Vodafone Institut
für Gesellschaft
und Kommunikation

BIG DATA
ETHISCHE FRAGEN

Ein Report von Anna Wehofsits

Herausgegeben vom Vodafone Institut für Gesellschaft und Kommunikation, Oktober 2016

Inhalt

Vorwort
Von David Deißner

Daten, so hört man immer wieder, seien „das Öl des 21. Jahrhunderts“. Wer diesen inzwischen etwas abgenutzten Vergleich bemüht, will sagen: Daten sind die zentrale Ressource unserer Zeit, eine unverzichtbare Quelle der Wertschöpfung, ein „Treibstoff“ moderner Ökonomien. Der Gesellschaft verspricht er Wachstum, cleveren Pionieren schnellen Reichtum. Die „Data-Miner“, schon der Begriff legt es nahe, stehen in der Erbfolge der Goldgräber und Ölsucher des 19. Jahrhunderts, nur dass sie nicht in der Erde wühlen, sondern in unermesslich großen Datenhaufen, in denen sich wertvolle Erkenntnisse verbergen.

Tatsächlich liegt die Erkundungsphase schon längst hinter uns: Big Data hat sich während der letzten Jahre nachweislich zu einem zentralen Wachstumstreiber entwickelt, nicht nur für Digitalwirtschaft und Online-Werber, sondern auch für klassische Handels- und Industrieunternehmen, die durch computergestützte Datenanalyse ihre Kunden besser verstehen oder interne Prozesse optimieren.

Wer Daten mit Öl vergleicht, verweist aber auch – möglicherweise unfreiwillig – auf die konfliktreiche Historie eines blutig umkämpften Rohstoffs. Der Vergleich verliert seine Leichtigkeit, wenn man sich vergegenwärtigt, dass Öl nicht nur Treibstoff der Industrialisierung, sondern auch Auslöser von Kriegen und andauernden geopolitischen Verwerfungen war. So gesehen bestünde die Herausforderung unserer Zeit darin, alles dafür zu tun, dass sich die noch junge Geschichte der Datenanalyse eben nicht zu einer Geschichte des Öls entwickelt – in weiten Teilen

eine Geschichte der autokratischen Kontrolle. Wenn wir vermeiden wollen, dass die Datenrevolution, mit der sich so viel Hoffnungen verbinden, am Ende ihre eigenen Kinder frisst, also Ungleichheit und Konflikte statt Teilhabe befördert, brauchen wir faire und transparente Nutzungsregeln, verbindliche rechtliche und ethische Standards sowie aufgeklärte Nutzer.

Welche Daten dürfen für welche Zwecke gesammelt, gespeichert und ausgewertet werden? In welchem Verhältnis steht der gesamtgesellschaftliche Mehrwert, den eine bestimmte Big-Data-Lösung verspricht, mit individuellen Persönlichkeitsrechten wie dem Schutz der Privatsphäre? Dürfen Daten im Interesse des Gemeinwohls – etwa für Stadtplanung oder Katastrophenschutz – genutzt werden, auch wenn sie anfänglich für andere Zwecke gesammelt wurden? Wie gehen wir damit um, dass die für Stadtentwicklung, öffentliche Statistik, Gesundheitsvorsorge und Katastrophenschutz besonders wertvollen Daten heute nicht in der Hand öffentlicher Institutionen, sondern in der Hand von Unternehmen liegen, deren Kunden diese Daten gleichsam als Nebenprodukt ihres digitalen Alltags produzieren? Welche Standards müssen gelten, wenn diese Daten geteilt und genutzt werden?

Die jüngere Geschichte hat gezeigt, dass weder private Unternehmen noch der Staat bei diesen Fragen moralische Erhabenheit genießen. Es sollte daher weder einzelnen Behörden noch den Unternehmen allein überlassen werden, die Spielregeln für das Datenzeitalter festzulegen. Stattdessen brauchen wir eine breite gesellschaftliche und politische Diskussion. Dabei dürfte klar sein: Ein Zurück wird es nicht geben. Auch wenn die allgegenwärtige Produktion, Sammlung und Analyse von Daten den ein oder anderen mit Unbehagen erfüllen mag: Big Data als technologisch-gesellschaftlichen Megatrend schlichtweg abzulehnen, wäre nicht nur kulturpessimistisch, sondern naiv: Big Data rettet schon heute Menschenleben, ermöglicht zielgenaue Intervention bei schweren Krankheiten, hilft bei der Früherkennung lebensbedrohlicher Krankheiten auf Säuglingsstationen, macht Entwicklungshilfe effektiver und hilft, die Ausbreitung von Epidemien vorauszusagen. Auch der öffentliche Sektor könnte durch Big Data Milliarden einsparen. Die durch Datenanalyse ermöglichten Erkenntnisse zu verhindern, indem man einzelne Schutzgüter absolut setzt, wäre mithin antiaufklärerisch. Oder, wie es der Daten-Experte des Economist, Kenneth Cukier, unlängst auf einer Veranstaltung des Vodafone Instituts provokativ formulierte: „Not using data is like burning books“.

Vielmehr muss es darum gehen, die sozialen, wissenschaftlichen und ökonomischen Chancen, die sich mit der Sammlung und Analyse von Daten eröffnen, optimal zu nutzen und zugleich Schutzmechanismen und Standards zu etablieren,

die Marktmachtkonzentration, Fremdbestimmung und mögliche Diskriminierung einzelner Konsumenten oder Gesellschaftsgruppen verhindern. Vor allem aber wird es darum gehen, sicherzustellen, dass die Nutzer die Kontrolle über ihre Daten haben und von ihrer Autonomie auch Gebrauch machen. „Data Literacy" gehört zur staatsbürgerlichen Grundausstattung eines jeden Menschen, der sich in der digitalen Welt autonom bewegen können soll, und verdient einen Platz in den Lehrplänen unserer Schulen.

Die gängige Praxis der „informierten Einwilligung" durch hilfloses Akzeptieren seitenlanger Nutzungsbedingungen ist dagegen wenig zielführend. Aber auch bei vereinfachter Darstellung wäre der einzelne Nutzer überfordert, wenn er alle Entscheidungen der Datenpreisgabe allein treffen müsste. Es bedarf daher unterstützender Schutzmechanismen. In einer Welt der kommunizierenden Dinge, in der wir allein durch den Gebrauch diverser Alltagsgegenstände Datenspuren hinterlassen, eine Welt, in der Algorithmen Entscheidungen übernehmen, müssen der Schutz der Privatheit und mögliche Diskriminierungen schon von den Entwicklern mitgedacht werden. Diese Forderung verbindet sich mit dem Begriff „privacy by design".

Das Vodafone Institut für Gesellschaft und Kommunikation widmet sich seit etwa zwei Jahren der Frage nach den ethischen und rechtlichen Standards von Big Data. In Workshops und Konferenzen diskutieren wir europaweit mit Vertretern aus Wirtschaft, Politik, Wissenschaft und Zivilgesellschaft über die Spielregeln des Datenzeitalters. Der vorliegende Bericht steht im Zusammenhang dieses sektorübergreifenden Dialogs. Unsere Autorin Dr. Anna Wehofsits, Philosophin an der Ludwigs-Maximilians Universität München, sprach mit international führenden Wissenschaftlern und Meinungsführern – Juristen, Philosophen und Computerwissenschaftler – aus dem In- und Ausland über die ethische Dimension von Big Data. Auf Grundlage ausführlicher Interviews entstand ein „panoramatischer Überblick" über die ethische „Herausforderungslandschaft" Big Data. Im Zentrum steht die Frage, inwiefern Big Data-Anwendungen mit dem Recht auf informationelle Selbstbestimmung in Konflikt geraten (können), welche Schäden aus der Preisgabe personenbezogener Daten entstehen können – und welche normativen Konsequenzen sich hieraus ergeben.

Wir wünschen Ihnen eine anregende Lektüre!

Dr. David Deißner leitet Strategie und Programme des Vodafone Instituts.

1

Die Welt abbilden

David Foster Wallace bringt das Versprechen von *Big Data* auf eine einfache Formel: „Terrain = Map“.[1] Diese Formel zitiert ein altes Phantasma der Literaturgeschichte, das schon Lewis Carroll, Jorge Louis Borges und Umberto Eco fasziniert hat: Eine Karte im Maßstab 1:1, die als perfektes Abbild der Wirklichkeit ohne jede Generalisierung, ohne Abstraktionen und Vereinfachungen auskommt. Jedes noch so winzige Detail wird von der Karte erfasst. In seiner Miniatur „Von der Strenge der Wissenschaft“ beschreibt Borges eine solche Karte als Höhe- und zugleich Endpunkt der Kunst der Kartographie in einem namenlosen Reich der Vergangenheit:

„In jenem Reich erlangte die Kunst der Kartographie eine solche Vollkommenheit, daß die Karte einer einzigen Provinz den Raum einer Stadt einnahm und die Karte des Reichs den einer Provinz. Mit der Zeit befriedigten diese maßlosen Karten nicht länger, und die Kollegs der Kartographen erstellten eine Karte des Reiches, die die Größe des Reiches besaß und sich mit ihm in jedem Punkte deckte. Die nachfolgenden Geschlechter, die dem Studium der Kartographie nicht mehr so ergeben waren, waren der Ansicht, diese ausgedehnte Karte sei unnütz, und überließen sie, nicht ohne Verstoß gegen die Pietät, den Unbilden der Sonne und der Winter.“[2]

1 Foster Wallace 2004, S. 64.

2 Borges 1982, S. 121.

Die Karte, obwohl oder gerade weil perfekt, verfehlt ihren Zweck. Ihre Detailgenauigkeit überfordert den Betrachter und kann ihm keine bessere Orientierung geben als die Wirklichkeit selbst. Die Karte des Reichs in der Größe des Reichs ist damit nutzlos und bedeutet das Ende der Kartographie.

Die Erwartungen an *Big Data* sind groß, wenn auch nicht ganz so groß – niemand glaubt ernsthaft an die Möglichkeit einer digitalen Datenkarte im Maßstab 1:1, also daran, dass sich die Wirklichkeit vollständig digital erfassen lässt. Spürbar aber ist die Hoffnung, die neuen computerbasierten Techniken zur Sammlung, Speicherung und Auswertung von Daten könnten zu einer Revolution der empirischen Erkenntnisproduktion führen und die Analyse von Datenmengen ermöglichen, die so groß oder komplex strukturiert sind, dass sie die menschlichen Erkenntnisvermögen überfordern und mit herkömmlichen Methoden der Informationsverarbeitung nicht bearbeitbar wären. Dort, wo Menschen die Orientierung verlieren und traditionelle statistische Verfahren teils zu gravierenden Fehleinschätzungen führen, sollen digitale Datenspeicher und leistungsstarke Algorithmen die Arbeit der Erkenntnisproduktion übernehmen. Mit *Big Data* verbindet sich die Hoffnung, Paul Valéry möge unrecht haben, wenn er schreibt: „Alles Einfache ist falsch, alles Komplizierte unbrauchbar.“[3]

Nach dem Wissenschaftstheoretiker Wolfgang Pietsch bereitet *Big Data* tatsächlich den Weg für eine „neue Wissenschaft des Komplexen“, die das Komplizierte nicht vereinfachen muss, um es für uns brauchbar zu machen. Zwei Kriterien lassen sich in diesem Zusammenhang besonders hervorheben: Erstens eine zunehmende Automatisierung der wissenschaftlichen Forschung, die von der Datenerfassung über ihre Verarbeitung bis hin zur Modellbildung reicht und darüber die epistemischen Rahmenbedingungen wissenschaftlicher Forschung grundlegend erweitert. Die Automatisierung erlaubt es, riesige Datenmengen und Stichprobenzahlen zu erfassen und zu verarbeiten. Dies macht es zweitens möglich, die wechselseitige Abhängigkeit einer großen Anzahl von Parametern zu untersuchen und Korrelationen aufzudecken, die es erlauben, zukünftige Entwicklungen der jeweiligen Abhängigkeitsbeziehungen vorherzusagen, ohne dafür „die Einbindung in einen erklärenden theoretischen Kontext“ zu benötigen.[4] In der Regel sollte eine solche Einbindung, so der Informatiker und Technikjournalist Jürgen Geuter, jedoch das Ziel späterer Forschungsschritte sein.[5]

3 „Ce qui est simple est toujours faux. Ce qui ne l‘est pas est inutilisable.“ Valéry 1960, S. 864.

4 Pietsch 2013.

5 Geuter 2015.

Das automatisierte Auffinden von Korrelationen ist in verschiedenen Anwendungskontexten sehr nützlich. Ein eindrucksvolles und viel zitiertes Beispiel ist die Arbeit der Gesundheitsinformatikerin Carolyn McGregor. Gemeinsam mit ihrem Team hat sie ein Big-Data-Frühwarnsystem entwickelt, das die Überlebenschancen frühgeborener Kinder deutlich verbessert. Dank einer automatisierten Auswertung von Millionen Daten zu den verschiedenen Vitalfunktionen eines Kindes pro Tag lassen sich Muster erkennen, die bereits viele Stunden vor dem Auftreten charakteristischer Symptome auf Infektionen hindeuten. Zeichnet sich eine Infektion ab, können sich Ärzte auch ohne genauere Kenntnis ihres ursächlichen Zusammenhangs für eine Behandlung entscheiden und so das Leben vieler Frühgeborener retten.[6] Die Überwachung von komplizierten Therapieverläufen, die, wenn nötig, ein frühes Eingreifen erlaubt, könnte „zur Königsdisziplin von Big Data in der Medizin“ werden.[7]

Auch zur Bekämpfung von Hunger und Armut wird *Big Data* erfolgreich eingesetzt: Auf der Grundlage von sozialen, politischen, (land)wirtschaftlichen und meteorologischen Daten erstellt das Famine Early Warning System jeden Monat Landkarten und Berichte, die Regierungen und Hilfsorganisationen dabei unterstützen, drohende Ernährungskrisen frühzeitig zu erkennen.[8] Die Beratungsgruppe für Internationale Agrarforschung (Consultative Group on International Agricultural Research, CGIAR) hat gemeinsam mit ihren Partnereinrichtungen einen „Climate Wizard“ entwickelt, der Klimaveränderungen und ihre Auswirkungen so veranschaulicht, dass auch Nicht-Spezialisten sie leicht nachvollziehen können. Unter Berücksichtigung von historischen Daten und Zukunftsprognosen soll er helfen, konkrete Maßnahmen, etwa zum Schutz vor Dürren oder Überschwemmungen, zu ergreifen.[9]

Diesen Chancen stehen Risiken gegenüber. Mein Report ist konzipiert als panoramatischer Überblick über die „Herausforderungslandschaft“ *Big Data* und zielt darauf ab, für zentrale Fragen und ihre Wechselwirkungen zu sensibilisieren und Vorschläge zu ihrer ethischen Bewertung zu unterbreiten.

6 McGregor 2013; vgl. Mayer-Schönberger, S. 17.

7 Langkafel 2015, S. 31.

8 www.fews.net.

9 https://ccafs.cgiar.org/climate-wizard, http://www.climatewizard.org/.

2

Was bedeutet *Big Data*?

Die öffentliche Diskussion um *Big Data* ist geprägt von einer, nicht selten undifferenzierten, begeisterten Rhetorik einerseits und, ihrerseits nicht selten diffusen, Ängsten andererseits.

Die öffentliche Diskussion um *Big Data* ist geprägt von einer, nicht selten undifferenzierten, begeisterten Rhetorik einerseits und, ihrerseits nicht selten diffusen, Ängsten andererseits. Die Frage nach Chancen und Gefahren der Anwendung geht einer systematischen Bestimmung des Gegenstands oft voraus. Was also ist *Big Data*? Daten sind in diesem Zusammenhang als Repräsentationen von Informationen zu verstehen, die elektronisch gespeichert und verarbeitet werden können. Das Wort „big“ lädt dazu ein, die Größe der Datenmengen für das entscheidende Kriterium zu halten. Nach einer gängigen Definition sind es jedoch mindestens drei „Vs“, die das notorisch unterbestimmte Phänomen *Big Data* definieren: volume, velocity und variety.[10] Volume bezeichnet die Menge an digital verfügbaren Informationen, deren Umfang aufgrund wachsender Computerkapazitäten und fallender Speicherpreise ständig zunimmt. Variety steht für die Möglichkeit, verschiedenste Daten miteinander zu verknüpfen, einschließlich solcher, die unstrukturiert vorliegen. So können beispielsweise E-Mails, Tweets, Suchanfragen, digitale Bilder, Standort- und

10 Laney 2001.

Verbindungsdaten und zukünftig vermehrt auch Daten, die vernetzte Alltagsgegenstände wie Kaffeemaschinen, Kühlschränke oder Kleidungsstücke übermitteln, gemeinsam ausgewertet werden. Velocity schließlich bezieht sich auf zwei Formen wachsender Geschwindigkeit: Zum einen auf die Geschwindigkeit, mit der neue Daten aus unterschiedlichen Lebensbereichen erfasst werden; zum anderen auf die Geschwindigkeit, mit der digitale Daten trotz ihrer Größe und Verschiedenartigkeit ausgewertet werden können.

Allein über das Volumen der Daten ist *Big Data* also unzureichend definiert. Nach Viktor Mayer-Schönberger, der an der University of Oxford die sozialen Auswirkungen von *Big Data* erforscht, wird zudem oft falsch verstanden, worauf sich dieses Kriterium bezieht: Er argumentiert, dass es weniger auf die absolute Zahl der Daten ankommt als auf ihre relative Größe. Big-Data-Anwendungen beziehen sich nicht notwendig auf gigantische Datenmengen wie sie etwa bei der Analyse des Erbguts eines Menschen anfallen oder bei Experimenten am größten Teilchenbeschleuniger der Welt, dem Large Hadron Collider (LHC) am Europäischen Kernforschungszentrum CERN, der pro Jahr etwa 20 Petabyte an Daten erzeugt. Charakteristisch für *Big Data* ist vielmehr, dass wir „relativ zum Phänomen, oder der Frage, die wir verstehen wollen, deutlich mehr Daten sammeln und auswerten."[11] Je mehr Daten über ein Phänomen vorhanden sind, desto detaillierter kann es analysiert werden und desto geringer wird die Gefahr, dass es aufgrund von einzelnen Messfehlern zu statistischen Verzerrungen kommt.

Ist eine Datenmenge ungeeignet, um eine Frage zu beantworten, dann hilft es nicht, die Zahl der Daten einfach zu erhöhen.

Aus dieser Definition von *Big Data* über volume, velocity und variety lässt sich nicht ableiten, dass die Qualität der zugrunde gelegten Daten keine Rolle mehr spielt. Die Möglichkeit systematischer Fehler besteht weiterhin; Daten erfassen nicht immer das, worauf es ankommt. Ist eine Datenmenge ungeeignet, um eine Frage zu beantworten, dann hilft es nicht, die Zahl der Daten einfach zu erhöhen: Auch aus einer großen Umfrage lassen sich schließlich keine zuverlässigen Aussagen über das weltweite Konsumverhalten ableiten, wenn die Gruppe der Befragten nicht alle relevanten Konsumentengruppen erfasst oder nicht auf angemessene Weise. „Die Größe der Datenmenge muss zu der Fra-

11 Mayer-Schönberger 2015, S. 15.

ge passen, die man lösen möchte“, so die Medienwissenschaftlerinnen Danah Boyd und Kate Crawford; und sie fügen hinzu: „[In] manchen Fällen ist kleiner einfach besser.“[12] Rafaela Hillerbrand, Professorin für Wissenschaftsphilosophie und Technikethik am Institut für Technikfolgenabschätzung und Systemanalyse in Karlsruhe, betont deshalb ein viertes „V“, veracity (Zuverlässigkeit), das als normatives Kriterium für die Anforderung steht, immer wieder zu prüfen, mit welchen Verfahren und nach welchen Kriterien Daten erhoben und zusammengeführt werden. Schwachstellen und Unsicherheiten müssen so weitgehend wie möglich offengelegt werden. Eine hinreichende Qualitätskontrolle vorausgesetzt, sind Big-Data-Analysen nach Hillerbrand „überall dort besonders vielversprechend, wo uns Theorien fehlen und Experimente auf zu wenigen Daten beruhen“.[13] Der korrelationsbasierte Ansatz kann dabei helfen, komplexe Probleme zu lösen, die sich aus einer Vielzahl von Einflussfaktoren ergeben – etwa im Bereich der Klimaforschung, der experimentellen Ökonomie, der Verkehrssteuerung oder im Gesundheitsbereich. Es bietet sich die Chance, neue Beziehungen zwischen ganz unterschiedlichen Bereichen zu entdecken. Auch hier stammt ein unmittelbar einleuchtendes Beispiel aus dem Gesundheitsbereich: „Wenn wir wissen, dass bis zu 80 Prozent der Gesundheit von psychosozialen Faktoren abhängig ist, warum konzentrieren wir uns so sehr auf das Genom? Sind Fahrradwege (Organisation) und der Kauf eines Fahrrades (persönliches Handeln) bessere Ansatzpunkte, um Gesundheit nachhaltig zu fördern? Kann *Big Data* helfen, hier auch neue Zusammenhänge zu erkennen – sowohl auf individueller als auch auf epidemiologischer Ebene?“[14]

Der korrelationsbasierte Ansatz kann dabei helfen, komplexe Probleme zu lösen, die sich aus einer Vielzahl von Einflussfaktoren ergeben – etwa im Bereich der Klimaforschung, der experimentellen Ökonomie, der Verkehrssteuerung oder im Gesundheitsbereich.

Diese neuen Erkenntnis- und Handlungsmöglichkeiten an den Schnittstellen mehrerer Forschungsfelder bedeuten ein anderes Verständnis der Produktion empirischer Erkenntnisse, das nicht von der Frage nach kausalen Zusammenhängen ausgeht, sondern von der Beobachtung von Korrelationen. Wie groß

12 Boyd, Crawford 2013, S. 202.

13 Interview Hillerbrand.

14 Langkafel 2015, S. 31f.

die Neuerungen aber tatsächlich sind, die dieses Verständnis zeitigt, und was sie für die Zukunft bedeuten, ist umstritten: Während manche Kommentatoren einen Paradigmenwechsel prognostizieren, der grundlegend verändern wird, wie wir Wissenschaft betreiben und politische Entscheidungen treffen, erwarten andere vor allem methodische Ergänzungen und Effizienzgewinne. In jedem Fall intensivieren derzeit sowohl staatliche als auch privatwirtschaftliche Akteure ihre Bemühungen um datenbasierte Erkenntnisse und Entscheidungshilfen deutlich. Befürworter begrüßen dies als wichtigen Schritt auf dem Weg zu einer Weltgesellschaft des Wissens, die auf sozialer, wissenschaftlicher und wirtschaftlicher Ebene enorm von *Big Data* profitieren wird. Kritiker dagegen sehen darin ein Wiederaufleben der Planungseuphorie der 1960er Jahre und nicht zuletzt das Ergebnis einer „gewaltigen Werbekampagne“[15], die dem Verkauf neuer informationstechnischer Angebote und den Machtinteressen bestimmter Firmen und Berufsgruppen dient und von einer Rhetorik der Verheißung („Datenrevolution“, „Öl des 21. Jahrhunderts“) begleitet und angetrieben wird.

15 Weichert 2013, S. 2; Vgl. Interview Weichert, Cohen 2013, S. 1923 u. Interview Kurz.

3

Big Data interpretieren

Zur Kehrseite der unzweifelhaften Erfolge, die Big-Data-Analysen zum Verständnis komplexer Probleme und bei der Prognose zukünftiger Entwicklungen erzielen, gehört, dass sie ein Phänomen verstärken, das oft als „blinde Zahlengläubigkeit“ bezeichnet wird. Es lässt sich aus drei Perspektiven beobachten: (1) mit Blick auf das Verhältnis von *Big Data* und Theorie, (2) im Sinne einer Verwechslung von Kausalitäten und Korrelationen und (3) vor dem Hintergrund normativer Vorgaben und Ziele, die unbemerkt in Big-Data-Analysen einfließen und unser Realitätsverständnis prägen.

Symptomatisch für ein übermäßiges Vertrauen in die Macht der Daten ist zunächst die Vorstellung, *Big Data* könne in Zukunft alles erklären und werde alle theoretischen Ansätze und bisherigen wissenschaftlichen Methoden ersetzen. In einem viel diskutierten Artikel von 2008 verkündete Chris Anderson, damals Chefredakteur des Technologiemagazins Wired, enthusiastisch das Ende aller Theorie: „Wir leben in einer Welt, in der riesige Mengen von Daten und angewandte Mathematik alle anderen Werkzeuge ersetzen, die man sonst noch so anwenden könnte. […] Raus mit all den Theorien des menschlichen Verhaltens! Vergessen Sie Taxonomien, die Ontologie und die Psychologie! […] Hat man erst einmal genug Daten, sprechen die Zahlen für

sich selbst."[16] So radikal wird diese Position nur selten vertreten. Ein Blick in den aktuellen Diskurs zeigt jedoch, dass die Vorstellung, *Big Data* als quantitatives Verfahren der Superlative sei theoriefrei, damit auch frei von subjektiven Verzerrungen und deshalb allen theoriegeladenen Methoden überlegen, nach wie vor eine prägende Rolle spielt. Nun fließen theoretische Vorannahmen in mehreren Hinsichten in Big-Data-Analysen ein: Sie beeinflussen, wie Daten erhoben und zusammengeführt werden, nach welchen Methoden sie analysiert werden, welche Ergebnisse dabei herauskommen, und sie beeinflussen schließlich auch die Interpretation der Ergebnisse und mögliche Handlungsempfehlungen. Laut Anderson benötigt man für die Untersuchung der Daten keine Hypothesen darüber, was sich möglicherweise in ihnen verbirgt. Tatsächlich sind echte Zufallsfunde möglich und manchmal auch sehr produktiv. Wie man weiß, verdankt Alexander Fleming seine Entdeckung der Penicilline dem Zufall einer verschimmelten Bakterienkultur. In der Regel aber, so betont der Züricher Soziologieprofessor und Simulationsexperte Dirk Helbig, genügt es nicht, „einfach nur blind in den Daten herumzustochern nach dem Motto »Irgendwas werden wir schon finden«." Produktiver sei es, Daten und theoretische Modelle und damit die Stärken beider Ansätze zu kombinieren.[17] Daten sind niemals selbsterklärend, sondern müssen immer interpretativ erschlossen werden.

Theoretische Vorannahmen fließen in mehreren Hinsichten in *Big-Data*-Analysen ein: Sie beeinflussen, wie Daten erhoben und zusammengeführt werden, nach welchen Methoden sie analysiert werden, welche Ergebnisse dabei herauskommen, und sie beeinflussen schließlich auch die Interpretation der Ergebnisse und mögliche Handlungsempfehlungen.

Eine automatisierte Auswertung kann es uns nicht abnehmen, die Ergebnisse zu deuten: „Ein Modell mag, was die Mathematik dahinter angeht, noch so solide, ein Experiment noch so valide sein – sobald ein Forscher fragt, was die Ergebnisse bedeuten, beginnt der Prozess der Interpretation."[18] Da Interpretationen fehlerhaft sein können und möglicherweise falsche Handlungsentscheidungen nahelegen, dürfen wir auch aus ganz praktischen Gründen nicht davon ausgehen, dass die Ergebnisse von Big-Data-Analysen schlicht die Wirklichkeit

16 Anderson 2013, S. 126. Nach Cukier und Mayer-Schönberger hat Anderson später manche seiner Thesen revidiert. Vgl. Cukier, Mayer-Schönberger 2013, S. 93.

17 Hagner, Helbing 2013, S. 241.

18 Boyd, Crawford 2013, S. 197.

abbilden – denn nur unter dieser Voraussetzung sind wir überhaupt in der Lage, Interpretationsfehler als solche zu erkennen.

In einem engen Zusammenhang mit der irrigen Auffassung einer Überwindung der Theorie steht die Gefahr einer Verwechslung von Korrelationen (»x und y treten häufig zusammen auf«) und Kausalitäten (»aus x folgt y«).[19] „Die gängigen Big-Data-Analysen identifizieren statistische Korrelationen mit den Datenbeständen, die auf Zusammenhänge hindeuten. Sie erklären damit im besten Fall, was passiert, nicht aber warum."[20] Werden Korrelationen für ursächliche Zusammenhänge gehalten, kann dies zu gravierenden Fehleinschätzungen führen: Je mehr Feuerwehrleute im Einsatz sind, desto größer fallen die Brandschäden aus. Das bedeutet jedoch keineswegs, dass die Feuerwehrleute die Brandschäden verursachen. Eine Verwechslung von Korrelation und ursächlichem Zusammenhang könnte den Schluss nahelegen, man sollte in Zukunft besser weniger Feuerwehrleute einsetzen – das aber wäre fatal, denn es ist die Größe des Brandes, die sowohl die Anzahl der Feuerwehrleute als auch die Größe der Schäden bedingt.[21] Korrelationen, die mit Hilfe von Big-Data-Analysen entdeckt werden, dürfen nicht vorschnell in Handlungsempfehlungen übersetzt werden. Sie können als Grundlage oder Absicherung von Handlungsentscheidungen fungieren, setzen aber eine kompetente Interpretation voraus. Ein gutes Beispiel ist hier erneut das Frühwarnsystem für Frühgeborene: Nur Ärzte, die sich hinreichend mit der Technik auskennen und die Situation des jeweiligen Patienten beurteilen können, sind in der Lage, kompetent und verantwortlich darüber zu entscheiden, ob eingegriffen werden sollte und, wenn ja, welche Maßnahmen geeignet sind.

Korrelationen, die mit Hilfe von *Big-Data*-Analysen entdeckt werden, dürfen nicht vorschnell in Handlungsempfehlungen übersetzt werden. Sie können als Grundlage oder Absicherung von Handlungsentscheidungen fungieren, setzen aber eine kompetente Interpretation voraus.

Nach Petra Grimm, Leiterin des Instituts für Digitale Ethik in Stuttgart, wird viel zu wenig darüber diskutiert, welche Wertvorstellungen der verbreiteten Begeisterung für eine zunehmende Quantifizierung aller Lebensbereiche implizit

19 Interview Hillerbrand.

20 Mayer-Schönberger 2015, S. 16 (m.H.).

21 Dubben, Beck-Bornholdt 2006.

zugrunde liegen. Sie sieht die momentane Entwicklung als „konsequente Fortsetzung eines ökonomistischen Weltbildes, wie es sich seit dem ausgehenden 18. Jahrhundert zunehmend durchgesetzt hat. Planbarkeit, Messbarkeit und Steuerung sind die Leitwerte, die die Ökonomisierung unserer Gesellschaft noch weiter vorantreiben und sich bestens mit den neuen Big-Data-Techniken verbinden lassen."[22] Einen Zusammenhang von Datenorientierung und radikaler Ökonomisierung sieht auch Julie Cohen, Jura-Professorin und Expertin für Datenschutz an der Georgetown University: „In a consumption-driven economy, the innovations that emerge and find favor will be those that fulfill consumption-driven needs."[23] Beide bestreiten nicht, dass *Big Data* großartige Möglichkeiten bietet, etwa zur Verbesserung von Bildungschancen, zur bedarfsgerechten Verkehrssteuerung und zum Schutz von Ökosystemen. Welche Möglichkeiten aber kommen dominant zum Einsatz? Welche Ziele werden dabei verfolgt? Welche Mittel angewandt? Wer profitiert vor allem von den jeweiligen Anwendungen? Wem schaden sie? Welchen Personen und Institutionen verleihen sie besondere Macht? Wenn in Zukunft nicht nur wenige von *Big Data* profitieren sollen, müssen die Ziele und normativen Vorgaben hinterfragt werden, mit denen Big-Data-Analysen durchgeführt werden. Da *Big Data* kein einheitliches Phänomen ist, können diese Ziele und Vorgaben je nach Kontext ganz unterschiedlich ausfallen. Sie müssen deshalb in konkreten Zusammenhängen analysiert und öffentlich diskutiert werden; die drei hier skizzierten Verwechslungsphänomene stellen dabei mögliche Ausgangspunkte dar. Laut Helbig müssen insbesondere „[e]thische Betrachtungen […] viel mehr Gewicht erhalten, und wir müssen uns viel bewusster entscheiden, wofür wir Informationstechnologien einsetzen wollen." Nur so können wir herausfinden, „wie wir von einer technologiegetriebenen Gesellschaft zu einer sozial orientierten Technologie kommen können",[24] die wirklich zu einer Verbesserung der Lebensumstände weltweit beiträgt.

Wenn in Zukunft nicht nur wenige von *Big Data* profitieren sollen, müssen die Ziele und normativen Vorgaben hinterfragt werden, mit denen Big-Data-Analysen durchgeführt werden.

22 Interview Grimm.

23 Cohen 2013, S. 1926.

24 Hagner, Helbing 2013; S. 254.

4

Privatheit und informationelle Selbstbestimmung

Big Data wirft eine Vielzahl ethischer Fragen auf. Dies sind neben den Fragen zu Profiteuren und Machtverhältnissen etwa Fragen der professionellen Verantwortung (welche Verantwortung trage ich als Softwareentwickler für negative Auswirkungen einer Technologie, die ich mitentwickelt habe?[25]), Fragen des Eigentums (wem gehören die Daten, die bei der Nutzung digitaler Geräte und Dienstleistungen anfallen?), Fragen der Zugangsgerechtigkeit (wer darf die gesammelten Daten zu welchen Zwecken auswerten?) und die Frage, wie mit Wertkonflikten umzugehen ist (was sollte getan werden, wenn Chancen, die *Big Data* eröffnet, mit Persönlichkeitsrechten kollidieren?). Ins Zentrum der öffentlichen Aufmerksamkeit gerückt sind durch jüngste staatliche und privatwirtschaftliche Überwachungsexzesse Fragen aus dem Themenkomplex Privatheit, Selbstbestimmung und Datenschutz, auf die ich mich im Folgenden konzentriere. Sie sind mit den anderen Fragen in begrifflicher und praktischer Hinsicht verbunden und bilden einen geeigneten Ausgangspunkt.

25 Interview Baum. An der Universität des Saarlands werden solche interdisziplinären Fragen in die Ausbildung von Software-Ingenieuren und Programmierern eingebunden. Nach einem erfolgreichen Proseminar „Ethik für Nerds“ im Sommersemester 2015 wurde inzwischen eine Vertiefungsvorlesung ins dauerhafte Programm aufgenommen; vgl.: https://dcms.cs.uni-saarland.de/ethics/.

In der liberalen Tradition, die sowohl die öffentliche Diskussion wie auch die Rechtsprechung in Deutschland und der Europäischen Union maßgeblich prägt, wird Privatheit allgemein als Ermöglichungsbedingung und auch als Ausdruck von Autonomie im Sinne selbständigen Denkens und Handelns verstanden.

Es gibt eine komplexe moral- und rechtsphilosophische Debatte darüber, was „Privatheit“ bedeutet und in welcher Beziehung sie zu anderen grundlegenden Interessen, Werten oder Rechten steht. In der liberalen Tradition, die sowohl die öffentliche Diskussion wie auch die Rechtsprechung in Deutschland und der Europäischen Union maßgeblich prägt, wird Privatheit allgemein als Ermöglichungsbedingung und auch als Ausdruck von Autonomie im Sinne selbständigen Denkens und Handelns verstanden. Privatheit ist der ersten Annahme zufolge unverzichtbare Voraussetzung für die Entwicklung individueller Fähigkeiten, die eine selbstbestimmte Lebensführung ermöglichen. Sie ist Voraussetzung für die Herausbildung und den Erhalt persönlicher Integrität, für individuelles Wohlbefinden, die Entwicklung einer selbständigen moralischen und politischen Urteilsfähigkeit und zwischenmenschliche Beziehungen von unterschiedlicher Intimität. Als privat werden dabei zumeist diejenigen Bereiche oder Angelegenheiten bezeichnet, über die jedes Individuum grundsätzlich selbst bestimmen darf bzw. dürfen sollte (sofern mit den Grundrechten Anderer vereinbar) – etwa private Wohnung, individuelle Lebensweise, politische Überzeugungen oder eben auch personenbezogene Daten. Der Wert des Privaten wird in diesem Zusammenhang zwar zunächst individuell bestimmt, verfügt aber deutlich über eine soziale Dimension: Als Voraussetzung der Entwicklung einer selbständigen moralischen und politischen Urteilsfähigkeit ist Privatheit auch Voraussetzung einer freien und demokratischen Gesellschaft.

Als Voraussetzung der Entwicklung einer selbständigen moralischen und politischen Urteilsfähigkeit ist Privatheit auch Voraussetzung einer freien und demokratischen Gesellschaft.

Mit Blick auf den Schutz personenbezogener Daten hat sich im englischsprachigen Diskurs die Rede von „informationeller Privatheit“ (informational privacy) durchgesetzt. In Deutschland spricht man eher von „informationeller Selbstbestimmung“, ein Ausdruck, der seine Prominenz einem wirkmächtigen Urteil des Bundesverfassungsgerichts von 1983 verdankt, das die spätere Entwicklung des Datenschutzes auf deutscher

und europäischer Ebene maßgeblich beeinflusst hat. Schon im Wortlaut werden Schutz der Privatheit und Autonomie besonders eng miteinander verknüpft. Das Recht auf informationelle Selbstbestimmung wird aus dem allgemeinen Persönlichkeitsrechts abgeleitet:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. […] Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“[26]

Praktisch umgesetzt wird das Recht auf informationelle Selbstbestimmung durch die Notwendigkeit einer informierten Einwilligung und das Zweckbindungsprinzip: Personenbezogene Daten dürfen demnach grundsätzlich nur für Zwecke genutzt werden, die durch die jeweilige datengebende Person in Kenntnis aller relevanten Informationen autorisiert wurden. Fehlt eine solche Autorisierung, dürfen die Daten nur verarbeitet werden, wenn es dafür eine gesetzliche Regelung gibt.[27]

Das Recht, grundsätzlich selbst über Daten zur eigenen Person zu bestimmen, kann keine absolute Kontrolle bedeuten. Absolute Kontrolle über Daten zur eigenen Person wäre weder möglich noch wünschenswert. Ein großer Teil alltäglicher Interaktionen geht unweigerlich mit der Preisgabe personenbezogener Informationen oder Daten einher, und zwar nicht nur an Freunde und Familienmitglieder, sondern auch an Unbekannte – etwa an die Schaffnerin, die mein Zugticket kontrolliert, den Mitreisenden, der mir im Zug gegenüber sitzt, oder den Bäcker am Bahnhof, bei dem ich mir jeden Morgen vor der Abreise ein Brötchen kaufe. Es wäre absurd, hier von einer Verlet-

26 BVerfGE 65, 43

27 Vgl. z.B. Weichert 2013.

zung meiner informationellen Privatheit bzw. Selbstbestimmung zu sprechen, die mich in der Ausübung meiner Grundrechte behindert. Ich kann und muss nicht verhindern, dass der Bäcker Informationen zu meinen Frühstücksgewohnheiten erhält und von meinen täglichen Besuchen darauf schließt, dass ich Berufspendlerin bin.

Entscheidend ist, dass ich zumindest abschätzen kann, was andere in den jeweiligen Kontexten über mich erfahren. Nur unter dieser Voraussetzung kann ich beurteilen, ob Art und Umfang der Informationsweitergabe im jeweiligen Kontext angemessen sind und mich, wenn nötig, gegen unangemessene Formen der Informationsweitergabe und deren Konsequenzen zur Wehr zu setzen.[28] Nach den gängigen Normen, die den Informationsfluss zwischen Schaffnern und Zugreisenden regeln, ist es angemessen, dass die Schaffnerin auf meinem Ticket sieht, dass ich Besitzerin einer Bahncard bin und mich darum bittet, sie vorzuzeigen. Sollte sie mich aber außerdem zu meinen persönlichen Verhältnissen oder meiner finanziellen Situation befragen, werden diese Informationsnormen überschritten, und ich werde ihr vermutlich keine Auskunft geben, ohne deshalb befürchten zu müssen, aus dem Zug geworfen zu werden.

Absolute Kontrolle über Daten zur eigenen Person wäre weder möglich noch wünschenswert. Ein großer Teil alltäglicher Interaktionen geht unweigerlich mit der Preisgabe personenbezogener Informationen oder Daten einher […] Entscheidend ist, dass ich zumindest abschätzen kann, was andere in den jeweiligen Kontexten über mich erfahren.

Gerade eine solche Entscheidung – Verzicht auf Nutzung oder dem Kontext unangemessene Preisgabe personenbezogener Informationen – wird von vielen Anbietern digitaler Dienstleistungen verlangt. Die Konsequenzen eines Verzichts können dabei weitaus unangenehmer sein als ein Rauswurf aus dem Zug, und in einigen Fällen – etwa wenn berufliche Verpflichtungen die Verwendung bestimmter digitaler Dienste erfordern – lässt sich eine unangemessene Informationspreisgabe kaum umgehen.

Kontextspezifische Informationsnormen sind das zentrale Element einer dynamischen Privatheitskonzeption, wie sie die Philosophin Helen Nissenbaum vorschlägt, die an der New York University zum Verhältnis von Informationstechnologien und Privatheit forscht. Die Frage, an wen und unter welchen Be-

28 Rössler 2010.

dingungen personenbezogene Informationen weitergegeben werden dürfen, ist demnach abhängig von Normen, die den Informationsfluss zwischen bestimmten Akteuren in bestimmten sozialen Kontexten regeln. Um zu entscheiden, ob die Weitergabe bestimmter Informationen über eine Person die Privatheit dieser Person verletzt oder nicht, muss also nicht nur die Art der Information berücksichtigt werden, sondern auch das Verhältnis der beteiligten Akteure in der betreffenden Situation. Eine Ärztin beispielsweise darf ihren Patienten ausführlich zu seinem Gesundheitszustand befragen. Die meisten Arbeitgeber dürfen das nicht, wenn ihnen dieselbe Person als Bewerber gegenüber sitzt. Auch die Ärztin muss allerdings bestimmte Informationsnormen wie etwa den Grundsatz der Vertraulichkeit berücksichtigen; tut sie das nicht, verletzt sie die Privatheit bzw. die „kontextuelle Integrität“ ihres Patienten.[29] Kontrolle über Informationen zur eigenen Person ist laut Nissenbaum nur eine Informationsnorm unter vielen, wenn auch eine, die in vielen Kontexten eine wichtige Rolle spielt. Welche Informationsnormen gelten bzw. welches Gewicht sie haben, lässt sich erneut nur kontextabhängig bestimmen: Reziprozität beispielsweise ist eine wichtige Informationsnorm unter Freunden, nicht aber für das Verhältnis eines Psychiaters zu seinen Patienten.[30] Entscheidend ist Nissenbaum zufolge, dass personenbezogene Informationen aus einem bestimmten Kontext nicht ohne weiteres in andere Kontexte gelangen dürfen, in denen möglicherweise ganz andere Normen für den Umgang mit ihnen gelten.

Um zu entscheiden, ob die Weitergabe bestimmter Informationen über eine Person die Privatheit dieser Person verletzt oder nicht, muss also nicht nur die Art der Information berücksichtigt werden, sondern auch das Verhältnis der beteiligten Akteure in der betreffenden Situation.

29 Zum Zusammenhang von Privatheit, Informationsnormen und kontextueller Integrität vgl. Nissenbaum 2009, bes. Teil III.

30 Barth, Datta, Mitchell, Nissenbaum 2006.

5

Big Data und Datenschutz

Big-Data-Analysen, die einen Personenbezug aufweisen oder herstellen, sind dieser kontextbasierten Herangehensweise zufolge dann problematisch, wenn sie wichtige, kontextspezifische Informationsnormen verletzen und Betroffenen keine echten Handlungsspielräume lassen. Werden personenbezogene Daten auf inadäquate Weise erhoben, gespeichert, verwendet oder in andere Kontexte transferiert, kann dies zu Freiheitseinschränkungen, Diskriminierung und ungerechten Machtverhältnissen führen, von denen Individuen, aber auch Gruppen und ganze Gesellschaften betroffen sein können. Datenschutz – bzw. die Verpflichtung zur Einhaltung wichtiger Informationsnormen – ist kein Selbstzweck, sondern der Versuch, solche negativen Auswirkungen durch konkrete Maßnahmen zu verhindern und die Bedingungen zu formulieren, unter denen personenbezogene Daten verwendet werden dürfen.

Das Ausmaß, zu dem im frühen 21. Jahrhundert Daten über Interessen, Gewohnheiten, soziale Beziehungen, Fähigkeiten und Schwächen gesammelt, gespeichert, mit anderen Daten kombiniert, ausgewertet, an Dritte weitergegeben und wiederverwendet werden, ist historisch beispiellos. Dabei kommt es regelmäßig zu Verletzungen kontextspezifischer Privatheitsansprüche, wie sie hier in Grundzügen skizziert wurden. Es besteht ein auffälliges Transparenzgefälle: Die zunehmende Durchleuchtung von Individuen und Gruppen kontrastiert mit intransparenten Datenverwendungen und Geschäftspraktiken. Datengeber

können häufig weder in hinreichendem Maße abschätzen noch beeinflussen, wer die beteiligten Akteure sind, welcher Art die Daten sind, welchen Umfang sie haben, zu welchen Zwecken sie verwendet werden und welche praktischen Konsequenzen daraus für sie selbst und Andere entstehen. Alternative, weniger datenintensive Geräte und Dienstleistungen stehen oft nicht zur Verfügung, und ein Verzicht auf ihre Nutzung ist unter den gegenwärtigen Bedingungen einer zunehmend vernetzten Lebenswelt keine realistische oder auch nur wünschenswerte Option.

Im Rahmen einer Studie zu 71 der beliebtesten US-Webseiten 2012, die eine Anmeldung erfordern, hat das Wall Street Journal herausgefunden, dass über ein Viertel von ihnen Nutzerdaten wie Name, Benutzername und Emailadresse an Dritte weitergab. Eine große Dating-Plattform reichte sogar Angaben zu sexueller Orientierung und Drogengebrauch an Werbefirmen weiter.[31] Dagegen ausdrücklich um Datenschutz und das Vertrauen seiner Nutzer bemüht ist die Wikimedia-Stiftung, die mit Wikipedia nach eigenen Angaben[32] eine der zehn weltweit populärsten Webseiten betreibt.[33] Wikimedia ist damit ein Gegenbeispiel zu der verbreiteten These, dass Unternehmen Nutzerdaten an Dritte weitergeben müssen, um „kostenlose“ Dienstleistungen anbieten zu können. Auch im deutschen Sprachraum ist die Weitergabe von Nutzerdaten gängige Praxis, wie eine beispielreiche Cracked-Labs-Studie im Auftrag der österreichischen Arbeiterkammer zeigt: „Populäre deutsche Nachrichten-Websites übertragen 2014 bei jedem Seiten-Aufruf Nutzungsdaten an bis zu 59 externe Services. Mit dem Angebot segment.io können BetreiberInnen von Websites ein Service in deren Seiten einbauen, das die Daten der NutzerInnen unkompliziert und automatisiert gleich an über 100 weitere Dritt-Unternehmen weiterleitet – ohne dass dies für NutzerInnen in irgendeiner Weise erkennbar oder nachvollziehbar ist.“[34]

Auch solche Datensätze, die keinen direkten Personenbezug aufweisen, können durch die Kombination mit anderen Datensätzen personenbeziehbar werden und sehr spezifische, möglicherweise sensible Details über bestimmte Personen oder Gruppen verraten.

31 The Wall Street Journal 2012.

32 Vgl. https://www.wikimedia.de/wiki/Hauptseite.

33 https://meta.wikimedia.org/wiki/Privacy_policy/de; Süddeutsche Zeitung 2015; Zeit Online 2015.

34 Christl 2014.

Das Risiko, dass personenbezogene Informationen dabei in unangemessene Verwendungskontexte gelangen, ist groß und wird noch erhöht durch die Aussagekraft auch scheinbar belangloser Daten in Zeiten von *Big Data*. Auch solche Datensätze, die keinen direkten Personenbezug aufweisen, können durch die Kombination mit anderen Datensätzen personenbeziehbar werden und sehr spezifische, möglicherweise sensible Details über bestimmte Personen oder Gruppen verraten. Allein aus Meta-Daten lassen sich umfassende Persönlichkeitsprofile erstellen, für die sich Firmen in verschiedensten Geschäftsbereichen, aber auch staatliche Einrichtungen und Geheimdienste interessieren (aus Gründen, deren Legitimität jeweils im Verhältnis zu Datenschutzinteressen beurteilt werden muss). GPS-Standortdaten beispielsweise erlauben zuverlässige Prognosen über zukünftige Aufenthaltsorte von Personen, die noch genauer werden, wenn dabei auch die Bewegungsprofile von Personen aus dem Bekanntenkreis berücksichtigt werden.[35] Leicht zugängliche Daten wie Facebook-Likes ermöglichen automatisierte Rückschlüsse auf Alter, Geschlecht, sexuelle Orientierung, ethnische Zugehörigkeit, politische Einstellung, Intelligenz, Zufriedenheit oder den Gebrauch von Genussmitteln.[36]

35 Talbot 2012.

36 Kosinski, Stillwell, Graepel 2013.

6

Manipulation, Anpassungsdruck und fehlende Gestaltungsmöglichkeiten

Die Schäden, die aus der mal mehr, mal weniger freiwilligen Preisgabe personenbezogener oder -beziehbarer Daten entstehen können, sind nicht pauschal zu bestimmen. Zum einen handelt es sich um sehr direkte Einschränkungen äußerer Freiheit wie die illegitime Verweigerung[37] eines Kredits oder einer Aufenthaltsgenehmigung. Zum anderen geht es aber auch um indirekte Einschränkungen, um subtile Formen der Diskriminierung, der Verhaltenssteuerung und der Manipulation des Denkens, die zu Verlusten innerer Freiheit führt. Als drei wichtige Gefahren lassen sich identifizieren: (1) Manipulation, (2) Anpassungsdruck und (3) fehlende Gestaltungsmöglichkeiten:

(1) Werbemaßnahmen werden mit Hilfe von Big-Data-Techniken so effektiv wie nie zuvor. Angebote und die Art ihrer Präsentation lassen sich mit zunehmender Genauigkeit auf individuelle Vorlieben und Schwächen ausrichten. „You may also like“ mag dafür ein recht harmloses Beispiel sein und den Betroffenen vielleicht sogar willkommen. Längst aber gibt es viel aggressivere Werbe-

37 Ob eine solche Verweigerung legitim ist oder nicht, hängt u.a. maßgeblich davon ab, welcher Art die Daten sind, die die entscheidende Instanz, etwa eine Bank, ihrer Entscheidung zugrunde legt. Darf eine Bank zu diesem Zweck Daten verwenden, die Auskunft über die gesundheitliche Situation des Kreditstellers geben oder über seine politischen Ansichten?

praktiken. Auf Basis individueller Emotionsanalysen werden Angebote gezielt in Momenten höchster Ansprechbarkeit platziert oder solche Momente sogar herbeigeführt: „Today's firms fastidiously study consumers and, increasingly, personalize every aspect of their experience. They can also reach consumers anytime and anywhere, rather than waiting for the consumer to approach the marketplace. These and related trends mean that firms can not only take advantage of a general understanding of cognitive limitations, but can uncover and even trigger consumer frailty at an individual level."[38]

Politische Argumente durch psychologische Überzeugungsstrategien zu ersetzen, ist natürlich kein neuartiges Verfahren im Wahlkampf. Neu und ethisch fragwürdig ist jedoch der Grad, zu dem die Ansprache personalisiert und darüber eine effektive Beeinflussung der Wähler erreicht werden kann.

Auch *Big Data*-basierte Wahlkampfstrategien, wie sie in den US-amerikanischen Wahlkämpfen seit 2008 zum Einsatz kamen, bewegen sich an der Grenze zu problematischer Manipulation. Big-Data-Techniken wurden eingesetzt, um unentschiedene Wähler zu identifizieren, die dann mit trickreichen, maßgeschneiderten Strategien angesprochen wurden, die in mehrstufigen Testverfahren auf ihre Wirksamkeit überprüft worden waren.[39] Politische Argumente durch psychologische Überzeugungsstrategien zu ersetzen, ist natürlich kein neuartiges Verfahren im Wahlkampf. Neu und ethisch fragwürdig ist jedoch der Grad, zu dem die Ansprache personalisiert und darüber eine effektive Beeinflussung der Wähler erreicht werden kann. Dies gefährdet die individuelle politische Meinungsbildung und letztlich auch die Demokratie, die darauf angewiesen ist, dass möglichst viele Wähler sich ihre Meinung auf Basis sachgerechter Informationen und in Auseinandersetzung mit Gegenpositionen bilden und nicht, weil politische Akteure wissen, wie sie die emotionalen Dispositionen und Entscheidungsmuster der Wähler für ihre Zwecke nutzen können.

(2) Das Bundesverfassungsgericht betont im oben zitierten Urteil – zu einer Zeit, in der *Big Data* noch kein Thema war – die Gefahr, dass die (inzwischen vielfach potenzierten) Möglichkeiten automatischer Datenverarbeitung einen hohen sozialen Anpassungsdruck entfalten, der das Individuum darin einschränkt, seine Grundfreiheiten wahrzunehmen. Wer nicht mit hinreichender Sicherheit

38 Calo 2014.

39 Vgl. Kucklick 2014, S. 33-46; Moorstedt 2013; Schulz 2013.

abschätzen könne, ob abweichende Verhaltensweisen notiert und als Informationen dauerhaft gespeichert, verwendet oder weitergegeben werden, werde sein Verhalten aus Vorsicht anpassen.[40] Der zunächst äußere Freiheitsverlust einer Verhaltensanpassung kann durch Selbstzensur und Internalisierung der (vermeintlichen) Beobachterperspektive zu inneren Freiheitsverlusten führen, die sich als Verluste von Spontaneität und Denkfreiheit äußern; ein Effekt, der im Anschluss an Michel Foucaults Überlegungen zur westlichen Disziplinargesellschaft[41] auch als panoptischer Effekt bezeichnet wird. Durch diesen Effekt werden, so das Bundesverfassungsgericht, nicht nur die Entfaltungsmöglichkeiten des Einzelnen beeinträchtigt, sondern auch „das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[42]

Der zunächst äußere Freiheitsverlust einer Verhaltensanpassung kann durch Selbstzensur und Internalisierung der (vermeintlichen) Beobachterperspektive zu inneren Freiheitsverlusten führen, die sich als Verluste von Spontaneität und Denkfreiheit äußern.

(3) Im Kontrast (wenn auch nicht notwendig im Widerspruch) zur Anpassungsthese des Bundesverfassungsgerichts steht die Tatsache, dass sehr viele Menschen nach wie vor sehr freigiebig mit Daten zu ihrer Person umgehen – und zwar trotz geheimdienstlicher Überwachungsprogramme wie PRISM und Tempora und dem chinesischen „Reputationssystem" Citizen Score.[43] Eine allgemeine Konjunktur von Vorsichtsmaßnahmen und Verhaltensanpassungen bei der Nutzung von Informationstechnologien ist nicht erkennbar. (Noch) sind es Minderheiten, die sich konsequent um den Schutz ihrer Daten bemühen, etwa indem sie auf Emailanbieter, Cloudspeicher und Kurznachrichtendienste mit hohem Datenschutz umsteigen, ihre Nutzung von Informationstechnologien einschränken, Verschlüsselungs- und Verschleierungstechniken (data masking, obfuscation) nutzen oder

40 In einer umfangreichen Studie des Vodafone Instituts für Gesellschaft und Kommunikation geben 51 Prozent der Befragten an, persönliche Inhalte in Emails zu vermeiden, weil sie befürchten, dass unbekannte Dritte Zugriff auf diese Inhalte haben könnten. Vgl. Vodafone Institut für Gesellschaft und Kommunikation 2016, S. 17.

41 Foucault 1977; Interview Orrù.

42 BVerfGE 65, 43

43 Vgl. Plass-Fleßenkämper 2015.

politisch aktiv werden. Woran liegt das? Ein Erklärungsversuch lautet, Privatheit als Paradigma sei einfach nicht mehr zeitgemäß bzw. schlicht „überholt“.[44] Ein anderer besagt, die meisten Menschen würden den Tausch von personenbezogenen Daten gegen Preisnachlässe oder Dienstleistungen als fairen Tausch begreifen, als „fair deal“ oder legitimen „tradeoff“; statt mit Geld würde eben mit Daten bezahlt.[45] Beiden widersprechen zahlreiche Studien, die darauf hindeuten, dass die Gemengelage komplizierter ist: Den meisten Menschen sind Privatheit und ein selbstbestimmter Umgang mit ihren Daten offenbar sehr wichtig – sie geben selbige aber trotzdem preis.[46] Eine repräsentative Umfrage des Vodafone Instituts für Gesellschaft und Kommunikation zeigt diese Spannung deutlich auf: „Über die Hälfte aller Befragten (55 Prozent) gibt an, eher Geld für die Nutzung eines Service bezahlen zu wollen, anstatt persönliche Daten vom Anbieter sammeln und nutzen zu lassen.“[47] Kostenpflichtige Alternativen stehen oft nicht zur Verfügung. Doch selbst wenn es sie gibt, entscheiden sich die Nutzer mit großer Mehrheit für Angebote, die nicht mit Geld, sondern mit Daten bezahlt werden. Hinzu kommt, dass viele Menschen die allgemeinen Geschäftsbedingungen akzeptieren, „ohne diese im Vorfeld genau durchgelesen zu haben: vier von zehn Nutzern (40 Prozent) verwenden einen Online-Service, ohne genau geprüft zu haben, was mit ihren Daten passieren wird.“[48] Diese auffällige Diskrepanz zwischen Einstellung und tatsächlichem Verhalten wird oft als „Privatheitsparadox“ bezeichnet. Auch hierfür gibt es verschiedene Erklärungsansätze. Sie reichen von Interessenkonflikten (Privatheit vs. freie Kommunikation oder Komfort, kurzfristige Vorteile vs. langfristige Vorteile) bis hin zu fehlendem bzw. inakkuratem Wissen (in Bezug auf mögliche Folgen, bestehende Schutzvorkehrungen und das Ausmaß eigener Kontrolle).

Den meisten Menschen sind Privatheit und ein selbstbestimmter Umgang mit ihren Daten offenbar sehr wichtig – sie geben selbige aber trotzdem preis.[46]

44 Vgl. Schneider 2014.

45 Vgl. z.B. Yahoo! 2014, S. 7.

46 Vgl. z.B. Utz, Kramer 2009 u. Barnes 2006.

47 Vodafone Institut für Gesellschaft und Kommunikation 2016, S. 21. Es wurden über 8000 Menschen in acht europäischen Ländern befragt.

48 Vodafone Institut für Gesellschaft und Kommunikation 2016, S. 18; zu länderspezifischen Unterschieden vgl. S. 18-21.

Eine aktuelle Annenberg-Studie bestätigt das Problem inakkuraten Wissens, hebt aber einen anderen, bisher wenig diskutierten Aspekt besonders hervor: Die Tatsache, dass US-Bürger zahlreiche persönliche Informationen an Unternehmen weitergeben, reflektiere nur scheinbar eine entsprechende Bereitschaft. Der wahre Grund sei Resignation. Die große Mehrheit lehne den Tausch von Preisnachlässen und verbesserten Verfügungsmöglichkeiten gegen personenbezogene Daten als unfair ab. Die ungewollte Preisgabe personenbezogener Daten werde jedoch als unvermeidlich empfunden und jeder Versuch, dagegen etwas zu unternehmen, als vergeblich: „[A] majority of Americans are resigned to giving up their data – and that it is why many appear to be engaging in tradeoffs. […] Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them."[49] Wenn diese Diagnose richtig ist, handelt es sich auch hierbei um einen indirekt herbeigeführten Freiheitsverlust, der sich als Mangel an Gestaltungsmöglichkeiten äußert.

Die politische Bedeutung der Ergebnisse dieser Studie liegt vor allem darin, der gängigen These einer allgemein akzeptierten Tauschbeziehung zu widersprechen, die vermeintlich beide Seiten, Datengeber und Datenverwender, als überwiegend vorteilhaft begreifen. Die Autoren weisen eine Grundannahme dieser Tauschtheorie als falsch zurück, nämlich die implizite Annahme mächtiger Konsumenten, die maßgeblich mit darüber bestimmen können, unter welchen Bedingungen der Tausch zustande kommt: „This image of a powerful consumer has become a way to claim to policymakers and the media that Americans accept widespread tracking of their backgrounds, behaviors, and lifestyles across devices, even though surveys repeatedly show they object to these activities." Das Tradeoff-Argument kaschiere das Transparenz- und Machtgefälle zwischen datengebender und datenverwendender Seite und verstelle so den Blick auf nötige Maßnahmen. „By misrepresenting the American people and championing the tradeoff argument, marketers give policymakers false justifications for allowing the collection and use of all kinds of consumer data often in

Die Rechteinhaber müssen befähigt werden, das Auskunftsrecht auch in Anspruch zu nehmen.[51] Aus dieser Forderung lassen sich zwei Notwendigkeiten ableiten: Erstens die Notwendigkeit einer umfassenden digitalen Kompetenzförderung, die nicht allein auf technische Fähigkeiten abzielt, sondern auch auf Reflexion und Kritikfähigkeit.[52]

49 Turow, Hennessy, Draper 2015, S. 3.

ways that the public finds objectionable."[50] Ein Lösungsansatz für dieses Problem läge in einem umfassenden Auskunftsrecht, das Individuen ermöglicht, herauszufinden, was Firmen über sie wissen und wie sie dieses Wissen nutzen (anders als in der EU ist das Recht auf Selbstauskunft in den USA derzeit sehr beschränkt). Dabei darf es nicht bei einem theoretischen Auskunftsrecht bleiben: Die Rechteinhaber müssen befähigt werden, dieses Recht auch in Anspruch zu nehmen.[51] Aus dieser Forderung lassen sich zwei Notwendigkeiten ableiten: Erstens die Notwendigkeit einer umfassenden digitalen Kompetenzförderung, die nicht allein auf technische Fähigkeiten abzielt, sondern auch auf Reflexion und Kritikfähigkeit.[52] Die EU-Initiative „klicksafe" beispielsweise versteht sich als „Sensibilisierungskampagne zur Förderung der Medienkompetenz im Umgang mit dem Internet und neuen Medien".[53] In Zusammenarbeit mit dem Institut für digitale Ethik (IDE) an der Hochschule der Medien (HdM) Stuttgart wurde in ihrem Rahmen das Unterrichtsmodul „Ethik macht klick - Wertenavi fürs digitale Leben" entwickelt, das Jugendliche dabei unterstützen soll, netzbezogene Wertkonflikte[54] zu erkennen, sie eigenständig zu reflektieren und verantwortlich mit ihnen umzugehen. Zweitens braucht es vermittelnde und kontrollierende Instanzen, die den individuellen Nutzer dabei unterstützen, zu verstehen, wie Daten in konkreten Fällen erhoben, gespeichert und verwendet werden, und welche Folgen daraus entstehen.[55] Solche institutionellen Rahmenbedingungen werden notwendig sein, um Resignation abzubauen und dem Einzelnen sinnvolle Gestaltungsspielräume zurückzugeben.

Zweitens braucht es vermittelnde und kontrollierende Instanzen, die den individuellen Nutzer dabei unterstützen, zu verstehen, wie Daten in konkreten Fällen erhoben, gespeichert und verwendet werden, und welche Folgen daraus entstehen.[55]

50 Turow, Hennessy, Draper 2015, S. 3.

51 Turow, Hennessy, Draper 2015, S. 21.

52 Vgl. Letouzé, Noonan, Bhargava, Deahl, Sangokoya, Shoup 2015; Interview Letouzé; Interview Grimm.

53 http://www.klicksafe.de/ueber-klicksafe/die-initiative/projektinfo/wer-ist-klicksafe/

54 Ein solcher liegt beispielsweise vor, wenn mir einerseits soziale Teilhabe und Verbundenheit mit meinen Freunden wichtig sind, ich andererseits aber meine Privatsphäre schützen möchte. Entscheide ich mich also z.B. für oder gegen die Nutzung von WhatsApp? Hilfestellung für die Entscheidungsfindung bietet die medienethische Roadmap." Petra Grimm im Interview auf http://www.digitale-ethik.de/beratung/klicksafe-2/.

55 Vgl. Cukier, Mayer-Schönberger 2013, S. 227f.

Natürlich können Informationstechnologien informationelle Selbstbestimmung nicht nur einschränken, sondern auch entscheidend fördern. Suchmaschinen erleichtern den Zugang zu Informationen, soziale Netzwerke und Nachrichtendienste bieten unkomplizierte Möglichkeiten zu weltweitem Austausch, zu sozialer und politischer Partizipation. Warum aber sollten diese Möglichkeiten nur um den Preis der unkontrollierten und unkontrollierbaren Abgabe umfangreicher personenbezogener Daten zu haben sein? Nach Evgeny Morozov zeugt diese Annahme von einem Mangel an Phantasie: „Es geht […] um unsere Unfähigkeit, uns ein Szenario vor Augen zu führen, wie die Dienste, auf die wir mittlerweile angewiesen sind – von Suchmaschinen zu sozialen Netzwerken – außerhalb werbeabhängiger Silicon-Valley-Geschäftsmodelle funktionieren könnten. […] Letzten Endes erfordern weder Internetsuchen, noch Onlinenetworking, noch Vermittlungsdienste für Autofahrten wie Uber, dass wir Einzelheiten unserer Identität preisgeben. […] Sind solche Dienste erst einmal abgekoppelt von der Werbung, ihrem Hauptgeschäftsmodell, verschwindet die Notwendigkeit ausgiebiger Überwachung.“[56] Zu denkbaren Alternativen, die bereits heute in einigen Bereichen erfolgreich sind, gehören Open-Source-Projekte, die auf Spenden oder freiwilliger Mitarbeit beruhen, öffentlich-rechtliche Angebote und Unternehmen, die sich genau dadurch am Markt behaupten, dass sie datenschutzfreundliche Geräte und Dienstleistungen in einer Weise anbieten, die den Selbstbestimmungsrechten ihrer Kunden entspricht (privacy by design, value sensitive-design).

Natürlich können Informationstechnologien informationelle Selbstbestimmung nicht nur einschränken, sondern auch entscheidend fördern. Suchmaschinen erleichtern den Zugang zu Informationen, soziale Netzwerke und Nachrichtendienste bieten unkomplizierte Möglichkeiten zu weltweitem Austausch, zu sozialer und politischer Partizipation.

56 Morozov 2015, S. 6; Interview Kurz.

7

Anonymisierung und informierte Einwilligung

Klassische Maßnahmen, um Daten zu schützen, und damit informationelle Privatheit bzw. Selbstbestimmung, stehen durch Big-Data-Techniken besonders unter Druck. Die Frage, ob Anonymisierung und Pseudonymisierung,[57] Datensparsamkeit, Zweckbindung und informierte Einwilligung noch zeitgemäße Datenschutz-Instrumente sind oder einer grundsätzlichen Modifikation bedürfen, wird kontrovers diskutiert. So wird argumentiert, dass diese Instrumente nicht mehr greifen bzw. aus verschiedenen Gründen nicht mehr die Schutzwirkung entfalten, um derentwillen sie konzipiert worden sind. Ein anderer Einwand gegen das klassische Instrumentarium lautet, dass seine Wirkungen den Funktionsweisen von *Big Data* diametral entgegenstehen und die Potentiale dieser Technologie allzu stark einschränken. Dem wird entgegnet, dass der Beweis, dass diese Potentiale wirklich größer sind als die Risiken, noch aussteht und von

57 Die Wörter Anonymisierung und Pseudonymisierung werden in unterschiedlichen Bedeutungen verwendet; im Bundesdatenschutzgesetz (BDSG §3 Abs.6 und BDSG §3 Abs.6a) sind sie folgendermaßen definiert: „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“

denjenigen erbracht werden muss, die eine Einschränkung oder gar Aufhebung der genannten Maßnahmen fordern.

Der Schutz informationeller Selbstbestimmung ist in Zeiten von *Big Data* gleichzeitig so wichtig und so schwierig wie nie zuvor. Dass *Big Data* die effektive Implementierung klassischer Datenschutz-Instrumente erschwert, wird von deren Befürwortern in der Regel nicht bestritten. Einige dieser Schwierigkeiten will ich am Beispiel von Anonymisierung bzw. Pseudonymisierung und informierter Einwilligung kurz skizzieren. Gerade die Kombination dieser Instrumente erscheint zunächst besonders aussichtsreich, um den Konflikt zwischen Erkenntnisinteressen auf der einen und Privatheitsinteressen auf der anderen Seite zu überwinden:[58] Die Entfernung (Anonymisierung) oder Ersetzung (Pseudonymisierung) von Identifikatoren – etwa Name, Geburtsdatum, Adressen, Telefon- oder Versicherungsnummern – scheint die Gefahr einer Privatheitsverletzung von vornherein auszuschließen. Weisen die Daten keinen Personenbezug mehr auf, dann spricht zumindest aus datenschutzrechtlicher Perspektive zunächst nichts gegen ihre freie Verwendung. Anonymisierung und Pseudonymisierung scheinen deshalb ideale Problemlösungsstrategien für all diejenigen Kontexte zu sein, in denen ein Personenbezug verzichtbar ist. Für alle übrigen Kontexte, in denen die Verwendung personenbezogener Daten mit Blick auf bestimmte Forschungszwecke, individualisierte Behandlungen, Angebote oder Dienstleistungen notwendig ist, scheint die Lösung darin zu bestehen, die betreffenden Verwendungen durch informierte Einwilligungen der datengebenden Personen zu legitimieren. Tatsächlich aber bieten Anonymisierung, Pseudonymisierung und informierte Einwilligung einen weit weniger umfassenden und sicheren Schutz von informationeller Privatheit bzw. Selbstbestimmung als gemeinhin angenommen – und dies liegt nicht nur an technischen Schwierigkeiten ihrer Implementierung.

Unter den Bedingungen von *Big Data* ist die Sicherheit von Pseudonymisierungstechniken massiven Zweifeln ausgesetzt, und auch Anonymisierungstechniken können keinen absoluten Schutz garantieren.[59] Je detaillierter und umfangreicher ein anonymisierter oder pseudonymisierter Datensatz nämlich

58 Vgl. Barocas, Nissenbaum 2014, S. 45.

59 Ich danke Yves-Alexandre de Montjoye für seine sehr hilfreichen Auskünfte zu den Problemen von Pseudonymisierungs- und Anonymisierungstechniken. Zwei neue Vorschläge, wie Erkenntnis- und Privatheitsschutzinteressen bei der Erhebung, Speicherung und Nutzung von Daten vereinbart werden können, sind „openPDS“ und „SafeAnswers“; vgl. dazu: de Montjoye, Shmueli, Wang, Pentland 2014.

ist, desto leichter lässt er sich durch Kombination mit weiteren Daten wieder Individuen zuordnen.[60] Die Tatsache, dass wir im digitalisierten Alltag absichtlich und unabsichtlich gewaltige Mengen verschiedenster Daten hinterlassen, macht eine Rekombination möglich. „Über Kontextwissen können Sachdaten und (anfänglich) anonyme Daten Personen zugeordnet werden und somit der Informationsgehalt der diese Person betreffenden Erkenntnisse erhöht werden. Unter diesem Gesichtspunkt können sämtliche Daten grundsätzlich geeignet sein, das Risiko der Persönlichkeitsausforschung zu verstärken."[61] Problematisch ist, „wenn anonymisierte, aggregierte Daten beim Dritt- oder Viertverwender durch Kombination mit anderen Daten plötzlich wieder Personenbezug erhalten."[62] Wie der IT-Sicherheits-Experte Yves-Alexandre de Montjoye gemeinsam mit Kollegen nachgewiesen hat, genügen oft minimale Zusatzinformationen, um pseudonymisierte Daten mit einzelnen Personen in Verbindung zu bringen. Ihre in *Science* veröffentlichte Studie beruht auf einem pseudonymisierten Datensatz von Kreditkartentransaktionen, die 1,1 Millionen Menschen innerhalb von drei Monaten in 10 000 Geschäften getätigt haben. Vier nur vage bestimmte Informationen zu Ort und Datum der Transaktionen reichte aus, um 90 Prozent der Kreditkartennutzer zu reidentifizieren; wurde außerdem noch die ungefähre Höhe der Transaktionen berücksichtigt, wurde die Reidentifikation sogar noch einfacher.[63]

Es gibt verschiedene Versuche, dieses Problem auf technischer Ebene zu lösen. Verbesserte Anonymisierungstechniken (Verrauschung, differentielle Privatheit, K-Anonymität) sollen eine De-Anonymisierung ausschließen oder zumindest erheblich erschweren, ohne den Erkenntnisnutzen der Daten allzu stark einzuschränken. Doch auch wenn diese Bemühungen erfolgreich sein sollten, bleiben zentrale ethische Probleme informationeller Privatheit bzw. Selbstbestimmung im Kontext von *Big Data* ungelöst. Die Gefahren von Manipulation und Diskriminierung bestehen weiterhin: „If a company knows 100 data points about me in the digital environment, and that affects how that company treats me in the digital world, what's the difference if they know my name or not?"[64] Um digitale Angebote und Dienstleistungen auf Individuen zuschneiden zu können,

60 Weichert 2014, S. 836.

61 Smart-Data-Begleitforschung. FZI Forschungszentrum Informatik 2015, S. 7.

62 Smart-Data-Begleitforschung. FZI Forschungszentrum Informatik 2015, S. 19.

63 Interview de Montjoye; de Montjoye, Radaelli, Singh, Pentland 2015.

64 Turow 2011.

ist es nicht unbedingt nötig, die „analoge“ Identität einer Person zu kennen – Eigenschaften, die sich einem digitalen Abbild zuordnen lassen, reichen oft völlig aus. [65]

Noch problematischer aber ist, wie Solon Barocas und Helen Nissenbaum betonen, dass *Big Data* neue indirekte Möglichkeiten eröffnet, auf sensible Charakteristika von Menschen zu schließen. Gerade dasjenige Potential, das Big-Data-Analysen so attraktiv macht, nämlich die Möglichkeit, verborgene Korrelationen aufzufinden, die möglicherweise handlungsrelevant sind, bedeutet eine markante Schwächung der Schutzwirkung von Pseudonymisierungen und Anonymisierungen: „Rather than attempt to de-anonymize medical records, for instance, an attacker (or commercial actor) might instead infer a rule that relates a string of more easily observable or accessible indicators to a specific medical condition, rendering large populations vulnerable to such inferences even in the absence of PII [personal identifying information].”[66] Tatsächlich kann das Versprechen einer sicheren Anonymisierung mit Blick auf das Ziel, informationelle Privatheit zu schützen, auch kontraproduktive Effekte haben: „However much these protect volunteers, such techniques may license research studies that result in findings that non-volunteers perceive as menacing because they make certain facts newly inferable that anonymity once promised to keep beyond reach.” So kommt beispielsweise eine Studie von 2012 zu dem Ergebnis, dass Studenten mit Depressionen anhand bestimmter Muster der Internetnutzung identifiziert werden können. Die Anonymität der Studienteilnehmer wurde durch verschiedene Vorkehrungen geschützt. Die Ergebnisse aber können Konsequenzen für alle Menschen haben, deren Internetnutzung dieselben Muster aufweist – Muster, die möglicherweise über die Vergabe von Versicherungen, über berufliche Optionen und Bildungschancen entscheiden.[67]

Zumindest dieses Problem kann auch das Instrument einer informierten Einwilligung nicht lösen. Schließlich handelt es sich dabei immer um eine Einwilligung seitens der datengebenden Person, nicht aber seitens aller potentiell Betroffenen. Wer sich – informiert oder nicht – bereiterklärt, private Informationen an Firmen oder Einrichtungen weiterzugeben, gibt ihnen möglicherweise auch private Informationen über Andere, die deren Handlungspielräume massiv

65 Barocas, Nissenbaum 2014, S. 54; Interview Scott.

66 Barocas, Nissenbaum 2014, S. 55.

67 Kotikalapudi, Chellappan, Montgomery, Wunsch, Lutze 2012; vgl. Barocas, Nissenbaum 2014, S. 56.

einschränken können. Wenn aber die Auswertung personenbezogener Daten maßgebliche Konsequenzen für Dritte haben kann, kann ihre Preisgabe nicht Gegenstand rein individueller Abwägungen sein.

Wenn die Auswertung personenbezogener Daten maßgebliche Konsequenzen für Dritte haben kann, kann ihre Preisgabe nicht Gegenstand rein individueller Abwägungen sein.

Überhaupt ist es ein Irrtum, anzunehmen, Zustimmung allein könne über die Legitimität einer Datenverwendung entscheiden. Ein viel diskutiertes Problem von Zustimmungspraktiken ist das einer Überforderung der Einwilligenden: Selbst wenn ein umfassender Einblick in die Daten möglich ist, werden die meisten Menschen „nicht das notwendige statistische und mathematische Wissen mitbringen, oder auch nur die zum völligen Verständnis notwendige Zeit beziehungsweise Ausdauer.“[68] Sie können deshalb kaum abschätzen, welche Folgen ihre Einwilligung für sie selbst und Andere haben kann – und mit Blick auf letztere überschreiten sie möglicherweise ihre Befugnisse. Der Versuch, das Informationsdefizit durch klare und verständliche Vertragsbedingungen und Datenschutzerklärungen auszugleichen, hilft nur bedingt; denn die dafür nötige Vereinfachung komplexer Vorgänge birgt immer die Gefahr, sie zu verfälschen.

68 Interview Mayer-Schönberger.

8

Perspektiven

Die hier skizzierten Schwierigkeiten bedeuten nicht, wie manche behaupten, dass Anonymisierung, Pseudonymisierung und informierte Einwilligung überholt und deshalb verzichtbar wären. Sie markieren vielmehr die Grenzen dieser Instrumente und zeigen damit, dass weitere Schutzmaßnahmen nötig sind. Eine sichere Anonymisierung oder das Vorliegen einer informierten Einwilligung legitimieren gerade nicht jede denkbare Verwendung der betreffenden Daten. Nach Mayer-Schönberger sollten „auch bei Zustimmung bestimmte Big-Data-Verwendungen in Zukunft beschränkt oder verboten werden“, wie dies in anderen komplexen Bereichen, etwa im Lebensmittelbereich, längst der Fall ist: „Von Konsumenten wird nicht erwartet, dass sie mit einem Chemie-Labor einkaufen gehen, um die richtigen Entscheidungen zu treffen […]; der Fokus muss sich von der Einwilligung hin zur Regulierung der Verwendung verlagern.“ Die Verantwortung für eine moralisch und rechtlich legitime Datenverarbeitung darf nicht allein auf datengebender Seite liegen. Sie muss viel stärker als bisher

Die hier skizzierten Schwierigkeiten bedeuten nicht, wie manche behaupten, dass Anonymisierung, Pseudonymisierung und informierte Einwilligung überholt und deshalb verzichtbar wären. Sie markieren vielmehr die Grenzen dieser Instrumente und zeigen damit, dass weitere Schutzmaßnahmen nötig sind.

Die Verantwortung für eine moralisch und rechtlich legitime Datenverarbeitung darf nicht allein auf datengebender Seite liegen. Sie muss viel stärker als bisher von Datenverwendern und von Technikentwicklern getragen werden.[69]

von Datenverwendern und von Technikentwicklern getragen werden.[69] Entsprechende gesetzliche Regelungen und Kontrollverfahren führen Mayer-Schönberger zufolge nicht notwendig zu einer Einschränkung der Innovationsmöglichkeiten beim Einsatz von *Big Data*: „[G]anz im Gegenteil: Gerade eine gesetzlich verankerte Zulässigkeit einer verantwortungsvollen Datenverwendung (auch für neue Zwecke) ohne die ausdrückliche Zustimmung der Betroffenen kann verantwortungsbewussten Datennutzern Raum für innovative neue Möglichkeiten geben."[70]

Nötig ist ein pluralistischer Ansatz, der verschiedene Schutzinstrumente kombiniert und dem Ziel fairer und gerechter Rahmenbedingungen für Big-Data-Anwendungen verpflichtet ist. Innerhalb eines solchen Ansatzes werden Anonymisierung, Pseudonymisierung und informierte Einwilligung weiterhin eine wichtige Rolle spielen. Anonymisierungs- und Pseudonymisierungstechniken können keinen umfassenden Schutz garantieren und nicht alle Privatheitsverletzungen ausschließen, lassen sich aber sinnvoll einsetzen, um unangemessene Verwendungen personenbezogener Informationen zumindest zu erschweren. Auch informierte Einwilligung bleibt relevant; zum einen, weil gesetzliche Regelungen nur einen basalen Schutz bieten können, der nicht alle zustimmungsbedürftigen Verwendungen abdecken wird. Zum anderen ist die Möglichkeit, bestimmten Verwendungen von personenbezogenen Daten zuzustimmen oder sie abzulehnen, nicht einfach nur ein Mittel, um Autonomie zu fördern, sondern sie ist selbst Ausdruck von Autonomie. Wie Barocas und Nissenbaum

Nötig ist ein pluralistischer Ansatz, der verschiedene Schutzinstrumente kombiniert und dem Ziel fairer und gerechter Rahmenbedingungen für Big-Data-Anwendungen verpflichtet ist. Innerhalb eines solchen Ansatzes werden Anonymisierung, Pseudonymisierung und informierte Einwilligung weiterhin eine wichtige Rolle spielen.

69 Interview Baum. Siehe auch: „Regelungen, die sich nur an Datenverarbeiter richten, dürften viele Gestaltungsziele nicht erreichen. In viel stärkerem Maß sind daher die Technikgestalter als Regelungsadressaten anzusprechen. […] Was technisch verhindert wird, muss nicht mehr verboten werden." Roßnagel 2006.

70 Vgl. Vodafone Institut für Gesellschaft und Kommunikation 2016, S. 5; Interview Scott.

argumentieren, heißt das nicht, dass wirklich jede Verwendung personenbezogener Daten durch die datengebende Person autorisiert werden muss. In Anlehnung an philosophische Arbeiten im Bereich der Bioethik[71] schlagen sie vor, die Notwendigkeit einer informierten Einwilligung auf solche Datenverwendungen zu beschränken, die von moralisch akzeptablen, kontextspezifischen Normen, Standards und Erwartungen abweichen. „The burden on notice, therefore, is to describe clearly the violations of norms, standards, and expectations for which a waiver is being asked and not to describe everything that will be done and not be done in the course of treatment or research, which both the researcher and the subjects can safely presume.“[72] Es sei Aufgabe des Datenverwenders, jede solche Abweichung zu rechtfertigen. Darüber hinaus dürfe er überhaupt nur dann um Zustimmung zu bestimmten Datenverwendungen bitten, wenn davon ausgegangen werden kann, dass entweder die datengebende Person gute Gründe hat, sie zu erteilen, oder Andere daraus einen bedeutenden Nutzen ziehen würden.

Wie ein pluralistischer Ansatz im Detail aussehen könnte, sodass die einzelnen Maßnahmen sinnvoll ineinandergreifen, kann im Rahmen dieses Reports nicht ausgeführt werden. Nach Alex (Sandy) Pentland, Direktor des Connection Science und des Human Dynamics Laboratory am Massachusetts Institute of Technology, beginnt ein verantwortlicher Umgang mit *Big Data* mit dem Eingeständnis, dass es einfache Lösungen und abschließende Antworten nicht gibt: „[P]erhaps [the] most important step is for us to admit that we do not have all the answers, and, indeed, there are no final answers. All we know for sure is that as technology changes, so must our regulatory structures.”[73] Pentlands Plädoyer für eine experimentelle Vorgehensweise lässt sich als Aufforderung verstehen, die Angemessenheit bestehender regulativer Strukturen immer wieder neu zu überprüfen – und sie gegebenenfalls zu korrigieren.

71 Manson, O’Neill 2012.

72 Barocas, Nissenbaum 2014, S. 65. Damit ist natürlich nicht gesagt, dass es immer leicht wäre, zu bestimmen, ob eine konkrete Datenverwendung moralisch akzeptablen Informationsnormen genügt oder nicht.

73 Pentland 2014, S. 67; Interview Pentland.

Interviews

Für die Zeit, die sie sich genommen haben, und ihre Auskünfte danke ich meinen Interviewpartnern. Die im Report vertretenen Auffassungen werden nicht notwendig von allen Experten geteilt.

Kevin Baum, Wissenschaftlicher Mitarbeiter am Institut für Philosophie, Universität des Saarlandes (19. August 2015)

Prof. Dr. Petra Grimm, Leiterin des Institut für digitale Ethik, Stuttgart (19. August 2015)

Prof. Dr. Dr. Rafaela Hillerbrand, Leiterin der Forschungsgruppe Ethics for Energy Technology, Institut für Philosophie, RWTH Aachen (21. August 2015)

Dr. Constanze Kurz, Informatikerin und Sachbuchautorin, Sprecherin des Chaos Computer Clubs (11. August 2015)

Emmanuel Letouzé, Direktor und Mit-Gründer der Data Pop Alliance, New York City (14. September 2015)

Prof. Dr. Viktor Mayer-Schönberger, Professor für ‚Internet Governance and Regulation', Oxford Internet Institute (19. Oktober 2015)

Dr. Yves-Alexandre de Montjoye, Research Scientist, MIT Media Lab (18. August 2015)

Dr. Elisa Orrù, Wissenschaftliche Mitarbeiterin, Philosophische Fakultät der Albert-Ludwigs-Universität, Freiburg im Breisgau (21. August 2015)

Prof. Dr. Alex (Sandy) Pentland, Toshiba Prossor, Massachusetts Institute of Technology, Mit-Gründer des MIT Media Lab (29. September 2015)

Dr. Ben Scott, Senior Advisor to the Open Technology Institute/New America Foundation, Washington D.C., Visiting Fellow der Stiftung Neue Verantwortung, Berlin (14. August 2015)

Dr. Thilo Weichert, Vorstandsmitglied der Deutschen Vereinigung für Datenschutz e.V. (DVD) und ehem. Datenschutzbeauftragtes des Landes Schleswig-Holstein (12. August 2015)

Literatur

Anderson, Chris. „Das Ende der Theorie. Die Datenschwemme macht wissenschaftliche Methoden obsolet". In: Heinrich Geiselberger; Tobias Moorstedt (Hg.), Big Data: Das neue Versprechen der Allwissenheit. Berlin 2013.

Barnes, Susan. „A privacy paradox: Social networking in the United States". First Monday 2006. Vol. 11, Nr. 9. http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312.

Barocas, Solon; Nissenbaum, Helen. „Big data's end run around anonymity and consent". In: J. Lane; V. Stodden; S. Bender; H. Nissenbaum (Hg.), Privacy, Big Data, and the Public Good: Frameworks for Engagement. New York 2014.

Barth, A.; A. Datta; J. C. Mitchell, H. Nissenbaum. „Privacy and Contextual Integrity: Framework and Applications". Proceedings of the 2006 IEEE Symposium on Security and Privacy, S. 184-198.

Borges, Jorge Luis. „Von der Strenge der Wissenschaft". In: ders., Borges und ich. München 1982.

boyd, danah; Kate Crawford. „Big Data als kulturelles, technologisches und wissenschaftliches Phänomen. Sechs Provokationen". In: Heinrich Geiselberger; Tobias Moorstedt (Hg.), Big Data: Das neue Versprechen der Allwissenheit. Berlin 2013.

Calo, Ryan. „Digital Market Manipulation“. 82 George Washington Law Review 995. University of Washington School of Law Research Paper No. 2013-27, 2014.

http://dx.doi.org/10.2139/ssrn.2309703

Christl, Wolfie. „Durchleuchtet, analysiert und einsortiert“. Online-Kurzfassung der Cracked Labs-Studie „Kommerzielle digitale Überwachung im Alltag“. Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data: Internationale Trends, Risiken und Heraus-forderungen anhand ausgewählter Problemfelder und Beispiele“. Wien 2014. http://crackedlabs.org/studie-kommerzielle-ueberwachung.

Cohen, Julie E. „What Privacy is for“. 126 Harvard Law Review 1904, 2013.

Cukier, Kenneth; Viktor Mayer-Schönberger. Big Data: Die Revolution, die unser Leben verändern wird. München 2013.

Dubben, Hans-Hermann; Hans-Peter Beck-Bornholdt. Der Hund, der Eier legt: Erkennen von Fehlinformation durch Querdenken. Reinbek 2006.

Foster Wallace, David. Oblivion: Stories. New York 2004.

Foucault, Michel. Überwachen und Strafen: Die Geburt des Gefängnisses. Frankfurt 1977.

Geiselberger, Heinrich; Tobias Moorstedt. „Vorwort“. In: Heinrich Geiselberger; Tobias Moorstedt (Hg.), Big Data: Das neue Versprechen der Allwissenheit. Berlin 2013.

Geuter, Jürgen. „Big Dada statt Big Data — warum viele Big-Data-Analysen Blödsinn sind“. Wired 2015. https://www.wired.de/collection/latest/jurgen-geuter-erklart-warum-big-data-analysen-oft-falsch-interpretiert-werden.

Hagner, Michael; Dirk Helbing. „Technologiegetriebene Gesellschaft oder sozial orientierte Technologie. Ein Gespräch“, In: Heinrich Geiselberger; Tobias Moorstedt (Hg.), Big Data: Das neue Versprechen der Allwissenheit. Berlin 2013.

Kotikalapudi, Aghavendra; Sriram Chellappan; Frances Montgomery; Donald Wunsch; Karl Lutze. „Associating Internet Usage with Depressive Behavior Among College Students“. IEEE Technology and Society Magazine 2012, S. 73-80. http://web.mst.edu/~chellaps/papers/TSM.pdf.

Kosinski, Michal; David Stillwell; Thore Graepel. „Private traits and attributes are predictable from digital records of human behavior". PNAS 2013. Vol. 110, Nr. 15, S. 5802–5805. http://www.pnas.org/content/110/15/5802.full.pdf.

Kucklick, Christoph. Die granulare Gesellschaft. Berlin 2014.

Kurz, Constanze; Frank Rieger. Die Datenfresser. Frankfurt 2012.

Langkafel, Peter. „Dr. Algorithmus? Big Data in der Medizin." In: Aus Politik und Zeitgeschichte 11-12/2015, S. 27-32.

Laney, Doug. „3D data management: Controlling data volume, variety and velocity". META Group 2001. http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Letouzé, E.; A. Noonan; R. Bhargava; E. Deahl; D. Sangokoya; N. Shoup. „Beyond Data Literacy: Reinventing Community Engagement and Empowerment in the Age of Data". Data-Pop Alliance 2015.

Manson, Neil C.; Onora O'Neill. Rethinking Informed Consent in Bioethics. New York 2012.

Mayer-Schönberger, Viktor. „Zur Beschleunigung menschlicher Erkenntnis". In: Aus Politik und Zeitgeschichte 11-12/2015, S. 14-19.

McGregor, Carolyn. „Big Data in Neonatal Intensive Care". IEEE Computer Society 2013. http://lifesciences.ieee.org/images/pdf/06513228.pdf

de Montjoye Y.-A., Shmueli E., Wang S.S., Pentland A.S., „openPDS: Protecting the Privacy of Metadata through SafeAnswers". PLoS ONE 9(7) 2014. http://dx.doi.org/10.1371/journal.pone.0098790.

de Montjoye Y.-A., Radaelli L., Singh V. K., Pentland A. S., „Unique in the shopping mall: On the reidentifiability of credit card metadata". Science 2015, S. 536-539.

Moorstedt, Tobias. „Obamas Datenakrobaten". In: Heinrich Geiselberger; Tobias Moorstedt (Hg.), Big Data: Das neue Versprechen der Allwissenheit. Berlin 2013.

Morozov, Evgeny. „Ich habe doch nichts zu verbergen". In: Aus Politik und Zeitgeschichte 11-12/2015, S. 3-7.

Nissenbaum, Helen. Privacy in Context. Technology, Policy, and the Integrity of Social Life. SUP, CA 2009.

Pentland, Alex "Sandy". „Saving Big Data from Itself". Scientific American 2014, S. 64-67. http://www.nature.com/scientificamerican/journal/v311/n2/full/scientificamerican0814-64.html

Pietsch, Wolfgang. „Big Data –über Chancen und Risiken einer neuen Wissenschaft des Komplexen". Universitas 2013.

Plass-Fleßenkämper, Benedikt. „Citizen Score: China bewertet seine Bürger und ihre Lebensweise". Wired 2015. https://www.wired.de/collection/latest/china-fuhrt-citizen-scores-ein-um-seine-burger-nach-ihrer-lebensweise-zu-bewerten.

Roßnagel, Alexander. „Datenschutz im 21. Jahrhundert". In: Aus Politik und Zeitgeschichte 5-6/2006. http://www.bpb.de/apuz/29935/datenschutz-im-21-jahrhundert?p=all

Rössler, Beate. Der Wert des Privaten. Frankfurt 2001.

Rössler, Beate. „Privatheit und Autonomie: zum individuellen und gesellschaftlichen Wert des Privaten". In: Sandra Seubert; Peter Niesen (Hg.), Die Grenzen des Privaten. Baden-Baden 2010.

Schneider, Johannes. „Offen für alle". Der Tagesspiegel 2014. http://www.tagesspiegel.de/politik/privatheit-und-privatsphaere-offen-fuer-alle/9871342.html.

Schulz, Stefan. „Wir wissen, wen Du wählen wirst. Wie Big Data das Wahlgeheimnis aushebelt". Frankfurter Allgemeine Zeitung 2013. http://www.faz.net/aktuell/feuilleton/wie-big-data-das-wahlgeheimnis-aushebelt-wir-wissen-wen-du-waehlen-wirst-12553613.html.

Smart-Data-Begleitforschung. FZI Forschungszentrum Informatik (Hg.), Smart Data – Smart Privacy? Impulse für eine interdisziplinär rechtlich-technische Evaluation. Technical Report des BMWi-Technologieprogramms „Smart Data – Innovationen aus Daten" 2015. http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SmartData_Thesenpapier_smart_Privacy.pdf?__blob=publicationFile&v=7

Stöcker, Christian. „Politikfeld Big Data: Hoffnungen, Vorhaben und viele offene Fragen." In: Aus Politik und Zeitgeschichte 11-12/2015, S. 8-13.

Süddeutsche Zeitung. „Wikipedia verbessert Datenschutz." 2015. http://www.sueddeutsche.de/news/wirtschaft/internet-wikipedia-verbessert-datenschutz-dpa.urn-newsml-dpa-com-20090101-150615-99-05188.

Talbot, David. „A Phone that Knows Where You‘re Going“. MIT Technology Review 2012. http://www.technologyreview.com/news/428441/a-phone-that-knows-where-youre-going/.

The Wall Street Journal. „Which Websites Are Sharing Your Personal Details?“. 2012. http://blogs.wsj.com/digits/2012/12/07/which-websites-are-sharing-your-personal-details/ & http://www.wsj.com/public/page/what-they-know-digital-privacy.html.

Turow, Joseph. „‚Drinking from a Fire Hose‘: Has Consumer Data Mining Gone Too Far?“. Knowledge@Wharton 2011. http://knowledge.wharton.upenn.edu/article/drinking-from-a-fire-hose-has-consumer-data-mining-gone-too-far/.

Turow, Joseph; Michael Hennessy; Nora Draper. „The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation”. Annenberg School for Communication at U. of Pennsylvania 2015.

https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

Utz, S.; Kramer, N. „The privacy paradox on social network sites revisited: The role of individual characteristics and group norms“. Cyberpsychology: Journal of Psychosocial Research on Cyberspace 2009, 3(2), article 2.

http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2 .

Valéry, Paul. Mauvaises pensées et autres. In: ders., Oeuvres II, Paris 1960.

Vodafone Institut für Gesellschaft und Kommunikation. „Big Data. Wann Menschen bereit sind, ihre Daten zu teilen“. 2016. http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-Highlights-de.pdf

Weichert, Thilo. „Big Data, Gesundheit und der Datenschutz“. In: Datenschutz und Datensicherheit – DuD 2014, Vol. 38, Issue 12, S. 831-838

Weichert, Thilo. „Big Data und Datenschutz“. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein 2013. https://www.datenschutzzentrum.de/bigdata/20130318-bigdata-und-datenschutz.pdf

Yahoo! „The Balancing Act. Getting Personalization Right“. 2014. https://advertising.yahoo.com/Insights/BALANCING-ACT.html.

Zeit Online. „Wikipedia-Stiftung verklagt die NSA“. 2015. http://www.zeit.de/digital/datenschutz/2015-03/wikipedia-nsa-klage-ueberwachung.

Über die Autorin

Anna Wehofsits ist Akademische Rätin am Institut für Philosophie der Ludwigs-Maximilians-Universität in München. Sie hat zur Rolle von Emotionen in Kants Ethik an der Freien Universität Berlin promoviert und forscht zu Themen an der Schnittstelle von Ethik und Erkenntnistheorie, zu Fragen der Moralpsychologie, zu Gesundheitsgerechtigkeit sowie zu ethischen und politischen Fragen im Kontext neuer Informationstechnologien.

Über das Vodafone Institut

Das Vodafone Institut für Gesellschaft und Kommunikation beschäftigt sich mit der Frage, wie digitale Technologien politische, soziale und ökonomische Teilhabe erhöhen sowie den Zugang zu Bildung eröffnen. Als ‚Think and Do Tank' fördert das Institut den Dialog zwischen Wissenschaft, Wirtschaft und Politik. Hierzu entwickelt es eigene Projekte, initiiert Forschungskooperationen, publiziert Studien und praktische Handlungsempfehlungen.

Impressum

Herausgeber:
Vodafone Institut für Gesellschaft und Kommunikation GmbH
Behrenstraße 18
10117 Berlin

www.vodafone-institut.de

Autorin:
Dr. Anna Wehofsits,
Ludwig-Maximilians-Universität München

Verantwortlich für den Herausgeber:
Dr. Mark Speich
Dr. David Deißner

Kommunikation:
Friedrich Pohl

Layout:
Nick Böse

www.vodafone-institut.de
www.facebook.com/VodafoneInstitute
Twitter: @vf_institute

© Vodafone Institut für Gesellschaft und Kommunikation GmbH
Oktober 2016