C. Big Data und dessen Gefahren

I. Big Data, Datenökonomie und Überwachung

Alle Geräte im IoT erheben ständig Daten. Das Fitnessarmband misst den Herzschlag, erhebt die gelaufenen Schritte und Kilometer, die smarte Steckdose zeichnet auf, wann wieviel Strom verbraucht wird, die smarten Glühbirnen, wann in welchem Raum das Licht an ist und das Smartphone fungiert als zentrale Steuerungseinheit, bei der alle Daten zusammenlaufen. Bei den enormen Datenmengen, die dabei entstehen, spricht man heutzutage von Big Data. Obwohl Big Data ein sehr unscharfer und nicht einheitlich definierter Begriff ist,[134] kann zusammenfassend behauptet werden, dass darunter enorme, heterogene und sich ständig wandelnde Datensätze zu verstehen sind, die nicht ohne sorgfältige Analyse oder sog. Data Mining[135] mithilfe neuer Technologien und Ressourcen verstanden und genutzt werden können.[136] Geschätzt lag die Größe der weltweiten Datensphäre 2018 bei ca. 33 Zettabytes, wobei davon ausgegangen wird, dass bis 2025 eine Menge von 175 Zettabytes erreicht wird.[137] Für Unternehmen ist Big Data und dessen Analyse insofern attraktiv, da Daten heutzutage einen hohen wirtschaftlichen Stellenwert einnehmen, auf deren Grundlage etliche Geschäftsmodelle basieren.[138] Hauptaugenmerk bei der Analyse ist die Optimierung der Unternehmensprozesse, besonders im Bereich Marketing, Kundenbindung und Service.[139] Dementsprechend werden die Datensätze vermehrt dazu genutzt, Prognosen wie z.B. über den Beziehungsstatus, den Gesundheitszustand, den Charakter, die Persönlichkeit und die Emotionen

134 *Chen/Mao/Liu*, Mobile Networks and Applications 2014, S. 171 (173).
135 *Gandy,* in: Haggerty/Ericson, The New Politics of Surveillance and Visibility, 2006, S. 363 (364); *Boehme-Neßler,* Datenschutz und Datensicherheit 2016, S. 419 (421).
136 *Rajaraman,* Resonance 2016, S. 695 (697); *Faaique,* International Journal of Mathematics, Statistics, and Computer Science 2024, S. 96 (99 f.).
137 *Reinsel/Gantz/Rydning,* The Digitization of the World, 2018, S. 3; Durch das gestiegene Datenaufkommen aufgrund der Corona Pandemie (mehr Streaming, Videokonferenzen, mehr Nutzung von Online-Diensten) werden die 175 Zettabytes bis 2025 jedoch wahrscheinlich bei Weitem übertroffen werden.
138 *Jöns,* Daten als Handelsware, 2016, S. 16.
139 *Ohlhorst,* Big Data Analytics, 2013, S. 11 f.

zu erstellen, um gezielte Werbung oder Services anbieten zu können.[140] Diese Analyseergebnisse und Prognosen, und nicht die Daten selbst, werden nicht nur für die Optimierung der eigenen Unternehmensprozesse und des eigenen Marketings genutzt,[141] sondern auch Dritten angeboten, wie z.B. im Falle von Googles personalisierter Werbung.[142] Im Gegensatz dazu besteht aber auch ein expliziter Handel mit Daten wie z.B. Adresshandel, Scoring oder Data Broking.[143] Das wirtschaftliche Interesse an Daten ist dementsprechend groß.

Allerdings hat Big Data nicht nur kommerzielle Vorteile. Es kann genauso gut genutzt werden, um gesamtgesellschaftliche und wissenschaftliche Ziele zu verfolgen. So könnte die Big Data Auswertung im Gesundheitssektor bspw. hilfreich in der Diagnostik sein.[144] Außerdem könnte mittels Big Data ein digitaler Zwilling der Erde erzeugt werden, um bspw. Umweltauswirkungen besser vorherzusagen.[145] In der Astronomie werden durch einige Projekte bereits 100-200 Petabytes an Daten jährlich erzeugt, die ausgewertet werden können, um weitere Erkenntnisse über das Universum zu erhalten.[146]

Jedoch ist das Sammeln von solchen enormen Datensätzen und deren Analyse ein ambivalenter und umstrittener Prozess, denn auf der einen Seiten ist zwar das wirtschaftliche,[147] gesellschaftliche[148] und wissenschaftliche[149] Wertschöpfungspotential von Big Data enorm, auf der anderen Seite kann der Missbrauch dieser Daten aber auch schwerwiegende Konsequenzen haben. Im Zuge der Datenökonomie werden Privatpersonen ständig überwacht, da deren Daten und Erfahrungen als kostenloser Rohstoff für

140 *Christl,* Kommerzielle digitale Überwachung im Alltag, 2014, S. 12-24.
141 *Acciarini et al.,* Technovation 2023, S. 1 (4 ff.); *Krishna et al.,* 2023 International Conference on Inventive Computation Technologies 2023, S 1073 (1073 ff.).
142 *Jöns,* Daten als Handelsware, 2016, S. 17.
143 *Christl,* Kommerzielle digitale Überwachung im Alltag, 2014, S. 51-64.
144 *Akindote,* World Journal of Advanced Research and Reviews 2023, S. 1293 (1295 ff.).
145 *Li et al.,* Nature Reviews Earth & Environment 2023, S. 319 (320 ff.).
146 *Faaique,* International Journal of Mathematics, Statistics, and Computer Science 2024, S. 96 (100 ff.).
147 *Spiekermann,* Aus Politik und Zeitgeschichte 2019, S. 16 (18); *Acciarini et al.,* Technovation 2023, S. 1 (4 ff.); *Krishna et al.,* 2023 International Conference on Inventive Computation Technologies 2023, S 1073 (1073 ff.).
148 *Bitkom,* Leitlinien für den Big-Data-Einsatz, 2015, S. 22 ff.; *Akindote,* World Journal of Advanced Research and Reviews 2023, S. 1293 (1295 ff.).
149 *Spindler,* Medizinrecht 2016, S. 691 (691); *Li et al.,* Nature Reviews Earth & Environment 2023, S. 319 (320 ff.); *Faaique,* International Journal of Mathematics, Statistics, and Computer Science 2024, S. 96 (100 ff.).

Internetkonzerne fungieren können.[150] Da der Zugang zu Big Data restriktiv nur für einige wenige gewährleistet ist, wird Forschung verzerrt. Die großen Internetkonzerne, die in diesem Punkt als Gatekeeper bezeichnet werden können, können nach eigenem Ermessen entscheiden, wer Zugang zu den Datensätzen bekommt, zu welchem Zweck dies geschieht und so gezielt Einfluss auf die Forschung nehmen.[151]

Die größten Bedenken gegenüber Big Data gelten jedoch der Privatsphäre der betroffenen Personen und damit einhergehend auch deren Selbstbestimmung und Handlungsfreiheit. Denn mit der Verknüpfung und fortlaufenden Analyse von mehr und mehr Daten, hat alles plötzlich einen Personenbezug.[152] Jedes noch so unscheinbare Datum liefert neue Erkenntnisse über eine Person, da es mit bereits bestehenden Daten in Bezug gesetzt und entsprechend ausgewertet wird.[153] Auf staatlicher Ebene kann diese Dauerüberwachung von Einwohnern und die Erstellung detaillierter Profile auch als moderner Kontrollmechanismus ganz im Sinne des Orwellschen Big Brothers gesehen werden.[154] Dieser staatliche Kontrollmechanismus findet derzeit in Chinas Social Credit System seinen Höhepunkt. Dort werden gesellschaftsübergreifend auf Basis jeder sozialen und ökonomischen Tätigkeit der Einwohner Punkte verteilt, anhand derer entschieden wird, ob die jeweilige Person eine Belohnung oder eine Bestrafung für ihr Handeln erhält.[155] Die möglichen Implikationen eines solchen Systems, wie z.B. flächendeckende Zensur und Massenmanipulation, stellen eine ernstzunehmende Bedrohung der demokratischen Gesellschaft dar. Diese unterschwellige Beschneidung der individuellen Selbstbestimmung lässt sich jedoch auch in gewissen Zügen in Europa und den USA beobachten. In diesem Fall spielt Microtargeting, also das personen- und interessenspezifische Schalten von Inhalten,[156] eine große Rolle. Genau dieses Microtargeting wird vermehrt in der Konzeption von politischen Wahlkampagnen genutzt, indem anhand von Wahlprognosen und Scores, individuelle, auf Gruppen und Einzelpersonen zugeschnittene Maßnahmen entwickelt wer-

150 *Zuboff,* Aus Politik und Zeitgeschichte 2019, S. 4 (8).
151 *boyd/Crawford,* Information, Communication & Society 2012, S. 662 (675).
152 *Quinn/Malgieri,* German Law Journal 2021, S. 1583 (1596 f. und 1599); *Frenzel* (2021), Art. 9 Rn. 8*; Boehme-Neßler,* Datenschutz und Datensicherheit 2016, S. 419 (422).
153 *Boehme-Neßler,* Datenschutz und Datensicherheit 2016, S. 419 (422).
154 *Bogard,* in: Haggerty/Ericson, The New Politics of Surveillance and Visibility, 2006, S.55 (59).
155 *Liang et al.,* Policy & Internet 2018, S. 415 (416).
156 *Zuiderveen Borgesius et al.,* Utrecht Law Review 2018, S. 82 (82).

den, welche die Stimmenvergabe bei Wahlen beeinflussen sollen.[157] Der wohl prominenteste Fall hierbei ist die Einflussnahme von Facebook und Cambridge Analytica auf die Präsidentschaftswahl 2016 in den USA.[158]

II. Bedeutung von Datenschutz

Big Data ist in der heutigen Gesellschaft ein Fakt und die Entwicklung lässt sich nicht mehr rückgängig machen. Die sinnvolle Gestaltung des Umgangs mit diesen Daten bleibt jedoch eine weitreichende rechtliche, ethische und technische Frage,[159] die es zu beantworten gilt.[160] Besonders die Bevölkerung sehnt sich nach einem effektiven Datenschutz, da diese vermehrt das Gefühl hat, Opfer von Datenklau und Datenmissbrauch zu sein[161] und sich wünscht, dass gerade sensible personenbezogene Daten, wie z.B. Gesundheitsdaten, vor Missbrauch geschützt werden.[162] Dementsprechend ist es nur 3 % der deutschen Internetnutzer egal, was mit ihren Daten passiert.[163] 42 % sind besorgt über die Menge an Daten, die Unternehmen über sie sammeln.[164] Ca. 26 % halten das Internet für wenig sicher – unsicher, wenn es um ihre personenbezogenen Daten geht.[165] Im Bereich Smart Home ist mangelnder Datenschutz bspw. ein Kriterium für die Nicht-Nutzung der Technologien.[166]

Auf der anderen Seite besteht jedoch auch das sog. Privacy Paradoxon, bei dem der Schutz von personenbezogenen Daten und der Privatsphäre

157 *Christl,* Aus Politik und Zeitgeschichte 2019, S. 42 (46 ff.).
158 *Chester/Montgomery,* Internet Policy Review 2017, S. 1 (7).
159 *boyd/Crawford,* Information, Communication & Society 2012, S. 662 (671 f.); *Boehme-Neßler,* International Data Privacy Law 2016, S. 222 (224); *Kasera et al.,* 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) 2023, S. 1122 (1122 ff.); *Vasa/Thakkar,* Journal of Computer Information Systems 2023, S. 608 (608 ff.).
160 *Boehme-Neßler,* Datenschutz und Datensicherheit 2016, S. 419 (423).
161 *Opaschowski,* in: Bäumler/von Mutius, Datenschutz als Wettbewerbsvorteil, 2002, S. 13 (14 ff.).
162 *Richter/Kliner/Rennert,* in: Knieps/Pfaff, Digitale Arbeit – Digitale Gesundheit, 2017, S. 107 (121).
163 *Bitkom,* Datenschutz in der digitalen Welt, 2015, S. 2.
164 Abrufbar unter: https://de.statista.com/statistik/daten/studie/1286512/umfrage/meinungen-der-deutschen-zum-thema-datenschutz-nach-generationen/ (abgerufen 7.4.2024).
165 Abrufbar unter: https://www.sicher-im-netz.de/file/14331/download?token=i7DCJrK4 (abgerufen 7.4.2024).
166 *Deloitte*, Smart Home Consumer Survey 2018, 2018, S. 15.

zwar als wichtig eingestuft wird, aber nicht zwangsläufig das Verhalten der Nutzer bestimmt.[167] Dabei findet eine einfache Kosten-Nutzen-Abwägung statt, bei der die erhaltene Leistung, die auf Preisgabe von Daten basiert, als größerer Vorteil eingestuft wird, als der Erhalt der Privatsphäre.[168] Erklärungen für dieses Phänomen gibt es viele,[169] hier soll jedoch zusätzlich argumentiert werden, dass eine Korrelation zwischen der Angst, etwas zu verpassen,[170] und dem Mangel an datenschutzfreundlichen und vergleichbaren Alternativen zu den etablierten Anbietern besteht. Um nicht vom gegenwärtigen gesellschaftlichen Leben ausgeschlossen zu werden, hat sich die Nutzung von Social Media, Smartphones, Apps etc. zu einem essenziellen Bestandteil der Moderne entwickelt, der nur durch die Beschränkung der Privatsphäre erhalten werden kann. Erschwerend kommt hinzu, dass die deutschen Internetnutzer größtenteils Angst vor dem Kontrollverlust über ihre Daten haben und kaum wissen, was sie selbst unternehmen können, um ihre Daten besser zu schützen.[171] Diese Unsicherheit gepaart mit dem Privacy Paradoxon kommt dann oftmals Internetunternehmen zugute.[172]

167 *Engels,* IW-Trends 2018, S. 3 (6).
168 *Engels/Grunewald,* IW-Kurzberichte 2017 (57), S. 1 (1).
169 *Barth/de Jong,* Telematics and Informatics 2017, S. 1038 (1038 ff.).
170 *Przybylski et al.,* Computer in Human Behavior 2013, S. 1841 (1842).
171 *Bitkom,* Datenschutz in der digitalen Welt, 2015, S. 3.
172 *Engels,* IW-Trends 2018, S. 3 (6).