November 2017 · Julia Manske und Dr. Tobias Knobloch

Datenpolitik jenseits von Datenschutz

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Gegenwärtige technologische Entwicklungen - vom Internet der Dinge über die Digitalisierung staatlicher Leistungen bis hin zur Künstlichen Intelligenz - befeuern die Datafizierung. Die Fähigkeit zur Erhebung, Verarbeitung, Verbreitung und Analyse großer Datenmengen ist der Kern von immer mehr Geschäftsmodellen und Lebensweisen. Kurz: Der Zugang zur Welt eröffnet sich in immer stärkerem Maße über digitale Daten. Dieses Phänomen ist nicht sehr neu, wenngleich sich das Ausmaß zuletzt stark beschleunigt hat. Viel älter, namentlich einige Dekaden, ist dagegen das vorherrschende Datensteuerungsregime unserer Zeit: der Datenschutz.

Mit dem Volkszählungsurteil von 1983 hat das Bundesverfassungsgericht interdependente Grundprinzipien aufgestellt, die anschließend zunächst im deutschen und später dann auch in den Datenschutzgesetzen anderer europäischer Länder umgesetzt wurden. Diese Prinzipien - vor allem Datensparsamkeit, Einwilligung und Zweckbindung - werden von der Datenschutzgrundverordnung (DSGVO) prinzipiell, wenn auch um einige Maßnahmen und Instrumente erweitert, fortgeschrieben. Die zentralen Prinzipien des Datenschutzes und damit auch der DSGVO wurden zu einer Zeit definiert, als es zwar bereits erste Ansätze der digitalen Datenverarbeitung gab, der Stand der Technik aber in keiner Weise mit dem heutigen Datenverkehr vergleichbar war. Trotz neuer regulativer Ansätze wie der DSGVO und aktuell der ePrivacy-Verordnung kann die derzeitige Datenpolitik Grundwerte im digitalen Raum nicht effektiv schützen und im Digitalbereich kaum funktionierende, kompetitive Märkte etablieren oder erhalten.

Zusammenfassend zeichnen sich fünf zentrale Problemfelder ab, die wir im vorliegenden Papier ausführlich erläutern:

1. die erschwerte Differenzierung von personenbezogenen und nicht-personenbezogenen Daten;
2. Verlust der Kontrolle seitens der Verbraucher im Zuge der Einwilligung;
3. Probleme mit anderen Datenschutzprinzipien und rechtliche Grauzonen;
4. eine unübersichtliche Akteurslandschaft und Datenhandel;
5. kollektive Effekte datenbasierter Entscheidungen.

Unsere zentrale These lautet: Der in der gegenwärtigen Datenpolitik weithin verfolgte dichotomische Ansatz - hier Personenbezug, dann Datenschutzregime; dort kein Personenbezug, dann Freifahrtschein - ist dafür verantwortlich, dass Grundrechte im digitalen Raum heute de facto nicht effektiv geschützt sind. Auch abgesehen davon wird dieser Datensteuerungsansatz den komplexen Anforderungen des Datenzeitalters nicht gerecht. Daten gleich welcher Herkunft sind in der Praxis immer Teil eines Datenökosystems, in dem sie verarbeitet und genutzt werden

Wenn wir keine Modelle finden, die es ermöglichen, Daten zu gesellschaftlich akzeptieren Zwecken zu nutzen, ohne dass Bürger ihrer Grundrechte beraubt werden, dann werden uns auch die damit verbundenen Chancen zur

Förderung des Gemeinwohls entgehen. Dem können wir nur durch die datenpolitische Berücksichtigung zweier wesentlicher Erkenntnisse vorbeugen: Erstens müssen avancierte technische Maßnahmen Teil einer jeden effektiven Datensteuerung sein - ob im öffentlichen oder im privatwirtschaftlichen Bereich. Zweitens müssen wir neue institutionelle, bereichsspezifische und gesellschaftliche Datenmanagement-Ansätze entwickeln, wobei die rechtlichen Rahmenbedingungen nur eine von mehreren dabei zu berücksichtigenden Perspektiven sind.

Inhalt

1 Das Dilemma des Datenzeitalters

1.1 Zentrale Charakteristika aus Gemeinwohlperspektive

Aufgrund des großen Potenzials von Datenanalysen für eine verbesserte Gesundheitsversorgung beschloss die britische Regierung 2013, Gesundheits- und Sozialdaten auf der zentralen Plattform care.gov zusammenzuführen, um Innovation in diesem Bereich zu fördern und das britische Gesundheitssystem effizienter zu machen. Doch der gewünschte Effekt blieb aus. Die Bürger reagierten mit Ablehnung. Sie fühlten sich nicht ausreichend informiert und ihrer Zustimmung beraubt. Sie fürchteten um den Verlust ihrer Privatsphäre, als sie ihre Daten in pseudonymisierter Form auf der Plattform wiederfanden. Zu wenig verstanden sie, wer nun was mit ihren sensiblen Gesundheitsdaten machen dürfte. Über Nacht erhielten nämlich nicht nur Forscher und Wissenschaftler, sondern auch kommerzielle Anbieter Zugriff auf ihre Daten. Datenschützer, aber auch Ärzte kritisierten das Projekt. Das Vertrauen der Bürger in die sinnvolle Nutzung von Gesundheitsdaten hatte die Regierung auf diese Weise verloren, noch bevor das Projekt richtig starten konnte. Das Projekt ist inzwischen eingestellt.

Die Plattform hätte für Patienten und die Verwaltung gleichermaßen große Erfolge bringen können. Doch das Beispiel NHS verdeutlicht das Dilemma, vor dem wir aktuell stehen: Sind Daten erst einmal erhoben und geteilt, ist es mitunter schwierig, zwischen ‘guten’ und ‘schlechten’ Verwendungsweisen zu unterscheiden. Offene Regierungsdaten etwa werden mit der Veröffentlichung Teil eines größeren Datenökosystems und werden inzwischen auf kaum überschaubare Weise von zahlreichen Akteuren weiterverarbeitet und kombiniert. Die Verbreitung des Internet der Dinge und entsprechender Anwendungen in unseren Häusern, an unseren Körpern und in unseren Städten wird die Komplexität des Datenökosystems zusätzlich erhöhen.

Fortschritte im Bereich der Künstlichen Intelligenz, etwa durch selbstlernende Algorithmen und Supercomputer, die voranschreitende Vernetzung aller Geräte und damit im Zusammenhang stehende Trends wie Smart Home, Smart City und Smart Country - sie alle befeuern die Datafizierung. Neue Technologien und Geschäftsmodelle beschleunigen nicht nur die weitere Generierung von Daten, sondern sie sind auch zunehmend von deren Verfügbarkeit abhängig.[1] Aus dieser Entwicklung ergeben sich zahlreiche datenpolitische Fragen: Wer soll bzw. darf beispielsweise Zugang zu Sensorda-

1 Bisweilen erzeugen sogenannte Trainingsdaten für Algorithmen einen negativen Zirkel, indem menschliche Vorurteile auf diese Weise in automatisierte Entscheidungssysteme eingehen; vgl. z.B. Jeffries, A. (2017). Machine learning is racist because the Internet is racist. Deep learning algorithms are often trained on data from the web, and their biases are getting hard to ignore. *The Outline* (online) https://theoutline.com/post/1439/machine-learning-is-racist-because-the-internet-is-racist

ten haben, die von heutigen Fahrzeuge und smarten Infrastrukturen erzeugt werden? Wie gehen wir mit der Machtasymmetrie um, die aus den gewaltigen Datenerhebungs- und -auswertungskapazitäten großer Technologiekonzerne erwachsen ist? Wie können die Menschen vom Gefühl (und von der Realität) der Ohnmacht befreit werden, was die Kontrolle ihrer digitalen Daten betrifft?

Der Schutz der Privatsphäre ist hierbei ein wichtiges Thema, das trotz der im kommenden Jahr in Kraft tretenden Datenschutzgrundverordnung (DSGVO) eine zentrale Herausforderung bleibt. Denn im Kern beruht der klassische Datenschutz auf Mechanismen der Zuteilung und des Schutzes von Rechten, die im Datenzeitalter zunehmend ins Leere laufen: Die Kenntnisnahme des Nutzers, seine Zustimmung zur Verarbeitung seiner Daten und die Einschränkung des Verwendungsbereichs für den Datenverarbeiter fordern im Grunde das Gegenteil derjenigen Praktiken, die wir mit dem Begriff „Big Data“ ansprechen. Im Grunde kann bei der Datenerhebung heute niemand vorab klar eingrenzen, was sich aus diesen Daten einmal wird ableiten und was sich mit ihnen wird machen lassen. Es ist gewissermaßen die Pointe des Datenzeitalters, dass dies zunächst offen bleibt, so dass wir immer wieder von ungeahnten Möglichkeiten überrascht - oder eben erschreckt werden.

Überraschung und Schrecken begleiten uns auch bei der Nutzung digitaler Dienste. Einerseits schätzen wir die sich täglich erweiternden Möglichkeiten, die sie uns bieten; andererseits erschrecken uns die Dinge, die Anbieter mit den dabei gesammelten Nutzerdaten treiben. Wenn der Nutzer eines digitalen Dienstes den Nutzungsbedingungen zustimmt und damit in die Verarbeitung seiner Daten einwilligt[2], dann ist er gewöhnlich im Unwissen darüber, wie viel das von ihm eingetauschte Gut - seine Daten - tatsächlich wert ist.[3] Dass dieser Wert existiert, macht beispielsweise die Datenschutzerklärung des Zimmervermittlungsdienstes Airbnb sehr deutlich, indem sie personenbezogene Daten als Vermögenswerte definiert und sich vom Nutzer eine Generalzustimmung zum Handel mit diesen - seinen - Daten geben lässt (was den Wenigsten bewusst sein dürfte): “Falls Airbnb eine Fusion, eine Übernahme, eine Umstrukturierung, einen Verkauf von Vermögenswerten, einen Konkurs oder ein Insolvenzverfahren durchführt oder daran beteiligt

2 Jeanette Hoffmann und Benjamin Bergmann nennen die Einwilligung, die gemäß Artikel 6 DSGVO (neben fünf weiteren Gründen) weiterhin eine legitime Datenverarbeitung begründen kann, daher auch ein “Datenschutzphantom” und bezeichnen sie als “unverzichtbare Rahmenbedingung für den modernen Datenkapitalismus, der unsere persönlichen Daten in eine international akzeptierte Währung verwandelt hat”. -- Hoffmann, J. & Bergmann, B. (2017). Die informierte Einwilligung: Ein Datenschutzphantom. *Netzpolitik.org* (online) https://netzpolitik.org/2017/die-informierte-einwilligung-ein-datenschutzphantom/

3 Vgl. Jentzsch, N. (2016). State-of-the-Art of the Economics of Privacy and Cybersecurity. *IPACSO - Innovation Framework for ICT Security Deliverable; 4.1* (online) https://www.econstor.eu/handle/10419/126223

ist, können wir unsere Vermögenswerte einschließlich Ihrer Daten verkaufen, übertragen oder weitergeben."[4]

Oft erschließt sich der Wert unserer Daten erst zu einem späteren Zeitpunkt und möglicherweise erst im Zusammenhang mit anderen Daten. Das liegt daran, dass Innovationen aus Daten wie alle Entdeckungsverfahren offen sind. Jede wie auch immer motivierte Vorfestlegung auf bestimmte Zwecke hemmt der Tendenz nach die Innovationsleistung und damit auch die Aussicht auf Profit. Das ist bei großen Plattformbetreibern wie Airbnb nicht anders als bei kleineren Anbietern datengetriebener Dienste. Die Politik muss demnach grundsätzlich dazu bereit sein, Innovationstätigkeiten und Gewinnaussichten zu beschränken, sollte sie zu dem Schluss kommen, dass die Praktiken, die datengetriebenen Geschäftsmodellen zugrunde liegen, demokratische Grundwerte aushöhlen und Persönlichkeitsrechte verletzen. Genau das aber scheint bei den derzeitigen Datenhandhabungsarten tatsächlich regelmäßig der Fall zu sein, und es besteht unserer Ansicht nach wenig Aussicht darauf, dass sich das mit dem Inkrafttreten der DSGVO ohne weiteres grundlegend ändern wird.

Gleichzeitig haben wir keine Zeit, die Hände in den Schoß zu legen und etwa auf mustergültige Gerichtsentscheidungen zur Auslegung der DSGVO in den Jahren 2018 ff. zu warten. Denn unsere Grundrechte stehen im Datenzeitalter in vielerlei Hinsicht unter Beschuss. Dabei geht es nicht allein um Privatsphäre. Es geht auch um soziale und wirtschaftliche Gerechtigkeit. Digitale Profile[5] mit hunderten Datenpunkten mögen bessere Dienstleistungen ermöglichen, sie können aber auch Entscheidungen über den Zugang zu wesentlichen Ressourcen wie Gesundheitsleistungen, Bildungsangeboten oder finanziellen Mitteln beeinflussen. Momentan fehlen uns Instrumente, um positive Effekte mit potenziellen Schäden adäquat auszutarieren. Trotz neuer regulativer Ansätze wie der DSGVO sehen sich politische Entscheidungsträger mit der Herausforderung konfrontiert, dass der bestehende rechtliche Rahmen für den Umgang mit (immer neuen und immer mehr) Daten nicht ausreicht, um Grundwerte zu schützen und funktionierende Märkte zu etablieren oder zu erhalten. Diesen sich ständig erneuernden Bedarf sehen wir aktuell in einer Vielzahl politischer Auseinandersetzungen, etwa an der Debatte über die Verwendung der Daten vernetzter (sowie autonomer bzw. teilautonomer) Fahrzeuge, aber natürlich auch an kontroversen Themen wie dem Nachverfolgen von Verbraucherwegen online und offline (Tracking) oder

4 Airbnb (2017). Airbnb Datenschutzerklärung, 3.13 Unternehmenszusammenschlüsse (online) https://www.airbnb.de/terms/privacy_policy

5 Eine gute Beschreibung der Einwanderung des Begriffs "Profil" aus der Welt der Nachrichtendienste und Kriminalistik in die Digitalkultur bietet Bernard, A. (2017). *Komplizen des Erkennungsdienstes: Das Selbst in der digitalen Kultur.* Frankfurt/M.: S. Fischer.

dem Profiling, dessen mögliche Folgen von Kreditzugang bis hin zu Wahlbeeinflussung[6] reichen.

Daten- und Verbraucherschützer auf der einen und Unternehmen der Digitalwirtschaft auf der anderen Seite verharren oft gleichermaßen in alten Grabenkämpfen, anstatt nach alternativen Lösungswegen zu suchen. Dabei zeigen Beispiele wie das oben aufgeführte des NHS in Großbritannien: Wenn wir keine Modelle finden, die es ermöglichen, Daten zu gesellschaftlich akzeptierten Zwecken zu nutzen, ohne dass Bürger ihrer Grundrechte beraubt werden, dann werden uns auch die damit verbundenen Chancen zur Förderung des Gemeinwohls entgehen. Gleichzeitig zeichnen sich sehr wohl bereits einzelne, meist noch unkoordinierte Steuerungsansätze ab, die über den klassischen Datenschutz hinausgehen.[7] Solche Ansätze erweitern unsere Perspektive um neue ethische, legale und technische Rahmenbedingungen für den produktiven gesellschaftlichen Umgang mit Daten.[8]

1.2 Unzureichender Schutz und ungenügend genutzte Chancen

Es vergeht buchstäblich kein Tag mehr, an dem nicht gleichzeitig Fälle von Datendiebstahl aufgrund von Datensicherheitslücken, Datenkompromittierung aufgrund arglosen Datenmanagements und zweifelhafte Praktiken unter formaler Beachtung von Datenschutzvorgaben bekannt würden. Gleichzeitig können wir uns über immer mehr Beispiele freuen, die sowohl ökonomischen Wert generieren als auch gesellschaftlichen Nutzen erzielen. Mapbox beispielsweise, ein Unternehmen, das eigenen Angaben zufolge weltweit knapp 1 Million Entwickler mit Geo- und anderen Kartografierungsdaten versorgt und als Konkurrent von namhaften Kartendiensten wie Google Maps und HERE fungiert, ist 2010 als ein Dienst für Nichtregierungsorganisationen und Regierungsinstitutionen gegründet wurden, um bei Wahlen und Epidemien essenzielle Geo-Informationen bereitzustellen. Kürzlich meldete das Wall Street Journal, dass der Investmentfonds SoftBank 164 Millionen US-Dollar in Mapbox investiert hat, weil die Technologie als Schlüssel bei der Realisierung des automatisierten Fahrens gilt.[9] Eine

6 Vgl. hierzu das SNV-Projekt “Medien im digitalen Wandel: Fake News”: https://www.stiftung-nv.de/de/projekt/medien-im-digitalen-wandel-fake-news

7 Vgl. dazu Kapitel 3 unten.

8 In unserem gerade gestarteten Datenprojekt werden wir im intersektoralen Austausch zwei Jahre lang intensiv daran arbeiten, über Datenschutzerwägungen hinausgehende, effektive Steuerungsmechanismen für den produktiven und sicheren Umgang mit Daten zu identifizieren und zu koordinieren. Ein erstes Positionspapier findet sich unter www.stiftung-nv.de/datagov .

9 Vgl. Higgins, T. (2017). SoftBank Leads $164 Million Bet on Digital-Mapping Startup Mapbox. Technology is key to self-driving vehicles. *The Wall Street Journal* (online) https://www.wsj.com/articles/softbank-leads-164-million-bet-on-digital-mapping-startup-mapbox-1507640404

ähnliche Erfolgsgeschichte mit ähnlicher Entstehungsgeschichte ist der offene Kartendienst OpenStreetMap.[10]

Der momentane politische Umgang mit dem skizzierten Datendilemma beruht auf der Grundunterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten. Für den Bereich der personenbezogenen Daten gilt ein starkes Datenschutzregime, das die Nutzung von Daten weitgehend einschränkt und unter anspruchsvolle Vorbehalte stellt. Andererseits werden zunehmende Anstrengungen unternommen, für Bereiche, in denen man keine so weitreichenden Gefahren erkennt, einen möglichst freien Datenfluss zu gewährleisten.[11] Das fängt bei Public Sector Information und Open Government Data an und endet gegenwärtig bei den Bemühungen um die Realisierung eines automatisierten Verkehrs, wozu Fahrzeuge eine Fülle an Positions- und Zustandsdaten im Millisekundentakt austauschen müssen. Gerade im Hinblick auf das riesige Wirtschaftspotenzial, das dem IoT-Anwendungsbereich zugeschrieben wird, ist die Europäische Union bemüht, unter der Überschrift “Digital Single Market” einen möglichst möglichst of-

10 https://www.openstreetmap.org/#map=6/51.330/10.453

Weitere Beispiele für den gesellschaftlichen Nutzen von Anwendungen, die ganz oder teilweise auf offenen Daten beruhen, haben wir unter http://datenwirken.de/ versammelt.

11 Ein Kristallisationspunkt dieser Bemühungen ist der Begriff “Datensouveränität”, der den politischen Datendiskurs in Deutschland seit 2016 beherrscht. Wie die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in einem Grundsatzpapier zur neuen Legislaturperiode kürzlich richtig feststellte, trifft dieser schillernde Begriff “datenschutzrechtliche Anforderungen ebenso wenig wie das mit dem neuen Begriff angestrebte Ziel, Daten zu einer rein wirtschaftlichen Größe zu machen und damit Einschränkungen des Datenschutzes zu verschleiern.” - DSK (2017). Grundsatzpositionen und Forderungen für die neue Legislaturperiode, S.1 (online) https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/datenschutz-und-informationsfreiheit-als-elemente-einer-stabilen-demokratie

fenen Fluss von Geräte- und Maschinendaten zu gewährleisten.[12] Ein Problem hier ist, dass bisherige rechtliche Regelungen für den Umgang mit Daten, wie Datenschutz oder Urheberrecht, die Rechte an solchen Daten und die Möglichkeiten ihrer Verarbeitung gar nicht oder nur unzureichend regeln. Das stellt zunächst keine Gefahr für die Privatsphäre, sondern eher ein wirtschaftspolitisches Problem dar. Daneben gibt es Graubereiche, in denen sich sehr wohl auch Datenschutzfragen stellen, Chancen und Gefahren aber eventuell durch den Einsatz avancierter Datenschutztechniken austariert werden können. Ein Beispiel ist die Bereitstellung von Echtzeit-Verkehrsdaten als Open Data: Hier ergeben sich durch die Art der Daten und den Kontext fast natürlicherweise Gefahren für die Privatsphäre - etwa von Lokführern und Busfahrern. Bestimmte Dienste, die unser Leben vereinfachen und Ressourcen schonen, lassen sich aber nur erbringen, wenn solche Echtzeitdaten zur Verfügung stehen. Um beides in Einklang zu bringen, haben wir in unserem Leitfaden für Open Data Privacy im März dieses Jahres zahlreiche mögliche Maßnahmen vorgeschlagen.[13] Momentan ist jedoch Überzeugung, dass Maßnahmen zum Schutz der Privatsphäre richtig verstanden der Ermöglichung dienen und nicht primär Verhinderungscharakter haben, zu selten; zu selten sind folgerichtig auch entsprechende Beispiele eines fruchtbaren Miteinanders von Datenschützern und intensiven Datennutzern.

Unsere zentrale These lautet: Der beschriebene und in der gegenwärtigen Datenpolitik weithin verfolgte dichotomische Ansatz - hier Personenbezug, dann Datenschutzregime; dort kein Personenbezug, dann Freifahrtschein - ist dafür verantwortlich, dass Grundrechte im digitalen Raum heute de facto nicht effektiv geschützt sind. Auch abgesehen davon wird dieser Datensteuerungsansatz den komplexen Anforderungen des Datenzeitalters nicht gerecht. Daten gleich welcher Herkunft sind in der Praxis immer Teil eines Datenökosystems, in dem sie verarbeitet und genutzt werden. In der Praxis spielt es eine nachrangige Rolle, ob Datensätze als Open Data aus dem

---

12 Vgl. European Commission (2017). State of the Union 2017: A framework for the free flow of non-personal data in the EU. Brussels, 19 September 2017 (online) http://europa.eu/rapid/press-release_IP-17-3190_en.htm

In anderen Bereichen vertritt die EU wieder eine ganz andere, durchaus inkonsistente Linie: So könnte die EU-Kommission noch in diesem Jahr durch die Reform des Urheberrechts zum Totengräber der europäischen Digitalwirtschaft werden. Dann nämlich, wenn - wie derzeit geplant - frei zugängliche Texte und anders strukturierte, bislang ebenfalls frei verfügbare Informationen nicht mehr, wie bisher, ohne explizite Einwilligung der Urheber maschinell verarbeitet werden dürfen (sog. text and data mining); vgl. Schulzki-Haddouti, C. (2017). EU-Copyright-Reform: Einschränkung von Text- und Data-Mining droht *heise* am 18.19.2017 (online) https://www.heise.de/ho/meldung/EU-Copyright-Reform-Einschraenkung-von-Text-und-Data-Mining-droht-3864658.html

13 Vgl. Manske, J. & Knobloch, T. (2017). Leitfaden für Datenschutz bei Open Data. *SNV Policy Brief* (online) https://www.stiftung-nv.de/sites/default/files/policy_brief_leitfaden_open_data_datenschutz.pdf

Staatsfundus stammen, ob sie als öffentlich zugängliche Informationen aus dem Netz gesammelt und strukturiert wurden, oder ob Dienstanwender sie 'freiwillig' preisgegeben haben. All diese Datenarten werden genutzt und kombiniert. Deshalb gibt es keinen leicht identifizierbaren Bereich persönlicher Informationen, durch deren besonders strengen Schutz man das Individuum und die Gesellschaft vor sämtlichen negativen Folgen der Datenverarbeitung schützen könnte. Zusätzlich, nicht alternativ zum Datenschutz brauchen wir auf mehreren Ebenen andere Steuerungsmechanismen für die Datennutzung: auf der Ebene der Datenarten (z.B. Personendaten oder Sensordaten), für unterschiedliche Datenbereiche (z.B. Mobilität oder Gesundheit), in verschiedenen Nutzungskontexten (z.B. öffentlicher Sektor oder Wirtschaft) und schließlich für die ganze Gesellschaft, welches letztere auf die selten gestellte Frage hinausläuft, was für eine von Daten befeuerte Gesellschaft wir eigentlich sein wollen.

Die Qualität wirksamer Datensteuerungsansätze auf all diesen Ebenen lässt sich allein danach beurteilen, inwieweit es gelingt, gesellschaftlich wünschenswerte Ziele mittels Datenauswertungen zu erreichen und Gefahren, die (potenziell) von Datenanalysen für die Gesellschaft ausgehen, abzuwenden. Das Mantra-artige Bekenntnis zu den Prinzipien des traditionellen Datenschutzes bei gleichzeitiger Artikulation des Willens, die positiven Möglichkeiten des Sammelns und Auswertens von Daten abseits der formalen Restriktionen des Datenschutzes nutzen zu wollen, bringt uns hier nicht weiter. Denn Daten können auch dann massiven persönlichen und gesellschaftlichen Schaden verursachen, wenn den derzeitigen datenschutzrechtlichen Vorgaben formal Folge geleistet wird. Die Kontrolle darüber, wer wann und zu welchem Zweck Daten aus unterschiedlichen Quellen zusammenführt, um individuelles Verhalten auszumessen, ist dabei nur eines der Probleme, mit dem wir es zu tun haben. Das zeigen wir ausführlich im zweiten Kapitel.

Der Datenschutz und die DSGVO stellen einen wichtigen Ordnungsrahmen dar, der grundsätzlich - gerade im Hinblick auf die Stärkung von Verbraucherrechten und den Schutz von Grundrechten - zu begrüßen ist. Auch deshalb haben wir gute Gründe, den Herausforderungen des Datenzeitalters hoffnungsfroh zu begegnen und die Chancen, die es bietet, beherzt zu ergreifen. Gerade in den am wenigsten entwickelten Ländern der Erde ist das Potenzial für eine wesentliche Verbesserung der Lebensbedingungen durch Verfahren der Erhebung, Bereitstellung und Analyse von Daten groß, wie wir an anderer Stelle gezeigt haben.[14] Bevor wir uns kritisch mit den Mechanismen des Datenschutzes auseinandersetzen, möchten wir daher grundsätzlich betonen, wie sehr wir die deutsche und europäische Rolle in der Welt schätzen, wenn es darum geht, Chancen und Risiken des Datenzeitalters auszutarieren. Da sich die oben skizzierte Entwicklung zur umfassenden Digitalisierung und Datafizierung sämtlicher Lebensbereiche rasant fortsetzen wird, begrüßen wir den deutschen und europäischen Ansatz eines starken Schutzes von

14 Knobloch, T. & Manske, J. (2017). Responsible Use of Data. *Cooperation & Development* am 11.1.2017 (online) https://www.dandc.eu/en/article/opportunities-and-risks-user-generated-and-automatically-compiled-data

Persönlichkeits-, Bürger- und Verbraucherrechten ausdrücklich. Unsere Kritik ist als konstruktives Weiterdenken dieser Prinzipien dort zu verstehen, wo bestehende Regelungen offensichtlich an Grenzen stoßen.

2 Ziele und Schwächen des Datenschutzes

Aktuell ist das zentrale Steuerungsinstrument für den Umgang mit Daten der Datenschutz. Erst in jüngerer und jüngster Zeit sind auf unterschiedlichen Regulierungsebenen weitere, rechtliche und operative Maßnahmen anleitende Instrumente wie die Public Sector Information Directive (PSI) der EU[15] oder das sogenannte Open-Data-Gesetz in Deutschland[16] hinzugetreten. Auch Datenbankregelungen, die in mancherlei Hinsicht problematisch sind, weil sie tendenziell freien Informationsaustausch behindern und Innovation bremsen, indem sie die Interessen etablierter Unternehmen vorzugsweise behandeln, sind hier zu nennen. Der Datenschutz nimmt jedoch eine bei weitem führende Rolle ein, wenn es darum geht, was mit Daten erlaubt und gesellschaftlich akzeptiert ist.

Bereits zu Beginn des letzten Jahrhunderts entwickelte sich mit den Veränderungen des öffentlichen Raumes durch die Verbreitung von Printmedien und die Verstetigung von Urbanisierungsprozessen ein modernes Verständnis von Privatheit, das einen Rückzugsraum gegenüber Dritten und ein Abwehrrecht gegenüber dem Staat begründen sollte. Mit Aufkommen der elektronischen Datenverarbeitung in den 1960er Jahren begann die Suche nach einem Steuerungsmodell, das den Schutz der Privatheit auch unter diesen veränderten Vorzeichen gewährleisten können sollte. Während das amerikanische Recht auf Privatsphäre zunächst als ausschließlich negatives Recht ausgelegt wurde (als “the right to be left alone”[17]), verstand man in Deutschland und Europa Datenschutz von Beginn an als positives Recht, das neben dem Recht auf den Schutz der Privatsphäre auch das Recht auf die Kontrolle

15 Online unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02003L0098-20130717

16 Eigentlich “Erstes Gesetz zur Änderung des E-Government-Gesetzes”, in Kraft getreten am 4.7.2017, §12a EGovG - Einzelnorm, online unter: https://www.gesetze-im-internet.de/egovg/__12a.html

17 Nach dem maßgebenden Artikel von Warren und Brandeis aus dem Jahr 1890: Warren, S.D. & Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review* 4 (5), S.193-220.

und das Wissen über die Verwendung der Daten ins Zentrum stellte.[18] Genau diese Idee spiegelt sich im deutschen Konzept der Informationellen Selbstbestimmung wider.

Beim Datenschutz steht einerseits der Schutz der Freiheit der Bürger vor Überwachung und andererseits das Recht auf die persönliche Kontrolle von privaten Informationen im Zentrum. Datenschutzgesetze sind insofern abgeleitet vom Selbstbestimmungsrecht und dem Schutz der Menschenwürde, die auch das Fundament der Europäischen Grundrechte-Charta bilden.

2.1 Kernelemente und Zweck des Datenschutzes

Datenschutz bezieht sich auf die Erhebung, die Verarbeitung und die Nutzung personenbezogener Daten. Unter personenbezogene Daten fallen alle Daten, die sich eindeutig einer bestimmten Person zuordnen lassen, durch die eine Zuordnung erfolgen kann, oder Daten, durch die sich ein Personenbezug leicht herstellen lässt (wie etwa Kfz-Kennzeichen)[19]. Mit dem Volkszählungsurteil von 1983 hat das Bundesverfassungsgericht verschiedene interdependente Grundprinzipien aufgestellt, die anschließend im zunächst im deutschen, und später dann auch in den Datenschutzgesetzen anderer europäischer Länder umgesetzt wurden.[20]

Verbot mit Erlaubnisvorbehalt

Im Datenschutz gilt das Prinzip des „Verbots mit Erlaubnisvorbehalt“. Die Verarbeitung personenbezogener Daten ist grundsätzlich untersagt, es sei denn, es liegt ein Erlaubnistatbestand vor, der eine Ausnahme vom Verbot rechtfertigt. Eine solche Ausnahme kann in zwei Fällen vorliegen: Erstens

18 Dies spiegelt sich schon im unterschiedlichen Freiheitsverständnis dies- und jenseits des Atlantiks wider. Während das angelsächsische Freiheitsverständnis eher ein negatives ist (Freiheit von Eingriff und Zwang) fußt das kontinentaleuropäische tendenziell eher auf einem positiven Freiheitsbegriff (Freiheit zu etwas, Ermöglichung). Eine grundlegende Untersuchung dieses Themas in deutscher Sprache liefert Steltemeier, R. (2015). *Liberalismus. Ideengeschichtliches Erbe und politische Realität einer Denkrichtung.* Baden-Baden: Nomos.

19 Nach Beschluss des Europäischen Gerichtshof (EuGH) fallen auch dynamische IP-Adressen unter diese Kategorie. Nach dem Urteil reicht es aus, wenn ein Dritter mit geringem Aufwand Personenbezug herstellen kann.

20 Eine gute Darstellung dieser Grundprinzipien findet sich z.B. in Boehmanwaltskanzlei (2015). Grundprinzipien des Datenschutzes (online) https://boehmanwaltskanzlei.de/kompetenzen/medienrecht/datenschutzrecht/datenschutz/grundprinzipien/212-grundprinzipien-des-datenschutzes

wenn ein Gesetz die Verarbeitung erlaubt, oder zweitens wenn der Betroffene in die Datenverarbeitung einwilligt.

Aus dieser Regelung heraus hat sich in den letzten Jahrzehnten das Prinzip der Informierten Einwilligung als ein dominierendes Instrument des Datenschutzes durchgesetzt. Der Verbraucher willigt bei Nutzung eines Dienstes ein, dass seine Daten zu einem bestimmten Zweck genutzt werden. In der Regel erfolgt dies über die Zustimmung zu den Allgemeinen Geschäftsbedingungen (AGB), die jeweils auch Datenschutzbestimmungen enthalten. Dem Verbraucher soll damit Kontrolle über die Nutzung seiner Daten gegeben werden. Aus rechtlicher Sicht gestattet der Verbraucher dem Verarbeitenden also den Eingriff in seine Grundrechte.

Direkterhebung

Nach dem Prinzip der Direkterhebung dürfen Daten ferner nur beim Betroffenen selbst erhoben werden und der Betroffene muss Kenntnis über die Erhebung der Daten haben, zumindest sofern keine Rechtsvorschrift vorliegt, die eine Abweichung gestattet.

Zweckbindung

Ein weiteres Prinzip des Datenschutzes ist die Zweckbindung. Diese bildet am Ende Voraussetzung dafür, dass eine Ausnahme gestattet werden kann. Der Zweck der Verarbeitung muss demnach bereits vor der Verarbeitung klar definiert sein. Wenn also eine Einwilligung durch den Verbraucher erteilt wird, so gilt diese nur für den in der Einwilligung ausbuchstabierten Zweck. Ändert sich der Verarbeitungsgrund so muss der Datenverarbeitenden die Erlaubnis einer Ausnahme ersuchen. Hinter dem Prinzip der Zweckbindung steht die bereits im Volkszählungsurteil ausgesprochene Forderung, dass Daten nicht auf Vorrat gespeichert werden sollen.

Erforderlichkeit

Daten dürfen nur gespeichert werden, wenn die Speicherung der Daten für die Erreichung des Zwecks (siehe Zweckbindung) erforderlich ist. Sofern der Zweck der Daten erfüllt wurde, müssen die Daten insofern werden, sofern keine Aufbewahrungspflichten bestehen. Erforderlichkeit ist also vor allem ein zeitlich-prozedurales Datenschutzprinzip, durch das beispielsweise die - unbeabsichtigte oder intendierte - Zusammenführung von Daten zu abweichenden Zwecken verhindert werden soll.

Datensparsamkeit und Datenminimierung

Die Prinzipien der Zweckbindung und der Erforderlichkeit dienen überdies der Sicherstellung des Prinzips der Datensparsamkeit und Datenminimie-

rung. Generell gilt also, dass so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden sollen. Damit im Zusammenhang steht beispielsweise auch das technische Design von Datenverarbeitungsverfahren, das Datenschutz begünstigen kann, etwa durch entsprechende Voreinstellung oder die Präferenz, Daten von Beginn an in anonymisierter oder mindestens in pseudonymisierter Form zu erheben.

Transparenz

Der Betroffene soll zu jeder Zeit wissen, wer welche Daten über ihn speichert. Diese Informations- und Benachrichtigungspflicht gilt sowohl für Fälle, in denen der Betroffene der Datenverarbeitung zugestimmt hat, als auch dann, wenn eine gesetzliche Zulässigkeit besteht.

Kontrolle und Sanktion

Das deutsche Datenschutz-Regime fußt außerdem auf den Prinzipien der Datenschutzkontrolle und der Sanktion. Die Kontrolle wird über ein Zwei-Säulen-Modell realisiert: Auf staatlicher Seite überprüfen die Datenschutzaufsichtsbehörden des Bundes und der Länder die Einhaltung der Regularien durch die staatlichen Stellen. Auf betrieblicher Seite sind - abhängig von Art der Daten, Art der Datenverarbeitung und Mitarbeiterzahl - betriebliche Beauftragte für die Datenschutz-Compliance zuständig. Unternehmen, Vereine oder Organisationen, die mit personenbezogenen Daten agieren, müssen also entsprechende technisch-organisatorische Maßnahmen zur Gewährleistung des operativen Datenschutzes treffen. Durch die Transparenz-Rechte können auch die Betroffenen selber zur Kontrolle des Datenschutzes beitragen. Die Datenschutz-Aufsichtsbehörden sind zudem berechtigt, die Einhaltung der datenschutzrechtlichen Bestimmungen in den Unternehmen zu prüfen und Verstöße zu ahnden. Je nach Schwere des Verstoßes kann eine Beanstandung ausgesprochen, ein Bußgeld verhängt oder - in schweren Fällen - ein Strafverfahren eingeleitet werden.

Von Deutschland nach Europa: die Datenschutzgrundverordnung (DSGVO)

Die Europäische Datenschutzrichtlinie von 1995, die wesentlich vom deutschen Konzept des Rechts auf Informationelle Selbstbestimmung beeinflusst wurde[21], baut auf den zuvor skizzierten sechs Prinzipien auf. Während die Richtlinie zwar als erstes internationales Gesetzesvorhaben für den Datenschutz einen wichtigen Meilenstein darstellt, lag die Umsetzung bei den Mitgliedstaaten und sorgte damit für ein ungleiches Datenschutzniveau. Dies ändert sich mit der 2016 verabschiedeten Datenschutzgrundverord-

21 Und übrigens auch für viele Datenschutzregelungen in anderen Teilen der Welt. Vgl. etwa die rechtliche Grundlagen des “Habeas Data” in vielen lateinamerikanischen Ländern und den Philippinen.

nung (DSGVO). Im Mai 2018 wird sie in allen europäischen Mitgliedsstaaten in Kraft treten. Aktuell finden in den Staaten die gesetzlichen Anpassungen sowie die Ausgestaltung der immerhin 70 Öffnungsklauseln des Regelwerkes statt.[22] Die DSGVO wird durch die ePrivacy-Richtlinie ergänzt, die zur Zeit überarbeitet wird und ebenfalls im Mai 2018 in Kraft treten soll.

Die DSGVO setzt sich einerseits zum Ziel, den technischen Entwicklungen der letzten Jahre gerecht zu werden und Verbraucher weiterhin bzw. besser zu schützen. Andererseits soll der europäische Binnenmarkt durch die Harmonisierung gestärkt werden: Ziel ist die Verringerung des Verwaltungsaufwands für in Europa agierende Unternehmen durch einheitliche Standards sowie die Auflösung bisherige datenschutzrechtlicher „Rückzugsräume" in Ländern mit niedrigerem Datenschutzniveau.[23] Eine wesentliche Errungenschaft der DSGVO ist insofern, dass zukünftig in allen EU-Mitgliedstaaten ähnliche Datenschutzstandards gelten. In der Folge wird in den meisten Ländern das Datenschutzniveau tendenziell angehoben und viele der Prinzipien, die in Deutschland bereits durch das Bundesdatenschutzgesetz gelten, werden damit auch in anderen EU-Ländern verpflichtend. Des Weiteren wird der Geltungsbereich ausgeweitet und die Regularie gilt nicht nur für in der EU ansässige Unternehmen, sondern auch für Unternehmen mit Sitz außerhalb der Union, die personenbezogene Daten von in der EU lebenden Personen erheben und verarbeiten.

2.2 Fortschreibung der Datenschutzprinzipien durch die DSGVO

Inhaltlich schreibt die DSGVO die zuvor beschriebenen sechs Prinzipien des Datenschutzes fort, wobei sie einige der Prinzipien durch gezielte Maßnahmen verstärkt. Darüber hinaus führt die DSGVO einige wesentliche Neuerungen ein. Auf viele dieser Aspekte werden wir im weiteren Verlauf intensiv eingehen und wollen daher an dieser Stelle nur einige Punkte aufführen.

Zunächst versucht die DSGVO eine präzisere Definition von personenbezogenen Daten vorzunehmen. Daraus resultiert, dass fortan auch pseudonymisierte Daten unter den Anwendungsbereich des Datenschutzes fallen. Ferner hält die DSGVO nicht nur am Prinzip der Einwilligung fest, sondern räumt ihr sogar eine Vorrangstellung gegenüber gesetzlichen Lösungen (DSGVO, Art.6, 1a) ein. Allerdings sind die Anforderungen an eine rechtsgültige Einwilligung im Vergleich zur Vorgänger-Direktive wesentlich strikter. Neben dem ursprüngliche Wortlaut "freely given, specific and informed" muss eine rechtsgültige Einwilligung explizit und affirmativ erfolgen. Für verschiedene Zwecke und Verarbeitungsvorgänge müssen separate Einwilligungen abge-

22 Vgl. dazu den Band Roßnagel, A. (Hrsg.) (2016). *Europäische Datenschutz-Grundverordnung – Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts.* Baden-Baden: Nomos.

23 Schürmann Wolschendorf Dreyer Rechtsanwälte (2016). EU-Datenschutzgrundverordnung (DSGVO) (online) https://www.swd-rechtsanwaelte.de/blog/eu-datenschutzgrundverordnung-dsgvo/

geben werden. Damit wird die Einholung der Einwilligung im Vergleich zur bisherigen Praxis in Europa deutlich anspruchsvoller.[24]

Mit Blick auf die Kontrollmechanismen sieht die DSGVO fortan für alle Mitgliedsländer die Einführung des in Deutschland etablierten Zwei-Säulen-Modells vor, das den Schutz durch betrieblichen Datenschutzbeauftragte und die Kontrolle durch staatliche Stellen beabsichtigt. Damit im Zusammenhang steht eine wesentliche Neuerung: Mit der DSGVO gilt zukünftig in Europa das One-Shop-Prinzip. EU-Bürger können sich demnach immer direkt an ihren nationalen Datenschutzbeauftragten wenden, unabhängig davon, in welchem Land der in Frage stehende Datenerhebende oder -verarbeitende seinen Sitz hat. Für Unternehmen verschärft sich ferner die Meldepflicht, etwa bei Datenschutzverletzungen, gegenüber dem zuständigen staatlichen Datenschutzbeauftragten.

Eine der wohl gravierendsten Änderungen der DSGVO im Vergleich zu bisherigen Datenschutzgesetzen sind die deutlich erhöhten Strafen, die im Zweifelsfall bei bis zu 4 Prozent des Jahresumsatzes eines Unternehmen liegen können.

Als weitere Schutzmaßnahmen verpflichtet die DSGVO einerseits zu sogenannten “Data Protection Impact Assessments” für den Umgang mit sensiblen Daten, andererseits soll unter dem Stichwort Data Protection by Design der Datenschutz bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden.

Generell wurden weiterhin die Auskunftspflichten verstärkt. Unternehmen müssen in größerem Umfang als bisher Auskunft über die durch sie gespeicherten Daten geben. Dies umfasst auch die Auskunftspflichten bezüglich des Einsatzes von automatisierten Entscheidungen und Profiling. Neben verschärfter Transparenz soll die Kontrolle der Verbraucher durch einzelne Prinzipien erhöht werden. Dazu zählen das sogenannte Recht auf Vergessenwerden und das Recht auf Datenportabilität. Gleiches gilt für das Widerspruchsrecht zur Verwendung der eigenen Daten zur Profilerstellung.

2.3 Schwächen der DSGVO

Die zentralen Prinzipien des Datenschutzes und damit auch der DSGVO wurden zu einer Zeit definiert, als es zwar bereits erste Ansätze der digitalisierten Datenverarbeitung gab, der Stand der Technik aber in keiner Weise mit

24 Die Veränderungen im Vergleich zu den Anforderungen einer Einwilligung nach aktueller deutschen Rechtsprechung sind allerdings gering. Ein wesentlicher Unterschied besteht zukünftig in der Einwilligung für Minderjährige, deren Schutzniveau deutlich angehoben wird, vgl. Datenschutzbeauftragter INFO (2016). Grundverordnung: Anforderungen an eine Einwilligung (online) https://www.datenschutzbeauftragter-info.de/grundverordnung-anforderungen-an-eine-einwilligung/

dem heutigen Datenverkehr vergleichbar war. Manche Kritiker halten das Festhalten an den Datenschutzprinzipien - ganz oder in Teilen - daher für nicht mehr angemessen in einer Zeit, in der Ressourcenallokation zunehmend über die Generierung, Verarbeitung und Weitergabe von Daten stattfindet.[25]

Nachfolgend diskutieren wir, warum wir der Meinung sind, dass der aktuelle bzw. demnächst in Kraft tretende regulative Rahmen Bürger- und Freiheitsrechte nicht ausreichend zu schützen vermag. Zusammenfassend zeichnen sich mindestens fünf zentrale Problemfelder ab:

1. Die erschwerte Differenzierung von personenbezogenen und nicht-personenbezogenen Daten;
2. Verlust der Kontrolle seitens der Verbraucher im Zuge der Einwilligung;
3. Probleme mit anderen Datenschutzprinzipien und rechtliche Grauzonen;
4. Eine unübersichtliche Akteurslandschaft und Datenhandel;
5. kollektive Effekte datenbasierter Entscheidungen.

2.3.1 Personenbezug und Personenbeziehbarkeit

Die DSGVO basiert wie andere Datenschutzgesetze auf der Prämisse einer Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten. Ausschließlich personenbezogene Daten fallen unter den Anwendungsbereich der Rechtsvorschriften des Datenschutzes. Dazu gehören alle Daten, die sich eindeutig einer bestimmten Person zuordnen lassen, durch die eine Zuordnung erfolgen kann, oder Daten durch die sich ein Personen-

25 Damit sind gar nicht mal jene gemeint, die einer Post-Privacy-Ära das Wort reden, sondern eher gemäßigte, aber gut informierte Vertreter wie der ehemalige Bundesbeauftragte für den Datenschutz, Hans Peter Bull. Vgl. etwa Bull, H.P. (2015). *Sinn und Unsinn des Datenschutzes*. Tübingen: Mohr Siebeck, S.55 ff.

bezug herstellen lässt (wie etwa Kfz-Kennzeichen)[26]. Auch pseudonymisierte Daten gelten nach DSGVO als personenbezogene Daten.[27]

Anders verhält es sich mit anonymisierten Daten. Durch das Verfahren der Anonymisierung werden Daten in einem Maße verändert, dass diese nicht mehr einer Person zuzuordnen sind.[28] Die Anonymisierung gilt daher auch in der DSGVO als eine wichtige Lösungsstrategie für das Dilemma, Daten zu nutzen, ohne Grundrechte zu kompromittieren. Nicht umsonst werden Befürworter einer verstärkten Datennutzung nicht müde zu bekräftigen, dass ihre Geschäftsmodelle auf anonymisierten Daten beruhen.[29] Daten, denen der Personenbezug vollständig entzogen wurde, sind nach deutscher und europäischer Rechtsprechung nicht mehr Gegenstand von Datenschutzgesetzen. Unternehmen, die mit anonymisierten Daten agieren, sind insofern vom Geltungsbereich des Datenschutzes ausgenommen.

In der Praxis zeigt sich jedoch, dass eine statische Einteilung in anonyme und nicht-anonyme Daten an der Realität der technologischen Möglichkeiten vorbeigeht. So häufen sich Fälle, in denen ehemals anonym geglaubte Daten re-identifiziert werden konnten. Bereits in den 1990er Jahren wies die US-Forscherin Latanya Sweeney mit ihren Forschungen auf das Risiko hin, dass Daten in Kombination mit anderen Datensätzen unter Umständen Rückschlüsse auf Personen in den Daten zulassen, "even when the sources of the information contains no explicit identifiers, such as name

---

26 Nach Beschluss des Europäischen Gerichtshof (EuGH) fallen auch dynamische IP-Adressen unter diese Kategorie. Nach dem Urteil reicht es aus, wenn ein Dritter mit geringem Aufwand Personenbezug herstellen kann.

27 Bei der Pseudonymisierung wird ein Merkmal in einem Datensatz durch ein anderes ersetzt. Da es die Möglichkeiten der Verknüpfung eines Datensatzes mit der Person verringert, ist das Verfahren der Pseudonymisierung ein wertvolles Instrument, um Sicherheit zu erhöhen. Die natürliche Person ist aber nachwievor durch das Hinzuziehen von Informationen zu identifizieren, so dass die Pseudonymisierung allenfalls als Hilfsmittel nicht aber als einzelne Schutzmaßnahme bewertet werden kann. Vgl. hierzu die Stellungnahme der Article 29 Data Protection Working Party (2014). Opinion 05/2014 on Anonymisation Techniques (online) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

28 Eine umfangreiche Übersicht und Bewertung gängiger Anonymisierungsverfahren wie etwa Randomisierung, k-anonymity, l-diversity, bietet die Article 29 Data Protection Working Party (ebd.).

29 Die Politik springt bisweilen allzu bereitwillig auf diesen Zug auf, vgl. z.B. diesen Artikel über ein internes Strategiepapier von CDU-Netzpolitikern: Reinbold, F. (2017). Wirtschaft soll mehr Daten sammeln dürfen. *Spiegel Online* am 13.6.2017 (online) http://www.spiegel.de/netzwelt/netzpolitik/geschaeft-mit-daten-cdu-will-sparsamkeit-beenden-a-1151862.html

and phone number"[30]. Tatsächlich ist es heute, rund 20 Jahre später, noch um ein Vielfaches leichter, Datensätze automatisiert zu verschneiden und sie so zu de-anonymisieren. Neben der weiteren Forschung von Sweeney belegten auch zahlreiche andere Forscher, wie Individuen in anonymisierte Netflix-Nutzerdaten[31], Mobilfunkdaten[32] oder Kreditkartendaten[33] re-identifiziert werden können.

Diese Beispiele zeigen: Daten, die einmal anonym geglaubt wurden, können in vielen Fällen zu personenbezogenen Daten werden. Sweeney konstatierte bereits im Jahr 2005 bei einer Befragung vor dem Privacy and Integrity Advisory Committee of the Department of Security: "The point is that data that may look anonymous is not necessarily anonymous"[34]. Zu Recht stellt der UN-Sonderberichterstatter für Privatsphäre in seinem Bericht von 2016 zur Disposition, ob die DSGVO als modernstes aller Datenschutzinstrumente adäquate Lösungen präsentieren könne, wenn sie nach wie vor auf der Annahme wirkungsvoller Anonymisierung basiere.[35] Und das, obwohl die ersten Hinweise auf die Grenzen der Anonymisierung bereits über 20 Jahre zurückliegen.

Der technische Fortschritt führt dazu, dass es nach heutigem Stand schier unmöglich ist, eine dauerhafte Anonymisierung zu garantieren. Denn es gibt nicht nur neue Verfahren, welche die automatisierte Verschneidung von Datensätzen erleichtern, sondern es gibt auch immer mehr öffentlich zur Verfügung stehende Daten, die anonym geglaubte Daten gefährden. Als in New York etwa Taxi-Daten auf der Open-Data-Plattform der Stadt frei zugänglich gemacht wurden, zeigten Programmierer, wie sie mit Hilfe von Ortsangaben in den öffentlich verfügbaren Twitter- und Instagram-Daten, die Taxifahrten

30 Samarati, P. & Sweeney, L (1998). *k*-anonymity: a model for protecting privacy. *Proceedings of the IEEE Symposium on Research in Security and Privacy* (S&P). May 1998, Oakland CA. Zitat aus dem Abstract, online verfügbar unter https://dataprivacylab.org/dataprivacy/projects/kanonymity/index3.html

31 Narayanan, A. & Shmatikov, V. (2007). Robust De-anonymization of Large Sparse Datasets (online) https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

32 De Montjoye, Y.-A.; C. Hidalgo, C.; Verleysen, M. & Blondel, V. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Nature* (Scientific Reports) (online) https://www.nature.com/articles/srep01376

33 De Montjoye, Y.-A.; Radaelli, L.; Singh, V. K. & Pentland, A. S. (2015): Unique in the shopping mall: On the re-identiability of credit card metadata. In: *Science* 347 (6221), S.536–539

34 Sweeney, L. (2005): Testimony to the Department of Homeland Security, S.2 (online) https://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf

35 UN General Assembly (2016). Report of the Special Rapporteur on the right to privacy, 24, November 2016 (online) http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/31/64

von Prominenten in den Datensätzen nachverfolgen konnten.[36] Auch Open Data sind also eine potenzielle Quelle für De-Anonymisierungstechniken. Dieses Problem verschärft sich weiter, wenn Daten durch zahlreiche verschiedene Akteure weiterverarbeitet werden. Oft gehen anonymisierte Datensätze durch so viele Hände, werden verarbeitet und angereichert, ohne dass die Akteure erkennen (oder erkennen wollen), ob und wann die Daten als anonymisiert gelten können.[37]

Damit soll nicht gesagt werden, dass man sich vom Verfahren der Anonymisierung verabschieden sollte. Die Anonymisierung von Daten ist eine wichtige Maßnahme, um den Schutz von Verbrauchern zu erhöhen. Doch die daraus resultierende statische Einteilung in personenbezogene und nicht-personenbezogene Daten und die daraus wiederum resultierende Praxis des "release-and-forget"[38], ist angesichts des aktuellen Kenntnisstandes schlicht nicht mehr sachgemäß. Anonymisierung ist kontextabhängig. Um ihre Qualität bewerten zu können, benötigt es Aufwand und Ressourcen. Diverse Komponenten des Datenökosystems, die sie beeinflussen können, müssen dabei berücksichtigt werden: etwa die Art der Daten, die Infrastruktur, die Akteure und die Datenumgebung.[39] Dieser Bewertungsprozess ist als dynamisch anzusehen.[40] Daten, die wir heute anonym glauben, können schon morgen

36 Tockar, A. (2014). Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset. *Neustar Research* (online) https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/

Eine Reihe weiterer Beispielen haben wir an anderer Stelle skizziert. Vgl. z.B. Manske, J. (2016). Offene Daten und der Schutz der Privatsphäre. *SNV Policy Paper* (online) https://www.stiftung-nv.de/de/publikation/offene-daten-und-der-schutz-der-privatsphaere

37 Wie später erläutert, ist dies auch auf die Rechtslage zurückzuführen. Denn verantwortlich wäre in diesem Fall letztlich nur der für die Datenerhebung Verantwortliche.

38 Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* 2010 (Vol. 57), S.1701-1777. Auch in: *University of Colorado Law Legal Studies* (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

39 Vgl. hierzu auch Elliot, M.; Mackey, E.; O'Hara, K. & Tudor, C. (2016). *The Anonymisation Decision-Making Framework.* Manchester: University of Manchester (UKAN). Die Autoren sprechen sich für ein Data-Environment-Model aus und verweisen auf "procedure-based approaches", wie man sie aus der IT-Sicherheit kennt.

40 Vgl. unsere Ausführungen zur regelmäßigen Risikoprüfung im Kontext der Veröffentlichung von anonymisierten Daten in Manske, J. & Knobloch, T. (2017). Leitfaden für Datenschutz bei Open Data, S.10. *SNV Policy Brief* (online) https://www.stiftung-nv.de/sites/default/files/policy_brief_leitfaden_open_data_datenschutz.pdf

einen Personenbezug aufweisen und damit Gegenstand von Datenschutzgesetzen werden.

2.3.2 Informierte Einwilligung und der Kontrollverlust der Verbraucher

Das Prinzip der Einwilligung verfolgt das Ziel, dem Verbraucher Kontrolle über die Nutzung seiner Daten zu geben. Doch tatsächlich belegen zahlreiche Studien, dass kaum ein Verbraucher die AGB tatsächlich liest.[41] Aus rechtlicher Sicht gestattet der Verbraucher hier also regelmäßig Eingriffe in seine Grundrechte, ohne wirklich über das, was im Hintergrund passiert, informiert zu sein.[42] Folglich wurde von vielen Seiten Kritik an diesem Vorgehen geübt. AGB sind meist umfangreiche Texte, die in einer für den Laien unverständlichen juristischen Sprache geschrieben sind und zudem teils widersprüchlich Querverweise enthalten. Überdies gibt es für den Verbraucher keinerlei Verhandlungsmöglichkeiten. Er kann nur zustimmen oder muss auf den Dienst verzichten. Schließlich wird der Verbraucher mit solchen Einwilligungserklärungen regelrecht überflutet, was seine Überforderung zusätzlich erhöht. Zu Recht wird daher von einer fehlenden Souveränität der Nutzer und vom Kontrollverlust in Bezug auf persönliche Daten gesprochen. Mehr als acht von zehn Befragten einer EU-Studie sind der Meinung, dass sie nicht genügend Kontrolle über ihre persönlichen Daten haben.[43] Aus all dem kann nur dieser Schluss gezogen werden:
"Die datenschutzrechtliche Idealvorstellung einer 'informierten Einwilligung' findet sich im realen Leben der Menschen faktisch kaum wieder."[44]

Die DSGVO hält jedoch am Prinzip der Einwilligung fest und räumt ihr sogar eine Vorrangstellung gegenüber anderen gesetzlichen Lösungen ein (vgl. DSGVO, Art.6,1a). Viele Datenschützer und Datenschutzbeauftragte befür-

41 Laut Studie des Vodafone Instituts lesen nur 12 Prozent der Befragten Europäer die AGBs: Vodafone Institut für Gesellschaft und Kommunikation (2016). Big Data. Wann Menschen bereit sind, Daten zu teilen: Eine Europäische Studie (online) http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-Highlights-de.pdf

42 Vgl. Hoffmann, J. & Bergmann, B. (2017): Die informierte Einwilligung: Ein Datenschutzphantom. *Netzpolitik.org* (online) https://netzpolitik.org/2017/die-informierte-einwilligung-ein-datenschutzphantom

43 European Commission (2015). Data Protection Report, Special Eurobarometer 431, S.4 (online) http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

44 Horn, N.; Riechert, A. & Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, S.7. *Stiftung Datenschutz* (online) https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf

worten dies.[45] Denn entsprechend der oben angeführten Kritik sieht die DS-GVO eine verbraucherfreundlichere Gestaltung der Einwilligung vor - etwa indem diese kürzer und verständlicher aufbereitet werden und der Verbraucher klarer darüber informiert wird, was mit den Daten passiert. Gegenüber ihrer EU-Vorgängerin ist die neue Regelung erheblich strenger. Neben dem ursprünglichen Wortlaut "freely given, specific and informed" muss eine rechtsgültige Einwilligung "explicit" erfolgen "and evidenced by a statement or by a clear affirmative action" abgelegt werden. Für verschiedene Zwecke und Verarbeitungsvorgänge müssen separate Einwilligungen abgegeben werden. Damit wird die Einholung der Einwilligung aus Anbietersicht tatsächlich deutlich komplizierter.

Verbraucher- und Datenschützer feiern dies als Erfolg im Kampf gegen das bisherige Wegklicken der Grundrechte. Allerdings stellt sich hier eher grundsätzlicher Zweifel ein, ob das letztlich angestrebte Ziel, der Schutz der Grund- und Freiheitsrechte tatsächlich weiterhin durch das Prinzip der Einwilligung erreicht werden kann.

Zwar mehren sich produktive Vorschläge[46], wie die Einwilligung nutzerfreundlicher und verständlicher gestaltet werden könnte. Dabei bleibt aber die Gefahr, dass selbst dann, wenn die Erklärungen kürzer sind, möglicherweise wesentliche Details verloren gehen, die für den Nutzer jedoch einen erheblichen Unterschied machen können.[47] Selbst wenn volle Transparenz über die Nutzung der Daten herrschen würde, würde dies aus verhaltensökonomischen Gründen kaum ausreichen, um den Verbraucher davon zu

45 Günther, O.; Hornung, G.; Rannenberg, K.; Roßnagel, A.; Spiekermann, S. & Waidner, M. (2013). Auch anonyme Daten brauchen Schutz. *Zeit Online* vom 14.2.2013 (online) http://www.zeit.de/digital/datenschutz/2013-02/stellungnahme-datenschutz-professoren/komplettansicht

46 Siehe z.B. die Studie der Stiftung Datenschutz zu neuen Wegen der Digitalen Einwilligung: Horn, N.; Riechert, A. & Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. *Stiftung Datenschutz* (online) https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf und die Vorschläge der britischen Design-Agentur If: If (2017). Design Patterns (online) https://projectsbyif.com/projects/data-sharing-design-patterns

47 Helen Nissenbaum beschreibt dies als Transparency Paradox: "An abbreviated, plain-language policy would be quick and easy to read, but it is the hidden details that carry the significance. Thus the transparency paradox: transparency of textual meaning and transparency of practice conflict in all but rare instances. We seem unable to achieve one without giving up on the other, yet both are essential for notice-and- consent to work." -- Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus* 140 (4), S.32-48, hier S.36 (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567042

überzeugen, sich nun intensiv mit etwas zu befassen, was früher am Rande stattfand.[48]

Darüber hinaus suggeriert das Prinzip der Einwilligung das Prinzip der Freiwilligkeit. Doch mag es in der Theorie auch möglich sein, sich bestimmten Online-Diensten zu entziehen, so kommt dies in der Praxis einer oftmals einer Verweigerung der modernen Welt eo ipso gleich. Selbst wenn es alternative, datenschutzfreundliche Dienste gibt, so sind die Netzwerk-Effekte anderer Dienste so stark, dass sich für die Verbraucher immer ein Nachteil ergeben wird, wenn sie ganz auf die Nutzung verzichten. Die theoretische Konsumentenmacht ist angesichts solcher Quasi-Monopole praktisch völlig ohnmächtig.[49] Hinzu kommt, dass der Verbraucher sich durch die Verbreitung des Internet der Dinge etwa im städtischen Bereich in immer mehr Szenarien wiederfinden wird, in denen es nach momentanem Lauf der Entwicklung schlicht gar keine Entscheidungsautonomie mehr geben wird. Etwa dann, wenn Verbraucher das vernetzte ÖPNV-System nutzen wollen oder die für das Funktionieren des zukünftigen Straßenverkehrs essentiellen Daten der Geschwindigkeitssensoren ihrer selbstfahrenden Autos teilen müssen.[50]

Doch schon heute sind die Implikationen von Datenspeicherungen, -verarbeitungen und -kombinierungen inzwischen so komplex geworden, dass es für den Einzelnen im Grunde unmöglich ist, eine adäquate Einschätzung der Folgen seiner Einwilligung vorzunehmen. Der unmittelbare Wert einer Applikation mag für den Nutzer einer Scan-App, in dem Moment, da er wichtige Dokumente scannen muss, so hoch sein, dass er den Wert seiner Kontakt- oder GPS-Daten für den Dienstanbieter weder erkennen kann noch dies in dem betreffenden Moment, in dem es um etwas ganz anderes geht, abzuwägen bereit wäre. Gleiches gilt für die Nutzung von Buchungsportalen, Dating-Apps und Sharing-Diensten aller Art: Die Aussicht darauf, ein konkretes Anliegen hier und jetzt rasch mittels digitaler Dienste bearbeiten zu können,

---

48 Horn, N.; Riechert, A. & Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, S.49. *Stiftung Datenschutz* (online) https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf

49 So spricht sich inzwischen selbst der Economist für eine Datenregulierung großer IT-Konzerne aus. Er argumentiert, dass die Datenmacht einiger weniger die traditionellen Regeln des Wettbewerbs überholt hat. Die Wahrscheinlichkeit, dass ein neues Technologie-Unternehmen sich noch einmal nur mittels freier Marktprinzipien gegen Google oder Facebook durchsetzen wird, wird inzwischen als unwahrscheinlich bewertet. Vgl. The Economist (2017). The world's most valuable resource is no longer oil, but data (online) https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resourcev

50 Vgl. Rähm, J. (2015). Gefahren und Chancen der digitalisierten Welt. *Deutschlandfunk* (online) http://www.deutschlandfunk.de/hintergrund.723.de.html

verstellt grundsätzlich den Blick auf Art und Umfang der Datenverarbeitung, die

1. im Hintergrund ablaufen muss, damit der Dienst bereitgestellt werden kann, und
2. den Anbietern weit darüber hinausgehende Verwertungsmöglichkeiten bietet.

Die US-Forscherin Helen Nissenbaum spricht in diesem Zusammenhang auch vom Verlust der "contextual integrity".[51] Für den Verbraucher ist schwer nachvollziehbar, warum die Nutzung eines Dienstes in einem Kontextes (etwa der Scan eines Dokuments), Konsequenzen in einem ganz anderen Bereich (etwa das Kreditscoring) haben könnte. Gleichzeitig ahnen Verbraucher aber, dass ihre Daten in einer Weise genutzt werden, die ihnen verborgen bleibt. Kaum überraschend zeigen sich 70 Prozent der Verbraucher in einer weiteren EU-Umfrage aus dem Jahr 2015 besorgt, dass ihre Daten zu anderen Zwecken verwendet werden als zu denen, für die sie ursprünglich erhoben wurden – etwa für Profilbildung oder interessenbezogene Werbung.[52]

Angesichts der hohen Strafen, die in der DSGVO bei Gesetzesbruch vorgesehen sind, ist es fraglich, ob sich Unternehmen auf die Wirksamkeit der Einwilligung grundsätzlich überhaupt verlassen wollen. Experten vermuten eher, dass viele Unternehmen versuchen werden, statt einer Einwilligung die Daten auf Basis rechtlicher Erlaubnisnormen zu verarbeiten. Insbesondere Artikel 6 f. DSGVO bietet hierfür Spielraum: Danach darf der Verarbeitende sich auf sein berechtigtes Interesse berufen.[53] Wie weit das berechtigte Interesse interpretiert werden darf - ob etwa Werbezwecke oder die Weiterentwicklung des Geschäftsmodelles dazu zählen - ist bislang unklar und gehört zu zahlreichen Unsicherheiten, die es durch die laufende Rechtsprechung von Mai 2018 an sukzessive abzubauen gilt. Daten- und Verbraucherschützer werden aufgrund ihrer chronischen Unterausstattung dabei nicht unbedingt die besten Karten haben.

2.3.3 Andere Datenschutzprinzipien und rechtliche Grauzonen

Abgesehen von all dem zuvor Gesagten ist fraglich, wie viele Unternehmen am Ende überhaupt den vom Gesetzgeber präferierten Weg der Einwilligung gehen werden, denn wie skizziert werden die Auflagen für eine rechtmäßige Einwilligung durch die DSGVO strenger. Gerade für kleinere Unternehmen und jene, deren Hauptgeschäft die Verarbeitung von Daten ist, ist dies eine Herausforderung. Geschäftsmodelle und Anwendungen ergeben sich, wie

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

52 European Commission (2015). Data Protection Report, Special Eurobarometer 431, S.69 (online) http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

53 Art. 6 f. DSGVO, online unter https://www.datenschutz-grundverordnung.eu/grundverordnung/art-6-ds-gvo/

ebenfalls oben schon erläutert, in der Datenwirtschaft oft aus bislang noch nicht bekannten Nutzungsmöglichkeiten von Daten; das ist das Wesen von Big Data Analytics. Unternehmen werden insofern tendenziell weiterhin angespornt sein, zunächst so viele Daten wie möglich zu sammeln. Dies verträgt sich aber nicht mit den Datenschutzprinzipien der Datensparsamkeit und Zweckbindung, die für eine rechtmäßige Einwilligung auch unter dem Regime der DSGVO unerlässlich sind.

Für Hersteller von Systemen für das Internet der Dinge ergibt sich daraus eine noch größere Herausforderung, denn hier geht es ja gerade darum, dass Daten reibungslos zwischen Systemen und Sektoren fließen können. Schließlich stellt sich auf einer rein praktischen Ebene zudem die Frage, wie Verbraucher in Zukunft der Nutzung ihrer Daten zustimmen können sollen, wenn viele Technologien gar keinen Bildschirm oder andere Nutzerinterfaces mehr vorsehen.[54]
Die DSGVO wird aus Sicht des Datenschutzes vermutlich einige Verbesserungen bringen, aber an den grundsätzlichen Mankos des Datenschutzes nichts ändern. Vielmehr schreibt sie die zentralen Datenschutzprinzipien - von einigen Neuerungen abgesehen - im Wesentlichen fort, ohne bestehende Missstände konsequent zu beseitigen. Der illegale Handel mit schlecht anonymisierten oder gar nur pseudonymisierten Daten kann etwa nur dann sanktioniert werden, wenn Strafverfolgungsbehörden darüber in Kenntnis gesetzt werden und hinreichend ausgestattet sind, um den Hinweisen nachzugehen. Das ist derzeit selten der Fall und daran wird sich nach jetzigem Umsetzungsstand auch unter dem Regime der DSGVO jedenfalls nicht von selbst etwas ändern. Dennoch könnte die DSGVO hier insofern positive Wirkung entfalten, als dass die hohen Bußgelder Unternehmen auch ohne regelmäßige Meldungen und Kontrollen von Verstößen zur Gesetzeskonformität zwingen könnten, weil schon ein einziger tatsächlicher Sanktionsfall existenzbedrohend wäre.

Problematisch ist jedoch, dass die DSGVO eine Reihe an Schlupflöchern lässt. Wie oben erörtert, ist beispielsweise davon auszugehen, dass Unternehmen die strengen Regeln einer informierten Zustimmung zu umgehen suchen werden, indem sie sich auf andere Artikel beziehen, die ihnen die Verarbeitung personenbezogener Daten ermöglichen, etwa auf das berechtigte Interesse oder Data Mining Operations.[55] Bislang fehlt es an Klarheit, was alles als berechtigtes Interesse gelten kann, ob beispielsweise Marketing und Werbung als ein solches legitimes Interesse anzusehen sind. Hier wird vom nächsten Jahr an viel von richterlichen Bewertungen abhängen. Doch auch hier gilt: um zu diesen zu kommen, müssen Verstöße zunächst einmal zur Anzeige gebracht werden. Überdies fürchten Verbraucherschützer, dass die Komplexität des Regelwerkes mit seinen zahlreichen Querverweisen letztlich nur von juristischen Experten wirklich durchschaubar ist. Viele Kanzlei-

54 Kupfer, D. (2015). Datenschutzrecht im Internet der Dinge. *Jaxenter* (online) https://jaxenter.de/datenschutzrecht-im-internet-der-dinge-16535

55 Zuiderveen Borgesius, F.J. (2015). Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law* 5 (3), S.163–176

en hängen aber wiederum von den Aufträgen großer Wirtschaftsunternehmen ab, so dass hier Interessenkonflikte zu Ungunsten des Datenschutzes zu befürchten sind.

Darüber hinaus häufen sich Fälle, in denen aus juristischer Sicht zwar kein Datenschutzproblem vorliegt, in denen der Verbraucher den Umgang mit Daten aber dennoch als Eingriff empfindet. Erst vor kurzem stellte sich etwa heraus, dass in Deutschland die Supermarktkette Real und die Deutsche Post Gesichtserkennungssoftware in ihren Filialen einsetzen, um so auf Basis von Alter und Geschlecht Personengruppen-spezifische Werbung auf ihren analogen Werbeflächen zu schalten.[56] Zwar wurde dies vom zuständigen Datenschützer mit der Begründung, dass es sich nicht um personenbezogene Daten handle[57], abgesegnet, die Kunden sind nach einer Umfrage des Bundesverbands der Verbraucherzentralen damit aber dennoch nicht einverstanden.[58] Dies zeigt erneut, dass eine rein juristische Betrachtungsweise womöglich nicht ausreicht, um das Datenzeitalter angemessen zu gestalten.

2.4 Intransparente Akteurslandschaft und Datenhandel

Die Nutzungsmöglichkeiten von Daten sind so vielfältig geworden, dass der Wert der Daten und die Folgen einer Datennutzung für den Verbraucher kaum noch nachvollziehbar sind. Hinzu kommt nun, dass das Netzwerk an Akteuren, die Daten sammeln, verarbeiten und verkaufen, derart komplex und verflochten geworden ist, dass aktuell weder der Verbraucher noch der Gesetzgeber genau weiß, wer was mit den Daten macht.

Der Verbraucher interagiert mit den Plattformen der Technologieriesen Google, Facebook u.a. oder mit seinem Mobilfunkanbieter, hinzu kommen zahlreiche weitere App- und Service-Hersteller. Dabei ahnt der Nutzer in vielen Fällen zwar, dass die Anbieter mit seinen Daten Geld verdienen. Mobilfunkanbieter handeln beispielsweise mit den besonders wertvollen Mobilfunkdaten, für die 2015 ein Marktvolumen von etwa 24,1 Milliarden US-Dol-

56 Kläsgen, M. & Martin-Jung, H. (2017). Abgescannt im Supermarkt. *Süddeutsche Zeitung* (online) http://www.sueddeutsche.de/wirtschaft/ueberwachung-im-supermarkt-abgescannt-im-supermarkt-1.3529017

57 Anger, H. (2017). Gesichtsscan im Supermarkt ist unbedenklich. *Handelsblatt* (online)

58 Vgl. Pressemitteilung der Verbraucherzentrale Bundesverband vom 21.6.2017: VZBV (2017). Beim Shoppen auf Schritt und Tritt überwacht (online) https://www.vzbv.de/pressemitteilung/beim-shoppen-auf-schritt-und-tritt-ueberwacht

lar kalkuliert wurde.[59] Und Facebook hält zum Beispiel inzwischen ein Patent auf sogenanntes Kredit-Scoring.[60] Doch tatsächlich sind dies nur die Spitzen einer Eisberglandschaft. Zahlreiche Unternehmen, die Daten sammeln, veredeln, verschneiden und veräußern, agieren im Hintergrund und treten dem Verbraucher gegenüber gar nicht in Erscheinung. So blieb das Geschäft des sogenannten Datenhandels lange im Verborgenen, bis es durch einen umfassenden Bericht der Federal Trade Commision von 2014 in den USA erstmals ans Licht gebracht wurde.[61] Datenhändler nutzen diverse Quellen, um Daten zu sammeln. Neben dem Erwerb von digitalen Daten oder der Nutzung von bestimmten Web-Diensten, die etwa das Sammeln von Browser-Daten ermöglichen, nutzen sie diverse öffentlich zugängliche Datenquellen, wie etwa offen einsehbare Social-Media-Daten und auch Daten, die über Open-Data-Plattformen verfügbar sind.[62]

Datenhändler gibt es spezialisiert auf verschiedene Bereiche, vom Finanzsektor über den Versicherungsbereich bis hin zu Marketing und Politik. Prinzipiell ist das Feld nicht neu. Schon vor dem Internet wurden Kundendaten gesammelt. Doch heute können diese Daten in einer ganz neuen Qualität zusammengeführt werden. So ermöglichen sie es nicht nur, Verbraucher individualisiert anzusprechen, sondern auch recht verlässliche Prognosen über sein Verhalten zu erstellen. Der Verbraucher bemerkt dies oft gar nicht. Viele Produkte von Datenhändlern übermitteln Daten, ohne dass die Nutzer davon etwas mitbekommen würden, etwa weil sie den AGB für die Nutzung von Cookies oder in Applikationen integrierten Add-Ons zugestimmt haben. Kürzlich sorgte in den USA die Enthüllung der Geschäftspraktiken des

59 Kaye, K. (2015). The $24 Billion Data Business That Telcos Don‘t Want to Talk About. *AdvertisingAge* (online) http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/

Vgl. hierzu auch die aktualisierte Rechtslage in den USA, nach dem Mobilfunkanbieter Daten ohne das Einholen einer Zustimmung verkaufen dürfen: Finley, K. (2017). The FCC seems unlikely to stop internet providers from selling your data. *Wired* am 3.1.2017 (online) https://www.wired.com/2017/03/fcc-graciously-sets-internet-providers-free-sell-data/

60 Meyer, R. (2015). Could a Bank Deny Your Loan Based on Your Facebook Friends? *The Atlantic* am 25.9.2015 (online) https://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287/

61 Federal Trade Commission (2014). Data Broker: A Call for Transparency and Accountability (online) https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

62 Federal Trade Commission (ebd.)

Dienstes Unroll.me für Aufsehen.[63] Der vorderhand kostenlose Dienst, der die Postfächer der Nutzer von Spam und Newslettern zu befreien verspricht, verdient sein Geld damit, dass er bei der Säuberung des Posteingangs auch den Postkorb analysiert. Findet der Dienst dabei beispielsweise Quittungen des Fahrdienstleisters Lyft, verkauft er die Daten anonymisiert an Lyfts Konkurrenten Uber. Diese Vorgehensweise, die den wenigsten Nutzern vor der medialen Aufmerksamkeit bewusst gewesen sein dürfte, ist rechtens, denn das Unternehmen gibt die Datenweitergabe in den AGB an und verlangt von den Nutzern zuvor eine Einwilligung.[64]

Datenhändler haben wenig Interesse, als solche öffentlich in Erscheinung zu treten, und es gibt nachwievor keine klaren Zahlen dazu, wie viele Data Broker global agieren.[65] In Deutschland und Europa ist die Debatte bislang marginal. So gibt es etwa auf EU-Ebene weder eine Erfassung von Datenhändlern, noch gibt es Untersuchungen darüber, wie Europäische Gesetze auf sie angewendet werden.[66] Dabei wächst auch hierzulande die Zahl der Unternehmen, deren Haupttätigkeit das Sammeln, Verknüpfen und Verkaufen von Daten ist. Dies wurde beispielsweise durch eine aufwändige Recherche der NDR-Journalistin Svea Eckert im Jahr 2016 bestätigt.[67] Der bekannteste Datenhändler, die Firma Acxiom, gibt an, inzwischen recht umfassende Daten

63 Isaac, M. & Lohr, S. (2017). Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data. *The New York Times* am 24.4.2017 (online) https://www.nytimes.com/2017/04/24/technology/personal-data-firm-slice-unroll-me-backlash-uber.html

64 Tatsächlich ist dies einer in einer Reihe von Fällen, in denen entdeckt wurde, dass Unternehmen Daten weitergeben, ohne die Kunden explizit zu informieren. Einige von ihnen wurden daraufhin strafrechtlich verfolgt, vgl. Bindi, T. (2017). Bose accused of tracking and sharing customer listening data. *ZDNet* (online) http://www.zdnet.com/article/bose-accused-of-tracking-and-sharing-customer-listening-data-report/

65 Kroft, S. (2014). The Data Brokers: Selling Your Personal Information. *CBS News* am 9.3.2014 (online) https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/

66 Rieke, A.; Yu, H.; Robinson, D. & von Hoboken, J. (2016). Data Brokers in an Open Society, S.21 *Upturn*, Open Society Foundation London (online) https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf

67 Das Fernsehmagazin “Panorama” berichtete darüber in seiner Sendung am 1.11.2016, vgl. http://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html

von rund 44 Millionen Deutschen zu haben.[68] Die wenigsten von uns wissen, geschweige denn verstehen, welche Daten über uns tatsächlich verarbeitet werden und welche Konsequenzen das haben kann.

Ein Bericht von Upturn im Auftrag der Open Society Foundation aus dem Jahr 2016 resümiert, dass Datenhändler so oft Daten untereinander kaufen und verkaufen, dass es für den Verbraucher nicht möglich sei nachzuvollziehen, woher die Daten eines bestimmten Händlers ursprünglich stammen, selbst wenn dieser entsprechende Informationen offen legen würde.[69] Denn die gehandelten Daten können sowohl "Factual Data" als auch modellierte Daten sein. Letztere sind Daten, die bereits weiterverarbeitet und interpretiert wurden. Das bedeutet, dass Händler oftmals gar nicht diejenigen Daten verkaufen, die ein Verbraucher durch seine Interaktion mit einem Dienst erzeugt hat, sondern eine Interpretation dieser Daten.

Dabei ist das Feld des Datenhandels in Europa noch wesentlich regulierter als in anderen Teilen der Welt, wo es vielfach überhaupt nicht limitiert ist. Auch die ePrivacy-Richtlinie könnte durch schärfere Regulierungen des sogenannten Trackings den Schutz von Grundrechten (Privatsphäre, Diskriminierungsverbot etc.) stärken. Dennoch fürchten Datenschützer, dass der zunehmende internationale Wettbewerb auch europäische Datenhändler dazu ermutigen wird, großflächig nach neuen Datenquellen zu suchen.[70] Tatsächlich ist davon auszugehen, dass wir erst am Beginn des Zeitalters des "Überwachungskapitalismus"[71] stehen. Aktuelle Geschäftsmodelle aufstrebender Startups legen nahe, dass sich der Trend, Daten mehr oder weniger direkt

68 Genauere Informationen über die Aktivitäten von Acxiom und anderen Datenhändern in Europa finden sich in: Christl, W. & Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy.* Wien: Facultas

69 Rieke, A.; Yu, H.; Robinson, D. & von Hoboken, J. (2016). Data Brokers in an Open Society, S.9. *Upturn*, Open Society Foundation London (online) https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf

70 Datatilsynet (2015). The Great Data Race: How commercial utilisation of personal data challenges privacy. Report November 2015 (online) https://www.datatilsynet.no/globalassets/global/english/engelsk-kommersialisering-endelig.pdf

71 Zu diesem Begriff vgl. z.B. Zuboff, S. (2014). A Digital Declaration. *Frankfurter Allgemeine Zeitung* am 14.9.2014 (online) http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshan-zuboff-on-big-data-as-surveillance-capitalism-13152525.html und Christl, W. & Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy.* Wien: Facultas.

in Geld verwandeln zu wollen, nicht nur gleichbleibend fortsetzen, sondern verstärken wird.

In der Regel argumentieren Datenhändler zur Rechtfertigung ihrer Praktiken damit, sie würden ausschließlich mit anonymisierten Daten agieren. Doch wie oben dargelegt, ist die dauerhafte Sicherstellung einer qualitativ hochwertigen Anonymisierung alles andere als trivial. Darüber hinaus ist durchaus fragwürdig, inwiefern die Datenhändler wirklich den Anspruch haben, mit anonymisierten Daten zu handeln. Schließlich ist es eines ihrer Ziele, einen Kunden über verschiedene Geräte hinweg wiederzuerkennen (etwa durch sogenanntes "Hashing"). De facto geht es entsprechend um die Identifikation einzelner Personen, wenn auch vielleicht nicht anhand ihres Namens. Und per Definition fällt dies allenfalls in den Bereich der Pseudonymisierung.[72] Doch aufgrund der fehlenden Transparenz im Markt der Datenhändler bleibt oft im Verborgenen, ob die Daten, mit denen die Händler agieren, unter das Datenschutzrecht fallen müssten oder nicht. Denn solange niemand auf einen illegitimen Datenhandel aufmerksam macht, werden auch keine Sanktionen ausgesprochen werden. Und die beteiligten Akteure werden wohl kaum selbst auf potentielle Missstände hinweisen.

2.5 Kollektive Effekte datenbasierter Entscheidungen

Der Umgang mit personenbezogenen oder personenbeziehbaren Daten entfaltet kollektive Wirkungen, auch wenn durch das individualisierte Prinzip der Einwilligung etwas anderes suggeriert wird. In der Realität kann die Einwilligung eines Einzelnen Konsequenzen für Personen haben, die in keinerlei Zusammenhang mit der einwilligenden Person stehen. Datenanalysen können auf Basis weniger Datensätze von Zustimmenden vorgenommen werden, dann aber für ganze Bevölkerungsgruppen generalisiert werden. Nicht zuletzt durch den zunehmenden Einsatz Algorithmen-basierter, automatisierter Entscheidungen wird der Umgang mit Daten um eine kollektive Dimension erweitert.[73] Viele aktuelle Nutzungsszenarien für Daten sind unabhängig von individuellen Informationen und beeinträchtigen nicht unbedingt das Datensubjekt. Potenzielle Schäden können für andere Individuen, für ganze

72 Vgl. Christl, W. & Spiekermann, S. (2016), ebd.

73 Vgl. auch Jaume-Palasí, L. & Spielkamp, M. (2017). Ethik und algorithmische Prozesse zur Entscheidungsfindung oder -vorbereitung. *AlgorithmWatch* Arbeitspapier Nr. 4 (online) https://algorithmwatch.org/wp-content/uploads/2017/06/AlgorithmWatch_Arbeitspapier_4_Ethik_und_Algorithmen.pdf

Gruppen oder Mitglieder einer Profil-Kategorie eintreten.[74] Trotzdem orientieren sich Datenschutzkonzepte durch den Fokus auf Instrumente wie die Einwilligung immer noch vornehmlich an den Folgen für Individuen und deren Schutz.[75]

Hier zeigt sich erneut die oben erläuterte Problematik einer Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten und dem darauf basierenden Prinzip der Einwilligung. Denn ihre Wirkung ist stark eingeschränkt, wenn automatisierte Entscheidungen letztlich auch Personen betreffen, die der Nutzung ihrer Daten nicht zugestimmt haben. Denn algorithmische Entscheidungen erfolgen nicht auf der Grundlage der Daten eines einzelnen Individuums, über das eine Entscheidung getroffen wird (z.B. wenn entschieden wird, welcher Werbebanner Person X beim Surfen angezeigt wird). Die Entscheidung mag zwar eine begrenzte Anzahl persönlicher Daten dieser Person benötigen, sie basiert aber auf einer Fülle von Daten anderer Personen oder Quellen. Das heißt, die Millionen von Daten, die zur Generierung von Wissen, Modellen oder Vorhersagen gesammelt und analysiert werden, stehen nicht unbedingt im Zusammenhang mit den Daten, die dann unter Anwendung dieses Wissens, dieser Modelle oder Vorhersagen genutzt werden.[76]

Darüber hinaus können Datenanalysen oder automatisierte Entscheidungen Menschen auch dann betreffen, wenn ihre eigenen Daten gar nicht verwendet werden. Einer Bank, die Interesse hat, eine neue Filiale zu öffnen, rei-

---

74 Vgl. Kammourieh, L.; Baar, T.; Berens, J.; Letouzé, E.; Manske, J.; Palmer, J.; Sangokoya, D. & Vinck, P. (2017). Group Privacy in the Age of Big Data. In: Taylor, L.; Floridi, L. & van der Sloot, B. (Hrsg.). *Group Privacy: New Challenges of Data Technologies*. Dordrecht: Springer.

Vgl. auch Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology* (online) https://link.springer.com/article/10.1007%2Fs13347-017-0253-7

75 Tatsächlich stand im deutschen Datenschutzgesetz zunächst auch immer das Gemeinwohl im Zentrum, indem es die informierte Selbstbestimmung als elementare Funktionsbedingung einer Gesellschaftsordnung definierte. “Gerade diese Verknüpfung von individuellen und gesellschaftlichen Bezügen im Volkszählungsurteil gerät leicht in Vergessenheit: Die Befürworter der informierten Einwilligung stützten sich in den folgenden Jahren hauptsächlich auf die individuelle Dimension des Datenschutzes. Seine gemeinwohlorientierte Dimension ist darüber ins Hintertreffen geraten.”- Hoffmann, J. & Bergmann, B. (2017). Die informierte Einwilligung. Ein Datenschutzphantom. *Netzpolitik.org* (online) https://netzpolitik.org/2017/die-informierte-einwilligung-ein-datenschutzphantom/

76 Oostveen, M. & Irion, K. (2017). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? *Amsterdam Law School Research Paper* No. 2016-68, S.9 (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885701

chen die Informationen über die Demographie und die Vermögensverhältnisse in einem Bezirk. Einem Werbetreibenden reicht es, Werbeangebote auf ein Geräte zu senden, deren Nutzern bestimmte Browsing-Gewohnheiten nachgesagt werden.[77] Bemerkenswert ist in diesem Zusammenhang, dass es sich unter Umständen auch negativ auswirken kann, nicht in bestimmten Datensätzen aufzutauchen. Man denke etwa an datenbasierte Entscheidungen über politischen Planung, in denen Gruppen nicht abgebildet sind, weil sie sich bewusst gegen eine Einwilligung entschieden haben, oder aus anderen Gründen nicht in den Daten auftauchen.[78]

Die österreichischen Forscher Wolfie Christl und Sarah Spiekermann zeigen in ihrem Buch „Networks of Control" eine Vielzahl von Beispielen, in denen Benachteiligungen weltweit im Online-Marketing auftreten.[79] Etwa indem ein Algorithmus entscheidet, einem Kunden ein Produkt zu einem höheren Preis anzubieten oder sogenannten "Vulnerable or Desperate Groups" Werbung für riskante Kreditangebote anzuzeigen.[80] Gerade in der Summe und insbesondere in der wechselseitig verstärkenden Wirkung (z.B. indem nur bestimmte Gruppen adressiert werden und die nur mit Angeboten, welche die Gruppenzugehörigkeit zementieren) können solche Auswirkungen durchaus signifikant sein und Ungleichheiten verstärken.

Fragen des Datenschutzes, bzw. In diesem Zusammenhang bereits besser: der Data Governance, gehen aufgrund der aufgezeigten kollektiven Dimension heutzutage weit über das Recht des Schutzes der Privatsphäre (nach Artikel 7 der EU Grundrechte-Charta) und auch über das Recht des Schutzes personenbezogener Daten (Artikel 8) hinaus. Beide dienen dazu, den Schutz anderer Grundrechte und Grundfreiheiten zu gewährleisten, z.B. das Recht auf Meinungsfreiheit, die Religionsfreiheit oder der Diskriminierungsschutz.[81] Wenn Menschen zunehmend in "ranked and rated Objects"

---

77 Rieke, A.; Yu, H.; Robinson, D. & von Hoboken, J. (2016). Data Brokers in an Open Society, S.10. *Upturn*, Open Society Foundation London (online) https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf

78 Crawford, K. (2013). The Hidden Biases in Big Data. *Harvard Business Review* (online) https://hbr.org/2013/04/the-hidden-biases-in-big-data

79 Christl, W. & Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Wien: Facultas

80 Christl, W. & Spiekermann, S. (ebd.) beziehen sich auf einen Bericht des *Committee on Commerce, Science and Transportation* von 2013, der online unter https://www.gpo.gov/fdsys/pkg/CHRG-113shrg95838/pdf/CHRG-113shrg95838.pdf verfügbar ist.

81 Oostveen, M. & Irion, K. (2017). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? *Amsterdam Law School Research Paper* No. 2016-68, S.8 (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885701

eingeteilt werden und jeder kontinuierlich auf Basis seines ökonomischen Potenzials sortiert und adressiert wird, gefährdet dies einerseits wichtige Grundprinzipien von Demokratien, wie Würde und Gleichheit, und beschneidet unter Umständen bereits Benachteiligte in den Möglichkeiten sozialer Teilhabe[82] sowie dem Recht auf Selbstbestimmung und Autonomie.[83] Mögen einige der Meinung sein, dass der Schutz der Privatsphäre an Wert verliert, so herrscht doch nachwievor Einigkeit, über die Notwendigkeit des Schutzes der anderen genannten Grundrechte. Und diese wiederum sind durch den aktuellen Umgang mit Daten gefährdet.

Die Datenschutzgrundverordnung hat durchaus versucht, die neuen Entwicklungen zu adressieren, insbesondere Artikel 22 ist an dieser Stelle zu nennen. Etliche Wissenschaftler haben allerdings auf Mängel in diesem Artikel hingewiesen. Diese Mängel könnten letztlich dazu führen, dass das Gesetz für den Verbraucher wirkungslos bleibt. So richtet sich Artikel 22 z.B. ausschließlich auf vollautomatisierte Entscheidungen. Tatsächlich gibt es aber in vielen Fällen durchaus menschliche Zwischeninstanzen - sie wären damit allerdings vom Gesetz nicht betroffen.[84] Mit Bezug auf Artikel 4(4), der Definition über Profiling, könnte Artikel 22 außerdem so ausgelegt werden, dass lediglich "personenbezogene Daten einer natürlichen Person" umfasst sind. Wie bereits dargestellt, können jedoch auch Anwendungen, die mit nicht-personenbezogenen Daten arbeiten, problematisch sein, wenn diese sich etwa im Zuge der Verarbeitung de-anonymisieren lassen[85], oder wenn auch ohne Personenbezug negative Effekte für Individuen eintreten. Auch die in der DSGVO aufgeführten Auskunftsrechte sind laut Expertenmei-

82 Christl, W. & Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Wien: Facultas

83 Bernal, P. (2014). *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge: Cambridge University Press.

84 Oostveen, M. & Irion, K. (2017). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? *Amsterdam Law School Research Paper* No. 2016-68, S.15 (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885701

85 Ebd.

nung nicht wirksam genug, um die Rechte von Verbrauchern ausreichend zu schützen.[86]

Neben der Datenschutzgrundverordnung gibt es außerdem eine Reihe an Gesetzen, die für Schutz der Verbraucher im Kontext von Datenverarbeitung relevant sind, etwa Verbraucherschutzgesetze[87] (zum Beispiel für den Bereich des Kreditscoring), oder Anti-Diskriminierungsgesetze (etwa für den Arbeitsmarkt, Geschlecht oder Herkunft) - allerdings fehlt es bislang noch an einer effektiven Nutzung der vorhandenen Gesetze in diesem Bereich. Zu sehr werden Datenthemen auf den Datenschutz reduziert. Dies mag nicht zuletzt daran liegen, dass sich sich das Thema inzwischen in einen höchst spezialisierten Fachbereich verwandelt hat, der von Datenschutzjuristen dominiert wird.

Im Zuge der Anpassung des Bundesdatenschutzgesetzes (BDSG) an die DSGVO seit Verabschiedung derselben im Dezember 2015 sind immer wieder Szenarien über Deutschlands Abstieg am Weltmarkt gezeichnet worden, sollte man mehr oder weniger als einziges Land Datenschutzprinzipien weiterhin streng auslegen und umsetzen.[88] Teilweise ist der Erfolg dieser Argumentationslinie an den Änderungen des BDSG sogar zu erkennen.[89] Und auch bei anderen Technologiethemen werden immer wieder Chancen gegen Gefahren ausgespielt. Diese Herangehensweise suggeriert vor dem Hintergrund der Alltagsrationalität - alles hat zwei Seiten - dass es hierbei um Zero-Sum-Spiele handelt. Wir setzen dieser Annahme unsere Überzeugung gegenüber, dass wir Chancen, die uns die Auswertung digitaler Daten bieten,

---

86 Wachter et al. erklären in einer Analyse, warum es aufgrund sprachlicher Ungenauigkeiten de facto kein Recht auf Erläuterung gibt und warum es nach Artikel 22(3), bzw. Erwägungsgrund 71 de facto nicht wirksam ist: Wachter, S.; Mittelstadt, B. & Floridi, L. (2016). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, Forthcoming (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

87 Rhoen, M. (2016). Beyond consent: improving data protection through consumer protection law. *Internet Policy Review* 5 (1) (online) https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law

88 Vgl. Krempl, S. (2017). De Maizière hält Losung “Meine Daten gehören mir” für falsch. *heise* am 18.2.2017 (online) https://www.heise.de/newsticker/meldung/De-Maiziere-haelt-Losung-Meine-Daten-gehoeren-mir-fuer-falsch-3630322.html

89 Vgl. z.B. die heftige Kritik, welche die Zivilgesellschaft am geleakten BSDG-Referentenentwurf des BMI Ende 2016 geübt hat, kompakt in Reuter, M. (2016). Neues Bundesdatenschutzgesetz: Weniger Kontrolle, weniger Auskunftsansprüche, mehr Videoüberwachung. *Netzpolitik.org* am 24.11.2016 (online) https://netzpolitik.org/2016/neues-bundesdatenschutzgesetz-weniger-kontrolle-weniger-auskunftsanspruche-mehr-videoueberwachung/

nutzen können, ohne uns gleichzeitig möglichen negativen Folgen ausliefern zu müssen. Diese Argumentation haben wir schon in unseren Policy Papier "Das Datenzeitalter gestalten" vom Sommer 2016 angeführt. Wir orientieren uns weiterhin an ihr, verlassen dabei aber den damals engen Fokus auf die Bereitstellung von Verwaltungsdaten. Jetzt geht es uns um eine humanistische, Demokratie-kompatible Gestaltung der von Datenanalysen angetriebenen Gesellschaft, die wir wir nicht erst werden, sondern die längst Realität ist.

3 Perspektiven über den Datenschutz hinaus

Unsere Argumentation in diesem Papier hat verdeutlicht, dass wir über den traditionellen Datenschutzansatz hinaus denken müssen, um auch im sogenannten Datenzeitalter weiterhin eine lebenswerte Gesellschaft konstituieren zu können. Einerseits müssen wir uns von der Vorstellung verabschieden, dass gesellschaftliche Probleme mit der Sammlung, Auswertung und Verbreitung von Daten nur dort entstehen können, wo personenbezogene Daten im Spiel sind oder wo von vornherein erkennbar Personenbeziehbarkeit gegeben ist.[90] Andererseits werden wir weiterhin damit rechnen müssen, dass Individuen selbst arglos mit persönlichen Informationen und mit den Informationen anderer umgehen werden, und dass Unternehmen sowohl davon als auch von den Schlupflöchern im Datenschutzrecht Gebrauch machen werden, um ihren Profit zu maximieren.
Praktiken der Datenerschließung und -verarbeitung unterscheiden sich in den verschiedenen Anwendungsbereichen zum Teil erheblich. One-size-fits-all-Lösungen sind daher sehr wahrscheinlich ungeeignet, den traditionellen Datenschutzansatz für die Zukunft sinnvoll zu erweitern.[91] Mobilitätsdaten sind anderer Natur als Steuerdaten oder Gesundheitsdaten, sie werden anders erfasst, verarbeitet und erlauben jeweils andere Schlüsse. Sobald wir jenseits des Datenschutzes, der seiner Natur nach ein Catch-all-Instrument ist, über Datensteuerung nachdenken, tun wir daher gut daran, das bereichsspezifisch und fallbezogen zu tun. Beispielsweise kann sinnvoll danach gefragt werden, welches Datensteuerungsregime - abgesehen vom Daten-

90 Dass die Grenzen hier fließend sind, lässt sich schon an zahlreichen juristischen Einzelfallentscheidungen zu der Frage ablesen, wann mit als plausibel anzunehmenden Mitteln Personenbezug herstellbar ist. Oben ist ferner gezeigt worden, dass sich wesentliche gesellschaftliche Probleme mittlerweile dadurch ergeben, dass durch Datenanalysen beispielsweise Gruppendiskriminierungen vorgenommen werden, die nichts mit der Verarbeitung personenbezogener Daten oder dem Herstellen eines Personenbezugs zu tun haben. Auch das völlige Fehlen von Informationen kann Personen stellenweise schon Nachteile bereiten, etwa wenn Sicherheitsbehörden ihre Social-Media-Accounts nicht auslesen können, weil sie keine haben, und sie alleine deshalb bereits als verdächtig einstufen.

91 Im ersten Positionspapier unseres neuen Datenprojekts bei der Stiftung Neue Verantwortung verwenden wir für diese Bestrebung die Arbeitsbezeichnung "Data Governance", siehe https://www.stiftung-nv.de/datagov

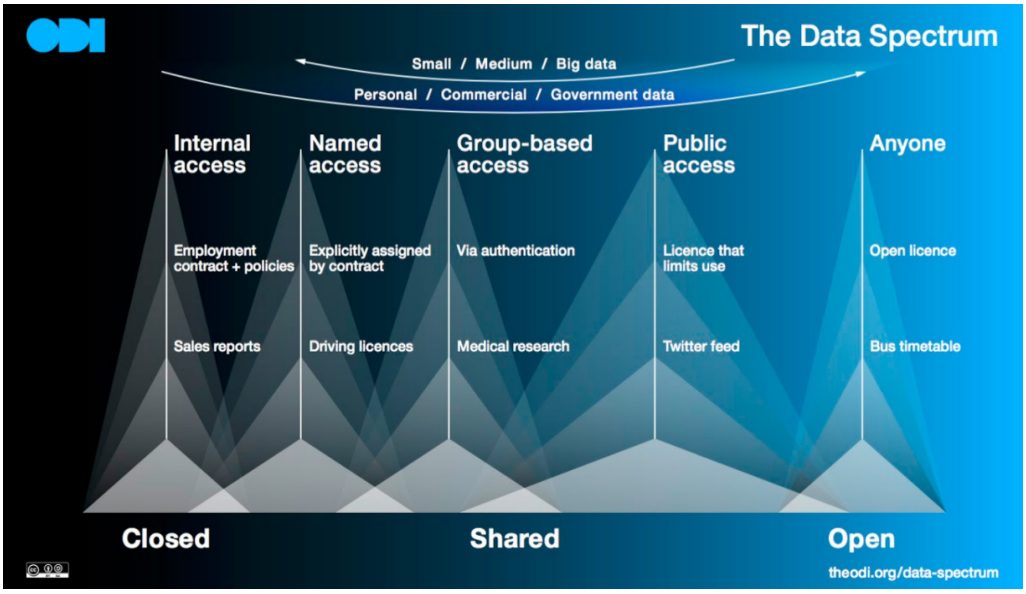

Abbildung 1: "The Data Spectrum", frei verfügbar unter https://theodi.org/data-spectrum

schutz, den wir nicht über Bord werfen wollen - etabliert werden sollte, um beispielsweise ÖPNV on demand flächendeckend auszurollen oder autonomes Fahren zu ermöglichen.[92] Dieselben Überlegungen werden mutmaßlich aber wenig dabei helfen zu entscheiden, was wir in Zukunft mit der persönlichen Patientenakte anfangen wollen oder was wir beim Targeted Advertising im Online-Marketing zulassen wollen.

Letztlich müssen wir uns in all diesen Bereichen - wiederum: nicht anstelle, sondern vielmehr über den Datenschutzansatz hinaus - die Frage stellen, welche Daten in welchem Umfang zwischen welchen Akteuren und Systemen geteilt werden müssen, damit wir erwünschte Ziele erreichen und unerwünschte Effekte vermeiden. Das Spektrum reicht dabei von geschlossen-vertraulicher Verwendung bis hin zu vollständig offener Verfügbarkeit, wie dieses inzwischen klassische Schaubild des britischen Open Data Institute veranschaulicht:

Beim Datenschutz geht es recht verstanden nicht um den Schutz von Daten, sondern um den Schutz von Menschen. Auch bei jedem neuen, erweiterten Datensteuerungsansatz, den wir für die Zukunft in Aussicht stellen, geht es um etwas anderes als die partielle Zurückhaltung von Informationen. Vielmehr geht es, ganz im Sinne eines Ermöglichungsdiskurses, um eine zeitgemäße Datenverbreitungskontrolle, um Datenzugangskontrolle und um

92 Weil dieser Bereich gerade für Deutschland als sogenannte Automobilnation von immenser Bedeutung ist, hat die "39th International Conference of Data Protection and Privacy Commissioners" im September 2017 in Hong Kong auf Antrag der deutschen BfDI eine "Resolution on Data Protection in Automated and Connected Vehicles" verabschiedet. Online unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2017/17_IDSK_HongKong.html

Datennutzungskontrolle. Wegen des abgestuften Charakters der einzuräumenden Zugänge und vorzunehmenden Restriktionen ist es offenkundig, dass technischen Lösungen hier eine entscheidende Rolle zukommt.[93] Personal Data Stores (PDS), Personal Information Management Services (PIMS), und Vendor Relationship Management (VRM) versuchen gewissermaßen die Not zur Tugend zu machen und zwei Fliegen mit einer Klappe zu schlagen: das Vertrauensproblem zu lösen, indem sie dem Verbraucher wieder mehr Kontrolle geben, aber gleichzeitig personenbezogene Daten - auch für gewerbliche Zwecke - nutzbar zu machen.[94] Neben neuen technischen Architekturen ist ein zentraler Aspekt der PIMS, dass sie den Datenschutz als als natürlichen Teil des Innovationsprozesses begreifen. Die Kernidee ist, das Individuum ins Zentrum des Datenmanagement-Prozesses zu stellen. Damit wird der Verbraucher zum zentralen Verbindungs- und Kontrollpunkt der eigenen Daten. Das Individuum entscheidet, wann, wie und mit wem Daten geteilt werden. Tatsächlich soll dieser "Mensch-zentrierte" Ansatz die Verbraucher ermutigen, ihre Daten zu teilen, wobei sie ihre Einwilligungen sie flexibel managen können. Da viele der PIMS umsetzenden Unternehmen und Organisationen ihren Ursprung in der Open-Data-Bewegung haben, ist ein zentrales technisches Design-Prinzip die Verwendung offener Schnittstellen, um Interoperabilität zwischen Diensten sicherzustellen.

Die Bewegung befindet sich noch in den Kinderschuhen. Sie wird aber auch deswegen mit Spannung beobachtet, weil sie viele der sehr theoretischen Ansätze der DSGVO in praktische Lösungen übersetzen würde. Ganz explizit können PIMS zugleich Förderer und Profiteure vom neuen Recht auf Datenportabilität nach Artikel 20 DSGVO werden. Dieses neue Recht soll es Verbrauchern ermöglichen, Anbieter leichter zu wechseln und damit eventuell auch die aktuelle Monopolstellung einiger weniger zu unterbinden. Doch bislang ist dieses Recht noch ein theoretisches, das von den PIMS jedoch anfassbar gemacht wird. Darüber hinaus könnten PIMS auf weitere, durch die DSGVO eröffneten Umsetzungsfragen eine Antwort bieten, etwa auf das Auskunftsrecht und das Recht auf Löschung oder Berichtigung. Doch auch

93 Zum Zusammenhang zwischen Datenschutz und Technik allgemein vgl. Hoepner, P. (2017). Datenschutz und Technik, ein Informationspapier. *Kompetenzzentrum Öffentliche IT* (online) http://www.oeffentliche-it.de/documents/10181/14412/Datenschutz+und+Technik+-+Ein+Informationspapier

94 Die am MIT entstandenen Projekt "Enigma" (https://www.media.mit.edu/projects/enigma/overview/) und "openPDS" (http://openpds.media.mit.edu/) sind einschlägige Beispiele, die finnische MyData-Bewegung (https://mydata.org/) ein weiteres.

für die Umsetzung der Prinzipien des Privacy-by-Design gemäß Artikel 25 liefern PIMS zumindest Inspirationen.[95]

Doch PIMS sehen sich einer Reihe von Herausforderungen gegenüber, um am Markt bestehen zu können. So müssen sie zwei Kundengruppen gleichzeitig erreichen und befriedigen: Datenanbieter und Datennutzer.[96] Voraussetzung dafür ist aber eine gewisse Reichweite. Um die aufbauen zu können, spielt wiederum das Vertrauen der Nutzer, das viele der PIMS erst noch gewinnen müssen, eine entscheidende Rolle. In diesem Zusammenhang ist noch weithin unklar, wie PIMS Geld verdienen können, ohne das Vertrauen der Nutzer zu gefährden. Die lukrativsten datenbasierten Geschäftsmodelle, die wir heute kennen, verarbeiten nunmal recht fein granulare Informationen über Individuen. Bei PIMS und anderen nutzerzentrierten Ansätzen geht es jedoch gerade darum, den Zugang zu solchen Informationen bereits von der technischen Anlage her zu limitieren. Trotz dieser und zahlreicher anderer, hier nicht angesprochener ungeklärter Fragen sind PIMS allerdings schon alleine deswegen gesellschaftlich sehr interessant, weil sie auf einer technischen Ebene Alternativen zu den aktuellen zentralisierten Modellen erproben.[97]

Schon diese kurze kritische Erörterung der PIMS zeigt, dass insbesondere neue, auf avancierten technischen Datensteuerungsmechanismen und datenethischen Prinzipien beruhende Geschäftsmodelle[98] ein probates Mittel sind, um wirksame Änderungen am Status quo zu erwirken. Denn am Ende ist es der - eben nicht vollständig rational handelnde, sondern in seinem Wissen, Wollen und Können eingeschränkte - Verbraucher, der darüber entscheidet, welche datenintensiven Anwendungen massenhaft genutzt werden und damit ökonomisch konkurrenzfähig sind; und er entscheidet damit letztlich auch darüber, welche neuen Technologien sich durchsetzen.

---

95 Vgl. European Data Protection Supervisor (2016). EDPS Opinion on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data. *Opinion 9/2016* (online) https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

96 Horn, N.; Riechert, A. & Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, S.48. *Stiftung Datenschutz* (online) https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf

97 In Deutschland findet das Thema bislang wenig Beachtung. Im März 2017 fand in Kooperation mit der Stiftung Neue Verantwortung und der Stiftung Datenschutz aber die erste MyData-Veranstaltung in Deutschland statt, zu der eine Reihe an PIMS-Startups ihre Lösungen in Berlin vorstellten; siehe https://www.stiftung-nv.de/de/veranstaltung/datenkontrolle-im-datenzeitalter

98 Einige interessante Beispiele sind versammelt in Hasselbalch, G. & Tranberg, P. (2016). *Data Ethics: The New Competitive Advantage*. Copenhagen.

Ansätze zu einer übergreifenden Datensteuerung

Wir haben hier dafür argumentiert, dass wir für das 21. Jahrhundert ganzheitliche, über Datenschutz, ePrivacy, Urheberrecht, Open Data und andere Spezialregelungen hinausgehende Datensteuerungsansätze brauchen. Nichtsdestoweniger müssen diese Ansätze bereichsspezifisch sein. Wie kann diese Kreisquadratur gelingen? Nun, zunächst müssen wir uns auf einige gesellschaftliche Grundprinzipien im Umgang mit Daten und datenverarbeitenden Systemen verständigen. Dies brauchen wir nicht von Null an zu tun, es gibt vielversprechende Anknüpfungspunkte. Der jüngst herausgegebene Bericht der British Academy und der Royal Society "Data management and use: Governance in the 21st century" formuliert beispielsweise solche grundlegenden Prinzipien, die auf der Grundannahme fußen "that society does not serve data but that data should be used to serve human communities"[99]. Daten sind eben nicht nur ein Rohstoff, wie es das Öl in früheren Tagen war. Daten sind viel wandlungsfähiger, potenzialreicher und letztlich etwas ganz anderes als ein gewöhnlicher Rohstoff. Nicht zuletzt können sie - je nach Kontext und Verwendung - auch (sozialer, politischer, ökonomischer) Sprengstoff sein, wie beispielsweise die Debatte um Wählerbeeinflussung durch sogenanntes Micro Targeting zeigt.[100]

Natürlich braucht es daneben auch praktische Datensteuerungsansätze, die zwar auf einer hohen institutionellen Ebene ansetzen, sich am Ende aber ganz konkret in der gestuften Zugänglichkeit von Daten innerhalb und außerhalb von Institutionen niederschlagen. Was größere und mittlere Unternehmen etwa schon seit geraumer Zeit unter dem Stichwort "Data Governance" implementieren, um die Datenflüsse in- und außerhalb ihrer Grenzen zu organisieren, das haben öffentliche Institutionen erst seit relativ kurzer Zeit und meist im Zuge der Bereitstellung von Regierungsdaten (Open Government Data) als Desiderat erkannt.[101] Auf dem europäischen Kontinent weit fortgeschritten ist man in Österreich, wo über die vergangenen Jahre im Rahmen eines Open-Government-Vorgehensmodells ein inzwischen schon recht reifes Data-Governance-Modell für Institutionen der öffentlichen Hand entwickelt wurde.[102] Wenn sich etwa jede in den Geltungsbereich des neuen deutschen Open-Data-Gesetzes fallende Bundesbehörde an diesem Modell

99 British Academy & Royal Society (2017). *Data management and use: Governance in the 21st century,* S.9 (online) https://royalsociety.org/~/media/policy/projects/data-governance/data-management-governance.pdf

100 Vgl. Albright, J. (2017). Who Hacked the Election? Ad Tech did. *Tow Center* on Medium (online)

101 Was erstaunlich ist, weil Institutionen der öffentlichen Hand eigentlich nichts anderes als Bereitsteller und Verwalter von für die Allgemeinheit relevanten Informationen und Ressourcen sind.

102 KDZ & Stadt Wien (2016). Open-Government-Vorgehensmodell. Umsetzung von Open Government (Version 3.0), S.18-36 (online) http://kdz.eu/de/open-government-vorgehensmodell

für die Organisation von behördlichen Datenflüssen orientieren würde, wäre schon viel gewonnen. Denn der größte Profiteur eines professionellen Datenmanagements seitens der Verwaltung wäre die Verwaltung selbst, wie wir in der Debatte um offene Regierungsdaten in Deutschland seit 2015 wieder betont haben.[103]

Teil einer jeden effektiven Datensteuerung, ob im öffentlichen oder im privatwirtschaftlichen Bereich, müssen - und hier wiederholen wir uns zum Ende gerne - avancierte technische Maßnahmen sein. Eine Möglichkeit, Daten zu nutzen und Datenschutzrisiken von vornherein zu minimieren, ist beispielsweise der Einsatz restriktiver Zugangsmechanismen. Hier bieten sich beispielsweise Verschlüsselungsverfahren wie "identity-based encryption" und "attribute-based encryption" an. Diese ermöglichen es, geschützte Daten für die exklusive Nutzung bestimmter Personengruppen bereitzustellen. Eine dritte Partei (z.B. eine zertifizierte Instanz) hat selbst keinen Zugang zu den Daten, ist aber befugt, deren Freigabe zu autorisieren. Weitere, in jüngerer Zeit entwickelte und in ihrem Potenzial noch nicht oder jedenfalls nicht vollständig erschlossene technische Verfahren der Datenkontrolle und -vertraulichkeit könnten an dieser Stelle genannt werden, etwa Differential Privacy, Homomorphe Verschlüsselung, Secure Multi-party Computation oder Safe-answer-Verfahren. Ohne diese Verfahren hier im Einzelnen vorstellen zu können, so verweist schon diese Aufzählung auf das noch unausgeschöpfte technische Potenzial für einen zugleich produktiven und sicheren Umgang mit Daten jenseits traditioneller Fehden, die unter dem Stichwort "Datenschutz" geführt werden. Deutschland zählt (noch?) nicht in all diesen Bereichen zur Speerspitze der internationalen Forschung und Entwicklung. Fraunhofer IESE hat beispielsweise ein anwendungsreifes technisches Tool der Datennutzungskontrolle im Industriebereich entwickelt; mit diesem lässt sich ein zielgenauer Zugang zu spezifischen Datenbereichen in größeren Datensätzen für bestimmte Personengruppen einrichten.[104] Es stünde dem EU-Mitglied Deutschland, auf dessen Datenschutztradition das aktuelle europäische Datenschutzregime der DSGVO wesentlich beruht, und das sich zugleich als Technologie-Vorreiter begreift, gut zu Gesicht, mehr Anstrengungen in Privacy Enhancing Technologies (PET) zu investieren und diesen Bereich in Forschung und Entwicklung sowie gegebenenfalls auch im Hinblick auf die Erprobung von Geschäftsmodellen staatlich zu fördern. Da es gewissermaßen schon fünf nach zwölf ist, müssen derlei Anstrengungen jetzt unternommen werden.

Erst ganz zum Schluss, gewissermaßen als Ultima Ratio, wären eventuell auch neue Regulierungsansätze in Betracht zu ziehen, sollte sich in einigen Jahren herausgestellt haben, dass die Datenschutzgrundverordnung und die in ihrem Fahrwasser entstandenen Privacy-by-design-Lösungen alleine noch

103 Vgl. Knobloch, T. & Manske, J. (2016). Das Datenzeitalter gestalten. Offene Daten sind der Schlüssel. *SNV Policy Paper* (online) https://www.stiftung-nv.de/sites/default/files/snv_datenzeitalter-gestalten_7.7.2016.pdf

104 Vgl. Fraunhofer IESE (2017). IND²UCE Framework (online) https://www.iese.fraunhofer.de/de/competencies/security/ind2uce-framework.html

nicht die erhoffte Wende zum Guten in der Datengesellschaft gebracht haben. Dafür gibt es bereits erste Beispiele: Australien hat unter dem Eindruck von De-Anonymisierungen von Gesundheitsdaten im vergangenen Jahr, zu denen auch offene Regierungsdaten herangezogen wurden, das gezielte De-Anonymisieren 2016 schlicht unter Strafe gestellt.[105] Die britische Regierung bereitet im Zuge der Reform der Privacy Bill derzeit eine ähnliche Maßnahme vor, wie Digitalminister Matt Hancock auf der Tech Crunch Disrupt im Sommer dieses Jahres verkündet hat.[106] Solche neuen regulativen Schritte werden von Wissenschaftlern und Vertretern der Zivilgesellschaft allerdings auch kritisiert, zum Beispiel weil Vulnerabilitätstests im Sinne des Privatsphärenschutzes durchaus zu einer erhöhten Sicherheit beitragen können. Auch ist unklar, wer in Fällen unbeabsichtigter De-Anonymisierung haften sollte. Durchweg plausibel erscheint es momentan allenfalls, die bewusste Weitergabe und den Handel mit de-anonymisierten Daten unter Strafe zu stellen.

Wir leben in einer Zeit, da sich Autofahrer alleine durch Auswertung ihrer individuellen Bremspedalbetätigungen auf gleicher Teststrecke mit großer Sicherheit eindeutig identifizieren lassen.[107] Daten sind in gewisser Weise zu einem Allmachtsmittel geworden[108] und Software dematerialisiert regelrecht die Welt[109]. Vor dem Hintergrund solcher Potenziale haben wir keine andere Wahl als bestimmte Datennutzungs- und Auswertungsmöglichkeiten gesellschaftlich und/oder gesetzlich zu ächten. Wir haben hier dafür plädiert, dass jedoch gleichzeitig sowohl starke technische Maßnahmen der Risikominimierung als auch adäquate institutionelle, bereichsspezifische und gesellschaftliche Datenmanagement-Ansätze unerlässlich sind, wenn wir gesell-

105 Vgl. https://www.legislation.gov.au/Details/C2016B00156/Html/Text

106 Vgl. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf
TechCrunch-Bericht zur Ankündigung Hancocks für Großbritannien unter https://techcrunch.com/2017/08/08/uk-to-criminalize-re-identifying-anonymized-personal-data/

107 Vgl. Enev, M.; Takakuwa, A.; Koscher, K. & Kohno, T. (2016). Automobile Driver Fingerprinting. *Proceedings on Privacy Enhancing Technologies* 2016 (1), S.34–51 (online) http://www.autosec.org/pubs/fingerprint.pdf; Kompaktdarstellung der Studie in Greenberg, A. (2016). A Car's Computer Can ‚Fingerprint' You in Minutes Based on How You Drive. *Wired* am 25.5.2016 (online) https://www.wired.com/2016/05/drive-car-can-id-within-minutes-study-finds/

108 Vgl. Knobloch, T. (2017). Allmachtsmittel Daten (Teile 1 & 2). *Forum Wirtschaftsethik* (online) https://www.forum-wirtschaftsethik.de/allmachtsmittel-daten/

109 Vgl. Land, K.-H. (2017). Dematerialisierung - Die Neuverteilung der Welt. *LinkedIn Pulse* am 27.10.2017 (online) https://www.linkedin.com/pulse/dematerialisierung-die-neuverteilung-der-welt-karl-heinz-land/

schaftlich nützliche Datennutzungen fördern und schädliche unterbinden wollen.

Literatur

Airbnb (2017). Airbnb Datenschutzerklärung. 3.13 Unternehmenszusammenschlüsse (online) https://www.airbnb.de/terms/privacy_policy

Albright, J. (2017). Who Hacked the Election? Ad Tech did. Tow Center on Medium (online) https://medium.com/tow-center/who-hacked-the-election-43d4019f705f

Anger, H. (2017). Gesichtsscan im Supermarkt ist unbedenklich. In: Handelsblatt (online) http://www.handelsblatt.com/politik/deutschland/datenschuetzer-zu-real-werbebildschirm-gesichtsscan-im-supermarkt-ist-unbedenklich/19921456.html

Article 29 Data Protection Working Party (2014). Opinion 05/2014 on Anonymisation Techniques (online) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Bernal, P. (2014). Internet Privacy Rights: Rights to Protect Autonomy. Cambridge: Cambridge University Press.

Bernard, A. (2017). Komplizen des Erkennungsdienstes: Das Selbst in der digitalen Kultur. Frankfurt/M.: S. Fischer.

Bindi, T. (2017). Bose accused of tracking and sharing customer listening data: Report. In: ZDNet (online) http://www.zdnet.com/article/bose-accused-of-tracking-and-sharing-customer-listening-data-report/

Boehmanwaltskanzlei (2015). Grundprinzipien des Datenschutzes (online) https://boehmanwaltskanzlei.de/kompetenzen/medienrecht/datenschutzrecht/datenschutz/grundprinzipien/212-grundprinzipien-des-datenschutzes

British Academy & Royal Society (2017). Data management and use: Governance in the 21st century (online) https://royalsociety.org/~/media/policy/projects/data-governance/data-management-governance.pdf

Brynjolfsson, E. & McAfee, A. (2014). The Second Machine Age: Work, Progress and Prosperity in a Time of Brilliant Technologies. New York / London: W.W. Norton & Company

Bull, H.P. (2015). Sinn und Unsinn des Datenschutzes. Tübingen: Mohr Siebeck

Christl, W.; Spiekermann, S. (2016). Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Wien: Facultas

Crawford, K. (2013). The Hidden Biases in Big Data. Harvard Business Review (online) https://hbr.org/2013/04/the-hidden-biases-in-big-data

Datatilsynet (2015). The Great Data Race: How commercial utilisation of personal data challenges privacy, Report November 2015 (online) https://www.datatilsynet.no/globalassets/global/english/engelsk-kommersialisering-endelig.pdf

Datenschutzbeauftragter INFO (2016). Grundverordnung: Anforderungen an eine Einwilligung (online) https://www.datenschutzbeauftragter-info.de/grundverordnung-anforderungen-an-eine-einwilligung/

De Montjoye, Y.-A.; C. Hidalgo, C.; Verleysen, M.; Blondel, V. (2013). Unique in the Crowd: The privacy bounds of human mobility. In: Nature (Scientific Reports) (online) https://www.nature.com/articles/srep01376

De Montjoye, Y.-A.; Radaelli, L.; Singh, V. K.; Pentland, A. S. (2015). Unique in the shopping mall: On the reidentiability of credit card metadata. In: Science, 347 (6221), S. 536–539.

DSK (2017). Grundsatzpositionen und Forderungen für die neue Legislaturperiode (online) https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/datenschutz-und-informationsfreiheit-als-elemente-einer-stabilen-demokratie

Elliot, M.; Mackey, E.; O'Hara, K.;Tudor, C. (2016). The Anonymisation Decision-Making Framework. Manchester: UKAN (University of Manchester).

Enev, M.; Takakuwa, A.; Koscher, K. & Kohno, T. (2016). Automobile Driver Fingerprinting. Proceedings on Privacy Enhancing Technologies 2016 (1), S.34–51 (online) http://www.autosec.org/pubs/fingerprint.pdf

European Commission (2015). Data Protection Report, Special Eurobarometer 431, S.4 (online) http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

European Commission (2017). State of the Union 2017: A framework for the free flow of non-personal data in the EU. Brussels, 19 September 2017 (online) http://europa.eu/rapid/press-release_IP-17-3190_en.htm

European Data Protection Supervisor (2016). EDPS Opinion on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data. Opinion 9/2016 (online) https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

Federal Trade Commission (2014). Data Broker: A Call for Transparency and Accountability (online) https://www.ftc.gov/system/files/documents/reports/data-brokers-call-

transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Finley, K. (2017). The FCC seems unlikely to stop internet providers from selling your data. In: Wired (online) https://www.wired.com/2017/03/fcc-graciously-sets-internet-providers-free-sell-data/

Fraunhofer IESE (2017). IND²UCE Framework (online) https://www.iese.fraunhofer.de/de/competencies/security/ind2uce-framework.html

Greenberg, A. (2016). A Car's Computer Can ‚Fingerprint' You in Minutes Based on How You Drive. Wired am 25.5.2016 (online) https://www.wired.com/2016/05/drive-car-can-id-within-minutes-study-finds/

Günther, O.; Hornung, G.; Rannenberg, K.; Roßnagel, A.; Spiekermann, S. & Waidner, M. (2013). Auch anonyme Daten brauchen Schutz. Zeit Online vom 14.2.2013 (online) http://www.zeit.de/digital/datenschutz/2013-02/stellungnahme-datenschutz-professoren/komplettansicht

Hasselbalch, G. & Tranberg, P. (2016). Data Ethics: The New Competitive Advantage. Copenhagen.

Higgins, T. (2017). SoftBank Leads $164 Million Bet on Digital-Mapping Startup Mapbox. Technology is key to self-driving vehicles. The Wall Street Journal (online) https://www.wsj.com/articles/softbank-leads-164-million-bet-on-digital-mapping-startup-mapbox-1507640404

Hoepner, P. (2017). Datenschutz und Technik, ein Informationspapier. Kompetenzzentrum Öffentliche IT (online) http://www.oeffentliche-it.de/documents/10181/14412/Datenschutz+und+Technik+-+Ein+Informationspapier

Hoffmann, J.; Bergmann, B. (2017). Die informierte Einwilligung: Ein Datenschutzphantom. In: Netzpolitik.org (online) https://netzpolitik.org/2017/die-informierte-einwilligung-ein-datenschutzphantom/

Horn, N.; Riechert, A.; Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. In: Stiftung Datenschutz, S. 7-57 (online) https://stiftungdatenschutz.org/fileadmin/

Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf

If (2017). Design Patterns (online) https://projectsbyif.com/projects/data-sharing-design-patterns

Isaac, M.; Lohr, S. (2017). Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data. In: The New York Times (online) https://www.nytimes.com/2017/04/24/technology/personal-data-firm-slice-unroll-me-backlash-uber.html

Jaume-Palasí, L. & Spielkamp, M. (2017). Ethik und algorithmische Prozesse zur Entscheidungsfindung oder -vorbereitung. AlgorithmWatch Arbeitspapier Nr. 4 (online) https://algorithmwatch.org/wp-content/uploads/2017/06/AlgorithmWatch_Arbeitspapier_4_Ethik_und_Algorithmen.pdf

Jeffries, A. (2017). Machine learning is racist because the Internet is racist. Deep learning algorithms are often trained on data from the web, and their biases are getting hard to ignore. The Outline (online) https://theoutline.com/post/1439/machine-learning-is-racist-because-the-internet-is-racist

Jentzsch, N. (2016). State-of-the-Art of the Economics of Privacy and Cybersecurity. IPACSO - Innovation Framework for ICT Security Deliverable; 4.1 (online) https://www.econstor.eu/handle/10419/126223

Kammourieh, L.; Baar, T.; Berens, J.; Letouzé, E.; Manske, J.; Palmer, J.; Sangokoya, D.; Vinck, P. (2017). Group Privacy in the Age of Big Data. In: Taylor, L.; Floridi, L.; van

der Sloot, B. (Hrsg.). Group Privacy: New Challenges of Data Technologies. Dordrecht: Springer

Kaye, K (2015). The $24 Billion Data Business That Telcos Don‘t Want to Talk About. In: AdvertisingAge (online) http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058//

KDZ & Stadt Wien (2016). Open-Government-Vorgehensmodell. Umsetzung von Open Government (Version 3.0), S.18-36 (online) http://kdz.eu/de/open-government-vorgehensmodell

Kläsgen, M.; Martin-Jung, H. (2017). Abgescannt im Supermarkt. In: Süddeutsche Zeitung (online) http://www.sueddeutsche.de/wirtschaft/ueberwachung-im-supermarkt-abgescannt-im-supermarkt-1.3529017

Knobloch, T. & Manske, J. (2016). Das Datenzeitalter gestalten. Offene Daten sind der Schlüssel. SNV Policy Paper (online) https://www.stiftung-nv.de/sites/default/files/snv_datenzeitalter-gestalten_7.7.2016.pdf

Knobloch, T. (2017). Allmachtsmittel Daten (Teile 1 & 2). Forum Wirtschaftsethik (online) https://www.forum-wirtschaftsethik.de/allmachtsmittel-daten/

Knobloch, T. & Manske, J. (2017). Responsible Use of Data. Cooperation & Development am 11.1.2017 (online) https://www.dandc.eu/en/article/opportunities-and-risks-user-generated-and-automatically-compiled-data

Krempl, S. (2017). De Maizière hält Losung “Meine Daten gehören mir” für falsch. heise am 18.2.2017 (online) https://www.heise.de/newsticker/meldung/De-Maiziere-haelt-Losung-Meine-Daten-gehoeren-mir-fuer-falsch-3630322.html

Kroft, S. (2014). The Data Brokers :Selling Your Personal Information. In: CBS News (online) https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/

Kupfer, D. (2015). Datenschutzrecht im Internet der Dinge. In: Jaxenter (online) https://jaxenter.de/datenschutzrecht-im-internet-der-dinge-16535

Manske, J. (2016): Offene Daten und der Schutz der Privatsphäre. SNV Policy Brief (online) https://www.stiftung-nv.de/de/publikation/offene-daten-und-der-schutz-der-privatsphaere

Manske, J. & Knobloch, T. (2017). Leitfaden für Datenschutz bei Open Data. Ansätze und Instrumente für die verantwortungsvolle Öffnung von Verwaltungsdaten. SNV

Policy Brief (online) https://www.stiftung-nv.de/sites/default/files/policy_brief_leitfaden_open_data_datenschutz.pdf

Meyer, R. (2015). Could a Bank Deny Your Loan Based on Your Facebook Friends? The Atlantic (online) https://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287/

Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. In: Philosophy & Technology (online) https://link.springer.com/article/10.1007%2Fs13347-017-0253-7

Narayanan, A.; Shmatikov, V. (2007). Robust De-anonymization of Large Sparse Datasets (online) https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

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

Nissenbaum, H. (2011): A Contextual Approach to Privacy Online. In: Daedalus, 140 (4), S. 32-48 (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567042

Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, 2010 (Vol. 57), S. 1701- 1777. Auch in: University of Colorado Law Legal Studies (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

Oostveen, M. & Irion, K. (2017). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? Amsterdam Law School Research Paper No. 2016-68, S.9 (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885701

Rähm, J. (2015). Gefahren und Chancen der digitalisierten Welt. In: Deutschlandfunk (online) http://www.deutschlandfunk.de/hintergrund.723.de.html

Reinbold, F. (2017). Wirtschaft soll mehr Daten sammeln dürfen. In: Spiegel Online (online) http://www.spiegel.de/netzwelt/netzpolitik/geschaeft-mit-daten-cdu-will-sparsamkeit-beenden-a-1151862.html

Reuter, M. (2016). Neues Bundesdatenschutzgesetz: Weniger Kontrolle, weniger Auskunftsansprüche, mehr Videoüberwachung. Netzpolitik.org am 24.11.2016 (online) https://netzpolitik.org/2016/neues-bundesdatenschutzgesetz-weniger-kontrolle-weniger-auskunftsansprueche-mehr-videoueberwachung/

Rieke, A.; Yu, H.; Robinson, D.; von Hoboken, J. (2016). Data Brokers in an Open Society. In: Upturn (Open Society Foundation London) (online) https://www.opensocie-

tyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf

Rhoen, M. (2016). Beyond consent: improving data protection through consumer protection law. In: Internet Policy Review, 5 (1) (online) https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law

Samarati, P. & Sweeney, L (1998). k-anonymity: a model for protecting privacy. Proceedings of the IEEE Symposium on Research in Security and Privacy (S&P). May 1998, Oakland CA. Online verfügbar unter https://dataprivacylab.org/dataprivacy/projects/kanonymity/index3.html

Schulzki-Haddouti, C. (2017). EU-Copyright-Reform: Einschränkung von Text- und Data-Mining droht. heise am 18.19.2017 (online) https://www.heise.de/newstikker/meldung/EU-Copyright-Reform-Einschraenkung-von-Text-und-Data-Mining-droht-3864658.html

Schürmann Wolschendorf Dreyer Rechtsanwälte (2016). EU-Datenschutzgrundverordnung (DSGVO) (online) https://www.swd-rechtsanwaelte.de/blog/eu-datenschutzgrundverordnung-dsgvo/

Steltemeier, R. (2015). Liberalismus. Ideengeschichtliches Erbe und politische Realität einer Denkrichtung. Baden-Baden: Nomos.

Sweeney, L. (2005): Testimony to the Department of Homeland Security, S.2 (online) https://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf

The Economist (2017). The world's most valuable resource is no longer oil, but data (online) https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resourcev

Tockar, A. (2014). Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset. In: Neustar Research (online) https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/

Vodafone Institut für Gesellschaft und Kommunikation (2016). Big Data. Wann Menschen bereit sind, Daten zu teilen: Eine Europäische Studie (online) http://www.

vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-Highlights-de.pdf

VZBV (2017). Beim Shoppen auf Schritt und Tritt überwacht (online) https://www.vzbv.de/pressemitteilung/beim-shoppen-auf-schritt-und-tritt-ueberwacht

Wachter, S.; Mittelstadt, B. & Floridi, L. (2016). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law, Forthcoming (online) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

Warren, S.D. & Brandeis, L.D. (1890). The Right to Privacy. Harvard Law Review 4 (5), S.193-220.

Zuboff, S. (2014). A Digital Declaration. Frankfurter Allgemeine Zeitung am 14.9.2014 (online) http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshan-zuboff-on-big-data-as-surveillance-capitalism-13152525.html

Zuiderveen Borgesius, F.J. (2015). Personal data processing for behavioural targeting: which legal basis? International Data Privacy Law 5 (3), S.163–176.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über das Projekt

Das Projekt “Datenpolitik” analysiert aktuelle Entwicklungen der Steuerung von Datenflüssen. Es prüft die Tauglichkeit etablierter Modelle (z.B. Datenschutz oder Open Data) und die Relevanz neuer Entwicklungen aus technischer, rechtlicher, politischer und gesellschaftlicher Sicht. Darauf aufbauend entwickelt und testet das Projekt im Austausch mit Experten aus allen Sektoren Vorschläge zu einem zeitgemäßen Umgang mit Daten, der über einen rein (datenschutz-)rechtlichen Blickwinkel hinausgeht. Im Zentrum des Projektes stehen folgende Fragen: Wie können wir Datenflüsse transparenter machen? Welche Instrumente brauchen wir, damit die Bürgerinnen Kontrolle über ihre persönlichen Daten (zurück) zu erlangen? Welche Grundprinzipien müssen bei der Nutzung von digitalen Daten gelten, und wie können diese Prinzipien praktisch implementiert werden?

So erreichen Sie die Autoren

Julia Manske
Stellvertretende Projektleiterin
"Open Data & Privacy"
jmanske@stiftung-nv.de
+49 (0)30 81 45 03 78 92

Dr. Tobias Knobloch
Projektleiter "Datenpolitik"
tknobloch@stiftung-nv.de
+49 30 814 503 7893

Impressum

stiftung neue verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Kostenloser Download:

www.stiftung-nv.de