Wettbewerbsfähigkeit* der deutschen oder europäischen Wirtschaft im politischen Diskurs eine zentrale Rolle als Argument für einen liberalen Umgang mit Big Data. Schon bei den oben dargestellten Folgeabschätzungen deutete sich an, dass solche gesamtwirtschaftlichen Zusammenhänge in der Einstellung der Bevölkerung wenig Beachtung finden. Entsprechend wird auch das Wettbewerbsargument von den Befragten nur sehr begrenzt angenommen (siehe Tab. 3.17).

3.6.2 Fairness als Mindestanforderung an Big Data

Werden Daten gesammelt und durch Algorithmen für Scorings oder sogar automatisierte Entscheidungen genutzt, ist der Einzelne dem in hohem Maße ausgeliefert. Wesentlich dafür, dass solche Verfahren akzeptiert werden, ist die Gerechtigkeit der zugrunde liegenden Prozesse.

Leventhal (1980) hat sechs Kriterien formuliert, die der wahrgenommenen Fairness von solchen Prozessen zugrunde liegen:

1. *Konsistenz*, also gleiche Regeln für Alle,
2. *Neutralität*, also Freiheit von persönlichen Interessen oder Voreingenommenheit des Entscheiders,
3. *Genauigkeit* der zugrunde liegenden Informationen,
4. *Repräsentativität* der Daten, auf deren Basis Entscheidungen gefällt werden,
5. *Revidierbarkeit* fehlerhafter oder unangemessener Urteile,
6. *Ethik*, also Übereinstimmung mit übergeordneten moralischen Standards.

Damit der Nutzer erkennen kann, inwieweit diese Kriterien erfüllt sind, bedarf es als Randbedingung der *Transparenz*, des *Vertrauens* in den Entscheider und/oder der *Kontrolle* durch eine übergeordnete Instanz. Zusätzlich ist die Sicherheit der Daten ein relevanter Faktor.

Dass Big-Data-basierte Computerentscheidungen derzeit keinesfalls als gerechter gesehen werden, das Vertrauen in die Einhaltung von Vorschriften zum Datenschutz gering ist und mit der Anwendung von Big Data die Sorge vor ungerechtfertigter Diskriminierung verbunden ist, zeigte sich schon in den bisherigen Ergebnissen. Ergänzend haben wir in Tab. 3.18 Antworten zu einigen der genannten Bedingungen zusammengefasst: Durchweg hohe

Tab. 3.18 Datenpolitik: Fairness als Mindestanforderung an Big Data (n = 479–501; alle Befragten [split half])

| These | Zustimmung der Bevölkerung | | |
|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------|----------|
| | Ja (%) | Teils/teils (%) | Nein (%) |
| <i>Jeder muss die Möglichkeit haben, Entscheidungen anzufechten, die von einem Computer auf Basis von verknüpften Daten getroffen wurden</i> | 86 | 12 | 2 |
| <i>Computerprogramme, die auf Basis von Nutzerdaten Entscheidungen fällen, sollten von einer staatlichen Instanz geprüft werden</i> | 62 | 27 | 11 |
| <i>Ich habe große Zweifel, ob Daten im Internet sicher sind vor dem Zugriff Unbefugter</i> | 69 | 25 | 6 |
| <i>Es stört mich sehr, wenn ich nicht weiß, ob ich am Telefon oder im Internet mit einem Menschen oder einem Computer spreche</i> | 64 | 21 | 15 |
| <i>Mir ist wichtig, dass ich weiß, für welche Zwecke meine Daten genutzt werden</i> | 80 | 15 | 5 |

Zustimmungswerte – selbst zur Frage einer staatlichen Algorithmenaufsicht („Algorithmenpolizei“) – verdeutlichen die große Bedeutung, die den Kriterien der Gerechtigkeit für eine breite gesellschaftliche Akzeptanz von Big Data und Künstlicher Intelligenz zukommt.

Während sich kein deutlicher Zusammenhang mit Bildung oder Geschlecht zeigt, nimmt die Zustimmung zu den in Tab. 3.18 abgebildeten Thesen ab, je jünger die Befragten sind (ohne Abbildung). Möglicherweise deutet sich hier ein allmählicher Einstellungswandel an. Allerdings liegen die Erwartungen auch bei den Jüngeren noch auf einem hohen Niveau.

3.6.3 Bewertung von Paradigmen in der Datenpolitik

In der Analyse der politischen Diskussion wurde in Kap. 1 ein vorsichtiger Wandel der Paradigmen, die von politischen Entscheidungsträgern für den gesellschaftlichen Umgang mit Big Data und Künstlicher Intelligenz formuliert werden, gezeigt. Da diese abstrakten Leitbilder die meisten Befragten überfordern würden, haben wir konkretere Aussagen bewerten lassen, die aus den jeweiligen Anschauungen abgeleitet wurden (siehe Tab. 3.19).

Vom Datenschutz zur Datensouveränität?

Während das Datenschutzkonzept neben Regulierung auf Aufklärung, Transparenz und Zustimmungsvorbehalte setzt, steht Datensouveränität (im Sinne einer aktiv ausgeübten Datenhoheit der Nutzer) für eine gezielte Verwendung der eigenen Daten. In den Antworten der Befragten werden beide Positionen (etwas mehr die ‚Datenschutz‘-Position) eher zustimmend bewertet. Das Selbstbild der Befragten widerspricht also nicht notwendigerweise einem Ideal des Bürgers als ein aktiver, aber selektiver Datengeber (wie auch im Folgenden deutlich wird), auch wenn dieses Ideal vor dem Hintergrund des zu beobachtenden Nutzerparadoxons zumindest derzeit wenig realistisch erscheint.

Von der Regulierung zur Daten-Ethik?

Die Gegenüberstellung enger Regulierung durch den Gesetzgeber versus subsidiär gestalteter, innerhalb eines flexiblen Handlungsrahmens auf Abwägungen und Selbstverpflichtungen beruhender Datenethik fällt eindeutig zugunsten der gesetzlichen Regulierung aus. Dennoch findet auch der Gedanke freiwilliger Selbstverpflichtungen eine recht breite Zustimmung, ein Hinweis darauf, dass solche Unternehmen oder Branchen, die ein hohes Vertrauen in der Öffentlichkeit genießen, hier einen Wettbewerbsvorteil erlangen könnten.

Tab. 3.19 Datenpolitik: Ein Wechsel in den Paradigmen?

| Paradigma | These | Zustimmung der Bevölkerung | | | ↔ | Paradigma | These | Zustimmung der Bevölkerung | | |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------|----------|---|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------|----------|
| | | Ja (%) | Teils/teils (%) | Nein (%) | | | | Ja (%) | Teils/teils (%) | Nein (%) |
| Datenschutz und Regulierung | <i>Jeder sollte genau wissen, was mit seinen persönlichen Daten im Internet geschieht</i> | 89 | 10 | 1 | ↔ | Daten-souveränität | <i>Am Ende muss jeder selbst entscheiden, wie er mit seinen persönlichen Daten umgeht</i> | 84 | 14 | 1 |
| | <i>Die Erfassung von persönlichen Daten durch Unternehmen sollte nur so viel wie nötig und nur solange wie nötig erfolgen dürfen</i> | 89 | 8 | 3 | | | <i>Ich finde, jeder ist selbst für den Umgang mit seinen Daten im Internet verantwortlich</i> | 56 | 38 | 6 |
| | <i>Den Umgang mit Daten von Kunden und Internutzern sollte der Staat durch detaillierte rechtliche Vorgaben regeln</i> | 69 | 25 | 6 | ↔ | Datenethik | <i>Anstelle von gesetzlichen Vorgaben, sollten die Unternehmen sich freiwillig auf verbindliche Regeln einigen, wie mit personenbezogenen Daten umzugehen ist</i> | 45 | 23 | 32 |
| | <i>Alle, die mit den Daten von Nutzern arbeiten, sollten laufend eng kontrolliert werden</i> | 76 | 20 | 5 | | | | | | |

(Fortsetzung)

Tab. 3.19 (Fortsetzung)

| | | | | | | | | | | |
|------------------|---------------------------------------------------------------------------|----|----|----|---|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|----|
| Wettbewerbsrecht | <i>Der Staat sollte die Macht der großen Internetkonzerne beschränken</i> | 57 | 32 | 10 | ↔ | Open Data | <i>Datenströme aus dem Internet sollten innerhalb bestimmter Regeln der Allgemeinheit zur Verfügung stehen – so wie das auch bei Straßen, Schienen oder Stromleitungen der Fall ist</i> | 43 | 33 | 24 |
|------------------|---------------------------------------------------------------------------|----|----|----|---|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|----|

Vom Wettbewerbsrecht zu Open Data?

Vielfach wird ein kartellrechtliches Eingreifen des Staates gegen die Marktmacht der ‚Internetgiganten‘ diskutiert. Diese Forderung wird von der Bevölkerung mehrheitlich unterstützt. Dabei findet auch das recht neue Modell ‚offener Daten‘, bei dem der Wettbewerbsvorsprung von ‚Monopolisten‘ durch erzwungenes Data-Sharing beschnitten wird, um Innovation und Wettbewerb zu stärken, ebenfalls mehr Zustimmung als Ablehnung – und könnte bei intensiverer Kommunikation durchaus ‚mehrheitsfähig‘ werden.

3.6.4 ‚Rohstoff‘ Daten

Das Konzept der *Datensouveränität* und insbesondere der *Datenethik* als Alternative zu einem engen, regulativen Datenschutzkonzept bedingt in seinem Kern ein bewusstes Abwägen der Bürger oder Kunden, für welche Gegenleistung und für welche Zweckbestimmung sie ihre Daten freigeben. Gerade auch in Zusammenhang mit der Eigentumsdiskussion um die Daten könnten das sein

- a) der unentgeltliche *Tausch der Daten* gegen das Nutzenversprechen einer Anwendung,
- b) ein *Verkauf der Daten*, also das Bereitstellen des ‚Rohstoffs‘ der eigenen Daten gegen Vergütung, sowie
- c) die gezielte ‚*Spende*‘, also die kostenfreie Bereitstellung für gesellschaftliche Zwecke.

Letzteres würde beispielsweise Anwendungen zur Verbesserung von Verkehrsflüssen oder der medizinischen Versorgung ermöglichen, welche derzeit aufgrund der gesetzlich verankerten Zweckgebundenheit und Datensparsamkeit nur sehr begrenzt möglich sind (vgl. Kap. 2).

Der *Datentausch* – also faktisch das ‚Bezahlen‘ von Diensten durch die Bereitstellung von Daten, ist bereits breite gesellschaftliche Realität. Entsprechend wird unsere Frage (die allerdings auch die Bezahlung durch Werbung miteinschließt) von den Befragten mehrheitlich bejaht oder zumindest nicht abgelehnt (siehe Tab. 3.20).

In unseren Fragen zu *Verkauf* und *Spende* wurde der Datenzugriff bewusst recht weitgehend formuliert. Im Ergebnis zeigt sich, dass sowohl der Verkauf als auch die bewusste *Spende* solch umfassender Daten von einer Mehrheit abgelehnt wird (siehe Tab. 3.20). Die im Vergleich deutlich höhere Zustimmung zur medizi-

Tab. 3.20 ‚Rohstoff‘ Daten – Datentausch, Datenhandel und Datenspende

| Konzept | These | Zustimmung der Bevölkerung | | | Anzahl und Art der Befragten |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------|----------|------------------------------------------------------------------------------------------------------|
| | | Ja (%) | Teils/teils (%) | Nein (%) | |
| Daten im Tausch | <i>Für Apps oder Onlinedienste bezahlte ich nur ungerne. Dann nehme ich lieber Werbung in Kauf oder dass meine Daten für andere Zwecke genutzt werden</i> | 26 | 40 | 34 | n = 214 (nur telefonisch Befragte, die zumindest mehrmals im Monat das Internet nutzen [split half]) |
| Daten als Ware | <i>Ich könnte mir vorstellen, gegen eine attraktive Bezahlung meine Internetaktivitäten von einem Unternehmen aufzeichnen zu lassen</i> | 11 | 11 | 78 | n = 221 (nur telefonisch Befragte, die zumindest mehrmals im Monat das Internet nutzen [split half]) |
| Daten als Spende | <i>Ich könnte mir gut vorstellen, meine Handydaten zur Verfügung zu stellen, wenn sie für die Weiterentwicklung von Onlinediensten genutzt werden würden</i> | 10 | 15 | 75 | n = 249 (nur telefonisch Befragte [split half]) |
| | <i>Ich könnte mir gut vorstellen, meine Handydaten zur Verfügung zu stellen, wenn sie für medizinische Forschungszwecke genutzt würden</i> | 29 | 20 | 51 | n = 241 (nur telefonisch Befragte [split half]) |

nischen Spende zeigt aber, dass Datenspende nicht pauschal verneint wird, sondern bei nachvollziehbar wichtigen Zwecken durchaus abgewogen wird.⁵

3.7 Alte und neue Narrative

Narrative sind ‚sinnstiftende Erzählungen‘ innerhalb einer Kultur, die in hohem Maße das öffentliche Bild und damit auch die Bewertung der zugrunde liegenden Themen prägen. Im Rahmen einer aktuellen Medienanalyse wurde in Kap. 1

⁵Zu obenstehenden Fragen wurden nur die Antworten aus der telefonischen Stichprobe ausgewertet, da die Mitglieder eines Onlinepanels in diesen Themen erwartungsgemäß aufgeschlossener sind als der Durchschnitt der Bevölkerung.

gezeigt, dass Big Data und Algorithmen ganz überwiegend mit negativen Narrativen verbunden sind. Positive Deutungen, die den möglichen Nutzen von Big Data thematisieren und in den gesellschaftlichen Vorstellungen verankern, sind bislang dagegen kaum zu erkennen.

Wir haben die Befragten daher um Auskunft gebeten, wie weit sie die vorherrschenden kritischen ‚Erzählungen‘ für zutreffend halten (siehe Tab. 3.21).

Tab. 3.21 Bewertung von Narrativen

| Konnotation | <i>Wenn Sie einmal insgesamt an Nutzen und Risiken bei der Erfassung und Verarbeitung persönlicher Daten denken, welcher der folgenden Vergleiche erscheint Ihnen dabei treffend? Ist das wie ein ...</i> | Bewertung der Bevölkerung | | |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------|---------------------|
| | | Trifft zu (%) | Teils/teils (%) | Trifft nicht zu (%) |
| Negativ | <i>Spion – der uns ausspäht und viel von uns preisgibt</i> | 54 | 34 | 12 |
| | <i>Ein Überwachungsapparat, der einen immer im Blick hat</i> | 51 | 28 | 21 |
| | <i>Verführer – der einen erst kennenlernt und dann damit beeinflussen will</i> | 44 | 30 | 26 |
| | <i>Eine Droge – die die Menschen erst lockt und dann von den großen Internetkonzernen anhängig macht</i> | 39 | 32 | 29 |
| | <i>Diktator – der erst hilfreich ist und dann die Kontrolle übernimmt</i> | 37 | 35 | 29 |
| | <i>Zensor – der Informationen nur gefiltert weitergibt und einem damit wichtige Dinge vorenthält</i> | 31 | 41 | 28 |
| Positiv | <i>Forscher und Entwickler – die für einen stetigen Fortschritt sorgt</i> | 32 | 51 | 18 |
| | <i>Persönlicher Assistent – der schnell da ist wenn man ihn braucht</i> | 32 | 36 | 33 |
| | <i>Heizelmännchen – das viel Arbeit für uns erledigt</i> | 23 | 41 | 36 |
| | <i>Einkaufsberater – der Kunden hilft, zu finden, was gut zu ihnen passt</i> | 23 | 39 | 38 |
| | <i>Wünscheerfüller – der Dinge möglich macht, die sonst gar nicht erreichbar wären</i> | 18 | 36 | 47 |
| | <i>Schutzengel – der aufpasst und uns vor vielen Risiken bewahren kann</i> | 14 | 33 | 53 |

Zugleich haben wir mögliche ‚Narrative‘ oder ‚Bilder‘ beschrieben, die die positive Seite der Datennutzung repräsentieren könnten und so möglicherweise ein Potenzial hätten, auch die Nutzenseite der neuen Techniken zu verankern.

Die Befragungsergebnisse zeigen ein analoges Bild zur Negativitäts-Dominanz in der Medienanalyse (und auch in der Folgenabschätzung, siehe Abschn. 3.3): Auch bei der Beurteilung der Narrative überwiegt die Zustimmung zu den negativen Positionen deutlich. Besonders die Bilder der *Ausspähung* und der *Überwachung* werden von einer Mehrheit geteilt. Aber auch andere gewählte Metaphern – *Verführer*, *Droge*, *Diktator* und (in etwas geringerem Ausmaß) *Zensor*, welche auf die zuvor dargestellten Aspekte wie *Kontrollverlust*, *Monopolismus* oder die *Filterblase* referieren, finden mehr Zustimmung als Ablehnung.

Deutlich differenzierter zeigt sich das Bild auf Seite der positiven Analogien: Die höchste Zustimmung findet sich bezüglich des *Forschers* und des persönlichen *Assistenten*. Weitergehende Rollen wie *Heinzelmännchen*, *Einkaufsberater*, *Wünscheerfüller* oder auch *Schutzengel*, die direkt auf Motive wie Bequemlichkeit, Sicherheit, Kontrolle oder Effizienz abzielen und damit die Mehrheit neuer Dienste und Geschäftsmodelle (siehe Kap. 2) repräsentieren, haben bislang kaum den Weg in die Vorstellungswelt der Menschen gefunden. Ähnliche Tendenzen hatten sich schon bei den Folgeabschätzungen gezeigt (siehe Abschn. 3.3).

Abb. 3.14 verdeutlicht noch einmal in Form eines ‚Waagen-Modells‘ die Gewichtung zwischen positiven und negativen Narrativen (die Zahlen sind identisch zu Tab. 3.21). Nur durchschnittlich 24 % stimmen den positiven Vergleichen zu (weitere 39 % zumindest teilweise). Den negativen Vergleichen stimmen im Mittel 43 % zu (weitere 33 % teilweise). Eine Mehrheit finden lediglich die negativen Analogien „Überwachungsapparat“ und „Spion“, während keines der positiven Bilder mehrheitsfähig ist.

Fazit Anwendungen auf Basis von Big Data haben aus technischer Sicht ein hohes Potenzial, grundlegende Motive zu bedienen und somit einen hohen direkten Nutzen für die Bürger zu generieren. Positive mit Assoziationen aufgeladene Codes könnten diese Seiten von Big Data in der Vorstellungswelt der Menschen verankern und so helfen, ein etwas balancierteres Bild der neuen Datenwelt zu schaffen. Bisher dominiert aber vor allem das *Big-Brother-Narrativ*, begleitet von weiteren Bedrohungsszenarien, neben denen optimistische Schilderungen bisher allenfalls eine Nebenrolle einnehmen konnten. Zur gesellschaftlichen Konstruktion positiver ‚sinnstiftender Erzählungen‘ ist es also noch ein weiter Weg.

Wenn Sie einmal insgesamt an Nutzen und Risiken bei der Erfassung und Verarbeitung persönlicher Daten denken, welcher der folgenden Vergleiche erscheint Ihnen dabei treffend? Ist das wie ein ...

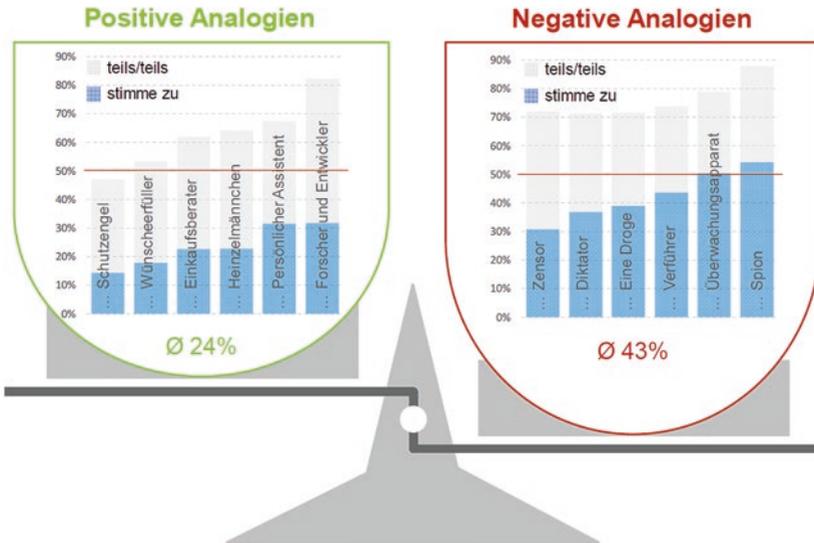


Abb. 3.14 Bürgerschreck oder Hoffnungsträger? Negative Narrative wiegen schwerer

3.8 Neue Rollen am Beispiel der Versicherungswirtschaft

Vernetzung, Big Data und Künstliche Intelligenz führen nicht nur zu zahlreichen Gründungen und Innovationen in technikhnen Branchen, sondern ändern auch die Rolle, die etablierte Branchen für Kunden und die Gesellschaft spielen. In Kap. 2 wird am Beispiel der Assekuranz aufgezeigt, wie sich die Rolle einer ganzen Branche auf Basis von Vernetzung und intelligenten Algorithmen wandeln kann. Darauf abgestimmt werden im Folgenden Erwartungen der Bürger an die Versicherungswirtschaft auf empirischer Basis beschrieben.

3.8.1 Anwendungsfelder von Big Data

Zu den wesentlichen Anwendungsfeldern von Big Data in der Versicherung gehören bereits heute

Tab. 3.22 Anwendungsfelder von Big Data in der Versicherungswirtschaft

| These | Bewertung der Bevölkerung | | | Anwendungsfeld |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-------------|----------------------------|---------------------------|
| | Das finde ich gut (%) | Neutral (%) | Das finde ich schlecht (%) | |
| Aufdeckung von Versicherungsbetrug | 67 | 25 | 8 | „Kriminalitätsbekämpfung“ |
| Eine Versicherung, die automatisch eine Erweiterung anbietet, wenn neue Risiken dazukommen (z. B. ein neuer Sport, ein zuvor nicht versicherter Fahrer im Auto oder eine lange Auslandsreise) | 29 | 35 | 37 | „Marketing“ |
| Ermittlung von Versicherungsprämien anhand des individuellen Risikos eines Kunden | 22 | 35 | 43 | „Marketing“ |
| Vorschlag eines passenden Versicherungsvertrages | 22 | 41 | 37 | |

- a) Betrugserkennung,
- b) Flexibilisierung der Produkte, z. B. durch situative Deckungen,
- c) Tarifierung⁶,
- d) Individualisierung des Angebots entsprechend dem Kundenprofil.

Bei der Beurteilung entsprechender Anwendungen (siehe Tab. 3.22) wiederholt sich das Muster, das schon in Abschn. 3.4 zu den Anwendungsfeldern zu erkennen war: Wenn es um die *Kriminalitätsbekämpfung* geht, überwiegt die Zustimmung bei Weitem. *Scorings und Selektionen im Marketing*, hier also Preissetzung sowie flexible oder individualisierte Produkte, werden dagegen eher skeptisch aufgenommen, wenngleich auch nicht mehrheitlich abgelehnt.

3.8.2 Akzeptanz neuer Rollen

Damit ist aber erst ein Teil möglicher Anwendungsfelder von Big Data und intelligenter Algorithmen im Kontext der Versicherungswirtschaft erfasst. Wenn es um neue und erweiterte Funktionen geht, die die Assekuranz dank Daten und

⁶Zur Bewertung datenbasierter Tarife siehe ausführlich Müller-Peters (2017).

Vernetzung übernehmen kann, dann ist vor allem über folgende Rollenbilder nachzudenken (siehe auch Kap. 2):

1. ‚*Retter*‘ oder ‚*Schadenmanager*‘: Ist ein Schaden eingetreten, tritt neben den eigentlichen finanziellen Schadenausgleich immer mehr das ‚Management‘ des Schadens, also z. B. die Unterstützung bei oder auch weitgehende Organisation von Reparaturen oder medizinischen Therapien. Mit zunehmender Vernetzung ergeben sich hier weitergehende Möglichkeiten, sowohl die Schäden zu erkennen als auch die Maßnahmen zu koordinieren und zu begleiten.
2. ‚*Coach*‘ oder ‚*Schadenverhüter*‘: Ebenso ermöglichen Vernetzung und die Analyse großer Datenbestände den Versicherern zunehmend, schon vorab mögliche Risiken zu erkennen und durch Aufklärung, Verhaltensfeedbacks oder konkrete Präventionsmaßnahmen zu minimieren. Aufklärung und Feedback erfolgt beispielsweise im Rahmen von telematischen Kfz-Policen oder im Kontext des Vitality-Programms der Generali Versicherung. Weitere Präventionsmaßnahmen sind zum Beispiel die Installation von Sensoren im Haushalt, regelmäßige Gesundheitschecks oder auch ein laufendes Gesundheitsmonitoring per Smartwatch oder Fitness-Tracker.
3. ‚*Kontrollleur*‘ oder ‚*Motivator*‘: Wenn Risiken gemessen und erkannt werden, dann ist auch eine unmittelbare Einflussnahme auf das Verhalten des Versicherungsnehmers durch positive oder negative Sanktionen nicht mehr weit. Dies kann zum Beispiel über die Bepreisung erfolgen (wie in Kfz-Telematik-Tarifen oder im „Vitality-Modell“ der Generali Versicherung bereits gegeben), aber auch in weitergehenden konkreten Handlungsvorschriften oder Verboten, welche wiederum durch Sensoren und Vernetzung überprüft werden können.

Die Befragten zeigen sich den neuen Rollen gegenüber differenziert, aber vielfach durchaus aufgeschlossen (siehe Tab. 3.23, 3.24 und 3.25). Inwieweit eine Rolle im Einzelfall befürwortet oder zumindest akzeptiert wird, hängt dabei mehr von der konkreten Ausgestaltung des Beispiels als von der Rolle selbst ab. So findet die gewählte Beschreibung des *Schadenverhüters* ausgerechnet im Kfz-Beispiel, in dem die Vernetzung faktisch ja schon weit fortgeschritten ist, die geringste Akzeptanz, im deutlich sensibleren Gesundheitsbereich dagegen die höchste. Ähnlich verhält es sich mit der Rolle des Schadenmanagers, während *Kontrolle* und *Sanktionen* in der Autoversicherung den meisten Zuspruch erfahren.

Analog zeigt sich auch kein eindeutiger Unterschied bezüglich der drei *Lebenswelten*: Die erweiterten Rollen finden in *Mobilität*, *Gesundheit* und *Wohnen* ungefähr in gleichem Ausmaß Akzeptanz, wobei die Zustimmung im Bereich

Tab. 3.23 Neue Rolle der Versicherungswirtschaft? Akzeptanz nach Rollen für die Autoversicherung (n = 312–325, alle Befragten)

| Rolle der Versicherungswirtschaft | Ein Autoversicherer sollte ... | Bewertung der Bevölkerung | | | Würden Sie dafür auch entsprechende Daten zur Verfügung stellen, zum Beispiel dem Versicherer erlauben, entsprechende Sensoren an Ihrem Auto zu installieren? (Zustimmung in Prozent) |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Stimme zu (%) | Teils/teils (%) | Stimme nicht zu (%) | |
| Retter/Schadenmanager | ... nicht nur Kosten erstatten, sondern auch helfen, also zum Beispiel einen Unfall erkennen und automatisch die Reparatur des Autos organisieren | 32 | 31 | 37 | 26 |
| Coach/Schadenverhüter | ... nicht nur Kosten erstatten, sondern mich schon vorab vor Risiken beschützen, zum Beispiel durch die Analyse meines Fahrstils oder die Bereitstellung von Sicherheitszubehör fürs Auto | 22 | 27 | 51 | 24 |
| Kontrollleur/Motivator | ... seinen Kunden Rabatte anbieten, wenn sie sich an bestimmte Vorgaben halten, zum Beispiel eine bestimmte Höchstgeschwindigkeit oder ein Alkoholverbot | 59 | 14 | 27 | 41 |

Tab. 3.24 Neue Rolle der Versicherungswirtschaft? Akzeptanz nach Rollen für die Krankenversicherung (n = 312–325, alle Befragten)

| Rolle der Versicherungswirtschaft | Ein Krankenversicherer sollte ... | Bewertung der Bevölkerung | | | Würden Sie dafür auch entsprechende Daten zur Verfügung stellen, zum Beispiel Daten aus Arzterminen oder einem Fitnesstracker? (Zustimmung in Prozent) |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Stimme zu (%) | Teils/teils (%) | Stimme nicht zu (%) | |
| Retter/Schadenmanager | ... nicht nur Kosten erstatten, sondern auch helfen, also zum Beispiel anstehende Behandlungstermine erkennen oder mir einen Termin beim Facharzt anbieten | 52 | 26 | 22 | 48 |
| Coach/Schadenverhüter | ... nicht nur Kosten erstatten, sondern mich schon vorab vor Risiken schützen, zum Beispiel durch Vorsorgemaßnahmen oder regelmäßige Gesundheitschecks | 67 | 22 | 11 | 50 |
| Kontrollleur/Motivator | ... seinen Kunden Rabatte anbieten, wenn sie sich an bestimmte Vorgaben halten, zum Beispiel was Alkoholkonsum oder Bewegung betrifft | 51 | 21 | 28 | 44 |

Tab. 3.25 Neue Rolle der Versicherungswirtschaft? Akzeptanz nach Rollen für die Wohnungsver-sicherung (n = 312–325, alle Befragten)

| Rolle der Ver-sicherungswirtschaft | Ein Wohnungsver-sicherer sollte ... | Bewertung der Bevölkerung | | | Würden Sie dafür auch entsprechende Daten zur Verfügung stellen, zum Beispiel dem Versicherer erlauben, entsprechende Sensoren in ihrer Wohnung zu installieren? (Zustimmung in Prozent) |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | Stimme zu (%) | Teils/teils (%) | Stimme nicht zu (%) | |
| Retter/Schadenmanager | ... nicht nur Kosten erstatten, sondern auch helfen, also zum Beispiel drohende Schäden an Wasserleitungen erkennen und Handwerker für Reparaturen beauftragen | 43 | 33 | 24 | 25 |
| Coach/Schadenverhüter | ... nicht nur Kosten erstatten, sondern schon vorab für mehr Sicherheit sorgen, zum Beispiel durch eine Risikoanalyse oder durch die Bereitstellung von Sensoren | 36 | 35 | 29 | 30 |
| Kontrollleur/Motivator | ... seinen Kunden Rabatte anbieten, wenn sie sich an bestimmte Vorgaben halten, zum Beispiel wenn sie bestimmte Sicherungsmaßnahmen in der Wohnung treffen | 52 | 27 | 21 | 23 |

der Gesundheit tendenziell etwas höher ist und im Bereich des Kfz am stärksten je nach beschriebener Maßnahme schwankt.

Deutlich zurückhaltender sind die Befragten aber in der Bereitschaft, sich dafür auch ‚vermessen‘ zu lassen. Je nach Anwendung wäre nur jeder Zweite bis jeder Vierte bereit, *Sensoren* zu installieren oder *anfallende Daten* aus Kfz, Arztbesuchen oder Fitnesstracker an den Versicherer weiterzugeben. Interessanterweise liegen hier die Zustimmungsraten im besonders datenschutzsensiblen Bereich der Gesundheit ganz vorne. Unter Berücksichtigung der Tatsache, dass eine solche Vernetzung einen recht weitgehenden Eingriff in die Privatsphäre darstellt, Datenschutz von den Befragten als wichtig erachtet wurde und die Erfahrung der meisten Befragten mit Sensoren und Trackern gering ist, sind die Zustimmungsquoten dennoch erstaunlich hoch.

Auch wenn die Verbreitung von ‚Wearables‘ sowie von Alexa oder vergleichbaren ‚Smart Speakers‘ noch moderat ist, wachsen die Nutzerzahlen rasant. Ein Blick auf die Nutzer kann also andeuten, inwieweit die Akzeptanz der Datenweitergabe mit einer weiteren fortschreitenden Vernetzung im Alltag steigt. Tatsächlich stimmen die von uns befragten Nutzer von Smartwatch, Alexa & Co. der Datenübertragung weitaus häufiger – in vielen Fällen sogar mehrheitlich – zu (siehe Tab. 3.26). Die Aussage ist wegen der geringen Zahl der Nutzer der Devices allerdings nur als Tendenzwert zu interpretieren. Ebenso steigt die Akzeptanz – wenig verwunderlich – mit dem Optimismus bezüglich Big Data. Keine wesentlichen Unterschiede zeigen sich dagegen in Abhängigkeit vom Lebensalter (ohne Abbildungen).

Ambivalent ist dagegen der Zusammenhang mit dem Datenschutzbewusstsein. Datenschutzbewusste unterscheiden sich in der Akzeptanz der erweiterten Rolle des Versicherers nicht grundsätzlich von wenig Datenschutzbewussten. Deutlichere Effekte zeigen sich zwar bei der Bereitschaft zur Datenweitergabe, aber auch dies gilt keinesfalls für alle beschriebenen Einsatzzwecke (ohne Abbildungen).

Fazit Aus den Vergleichen lässt sich schließen, dass nicht die Sorge um die Privatsphäre der Haupttreiber für Zustimmung oder Ablehnung ist, sondern auch hier das jeweilige Nutzenversprechen entscheidet. Verbunden mit zunehmender Gewöhnung an laufende Vernetzung und unter der Voraussetzung der in Abschn. 3.7 beschriebenen Kriterien ‚gerechter‘ Systeme (siehe auch Müller-Peters und Wagner 2017) kann eine insgesamt breite Akzeptanz für eine erweiterte Rolle der Versicherer erwartet werden – von der tradierten Funktion als *Kostenerstatter* hin zum *Schadenmanager*, zum *Schadenverhüter* und bis zum aktiven *Motivator* oder *Kontrolleur*.

Tab. 3.26 Akzeptanz der Datenweitergabe an Versicherer nach Grad der Vernetzung des Kunden (Tendenzaussagen, teils geringe Fallzahlen!)

| Würden Sie dafür auch entsprechende Daten zur Verfügung stellen, zum Beispiel ... | Rolle der Versicherungswirtschaft | Zustimmung der Bevölkerung (n = 312–325) (%) | Zustimmung bei Nutzern von Smartwatches (n = 23–43) (%) | Zustimmung bei Nutzern von Fitnessarmbändern (n = 47–57) (%) | Zustimmung bei Nutzern von Alexa oder einem vergleichbaren Gerät (n = 34–43) (%) |
|----------------------------------------------------------------------------------------|-----------------------------------|----------------------------------------------|---------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------------------------------------------|
| ... dem Versicherer erlauben, entsprechende Sensoren an Ihrem Auto installieren? | Retter/ Schadenmanager | 26 | 33 | 32 | 39 |
| | Coach/ Schadenverhüter | 24 | 30 | 31 | 28 |
| | Kontrollleur/ Motivator | 41 | 43 | 52 | 62 |
| ... Daten aus Arztterminen oder einem Fitnessstracker? | Retter/ Schadenmanager | 48 | 68 | 50 | 64 |
| | Coach/ Schadenverhüter | 50 | 43 | 56 | 68 |
| | Kontrollleur/ Motivator | 44 | 59 | 54 | 51 |
| ... dem Versicherer erlauben, entsprechende Sensoren in ihrer Wohnung zu installieren? | Retter/ Schadenmanager | 25 | 32 | 30 | 38 |
| | Coach/ Schadenverhüter | 30 | 49 | 43 | 48 |
| | Kontrollleur/ Motivator | 23 | 32 | 30 | 28 |

3.9 Fazit

Als Kernergebnisse dieser empirischen Studie lassen sich festhalten:

3.9.1 Wissen – Können – Wollen – Handeln

„Wissen“

Die digitale Welt ist für die Menschen in Deutschland kein ‚Neuland‘ mehr. Grundbegriffe der Digitalisierung sind ins Allgemeinwissen eingegangen. Bestehende Wissensdefizite finden sich aber gerade rund um die digitale Vernetzung und Big Data, jene Themen also, die besonders den Umgang mit den eigenen Daten tangieren.

„Können“

Die Bürger fühlen sich aufgrund von Informationsüberlastung und monopolistischer Marktstrukturen nur sehr bedingt handlungsfrei oder souverän, und zwar quer durch alle Altersgruppen und Bildungsschichten. Regulierungen wie z. B. aus der Europäischen Datenschutzgrundverordnung, die vom Ideal eines mündigen und kritischen Bürgers ausgehen und die Interessen der Verbraucher daher über umfassende Information- und Zustimmungspflichten absichern wollen, drohen dadurch vielfach ‚ins Leere‘ zu laufen.

„Wollen“

Der Schutz der eigenen Daten ist den Menschen unverändert wichtig. Dennoch ergibt sich eine ganz unterschiedliche Wahrnehmung von Big Data, je nach Blickwinkel, aus dem das Thema betrachtet wird:

Das *Fernbild* von Big Data:

- Sofern eher abstrakt nach möglichen Folgen gefragt wird, überwiegen aus Sicht der Bürger die Risiken.
- Nutzenpotenziale der neuen Techniken, wie ein Zugewinn an Sicherheit, Komfort oder Effizienz, werden vielfach nicht erkannt oder wiegen im Vergleich zu den möglichen Nachteilen weniger schwer.
- Auch bezüglich gesamtgesellschaftlicher und volkswirtschaftlicher Auswirkungen dominieren die Bedenken.

- In einer Klassifizierung nach Sorgen und Hoffnungen zeigen sich annähernd doppelt so viele Pessimisten (42 % der Befragten) wie Optimisten (22 % der Befragten). Die verbleibenden 36 % geben sich bezüglich der Chancen und Risiken annähernd indifferent.

Das *Nahbild* von Big Data:

- Das negative Bild ändert sich, wenn anhand konkreter Anwendungsfelder der Nutzen von Big Data deutlich wird. Zahlreiche der getesteten Anwendungen in den drei Lebenswelten Mobilität, Wohnen und Gesundheit werden mehrheitlich begrüßt.
- Das gilt besonders, wenn die Sicherheit erhöht wird, wenn lästige Alltags-tätigkeiten automatisiert werden oder wenn der Nutzer bei weitergehenden Tätigkeiten unterstützt wird, ohne dabei gleich die Kontrolle aus der Hand geben zu müssen.
- Ist der Nutzen der Anwendung ersichtlich, tritt selbst die Sorge vor Überwachung in den Hintergrund. Dies gilt sowohl für eine breite Anzahl von Anwendungen in den eigenen Lebenswelten als auch für eine (politisch derzeit höchst konträr diskutierte) polizeiliche Kriminalitätsbekämpfung mittels Big Data.
- Dennoch möchte der Bürger nicht zum ‚Objekt‘ der Algorithmen degradiert werden: Klassifizierungen (sog. ‚Scorings‘) oder gar automatisierte Entscheidungen werden mehrheitlich abgelehnt. Anwendungen im Marketing – z. B. durch ‚Mikrotargeting‘, dynamische Preissetzung oder der Kundenbetreuung über Sprachcomputer, wird überwiegend mit Skepsis begegnet.

‚Handeln‘

Die Bevölkerung ist im Netz, und zwar in doppeltem Sinne:

- Das Internet wird intensiv und über unterschiedlichste Geräte genutzt.
- Zugleich sind die Nutzer über zahlreiche Dienste und Geräte im ‚Netz‘ der Anbieter und hinterlassen dort umfangreiche Datenspuren. Dabei dominieren – ungeachtet monopolistischer, gesamtwirtschaftlicher und datenschutzrechtlicher Bedenken – die bekannten Internetgiganten. Reichweite und Nutzenumfang der globalen Player überkompensieren ‚Nähe‘ und höhere Datenschutzstandards nationaler Wettbewerber.
- Besorgte Bürger, aber sorglose Verbraucher – das Nutzer-Paradoxon findet demnach in unseren Daten weitgehende Bestätigung. Die Mehrzahl der Verbraucher ist sich dieses Konfliktes durchaus bewusst.
- Dennoch sind die Nutzer ‚im Kleinen‘ nicht gänzlich datenschutzpassiv:

- Datenschutzmaßnahmen an Computer und Smartphone werden – gerade von datenschutzsensiblen Bürgern – durchaus genutzt.
- Die große Mehrheit verhält sich in Bezug auf Datenschutzmaßnahmen ‚pragmatisch‘ (negativ formuliert ließe sich auch sagen: ‚leicht fahrlässig‘). Jeder fünfte Nutzer zeigt sich ‚datenschutz-phlegmatisch‘, nicht einmal jeder zehnte ist konsequent ‚datenschutz-aktiv‘.

3.9.2 Neue Paradigmen für Politik, Wirtschaft und Gesellschaft?

Bürger befürworten ein *persönliches Eigentum* an den eigenen Daten, sind skeptisch gegenüber allen Arten *automatisierter Entscheidungen* und sind nur sehr begrenzt bereit, den Datenschutz *zugunsten der internationalen Wettbewerbsfähigkeit der Wirtschaft* hintenanzustellen.

Es herrscht breiter Konsens bezüglich der *Grundanforderungen* an datengestützte Systeme, nämlich *Fairness* und *Nachvollziehbarkeit*. Das impliziert *Transparenz*, *Vertrauen* oder *Kontrolle* sowie *Diskriminierungsfreiheit*, *Neutralität*, *Datenqualität* und *Datensicherheit*. (Die Forderungen nach *Datenqualität* und *Transparenz* stellen den Einsatz unstrukturierter Daten und selbstlernender Algorithmen aus technischer Sicht vor eine große Hürde, siehe Kap. 2).

Neue Paradigmen in der politischen Diskussion betonen *Datensouveränität* statt *Datenschutz*, freiwillige *Datenethik* der Unternehmen anstelle strikter *Regulierung*, sowie *Open-Data*-Ansätze anstelle oder ergänzend zum klassischen *Wettbewerbsrecht*.

- Die Konzepte von Datenschutz versus eigenverantwortlicher Datensouveränität des Einzelnen schließen sich aus Sicht der Befragten nicht aus, sondern werden gleichermaßen geteilt. Dennoch ist den meisten der Gedanke eher fremd, Daten im Sinne einer Ware zu ‚tauschen‘ (auch wenn dies faktisch schon breite gesellschaftliche Realität ist) oder gar zu ‚verkaufen‘ oder zu ‚spenden‘. Ist der gesellschaftliche Nutzen aber offensichtlich (wie im Fall der medizinischen Forschung gegeben), erhöht sich die Bereitschaft zur Datenüberlassung ganz erheblich.
- Überwiegend fordern die Bürger jedoch eine enge staatliche Regulierung des Umgangs mit Daten. Der eigentlich gegenteilige Gedanke einer weitgehend freiwilligen Selbstverpflichtung der Unternehmen findet zwar ebenfalls eine recht breite Akzeptanz, dürfte aber im Detail stark vom Vertrauen in ebenjene abhängen.

- Ein Eingreifen des Staates gegen die Marktmacht der ‚Internetgiganten‘ wird in Mehrheit unterstützt. Dabei findet auch das recht neue Modell der ‚Open Data‘, bei dem der Wettbewerbsvorsprung von Monopolisten durch erzwungenes Data-Sharing beschnitten wird, um Innovation und Wettbewerb zu stärken, mehr Zustimmung als Ablehnung – und könnte bei intensiverer Kommunikation durchaus ‚mehrheitsfähig‘ werden.

Spion, Überwachungsapparat, Verführer, Droge und Diktator Wir haben die Befragten um Auskunft gebeten, wie weit sie positive und negative Analogien zum Einsatz von Big Data für zutreffend halten. Die fünf zuvor genannten Begriffe wurden mit Abstand meistgenannt und verdeutlichen die große Skepsis, die dem Thema aus der ‚Fernsicht‘ entgegenschlägt. Positive Narrative, die den konkreten Nutzen neuer Anwendungen in die Vorstellungswelt der Menschen transportieren könnten, wie *Schutzengel, Wünsche-Erfüller* oder *Heinzelmännchen*, folgen erst weit danach.

3.9.3 Rollenwandel für die Versicherungswirtschaft?

Die *Versicherungswirtschaft* könnte auf Basis von Daten und Vernetzung neue Rollen in der Gesellschaft übernehmen, indem sie sich vom *Kostenerstatter* wandelt zum ‚Retter‘ oder ‚Schadenmanager‘ zum ‚Coach‘ oder ‚Schadenverhüter‘ sowie zum ‚Kontrolleur‘ oder ‚Motivator‘.

- In der Summe zeigen sich die Befragten diesen neuen Rollen gegenüber durchaus aufgeschlossen.
- Deutlich zurückhaltender ist die persönliche Bereitschaft zur laufenden *Übermittlung der notwendigen Daten*, zum Beispiel durch Sensoren, Wearables oder auch durch den Arzt.
- Inwieweit ein Angebot – und auch die damit verbundene Weitergabe der Daten – im Einzelfall befürwortet wird, hängt mehr von dessen konkreter Ausgestaltung ab als von der dahinterstehenden Rolle. Gleiches gilt für die Frage, ob der Einsatz eher in der Lebenswelt *Mobilität, Wohnen* oder *Gesundheit* vorstellbar ist. Und selbst der Grad der Überwachung, der mit dem jeweiligen Angebot verbunden ist, tritt hinter die Attraktivität des jeweiligen Nutzenversprechens zurück.

In Summe lässt sich eine insgesamt hohe Bereitschaft der Bürger respektive Kunden erkennen, neue, erweiterte Rollen der Versicherer anzunehmen.

3.9.4 Conclusio

Im Gesamtbild zeigt sich in den Ergebnissen ein doppeltes Paradoxon:

- Die Bürger fordern Datenschutz, beklagen übermächtige Konzerne und fühlen sich in ihrer Freiheit beschränkt – aber handeln nicht danach, sondern folgen ‚brav der Herde‘.
- Die Bürger fürchten Big Data – aber sind gerne bereit, die aus der Vernetzung resultierenden Potenziale in ihre Lebenswelten einzulassen.

Die Antwort auf die Frage ‚Bürgerschreck oder Hoffnungsträger‘ ist also weder das eine noch das andere, sondern muss lauten:

Big Data: Bürgerschreck *und* Hoffnungsträger!

Angesichts der weiter rasant fortschreitenden Vernetzung und des zunehmenden Einsatzes von künstlicher Intelligenz besteht die Gefahr, dass sich das doppelte Paradoxon nicht etwa auflöst, sondern weiter verfestigt. Dies kann in einer fatalistischen Haltung enden oder darin, dass auf Dauer eine Anpassung der Einstellungen an das eigene Verhalten erfolgt. Beides steht diametral zum Ideal eines ‚soveränen Datenbürgers‘.

Ein politischer Paradigmenwechsel kann in Teilen dazu beitragen, Brücken zwischen den empfundenen Risiken und den erhofften Chancen zu bauen. Ebenso kann die Etablierung positiver gesellschaftlicher ‚Erzählungen‘ helfen, das bisherige Schwarz-Weiß-Bild zu überwinden. Wesentliche Grundbedingungen dazu sind – neben dem eigentlichen Nutzen der Anwendungen – Fairness und Sicherheit der Systeme sowie Transparenz und Vertrauen in die Akteure. Und schließlich bleibt essenziell, die digitale Bildung der Bevölkerung auch in Bezug auf Big Data zu intensivieren, um Akzeptanz zu gewinnen und dem Ideal eines souverän handelnden Bürgers zumindest in Schritten näherzukommen.

Literatur

- best 4 planning. (2018). Daten sinnvoll verbinden. I. Bericht. <https://gik.media/cms/wp-content/uploads/2018/10/Berichtsband-b4p-2018.pdf>. Zugegriffen: 10. Dez. 2018.
- Caplan, B. (2007). *The myth of the rational voter. Why democracies choose bad policies*. Princeton: University Press.

- Enste, D., Haferkamp, A., & Fetchenhauer, D. (2009). Unterschiede im Denken zwischen Ökonomen und Laien. Erklärungsansätze zur Verbesserung der wirtschaftspolitischen Beratung. *Perspektiven der Wirtschaftspolitik*, 10, 60–78.
- Fisher, S., & Petersen, T. (2018). *Was Deutschland über Algorithmen weiß und denkt. Ergebnisse einer repräsentativen Bevölkerungsumfrage*. Gütersloh: Bertelsmann Stiftung. <https://doi.org/10.11586/2018022>.
- GfK. (2018). Künstliche Intelligenz (KI). Meinungsumfrage im Auftrag des Bundesverbandes deutscher Banken. Bericht. Bankenverband. https://bankenverband.de/media/files/Umfrage_Kuenstliche_Intelligenz.pdf. Zugegriffen: 28. Aug. 2018.
- Heckhausen, J., & Heckhausen, H. (2010). *Motivation und Handeln* (4. Aufl.). Berlin: Springer.
- Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.
- Leventhal, G. S. (1980). What should be one with equity theory? New approaches to the study of fairness in social relationships. In K. Gergen, M. Greenberg, & R. Willis (Hrsg.), *Social exchange: Advances in theory and research* (S. 27–55). New York: Plenum Press.
- Marsden, P. (2017). *Sex, lies and A.I.* Ein SYZYGY Digital Insight Report. Frankfurt: SZG.
- McClelland, D. C. (1985). *Human motivation*. Glenview: Foresman.
- Müller-Peters, A. (Hrsg.). (2018). Repräsentativität. Wie hältst Du's mit der Zufallsstichprobe? <https://www.marktforschung.de/dossiers/themendossiers/repraesentativitaet-und-zufallsstichprobe/>. Zugegriffen: 8. Okt. 2018.
- Müller-Peters, H. (2012). Repräsentativität 2012 – Fakt, Fake oder Fetisch? <https://www.marktforschung.de/dossiers/themendossiers/repraesentativitaet-2012/>. Zugegriffen: 08. Okt. 2018.
- Müller-Peters, H. (2017). Die Wahrnehmung und Bewertung von telematikbasierten Versicherungstarifen. In H. Müller-Peters & F. Wagner (Hrsg.), *Geschäft oder Gewissen? Vom Auszug der Versicherung aus der Solidargemeinschaft* (S. 21–47). Goslar Institut: Goslar.
- Müller-Peters, H., & Wagner, F. (Hrsg.). (2017). *Geschäft oder Gewissen? Vom Auszug der Versicherung aus der Solidargemeinschaft*. Goslar: Goslar Institut.
- Pariser, E. (2011). *The filter bubble. What the Internet is hiding from you*. London: Penguin Press.
- Petty, R., & Cacioppo, J. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. New York: Springer.
- PwC. (2017). Bevölkerungsbefragung. Künstliche Intelligenz. <https://www.pwc.de/de/consulting/bevoelkerungsbefragung-kuenstliche-intelligenz-2017.pdf>. Zugegriffen: 10. Okt. 2018.
- YouGov. (2018). Künstliche Intelligenz. Deutsche sehen eher die Risiken als den Nutzen. <https://yougov.de/news/2018/09/11/kuenstliche-intelligenz-deutsche-sehen-ehere-die-ris/>. Zugegriffen: 10. Okt. 2018.

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.



Big Data: Bürgerschreck und Hoffnungsträger! Zusammenfassung und Fazit

4

Jeder von uns hinterlässt persönliche Daten, wenn er online ist. Ganz gleich, ob sparsam oder ungehemmt, gewollt oder ungewollt, anonym oder offenerzig – alles bleibt. Fotos oder Text, Emojis oder Likes – alles dient zum Re-Identifizieren. Massenhaft entstehen Datenmengen, deren Ausmaß kaum vorstellbar ist und die mit dem Begriff ‚Big Data‘ ebenso einfach wie euphemistisch beschrieben werden. Noch entstehen diese Daten vor allem dann, wenn ein onlinefähiges Endgerät eingeschaltet wird. Aber selbst das wird nicht mehr benötigt. Daten entstehen im wahrsten Sinne des Wortes auf Schritt und Tritt, in den eigenen vier Wänden genauso wie beim Fahren auf der Autobahn, ohne dass irgendjemand dafür ein Smartphone einschalten muss. Man muss kein Prophet sein, um vorherzusagen, dass Massendaten weiter exponentiell anwachsen werden. Die nächste Dekade wird zweifelsohne die Dekade von Big Data, in der wir beantworten müssen, wie wir damit umgehen und was wir damit machen.

Big Data ist dabei weder die Sache einiger weniger Unternehmen noch ein Thema für ausgewählte IT-Experten. Das ergibt sich aus der Natur der Sache, nämlich der Tatsache, dass Big Data aus den Online-Beziehungen bzw. ganz generell aus dem Handeln und Verhalten der Nutzer entstehen, mithin jeden einzelnen unmittelbar involvieren, so oder so. Wenn es also darum geht zu entscheiden, wie mit diesen Massendaten umzugehen ist, wer sie erhebt, speichert, handelt und für welche privaten, sozialen und öffentlichen Zwecke sie von wem eingesetzt werden, dann ist das ein Themenfeld, das der öffentlichen und politischen Meinungsbildung genauso unterliegt wie den ökonomischen Gesetzen des Marktes.

Wie bei allen Dingen, die nur schwer vorstellbar sind und sich den Alltagswahrnehmungen entziehen, ist jedoch genau diese Meinungsbildung mit erheblichen Schwierigkeiten behaftet. Wer kann schon sagen, wie man sich Big Data

ganz konkret vorzustellen hat? Und wenn man es könnte, würde es bei der Beurteilung weiterhelfen? Wohl eher nicht. Ohne ein kommunikativ verwertbares Bild vor Augen lässt sich aber schwer diskutieren und debattieren. Kein Wunder also, dass die öffentliche Meinungsbildung zu Big Data zwischen dystopischen Schreckensvisionen einerseits und utopischen Heilserwartungen andererseits changiert, d. h. unvorhersehbar schwankt, wobei die Schreckgeschichten dominieren. Deshalb ist es auch kein Wunder, wenn Politik und Gesetzgeber sich bislang darauf konzentriert haben, den Bürger vor dem Missbrauch seiner persönlichen Daten zu schützen.

Wer aber einen weitergehenden gesellschaftlichen Diskurs führen will, in dem nicht nur die Risiken von Big Data, sondern auch die Chancen ausgewogen betrachtet werden, der muss dickere Bretter bohren. Denn schon die kleinste Veränderung im vorherrschenden Datenschutz-Paradigma erweist sich als höchst schwierig und ist nur in kleinen Schritten denkbar. Vor allem der Blick auf alltagsnahe Lebenswelten, in denen erkennbar wird, was Big Data und selbstlernende Algorithmen beispielsweise für den Fortschritt in Sachen Gesundheit, Wohnen oder Mobilität konkret bringen, kann helfen, Big Data aus dem Abseits der Abstraktion zu holen und damit eine breitere Diskussionsgrundlage zu schaffen. Doch was kommt davon wirklich beim umsorgten und geschützten Bürger an, der ja immer zugleich auch Onlinekunde, App-Junkie oder Social-Media-Nutzer ist? Und wie können oder müssen sich Unternehmen zu alledem verhalten, deren Geschäft auf Big Data und deren Auswertung durch Algorithmen beruht?

4.1 Zur Gestaltung des öffentlichen Diskurses über Chancen und Risiken von Big Data: Die Ergebnisse im Überblick

Die hier vorgelegte wissenschaftliche Studie hat sich mit diesen Themen- und Fragestellungen befasst, und zwar interdisziplinär und mit unterschiedlichen qualitativen und quantitativen Methoden, so wie es das Thema Big Data mit seinen vielfältigen Facetten verlangt. Kap. 1 betrachtet den öffentlichen Diskurs über Big Data und gibt einen Überblick über politische Handlungsoptionen. Darauf aufbauend zeigt Kap. 2 konkrete Anwendungen von Big Data und Künstlicher Intelligenz in relevanten Lebenswelten und analysiert die Auswirkungen auf bestehende Geschäftsmodelle am Beispiel von Versicherern. Schließlich wird in Kap. 3 auf der Grundlage einer repräsentativen Erhebung der Frage nachgegangen, was von alledem bei den Bürgern ankommt und welche Schlussfolgerungen daraus zu ziehen sind.

Dies sind die wichtigsten Ergebnisse im Überblick:

- Der öffentliche, in den Medien ausgetragene, Diskurs zum Umgang mit Massendaten (Big Data) ist von Erzählungen dominiert, die um Konflikte und Kollisionen kreisen und nicht über diese hinauskommen. In der Medienanalyse sind sie als Varianten des Big Brother-Narratives einzuordnen und haben ganz überwiegend den Charakter von Dystopien.
- Diese Dominanz der negativen Narrative ist auch in der Bevölkerungsumfrage deutlich zu erkennen. Es überwiegt eine skeptische bis ablehnende Grundeinstellung gegenüber Big Data. Risiken sind in den Köpfen der Befragten gegenüber Chancen überrepräsentiert. Die Dominanz des Big Brother-Narratives behindert dementsprechend eine breit getragene Verständigung darüber, wie sich die Risiken von Big Data beherrschen lassen, ohne die Chancen unangemessen zu reduzieren.
- Der politische Diskurs ist ganz im Gegensatz zum Mediendiskurs weiterhin von optimistischen, ja idealistischen Grundannahmen geprägt. Tradierte Idealtypen wie das Aufklärungsideal des mündigen Bürgers oder das Menschenbild des Homo oeconomicus, des rationalen Marktteilnehmers, sind nach wie vor die basalen Leitbilder von Politik bzw. Gesetzgebung, denen mit geeigneten Maßnahmen, nicht zuletzt einer detaillierten Rechtsetzung, Geltung zu verschaffen ist.
- Das Bild des weitgehend rational denkenden und agierenden Bürgers lässt sich jedoch schon lange nicht mehr aufrechterhalten und wird auch in unserer Studie widerlegt. Bedingungen eines weitgehend rationalen, selbstbestimmten Handelns sind Wissen, Können sowie ausreichend Motivation, beides auch einzusetzen. Zwar sind Grundbegriffe der Digitalisierung und der Künstlichen Intelligenz in der Bevölkerung angekommen, und ein Großteil fühlt sich zumindest in Teilen kompetent. Aber Wissensdefizite bestehen gerade in den Themen, die die Vernetzung von Daten behandeln und damit den souveränen Umgang mit den persönlichen Daten besonders tangieren, z. B. Big Data, Telematik, Internet of Things und e-Privacy. Die Bürger fühlen sich – quer durch alle Bevölkerungsgruppen – aufgrund von Komplexität und Marktstrukturen nur sehr bedingt handlungsfrei oder souverän.
- Augenfällig ist, dass die Mehrheit der Nutzer kaum auf die Furchtappelle der Big-Brother-Narrationen durch entsprechende Verhaltensänderungen reagiert. Sie blicken einerseits skeptisch auf Big Data, konsumieren ausgiebig dystopische Big-Brother-Geschichten und messen dem Datenschutz nach wie vor hohe Relevanz zu. Andererseits gehen sie sorglos oder fatalistisch mit ihren Daten um und nehmen angebotene Informations- oder Schutzmöglichkeiten

nicht oder nur begrenzt wahr. Besorgte Bürger, aber sorglose Verbraucher – das Nutzer-Paradoxon findet auch in unserer Befragung Bestätigung. Datenschutzbedenken und Sorge vor Big Data halten kaum davon ab, als nützlich oder notwendig empfundene Dienste in Anspruch zu nehmen, und zwar ziemlich unabhängig vom digitalen Wissen und von der Einstellung zum Datenschutz.

- Die Bevölkerung ist im Netz und das in doppeltem Sinne: Das Internet wird intensiv und über unterschiedlichste Geräte genutzt. Zugleich sind die Bürger über zahlreiche Dienste und Geräte ‚im Netz‘ der Dienste und hinterlassen so umfangreiche Datenspuren. Dabei dominieren die US-amerikanischen Internetgiganten, die zumindest bis zur Inkraftsetzung der EU-Datenschutzgrundverordnung im Mai 2018 deutlich niedrigeren Datenschutzstandards unterlagen als ihre deutschen Wettbewerber. Reichweite und Nutzensumfang der globalen Player dominieren offenbar gegenüber Nähe und Datenschutz. Die Bürger fühlen sich in hohem Maße ausgeliefert und nutzen trotzdem munter die ‚Frightful 5‘.
- Insgesamt bleibt es bei der Dichotomie der Rollen und Einstellungen, die zu dem besagten Nutzer-Paradoxon führen: *Der Nutzer als Bürger ist skeptisch, schutzbedürftig und kulturpessimistisch, als Verbraucher ist er sorglos, bequem und pragmatisch.* Man könnte diese Beobachtung auch positiver formulieren: Das tatsächliche Verhalten der Bürger im Netz orientiert sich deutlich stärker an den Chancen von Big Data als an den Risiken.
- Dabei ‚hilft‘ digitale Bildung, denn sie führt laut Gruppenvergleichen in unserer Befragung dazu, dass die meisten Sorgen kleiner werden und die Chancen insgesamt stärker in den Fokus rücken. Wenn dann noch anstelle abstrakter Risiken und Chancen über ganz konkrete, nutzenstiftende Anwendungsfelder gesprochen wird, dann wandelt sich das Bild, und Big Data stößt in vielen Einsatzbereichen auf hohe Akzeptanz. Das erstreckt sich auf Smart Services aller Art bis hin zu Sicherheitsfragen, Kriminalitätsbekämpfung und Verkehrsüberwachung.
- Es herrscht breiter Konsens bezüglich Fairness und Nachvollziehbarkeit als Grundanforderung an datengestützte Systeme. Dies impliziert Transparenz, Vertrauen in (oder externe Kontrolle der) Anbieter, aber auch Neutralität, Diskriminierungsfreiheit, Datenqualität und natürlich Datensicherheit. All das sollen die agierenden Unternehmen und die Aufsichtsinstanzen gleichermaßen gewährleisten. Dann, so diese normative Sichtweise, kann auch die Akzeptanz von Big Data als Hoffnungsträger steigen. Doch ganz so einfach ist es nicht.

Vor allem bei unstrukturierten Daten (z. B. Fotos, Videos, Sprache), selbstlernenden Algorithmen oder Blockchains ist es schwer bis nahezu unmöglich, die normativen Vorgaben der diskriminierungsfreien Datenqualität und allgemeiner Nachvollziehbarkeit ganz praktisch zu erfüllen.

- Die Bürger wünschen sich vielleicht deshalb weiterhin eine klare Reglementierung und Regulierung durch den Staat. Dennoch ist unübersehbar, dass die Rechtsetzung im Kontext einer dynamischen Digitalisierung bereits an ihre Grenzen gestoßen ist. Selbstlernenden Algorithmen mit immer diffizileren juristischen Befehlsfolgen zum Datenschutz begegnen zu wollen, ist schon für sich keine wirklich einlösbare Schlussfolgerung. Darüber hinaus führt das eben beschriebene paradoxe Nutzerverhalten dazu, dass Regelungen z. B. aus der EU-DSGVO, die eigentlich Wahlfreiheiten und somit Konsumentensouveränität sicherstellen sollen, ins Leere zu laufen drohen.
- Umgekehrt kann das volle Potenzial datengetriebener Services erst dann entfaltet werden, wenn möglichst viele Daten unterschiedlicher Quellen generiert, auch ohne einengende Zweck- und Planvorgaben ausgewertet und miteinander kombiniert werden. Die Wirkmächtigkeit der Korrelationen wird sich in der Big-Data-Dekade erst noch voll entfalten. Datensparsamkeit, Zweckbindung von Daten und Datenlöschungen, wie sie die EU-DSGVO aus Datenschutzwägungen verständlicherweise fordern, sind vor diesem Hintergrund kontraproduktiv. Diese gesetzlichen Regelungen stehen infolgedessen zugleich im Widerspruch zur Entfaltung künstlicher Intelligenz.
- Mit diesen Restriktionen lassen sich auch die positiven Beiträge von Big Data und Künstlicher Intelligenz für gesellschaftlich relevante Zwecke nur unzureichend realisieren. Im Mittelpunkt stehen dabei Zwecke des Gemeinwohls (in der angelsächsischen Diskussion heißt dies ‚social goods‘). Big Data sowohl aus öffentlicher als auch privater Hand bieten ungeahnte Chancen, die gravierendsten Probleme der Welt nachhaltig, d. h. vor allem auf globaler Reichweite, zu lösen. Das beginnt bei Klimaschutz, geht über Gesundheit und Ernährung bis hin zu Bildung. Akzeptierte Regeln zu finden, mit denen Zugang und Einsatz von Big Data für Gemeinwohlzwecke erreicht werden kann, steht deshalb international auf der politischen Agenda.
- Die Open-Data-Bewegung ist dabei, dieses Terrain zu erobern. Die Idee einer Daten-Allmende („Commons“), in der öffentliche Massendaten nach definierten Regeln der Nachhaltigkeit zwischen Organisationen aller Art geteilt werden, ist ebenso faszinierend wie ganz praktisch umzusetzen, wie dies beispielsweise offene Datenbestände aus öffentlichen Verwaltungen oder

Forschungseinrichtungen aller Art zeigen. Noch weitergehender ist der Gedanke einer nach ethisch verantwortbaren Zwecken differenzierten Daten-Infrastruktur, für deren Sicherheit und Qualität dann sogar ein öffentlicher Auftrag besteht. Bemerkenswerterweise finden solche Ideen in unserer Umfrage eine beachtliche Zustimmung.

- Nicht zuletzt aufgrund der Grenzen des Datenschutzkonzeptes ist es sinnvoll, eine Verständigung über den ausgewogenen Umgang mit Big Data auf einem anderen Spielfeld bzw. mit einer anderen Agenda zu suchen. Das Konzept der Datenethik ist – insbesondere in Verbindung mit dem Open Data-Prinzip – so ein alternatives Spielfeld. Hier geht es darum, den Bürger in seiner Rolle als Nutzer digitaler Technologien dabei zu unterstützen, dass er seine Daten gezielt zu den von ihm gewünschten Zwecken weitergeben kann. Der Nutzer ist weniger Schutzobjekt, sondern als Datengeber, Datenspender oder gar Datenhändler Subjekt der Digitalisierung. Datenethik ersetzt das Datenschutzparadigma nicht, sondern baut auf den erreichten Schutzstandards auf und erweitert sie um ein echtes Handlungskonzept. Es weist nicht nur den Nutzern eine andere, nämlich aktive und gestaltende Rolle zu, sondern allen Akteuren rund um Big Data. Im Mittelpunkt stehen dabei die Chancen, die sich aus Big Data ergeben, die der Nutzer mit seinen Daten selbst aktiv unterstützen kann.
- Schon jetzt lässt sich sagen, dass Unternehmen, deren Umgang mit von ihnen gesammelten und genutzten Daten auf klaren ethischen Handlungsgrundsätzen beruht, die Gewinner dieser Entwicklung sein werden. Unternehmen sind nicht mehr nur zur Compliance mit den Datenschutzgesetzen aufgefordert. Sie werden darüber hinaus ethisch verpflichtet, die Chancen von Big Data bzw. Künstlicher Intelligenz proaktiv zu nutzen, und zwar sowohl für privatwirtschaftliche als auch soziale Zwecke. Corporate Digital Responsibility lässt sich schon jetzt als neue Dimension einer verantwortungsvollen Unternehmensführung ausmachen.
- Ordnungspolitisch motivierte Konzepte, die nicht zuletzt auf die Geschichte der ‚Frightful 5‘ Bezug nehmen, können die Vorstellung des souverän mit seinen Daten agierenden Nutzers wirkungsvoll flankieren. Das gilt beispielsweise für einen unternehmens- und branchenübergreifenden Datenaustausch (Daten-Sharing), zu dem Daten-Oligopole ggf. gezwungen werden können. Wettbewerb der Algorithmen statt Oligopol der Datenkraken – diese Geschichte scheint auch für die Bevölkerung interessant zu sein. Kartellrechtliche Maßnahmen werden ausdrücklich begrüßt, aber auch der Ansatz eines verbindlichen Daten-Sharings könnte zukünftig überzeugen.

4.2 Zum Nutzen von Big Data in konkreten Lebenswelten: Die Ergebnisse im Überblick

Big Data kann substantielle Mehrwert für die Bürger in ihren *Lebenswelten* generieren. In Bezug auf die Lebenswelten *Wohnen*, *Gesundheit* und *Mobilität* wurden Einsatzbereiche von Big Data dargestellt und beispielhaft an der Versicherungswirtschaft analysiert, wie weit sich daraus die Rolle einer Branche in der Gesellschaft ändern kann:

- Auf Basis von Big Data werden intelligente, digitalisierte Angebote ermöglicht, mit denen Bedürfnisse der Bürger erfüllbar sind (Smart Services). Smart Services erknüpfen Produkte, Dienstleistungen und Prozesse, die dem Kunden als individualisiertes Gesamtangebot und ‚as a service‘ zur Verfügung stehen. Im Mittelpunkt der Smart Services steht der Bürger mit seinen Wünschen und Bedürfnissen, die oftmals nicht durch einzelne Anbieter und deren Produkte erfüllt werden können. Zentral für nutzenstiftende Angebote in den Lebenswelten der Bürger ist daher der ganzheitliche Ansatz digitaler Ökosysteme.
- Datengetriebene Angebote in der *Lebenswelt Wohnen* schaffen ein Smart Home, in dem die Wohnumgebung komfortabler genutzt, eine erhöhte Sicherheit innerhalb des Hauses sowie ein verbesserter Schutz nach außen gewährleistet und der Ressourcenverbrauch effizienter gesteuert werden kann. Künftig ist mit ganzheitlichen Lösungen für das Smart Home des Bürgers zu rechnen. Das hat auch Konsequenzen für Versicherer, da es in größeren Netzwerken (Ökosystemen) künftig reichen könnte, daran jeweils nur einen Versicherer exklusiv zu beteiligen.
- Im Mittelpunkt der *Lebenswelt Gesundheit* stehen die Sammlung von Daten und deren Einsatz zur Verbesserung von Prävention, Diagnose und Therapie von Krankheiten. Versicherer könnten wegen ihres bereits vorhandenen Wissens über Krankheitsverläufe und das verhältnismäßig hohe Vertrauen, das Bürger ihnen bezüglich des Umgangs mit persönlichen Daten entgegenbringen, zum Orchestrator des Datenmanagements von Ökosystemen in der Lebenswelt Gesundheit werden. Durch die hohe Sensibilität der Daten geht damit eine besonders große Verantwortung einher.
- Drei Trends prägen die *Lebenswelt Mobilität*: die Sharing Economy, die Entwicklung zum autonomen Fahren und die intermodale Verknüpfung von Verkehrsmitteln. Das hat u. a. zur Folge, dass der Gesamtbestand zu versichernder Kraftfahrzeuge zurückgeht und sich die klassischen Deckungskonzepte nicht

mehr ohne Weiteres anwenden lassen. Die große Herausforderung der Versicherungswirtschaft besteht angesichts großer (Automobilhersteller) und teils neuer (Big Techs) Wettbewerber mit ihren Smart Services darin, den Kundenzugang zu erhalten und mit den neu gewonnenen Mobilitätsdaten echte Mehrwert für die Kunden und Nutzenpotenziale auch jenseits einer für einzelne Zielgruppen günstigeren Tarifierung und Prämieinstufung zu erzeugen.

- Die Bürger wertschätzen den Mehrwert, den diese Smart Services ihnen bieten können. Die Grundskepsis gegenüber Big Data kippt, wenn konkrete, nutzenstiftende Anwendungen genannt werden. Ein Großteil unserer Befragten kann sich eine Vielzahl von Anwendungen in den drei Lebenswelten Mobilität, Wohnen und Gesundheit durchaus vorstellen. Analog zu den gesellschaftlichen Einsatzfeldern ist die Akzeptanz besonders dann hoch, wenn es um die Abwendung von Gefahren geht – sei es im Feld der Gesundheit, beim Einbrecherschutz oder selbst zur Überwachung der Verkehrsregeln.
- Anwendungsfelder werden in der Tendenz umso negativer bewertet, je mehr sie den Alltag nicht nur unterstützen, sondern gefühlt die Kontrolle übernehmen. Werden aber keine als wesentlich empfundenen Handlungsspielräume eingeschränkt und ist der Nutzen offensichtlich, ist auch die Akzeptanz weitestgehend automatischer Steuerung hoch.
- Viele der Anwendungen in den genannten Lebenswelten (zum Beispiel im Gesundheitsmonitoring, der Verkehrssteuerung oder auch im ‚Smart Home‘) erfordern eine weitgehende ‚Überwachung‘ des Einzelnen. In den Antworten der Befragung lässt sich kaum ein klarer Zusammenhang zwischen dem Grad an Überwachung und der Akzeptanz des jeweiligen Angebotes feststellen. Vielmehr scheint – wiederum in Einklang mit dem Nutzerparadoxon – alleine der empfundene Nutzen über Befürwortung oder Ablehnung zu entscheiden.
- Mit neuen digitalen Lösungen ändert sich das Geschäftsmodell der Versicherer grundlegend. Durch den Einsatz von Sensoren können Schäden vorhergesehen und so zunehmend auch vermieden werden (Reduzierung klassischer Risiken). Auf der anderen Seite scheint es im Hinblick auf die wachsende Bedeutung der Vernetzung und der steigenden Relevanz von Daten- und Prozesssicherheit angezeigt, neu entstehende Kumulrisiken z. B. durch IT-Ausfälle oder Hackerangriffe abzusichern sowie für dabei entstehende Kosten aufzukommen (Entstehung neuer Risiken).
- Überhaupt stellt sich die Frage, welche *neuen Rollen* den Versicherern im Big Data-Zeitalter zuzuschreiben sind. Wie schon im Zusammenhang mit dem Datenethikkonzept erwähnt, liegt gerade in neuen Rollenbeschreibungen bzw. Zuschreibungen jenseits der eingefahrenen Routinen womöglich der Schlüssel für einen chancenorientierteren Umgang mit Big Data und Künstlicher

Intelligenz. Für Versicherer können solche neue Rollenmodelle jenseits der tradierten Rolle des Kostenerstatters etwa so aussehen:

- ‚*Retter*‘ oder ‚*Schadenmanager*‘: Ist ein Schaden eingetreten, tritt neben den eigentlichen finanziellen Schadenausgleich immer mehr das ‚Management‘ des Schadens, also z. B. die Organisation von Reparaturen oder medizinischen Therapien. Mit zunehmender Vernetzung ergeben sich hier weitergehende Möglichkeiten, sowohl die Schäden zu erkennen als auch die Maßnahmen zu koordinieren und zu begleiten.
 - ‚*Coach*‘ oder ‚*Schadenverhüter*‘: Ebenso ermöglichen Vernetzung, die Analyse großer Datenbestände und der Einsatz von Sensoren den Versicherern zunehmend, schon vorab mögliche Risiken zu erkennen und durch Aufklärung oder Verhaltensfeedbacks zu minimieren.
 - ‚*Kontrolleur*‘ oder ‚*Motivator*‘: Wenn Risiken vorausschauend gemessen und erkannt werden können, dann ist auch eine unmittelbare Einflussnahme auf das Verhalten des Versicherungsnehmers durch positive oder negative Sanktionen nicht mehr weit. Dies kann zum Beispiel über die Bepreisung erfolgen, aber auch in weitergehenden konkreten Handlungsvorschriften oder Verboten, welche wiederum durch Sensoren und Vernetzung überprüft werden können.
- Die Ergebnisse der Umfrage zeigen, dass die Kunden durchaus aufgeschlossen für eine solche Rollenerweiterung ihrer Versicherer sind. Fast alle der exemplarisch genannten Angebote werden von einem bis zu zwei Dritteln der Befragten begrüßt. Umgekehrt lehnen nur zwischen 11 und 37 % der Befragten die entsprechenden Angebote ab. Lediglich für eine laufende Analyse des Fahrstils fällt die Akzeptanz deutlich geringer aus.
 - Ob die Menschen eher die Rolle des Versicherers als Schadenmanager, als Schadenverhüter oder als Kontrolleur befürworten, lässt sich nicht eindeutig beantworten. Vielmehr hängt die Akzeptanz von der konkreten Ausgestaltung der Angebote innerhalb der jeweiligen Rolle ab.
 - Ebenso wenig besteht ein eindeutiger Unterschied zwischen den Lebenswelten. Die erweiterten Rollen fanden in unserer Befragung sowohl bezogen auf Mobilität als auch auf Gesundheit und Wohnen Akzeptanz, wobei die Zustimmung im besonders datensensiblen Bereich der Gesundheit insgesamt sogar noch etwas höher ausfiel.
 - Inwieweit sich daraus eine wirklich breite Nachfrage im Markt entwickelt, hängt von der konkreten Ausgestaltung der Angebote ab, bei denen es – besonders wenn auch Sanktionen im Spiel sind – darauf ankommt, dass die zugrunde liegenden Merkmale und Algorithmen nachvollziehbar und gerecht erscheinen. Verhaltensmerkmale, die durch Big Data gemessen werden und

möglichen Sanktionen durch den Versicherer zugrunde liegen, sollen durch den Kunden tatsächlich zu beeinflussen sein. Schließlich gilt auch in diesem Zusammenhang wieder: Die persönlichen Vorteile müssen offensichtlich und der Datenschutz muss gewährleistet sein.

- Gerade die Anforderungen der Transparenz und der Nachvollziehbarkeit stellen jedoch – wie schon ausgeführt – im Kontext von Big Data und künstlicher Intelligenz schwer erfüllbare Bedingungen dar. Vor allem selbstlernende Algorithmen im Rahmen der Künstlichen Intelligenz sind kaum noch durchschaubar, geschweige denn vermittelbar. Hier ist eine Balance zwischen mathematischer Genauigkeit einerseits und breiter Vermittelbarkeit auf der anderen Seite anzustreben.

Damit schließt sich der Kreis. Sowohl der beschriebene politische und ökonomische Paradigmenwechsel als auch die neuen Rollenzuschreibungen an nahezu alle Akteure werden umso erfolgreicher sein, je besser es gelingt, sie mit wirksamen Narrationen bzw. Narrativen zu verbinden, die nicht in Konflikten und Kollisionen hängen bleiben und die Komplexität des Themenfelds im Sinne einer breiten Verständigung sinnvoll reduzieren. Genau für diese Konstruktion von gesellschaftspolitisch relevanten Erzählungen eignen sich sowohl die genannten Überlegungen zur Datenethik sowie zur Daten-Infrastruktur als auch die Betrachtung der konkreten digitalen Lebenswelten grundsätzlich gut. Anwendungen auf Basis von Big Data haben aus technischer Sicht ein hohes Potenzial, Motive wie Sicherheit, Komfort, Effizienz oder Kontrolle zu bedienen und somit einen hohen direkten Nutzen für die Bürger zu generieren. Positive, mit Assoziationen aufgeladene Codes könnten diese Seiten von Big Data in der Vorstellungswelt der Menschen verankern und so helfen, ein etwas balancierteres Bild der neuen Datenwelt zu schaffen.

Bisher dominiert aber das Big-Brother-Narrativ mit seinen Abwandlungen die öffentliche Big-Data-Arena, neben dem bisher allenfalls die Vorstellung vom ‚Forscher und Entwickler‘ sowie vom praktischen ‚Alltagsassistenten‘ eine zumindest erwähnenswerte Statistenrolle einnehmen konnte. Zur gesellschaftlichen Konstruktion positiver, sinnstiftender Narrationen, die den Schutz des Bürgers vor Datenmissbrauch einerseits und den Nutzen von Big Data andererseits besser ausbalancieren helfen, ist es also zumindest noch ein weiter Weg.

Open Access Dieses Kapitel wird unter der Creative Commons Namensnennung 4.0 International Lizenz (<http://creativecommons.org/licenses/by/4.0/deed.de>) veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Kapitel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.



Anhang

Vollständige Fragetexte zu den Folgeabschätzungen:

Die Erfassung und automatischer Verarbeitung großer Datenmengen über den Einzelnen wird ...

- ... unser Leben in Zukunft deutlich sicherer machen – z. B. im Verkehr, der Gesundheit oder beim Schutz des Eigentums.
- ... unser Leben deutlich bequemer machen, weil viele Handlungen automatisiert, vereinfacht und besser auf unsere Bedürfnisse ausgerichtet sind.
- ... dem Einzelnen viele neue Möglichkeiten eröffnen, sein Leben zu gestalten.
- ... uns Dinge ermöglichen, von denen wir früher nicht zu träumen wagten.
- ... uns Spaß und neue Anregung geben, zum Beispiel durch neue Spiele oder Unterhaltungsangebote.
- ... den Kontakt mit Freunden und Familie erleichtern.
- ... uns helfen, Dinge schneller zu erledigen.
- ... uns helfen, Energie zu sparen.
- ... auf lange Sicht Geld sparen.
- ... insgesamt mehr Wohlstand schaffen.
- ... den Menschen helfen, besser und günstiger einkaufen zu können.
- ... für mehr Wissen und Aufklärung bei den Menschen sorgen.
- ... die Welt durch mehr Meinungsvielfalt demokratischer machen.
- ... neue Gefahren schaffen, z. B. durch Fehler in der Technik, in den Berechnungsmethoden oder durch den Verlust oder Missbrauch von Daten.
- ... viele Dinge des Alltags noch komplizierter und undurchschaubarer machen, als sie es jetzt schon sind.
- ... dem Einzelnen immer mehr Wahlfreiheit nehmen.

- ... uns abhängig machen von Entscheidungen, die Maschinen und Computer für uns treffen und die wir nicht beeinflussen können.
- ... den Schutz unserer Privatsphäre immer schwieriger machen.
- ... das Leben zunehmend stressiger machen.
- ... die Menschen immer mehr vereinsamen lassen.
- ... die Arbeitslosigkeit erhöhen.
- ... dazu führen, dass manche Menschen aufgrund ihrer Daten ungerecht behandelt werden.
- ... dafür sorgen, dass unser Wissen immer oberflächlicher wird.
- ... für eine zunehmende Entdemokratisierung sorgen.