verbraucherzentrale

Beiträge zur Verbraucherforschung
Band 5

Christian Bala und
Wolfgang Schuldzinski (Hrsg.)

Schöne neue Verbraucherwelt?

Big Data, Scoring und das Internet der Dinge

KVF | NRW

Kompetenzzentrum Verbraucherforschung Nordrhein-Westfalen

Beiträge zur Verbraucherforschung

herausgegeben von
Dr. Christian Bala
für das Kompetenzzentrum Verbraucherforschung NRW (KVF NRW) und
Wolfgang Schuldzinski
für die Verbraucherzentrale Nordrhein-Westfalen e. V.

ISSN 2197-943X

Band 5

Das 2011 gegründete KVF NRW hat die Aufgabe, die Verbraucherforschung zu unterstützen, um so eine Wissensbasis als Grundlage für effizientes verbraucher- und wirtschaftspolitisches Handeln zu schaffen. Mit den „Beiträgen zur Verbraucherforschung" dokumentiert das KVF NRW seine Workshops, die Wissenschaftlerinnen und Wissenschaftlern verschiedener Fachrichtungen die Gelegenheit bieten, sich interdisziplinär über verbraucherrelevante Fragen auszutauschen. Diese halbjährlichen Tagungen sollen die Diskussion zwischen Wissenschaft, Politik und Verbraucherorganisationen anregen. Die Schriftenreihe „Beiträge zur Verbraucherforschung" präsentiert sowohl die Vielfalt der Fragestellungen und Disziplinen als auch die Pluralität von Theorien und Methoden. Dies wird durch die Farbgebung der Umschläge unterstrichen: So wie sich das Licht aus verschiedenen Komponenten, den Spektralfarben, zusammensetzt, wird die Verbraucherforschung als ein gemeinsames Anliegen verstanden, das ein breites Spektrum an Zugängen und Themen vereint.

Das KVF NRW ist ein Kooperationsprojekt der Verbraucherzentrale NRW e. V. mit dem Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz (MKULNV) und dem Ministerium für Innovation, Wissenschaft und Forschung (MIWF) des Landes Nordrhein-Westfalen.

verbraucherzentrale Nordrhein-Westfalen

Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur und Verbraucherschutz des Landes Nordrhein-Westfalen

Ministerium für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen

Christian Bala und Wolfgang Schuldzinski (Hrsg.)

Schöne neue Verbraucherwelt?

Big Data, Scoring und das Internet der Dinge

Bibliografische Information der Deutschen Nationalbibliothek

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

1. Auflage, 2016

Die in diesem Band versammelten Beiträge geben die Meinung und die wissenschaftlichen Erkenntnisse der Autorinnen und Autoren wieder und müssen nicht mit den Meinungen und Positionen des KVF NRW, der Verbraucherzentrale NRW e. V., des MKULNV und des MIWF übereinstimmen.

ISSN 2197-943X
ISBN Print 978-3-86336-911-8
ISBN E-Book (PDF) 978-3-86336-912-5
DOI 10.15501/978-3-86336-912-5

Printed in Germany
Gedruckt auf 100 Prozent Recyclingpapier.

Inhalt

Einleitung: Schöne neue Verbraucherwelt?

Big Data, Scoring und das Internet der Dinge

Christian Bala und Wolfgang Schuldzinski

DOI 10.15501/978-3-86336-912-5_1

Abstract

Mit Big Data wird die Debatte um die Informatisierung des Alltags über die Frage nach dem Datenschutz hinaus geführt. Es geht nicht mehr allein um die Erfassung von Daten. Mit der Fähigkeit große, auch unstrukturierte Datenmengen zu speichern, miteinander zu verknüpfen und zu analysieren, können intelligente System Schlüsse ziehen. Verhaltensweisen werden vorhersagbar und auch manipulierbar, was Unternehmen die Möglichkeit gibt zielgenau zu werben, eine soziale Auslese zu betreiben und ihre Risiken zu minimieren. Verbraucherinnen und Verbraucher werden dabei zu Datenlieferanten, ohne dass ihnen die dahinter liegenden Strukturen und Mechanismen transparent sind.

1 Von Big Brother zu Big Barbie?

Durchdringend, mit kalten Augen, starrt der große Bruder von den Standbildern und Plakaten in den Verfilmungen der Orwellschen Dystopie „1984“. Ein Diktator, den das Volk lieben soll, und den es zugleich fürchtet, da jeder Einzelne weiß, dass er in dem totalitären Staat unter Beobachtung steht. Das ist die alte Fratze des Überwachungsstaates, vor der jeder zurückschreckt. So hässlich ist das neue Gesicht der Überwachung nicht mehr: Freundlich, mit großen Augen, lächelt die „Hello Barbie“ aus den Regalen und Online-Shops. Ein Spielzeug, das die Kinder lieben, aber nicht fürchten werden, denn schließlich sollen sie nicht nur mit der Puppe reden, sondern sich ihr auch anvertrauen: „Just like a real friend, Hello Barbie™ doll listens and remembers the user‘s likes and dislikes, giving everyone their own unique experience“, heißt es in der Produktbeschreibung auf der Webseite des Herstellers (Mattel, Inc. 2015). Dafür gab es 2015 den „Big Brother Award“ des Vereins Digitalcourage, denn die Puppe, die in Europa wegen Datenschutzbedenken (noch) nicht zu haben ist, überträgt die Gespräche an eine Serverfarm der Firma Toytalk, wo sie nicht nur für Marketingzwecke und zur Verbesserung des Produkts ausgewertet, sondern auch in Protokollen für die Eltern per E-Mail aufbereitet werden (siehe Neumann 2015). Käuferinnen und Käufer zahlen also rund 75 US-Dollar dafür, dass ihre Kinder zu Datenquellen für Unternehmen werden, kostenlos deren Produkte verbessern und über die kleinen Geheimnisse ihres Nachwuchses Bescheid wissen. Wobei das Produkt, kaum auf dem Markt, bereits durch den Kryptologen Matt Jakubowski gehackt war. Er konnte auf „Account-IDs, Audiodateien, das Mikrofon und Netzwerknamen“ zugreifen, „mit etwas mehr Aufwand“ ließ sich die Puppe „auch mit einem anderen Server verbinden – und damit dann auch steuern, was die Barbie sagt.“ (Schirrmacher 2015)

Überwachung in der Welt des Konsums hat, so der Jurist Daniel J. Solove (2004; 2011), weniger die Disziplinierung zum Ziel, weshalb er die Metapher vom „Big Brother“ für überstrapaziert hält. Vielmehr geht es um die Gewinnung eines Datenpools, um mehr über das Verhalten der Kundinnen und Kunden zu erfahren. „Consumer surveillance can be understood as a form of surveillance that aims at predicting and, in combination with (personalized) advertising, controlling the behavior of consumers.“ (Sandoval 2012, 148) Indem die Unterneh-

men das Verhalten der „Verbrauchenden“ besser kennen und daraus Vorhersagen ableiten, können sie nicht nur ihre Produkte besser an den Mann oder die Frau bringen, sondern zwischen begehrten und ungewollten Kundinnen und Kunden unterscheiden (siehe Bala und Müller 2014, 26; Bendrath 2007, 7). Dieses Ziel wird durch die „Datenfusion“ erreicht, also das Zusammenspiel verschiedener Datenquellen im Zusammenspiel mit Maschinen, die Muster erkennen und daraus Schlüsse ziehen, auf deren Basis Entscheidungen gefällt werden (siehe Hofstetter 2014; Schlieter 2015; Schneier 2015).

Dabei müssen noch nicht einmal die eigenen Daten unmittelbar negative Auswirkungen haben. Vielmehr ermöglicht es bereits die Masse der gesammelten Daten Menschen nach Gruppen zu klassifizieren, denen bestimmte Eigenschaften zugewiesen werden. Daraus wird dann abgeleitet, wie sich ein anderes Individuum, dessen Merkmale mit denen der identifizierten Gruppe übereinstimmen, wahrscheinlich verhalten wird, unabhängig davon, ob diese Voraussage zutrifft oder nicht. Big Data, also die Fähigkeit große, auch unstrukturierte Datenmengen nicht nur zu speichern, sondern auch miteinander zu verknüpfen und zu analysieren, kann dazu führen, dass Verbraucherinnen und Verbraucher, ohne dass sie es wissen und ohne dass ihr reales Verhalten dazu beigetragen hat, einer negativen Auslese durch Unternehmen ausgesetzt sind (siehe Bauman 2009, 11). „Als Schlagwort steht Big Data für die Überlagerung eines statistisch fundierten Kontrollwissens durch eine medientechnologisch fundierte Makroorientierung an der ökonomischen Verwertbarkeit von Daten und Informationen.“ (Reichert 2016, 22)

Die Grundlage dieses Scorings ist meist undurchsichtig und kann deshalb auch recht willkürlich sein. So berichtet Frank Pasquale in seinem Buch „The Black Box Society“, dass eine Kreditkartenfirma sich für die mentale Gesundheit ihrer Kundschaft interessierte. Datenauswertungen hatten ergeben, dass Paare, die eine Paartherapie aufsuchen, sich eher scheiden lassen, als Paare die das nicht tun. Scheidungen können aber zu finanziellen Belastungen und Kreditausfällen führen. Nun durchforstete das Unternehmen die Buchungen der Kundinnen und Kunden, mit der Folge, dass die Kreditwürdigkeit von Personen in Zweifel stand, nur weil sie eine Paarberatung aufsuchten (siehe Pasquale 2015, 37). „Put another way, credit-card companies are becoming much more interested in understanding their customers’ lives and psyches, because, the theory goes, knowing what makes cardholders tick will help firms

determine who is a good bet and who should be shown the door as quickly as possible.“ (Duhigg 2009). Obwohl keine Kausalität zwischen einer Eheberatung und verzögerter Kreditrückzahlung besteht, reichte dem Unternehmen die Korrelation zwischen Eheberatung und Scheidung aus, um die Kreditlinie von Kundinnen und Kunden zu kürzen, die versuchten, ihre ehelichen Probleme zu lösen – und den Fehler begingen, den Therapeuten mit ihrer Kreditkarte zu bezahlen (siehe Pasquale 2015, 37).

Die mit einem schlechten Scorewert versehenen Verbraucherinnen und Verbraucher wissen nichts, wie Joseph K. in Franz Kafkas „Der Prozess“ (2005), über die Gründe für die Entscheidung: „The Trial captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one’s life. At any time, something could happen to Joseph K.; decisions are made based on his data, and Joseph K. has no say, no knowledge, and no ability to fight back. He is completely at the mercy of the bureaucratic process.“ (Solove 2004, 38) Das Urteil in dieser schönen neuen Verbraucherwelt wird auf der Basis der verfügbaren Daten getroffen.

2 Wer hat schon was gegen ein gesünderes Leben?

Basierte die Praxis der Kreditkartenfirma noch auf konkreten Zahlungen ihrer Kundinnen und Kunden, sind die Daten die das Internet der Dinge generiert vielfältig, die Datenmengen sind riesig und der Datenstrom ist kaum zu kontrollieren. Zudem ist nicht ersichtlich, wer Zugriff auf diese Daten hat und wie sie verwertet werden. Einer Diskussion über diese Intransparenz und Unschärfe versuchen Anbieter zu entgehen, indem sie den Nutzen ihrer Technologien anpreisen und die Steigerung der Lebensqualität in den Vordergrund stellen. Das Internet der Dinge und Big Data sollen als Hilfe, ja als Lösung von Problemen erscheinen. Die Haltung Probleme durch Technik lösen zu wollen, ist Bestandteil einer Weltsicht, die Evgeny Morozov als Solutionismus bezeichnet

hat. Damit beschreibt er aber nicht nur einen technikzentrierten Blick auf soziale oder wirtschaftliche Herausforderungen, sondern die Tendenz Umstände als Problem zu identifizieren, die eigentlich keine sind (siehe Morozov 2013, 26). Wearables, also Smartwatches oder Fitnessarmbänder, sind Beispiele für eine „solution in search of a problem" (Piwek et al. 2016).

Wearables und Apps die eine Zulassung als Medizinprodukte haben, können sicherlich dazu beitragen, die Werte von Risikopatienten oder chronisch Erkrankten zu überwachen und so ihr Wohlbefinden und ihre Sicherheit zu steigern. Braucht man aber tatsächlich eine elektronische Zahnbürste mit Bluetooth, welche das Putzverhalten in einer App protokolliert? Ist es sinnvoll, ständig die Vitalzeichen eines gesunden Neugeborenen über einen Schnuller auf das elterliche Smartphone übertragen zu lassen (siehe Blue Maestro Limited 2016), um dann bei jedem Temperaturanstieg den Kinderarzt aufzusuchen?

Die Versicherer betonen den Nutzen einer Verknüpfung von Wearables und Big Data und übernehmen dabei die Argumentationen der Anbieter von Trackern und entsprechender Software. So verkündete der Vertreter eines großen Versicherungskonzerns auf einer Tagung über Big Data, dass die Nutzerinnen und Nutzer durch Selbstvermessung und die Auswertung von Vergleichsdaten auf mögliche schwere Erkrankung hingewiesen werden könnten. Wer könne denn schon etwas dagegen haben, wenn man durch Wearables und Health Apps ein gesünderes Leben führe? Und so auch der Vorstandsvorsitzende der Techniker Krankenkasse Jochen Baas in einem Interview mit der „Süddeutschen Zeitung": „Wir können über das Risiko einer Erkrankung informieren, wenn wir die Krankheiten, den Puls, das Ausmaß der Bewegung und so weiter zusammen analysieren." (Jochen Baas im Interview mit Bohsem und Schäfer 2016).

Abgesehen davon, dass man mit dieser Argumentation auch zu standardmäßigen DNA-Analysen und regelmäßige MRTs raten könnte, denn schließlich werden so Dispositionen für Krankheiten erkennbar, verschleiert sie nur mühsam die dahinter stehenden Interessen, nämlich die Risiken für das eigene Unternehmen zu minimieren. Mit seiner Argumentation schien der Versicherungsvertreter nicht allein die Datenschutzbedenken vom Tisch wischen zu wollen, sondern vor allem den Stachel gegen jene Stimmen zu löcken, welche vor den gesellschaftlichen Auswirkungen der Informatisierung warnen.

Fanden Wearables zunächst begeisterte Aufnahme in der Szene von Selbstvermessern und -optimierern (siehe Selke 2014), werden sie seit 2015 von privaten und gesetzlichen Krankenversicherern entdeckt. Vorreiter sind hier die USA: Arbeitgeber und betriebliche Krankenversicherer erhoffen sich, durch diese Geräte den Krankenstand der Belegschaft zu senken. Noch ist die Teilnahme an solchen Programmen weitgehend freiwillig, doch die christlich-evangelikale Oral Roberts University in Oklahoma hat für neue Studierende das Fitbit-Armband zur Pflicht gemacht. Diese erhobenen Daten werden an die Hochschule übermittelt und zur Grundlage der Bewertung in einigen Kursen. (Siehe Frankel 2016; Thielman 2016)

In Deutschland bot Anfang 2015 die Generali als einer der ersten Anbieter Kranken- und Berufsunfähigkeitsversicherungen an, die günstigere Tarife für diejenigen Kundinnen und Kunden versprachen, die regelmäßig Sport treiben und dies über einen Tracker und ihr Smartphone nachweisen. Die gesetzlichen Krankenkassen zogen nach, und belohnen Fitnessaktivitäten mit Wearables nun im Rahmen ihrer Bonusprogramme, die es seit 2004 erlauben eine gesunde Lebensführung mit Geld zu belohnen. Gemessen wird momentan nur aufgrund der geltenden Datenschutzgesetze, ob die Bedingungen für die Bonusprogramme erfüllt sind, beispielsweise eine bestimmte Anzahl an Schritten. (M. M. Becker 2016, 36)

Diese Haltung erscheint schon auf der Ebene der Grundannahmen problematisch und zeugt von solutionistischem Denken. Fast erinnert diese Strategie an das alte Bonmot, dass ein Gesunder nicht gesund, sondern nur schlecht untersucht ist. Da es nun die Möglichkeit gibt, den Puls, Atemfrequenz, Schweißproduktion, etc. direkt zu messen, sollte sie auch ausgeschöpft werden, auch wenn Ärzte mit den Tracking-Daten wenig anfangen können: „Für Franz Bartmann, Vorstandsmitglied der Bundesärztekammer, sind Tracking-Daten in Patientenakten „Datenmüll“. Die vorwiegenden Nutzer seien leistungsbereite junge Menschen, die meist kein Fall für den Arzt seien. Sinnvolle Daten, die vom Patienten erfasst werden und in die Behandlung einfließen, müssten darüber hinaus die strengen Kriterien des Medizinproduktegesetzes erfüllen.“ (K. B. Becker 2016)

Diese Sichtweise wird durch eine Studie über Consumer Health Wearables bestätigt, die betont, dass Personen, die einen gesunden Lebensstil pflegen,

ihre eigenen Fortschritte quantifizieren wollen (siehe Piwek et al. 2016). Darüber hinaus wird die tatsächliche medizinische Brauchbarkeit dieser Produkte infrage gestellt und ihre Reliabilität und Validität angezweifelt: „Devices are marketed under the premise that they will help improve general health and fitness, but the majority of manufactures provide no empirical evidence to support the effectiveness of their products." (Piwek et al. 2016). Die Gefahr von Fehlalarmen und Selbstdiagnosen, die zur Verunsicherung der Nutzerinnen und Nutzer beitragen, sind ebenfalls Risiken, vor denen gewarnt wird (siehe Piwek et al. 2016).

Neben Zweifeln an der Brauchbarkeit der verfügbaren Geräte für das Ziel der Gesundheitsüberwachung und Bedenken in puncto Datenschutz und Datensicherheit weist Health Tracking noch eine gesellschaftliche und politische Dimension auf: Bonusprogramme ziehen vor allem gesunde Versicherte an, die für sich einen Nutzen sehen, ihre Daten gegen Geld zu tauschen (siehe M. M. Becker 2016, 36). Dieses Verhalten ist in der wissenschaftlichen Literatur als Unraveling bekannt (siehe u. a. Benndorf, Kübler und Normann 2015; Jentzsch 2016; Peppet 2015). „Für jene Versicherte, die aufgrund ihrer Lebensumstände den größten gesundheitlichen Risiken ausgesetzt sind – kurz gesagt Alleinerziehende, Arme, Erwerbslose und Menschen ohne soziale Bezüge – sind die Anreize zu gering und die Hürden zu hoch, um ihr Verhalten zu ändern." (M. M. Becker 2016, 37) Dies kann aber zu diskriminierenden Effekten führen, die schon aus dem Scoring bekannt sind, denn nicht zufügbare Daten könnten als „schlechtes Riskio" interpretiert werden; als jene die nichts für ihre Gesundheit tun, keinen Präventionswillen oder Eigenverantwortung zeigen (siehe M. M. Becker 2014). Letztlich würde die Bereitschaft zur Einschränkung der Privatsphäre der einen, zu einer Schlechterstellung derjenigen führen, die nichts preisgeben wollen oder können. (Siehe auch Jentzsch 2016)[1]

1 Dieser Effekt kann auch im digitalen Wohnungsmarkt beobachtet werden. Bei Immobilienscout24 können Wohnungssuchende Einkommensnachweise, Bonitäts- und Selbstauskünfte hochladen, die dann von den potenziellen Vermietern eingesehen werden können. Ein auskunftsfreudiges Profil wird als „Top-Bewerber" angezeigt. Wer allerdings über ein geringeres Einkommen verfügt und deshalb keine Nachweise hochlädt, könnte bei der Vorauswahl bereits durchs Raster fallen. (Siehe Müller 2016)

Der Prozess der Offenlegung, warnt Nicola Jentzsch (2016) vom Deutschen Institut für Wirtschaftsforschung (DIW, Berlin), könnte aufgrund seiner inneren Logik zur sozialen Norm werden. Schon die Zukunftsvisionen der privaten und gesetzlichen Versicherer zeigen ambitioniertere Ziele: TK-Chef Baas träumt bereits jetzt davon, dass jedermann „so ein Gerät haben" wird (Jochen Baas im Interview mit Bohsem und Schäfer 2016). Wird aber die Selbstvermessung zur Norm, wird auch der damit verbundenen Ideologie der Selbstoptimierung, im Sinne einer fehlerfreien Funktion, zur Akzeptanz verholfen, was im Gegensatz zum Solidarprinzip steht: „Leistungsträger werden von Leistungsverweigeren getrennt, Kostenverursacher von Kosteneinsparern, ‚Health-On'-Menschen (Gesunde) von ‚Health-Off'-Menschen (Kranke)" (Selke 2015, 83).

3 Big Data – mehr als Datenschutz oder Datensicherheit

Big Data führt die Debatte über die Informatisierung über die engere Frage nach dem Datenschutz hinaus, denn die „Ordnung des Wissens ist immer auch eine politische Ordnung" (Grassmuck 2012, 15). Das Internet der Dinge hebt die Frage nach der Datensicherheit auf ein neues Niveau, wenn die Gebrauchsgegenstände angreifbar werden, siehe das Beispiel „Hello Barbie" (siehe Schirrmacher 2015). Mit Big Data und dem Internet der Dinge sind erhebliche gesellschaftliche, politische und soziale Fragen verbunden. Technik ist kein neutrales Werkzeug, sondern prägt das Denken und Verhalten (siehe Latour 1996; Mainzer 2014; Weizenbaum 1978). Und bei allen Beteuerungen der Anbieter mit ihren Produkten die Welt zu verbessern, haben sie ein wirtschaftliches Eigeninteresse, so stehen die Anbieter von Fitnesstrackern unter hohem Druck der Investoren (siehe Windeck 2016). Durch die Fähigkeit große, auch unstrukturierte Datenmengen zu speichern, miteinander zu verknüpfen und zu analysieren, können intelligente Systeme Schlüsse ziehen. Verhaltensweisen werden vorhersagbar und auch manipulierbar, was Unternehmen die Möglichkeit gibt, zielgenau zu werben, eine soziale Auslese zu betreiben und ihre Risiken zu minimieren. Verbraucherinnen und Verbraucher werden dabei

zu Datenlieferanten, ohne dass ihnen die dahinter liegenden Strukturen und Mechanismen transparent sind.

In diesem Spannungsfeld aus Recht, Informatik und Sozialwissenschaft bewegte sich der 7. Workshop Verbraucherforschung, der am 15. Juni 2015 in Düsseldorf in Kooperation mit dem Düsseldorfer Instituts für Wettbewerbsökonomie (DICE) der Heinrich-Heine-Universität stattfand und dessen Vorträge diesem Band zugrunde liegen:

- Der Physiker und Soziologe *Dirk Helbing*, der unlängst mit Yvonne Hofstetter, Gerd Gigerenzer und anderen ein „Digital-Manifest" für eine digitale Demokratie veröffentlicht hat (Helbing et al. 2016), hegt in seinem Artikel grundlegende Skepsis an den Hoffnungen, die mit Big Data als einer „Super-Intelligenz" verknüpft werden. Vielmehr sieht er die Drohung einer automatisierten Gesellschaft, die auf der Basis von Big-Data-Analysen Entscheidungen trifft. Im Gegensatz dazu entwirft er die Idee einer kollektiven Intelligenz, welche eine partizipative Form der Nutzung des Netzes darstellt.

- Der Beitrag von *Barbara Kolany-Raiser*, die an der Westfälischen Wilhelms-Universität Münster das interdisziplinäre Projekt ABIDA (Assessing Big Data) koordiniert, zeigt die rechtlichen Probleme, die mit smarten Alltagsgegenständen und insbesondere Wearables im Gesundheitsbereich verbunden sind. Sie zeigt die fehlende Transparenz der Anbieterseite auf und öffnet den Blick dafür, dass gegenwärtig vor allem die Verbraucherinnen und Verbraucher die Risiken tragen, welche sich durch Nutzung dieser Güter ergeben.

- Die Integration intelligenter Systeme und die Aussicht auf autonomes Fahren sollen die Sicherheit im Straßenverkehr erhöhen. Doch was ist, wenn das Auto *aufgrund* der smarten Technologie zu einem Sicherheitsrisiko wird? *Kerstin Lemke-Rust* gibt in ihrem Artikel einen Überblick, welche Bereiche besonders sensibel sind. Ihre daraus abgeleiteten Handlungsempfehlungen zeigen, dass noch viele Herausforderungen angegangen werden müssen.

- Die Debatte um die Implementierung eines smarten Stromnetzes greift *Ulrich Greveler* auf und stellt Interessenkonflikte zwischen dem Anspruch

eine moderne, effiziente und nachhaltige Infrastruktur zu schaffen und dem Recht auf Privatsphäre fest. Doch diese Interessen müssen nicht unvereinbar sein, wenn der Datenschutz bei der gesetzlichen Ausgestaltung ernst genommen und dessen Einhaltung auch konsequent umgesetzt wird. Auch müsse ein Opt-Out-Recht der Verbraucherinnen und Verbraucher in Erwägung gezogen werden.

- Smarte Autos und Netze, auf diese Datenquellen haben Verbraucherinnen und Verbraucher keinen Zugriff, da die Software eng mit der Hardware verbunden ist und keine Eingriffe Dritter erlaubt. Über ihre mobilen Endgeräte meinen die Nutzerinnen und Nutzer jedoch die Kontrolle zu haben, eine Illusion wie *Michael Schleusener* und *Sarah Hosell* in ihrem Beitrag zeigen, der die Ergebnisse eines im Rahmen des KVF NRW geförderten Forschungsprojektes zusammenfasst, das auch im Bericht zum Online-Handel des Sachverständigenrates für Verbraucherfragen (SVRV) beim Bundesministerium der Justiz und für Verbraucherschutz (BMJV) Erwähnung fand (siehe Reisch et al. 2016). Die Verbraucherinnen und Verbraucher sind, so belegen sie, durch die unkontrollierte Auswertung von Daten manipulierbar geworden.

Danksagung

Der Dank der Herausgeber gilt allen, die dabei geholfen haben, den fünften Band der „Beiträge zur Verbraucherforschung“ zu ermöglichen. An erster Stelle sind natürlich die Autorinnen und Autoren zu nennen. Besonderer Dank gebührt Prof. Dr. Justus Haucap vom DICE, der mit uns gemeinsam den 7. Workshop Verbraucherforschung ausrichtete. Wir danken unseren Kooperationspartnern, dem Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz (MKULNV) und dem Ministerium für Innovation, Wissenschaft und Forschung (MIWF) des Landes Nordrhein-Westfalen, für die Unterstützung bei der Produktion und der Verankerung der „Beiträge zur Verbraucherforschung“ als fester Bestandteil des KVF NRW. Kathrin Velewald und Corinna Koch haben die Artikel redaktionell betreut. Unsere Lektorin Heike Plank hat mit ihrer gründlichen Hand die kleinen und großen Schnitzer entdeckt. Aranka Schindler von der Gruppe Publikationen der Verbraucherzentrale Nordrhein-Westfalen hat den Band von der Verlagsseite her betreut.

Literatur

Bala, Christian und Klaus Müller. 2014. Der gläserne Verbraucher: Konsum und Überwachung. Sozialwissenschaftliche Vorbemerkungen. In: *Der gläserne Verbraucher: Wird Datenschutz zum Verbraucherschutz?*, hg. von Christian Bala und Klaus Müller, 11–40. Bd.1. Beiträge zur Verbraucherforschung. Düsseldorf: Verbraucherzentrale NRW. http://www.verbraucherzentrale.nrw/bzv1.

Bauman, Zygmunt. 2009. *Leben als Konsum.* Hamburg: Hamburger Edition.

Becker, Kim Björn. 2016. Kassen wollen Daten von Fitness-Armbändern nutzen. *Süddeutsche.de* (8. Februar). http://www.sueddeutsche.de/wirtschaft/gesundheit-kassen-wollen-daten-von-fitness-armbaendern-nutzen-1.2855193 (Zugriff: 9. März 2016).

Becker, Matthias Martin. 2014. *Mythos Vorbeugung: Warum Gesundheit sich nicht verordnen lässt und Ungleichheit krank macht.* Wien: Promedia.

—. 2016. Tracken, Checken, Sharen. *Gen-ethischer Informationsdienst,* Nr. 234 (Februar): 35–37.

Bendrath, Ralf. 2007. Der gläserne Bürger und der vorsorgliche Staat: Zum Verhältnis von Überwachung und Sicherheit in der Informationsgesellschaft. *kommunikation@gesellschaft 8* (Beitrag 7). http://www.soz.uni-frankfurt.de/K.G/B7_2007_Bendrath.pdf.

Benndorf, Volker, Dorothea Kübler und Hans-Theo Normann. 2015. Privacy concerns, voluntary disclosure of information, and unraveling: An experiment. *European Economic Review 75* (April): 43–59. doi:10.1016/j.euroecorev.2015.01.005.

Blue Maestro Limited. 2016. Pacif-i: the smart thermometer Pacifier for iOS and Android. https://www.pacif-i.io/ (Zugriff: 8. März 2016).

Bohsem, Guido und Ulrich Schäfer. 2016. „Jeder von uns wird so ein Gerät haben". *Süddeutsche Zeitung* (7. Februar). http://www.sueddeutsche.de/wirtschaft/montagsinterview-jeder-von-uns-wird-so-ein-geraet-haben-1.2852584?reduced=true (Zugriff: 9. März 2016).

Duhigg, Charles. 2009. What does your credit-card company know about you? *The New York Times Magazine* (12. Mai). http://nyti.ms/1Lwmum3 (Zugriff: 4. März 2016).

Frankel, Todd C. 2016. Fitbits now mandatory for students at this Oklahoma university. *The Washington Post* (2. Februar). https://www.washington-

post.com/news/the-switch/wp/2016/02/02/fitbits-now-mandatory-for-students-at-this-oklahoma-university/ (Zugriff: 3. März 2016).

Grassmuck, Volker. 2012. Exkursion in die Coy-Galaxis. In: *Per Anhalter durch die Turing-Galaxis,* hg. von Andrea Knaut, Christian Kühne, Rainer Rehak, Stefan Ullrich, Constanze Kurz, und Jörg Pohle, 9–15. Münster: Verl.-Haus Monsenstein und Vannerdat.

Helbing, Dirk, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari und Andrej Zwitter. 2016. Digitale Demokratie statt Datendiktatur: Das Digital-Manifest. *Spektrum der Wissenschaft,* Nr. 1: 50–61. http://www.spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933 (Zugriff: 11. März 2016).

Hofstetter, Yvonne. 2014. *Sie wissen alles: Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen.* München: C. Bertelsmann.

Jentzsch, Nicola. 2016. Auflösung der Privatsphäre – Ende der Solidarität. *DIW Wochenbericht* (8): 168.

Kafka, Franz. 2005. *Der Prozess: Roman.* Frankfurt am Main: Suhrkamp.

Latour, Bruno. 1996. *Der Berliner Schlüssel: Erkundungen eines Liebhabers der Wissenschaften.* Berlin: Akademie Verlag.

Mainzer, Klaus. 2014. *Die Berechnung der Welt: Von der Weltformel zu Big Data.* München: C. H. Beck.

Mattel, Inc. 2015. Hello Barbie™ Doll – Blonde Hair. *Mattel Shop.* http://shop.mattel.com/product/index.jsp?productId=65561726 (Zugriff: 2. März 2016).

Müller, Benedikt. 2016. Digitale Wohnungssuche: Wer sich auszieht, gewinnt. *Süddeutsche Zeitung* (23. März): 15.

Neumann, Linus. 2015. Technik: „Hello Barbie". *Big Brother Awards.* https://bigbrotherawards.de/2015/technik-hello-barbie (Zugriff: 2. März 2016).

Pasquale, Frank. 2015. *The black box society: The secret algorithms that control money and information.* Cambridge, Mass.: Harvard University Press.

Peppet, Scott R. 2015. Unraveling privacy: The personal prospectus and the threat of a full-disclosure future. *Northwestern University Law Review* 105 (3): 1153-1204. http://scholarlycommons.law.northwestern.edu/nulr/vol105/iss3/4.

Piwek, Lukasz, David A. Ellis, Sally Andrews und Adam Joinson. 2016. The rise of consumer health wearables: promises and barriers. *PLOS Medicine* 13, Nr. 2 (2. Februar): e1001953. doi:10.1371/journal.pmed.1001953.

Procter & Gamble Service GmbH. 2015. Oral-B SmartSeries. http://www.oralb-blendamed.de/de-DE/smartseries-app (Zugriff: 8. März 2016).

Reichert, Ramón. 2016. Das Politische der Großdatenforschung. *Politikum* 2, Nr. 1: 20–31.

Reisch, Lucia, Daniela Büchel, Gesche Joost und Zander-Hayat, Helga. 2016. *Digitale Welt und Handel: Verbraucher im personalisierten Online-Handel.* Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) beim Bundesministerium der Justiz und für Verbraucherschutz (BMJV). http://www.svr-verbraucherfragen.de/wp-content/uploads/2016/01/Digitale-Welt-und-Handel.pdf.

Sandoval, Marisol. 2012. A critical empirical case study if consumer surveillance on Web 2.0. In: *Internet and surveillance: The challenges of Web 2.0 and social media,* hg. von Christian Fuchs, Kees Boersma, Anders Albrechtsl und, und Marisol Sandoval, 147–169. New York: Routledge.

Schlieter, Kai. 2015. *Die Herrschaftsformel: Wie Künstliche Intelligenz uns berechnet, steuert und unser Leben verändert.* Frankfurt am Main: Westend.

Schneier, Bruce. 2015. Data and Goliath: *The hidden battles to collect your data and control your world.* New York, NY: Norton.

Schrirrmacher, Dennis. 2015. „Hello Barbie": Interaktive Barbie gehackt. *heise Security.* 27. November. http://heise.de/-3025550 (Zugriff: 2. März 2016).

Selke, Stefan. 2014. *Lifelogging: Wie die digitale Selbstvermessung unsere Gesellschaft verändert.* Berlin: Econ.

—. 2015. Lifelogging oder: Der fehlerhafte Mensch. *Blätter für deutsche und innternationale Politik* 60 (5): 79-86.

Solove, Daniel J. 2004. *The digital person: Technology and privacy in the information age.* New York: New York University Press. http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text.htm.

—. 2011. Nothing to hide: *The false tradeoff between privacy and security.* New Haven: Yale University Press.

Thielman, Sam. 2016. Fitbit used to track students' physical activity at Oral Roberts University. *The Guardian* (29. Januar). http://www.theguardian.

com/us-news/2016/jan/29/oral-roberts-university-fitibit-students-physical-fitness-freshman-15 (Zugriff: 3. März 2016).
Weizenbaum, Joseph. 1978. *Die Macht der Computer und die Ohnmacht der Vernunft.* Frankfurt am Main: Suhrkamp.
Windeck, Christof. 2016. Wearables: Nach Fitbit auch Jawbone schwächer bewertet. *heise online.* 17. Januar. http://heise.de/-3072904 (Zugriff: 9. März 2016).

Ferngesteuert oder selbstgesteuert

Perspektiven der digitalen Gesellschaft

Dirk Helbing

DOI 10.15501/978-3-86336-912-5_2

Abstract

Wären unsere Entscheidungen, wäre unsere Gesellschaft besser, wenn wir über größere Datenmengen verfügen würden? Könnte ein weiser König, oder ein wohlwollender Diktator mit Big Data die beste aller Welten schaffen? Überraschenderweise müssen wir diese Frage verneinen. Denn bereits die Grundannahmen hinter dieser Vorstellung sind fehlerhaft. Sowohl der Versuch, eine „digitale Kristallkugel" zu bauen, um unsere Zukunft vorherzusagen, ist zum Scheitern verurteilt, als auch das Unterfangen, einen „digitalen Zauberstab" zu entwickeln, um die Zukunft zu kontrollieren; beides unabhängig davon, wie mächtig die Informationssysteme sind, die wir noch entwickeln.

Der folgende Text ist das Transkript eines Vortrages, der am 28. September 2015 auf der Cologne Conference Futures 2015 gehalten wurde.

1 Einleitung

Es stimmt: Wir haben die Zeit, in der wir über zu wenige Daten verfügten, um evidenzbasierte Entscheidungen zu treffen, hinter uns gelassen. Dennoch klafft eine Lücke zwischen den Daten über unsere Welt und der Rechenleistung, um diese Daten zu verarbeiten. Diese Lücke vergrößert sich rasch und beständig. Überdies wächst die Komplexität der Welt mit der zunehmenden Vernetzung schneller als die Datenmenge. Ist also der Kampf gegen die Komplexität von vornherein verloren? Ja, das ist er – wenn wir nicht lernen, die Komplexität für uns zu nutzen. Das könnte uns aber durch den Übergang von zentralisierten Kontrollmechanismen zu Mechanismen verteilter Kontrolle gelingen.

Dieser Tage sind wir natürlich alle bewegt vom VW-Skandal. Wir machen uns Sorgen um die Auswirkungen für Deutschland, für die Marke „Made in Germany". Natürlich ist dies nicht der erste Fall von Vertrauensverlust, bei dem sich eine Branche selbst demontiert. Wir kennen das beispielsweise auch aus der Bankenbranche, wo die Finanzkrise zu Verlusten von 15 Billionen Dollar geführt hat. Das zeigt uns, wie groß die Herausforderungen sind, vor denen wir heutzutage stehen. Es stellt sich die Frage: Wie finden wir den besten Weg in die digitale Gesellschaft, in unsere digitale Zukunft?

Wir können dabei sicherlich viele Fehler machen. Und deswegen möchte ich ganz gerne an ein Projekt erinnern, das versucht hat hier einen Meilenstein zu setzen, Orientierung zu geben: FuturICT[1]. Dieses Projekt umfasste drei Hauptkomponenten, es wollte mit einer Milliarde Euro Fördergelder ein planetares Nervensystem bauen, um

1. Daten über diese Welt zu generieren,
2. diese Daten zu verwenden, um etwas über die möglichen Alternativen, die wir haben, zu lernen und
3. ein partizipatives System zu kreieren, sodass jeder diese Daten nutzen könnte.

1 http://www.futurict.eu

Dieses Projekt war damals wirklich auf einem sehr guten Weg. Es gab weit über hundert akademische Institutionen, die sich beteiligen wollten. Es gab viele Forschungsorganisationen und Unternehmen, die es unterstützt haben. Überdies waren wir damals der Favorit im Rahmen des Flagship-Wettbewerbs, und trotzdem wurden wir dann, wie der Vorredner es formuliert hat, „dem Schöpfer vorgestellt". Das heißt, dieses Projekt wurde abgesägt, und Sie werden im Laufe des Beitrags vielleicht auch besser verstehen, warum.

2 Fehlentwicklungen

Ich denke, jetzt ist es an der Zeit, die Zukunftsherausforderungen zu bewältigen. Lange Zeit haben wir an eine magische Formel geglaubt, die heißt: Mehr Daten bedeutet mehr Wissen, mehr Wissen bedeutet mehr Macht und mehr Macht bedeutet mehr Erfolg. Leider Gottes funktioniert diese Formel nicht, und Sie werden nach diesem Vortrag verstehen, warum wir einen anderen Ansatz brauchen.

Warum kann ich das behaupten? Wir haben heute natürlich mehr Daten denn je, die beste Wissenschaft, die beste Technologie und die besten Absichten, und trotzdem stehen wir in der Welt vor einem Berg von ungelösten Problemen, wie dem Klimawandel, der Finanz- und Wirtschaftskrise, der Schuldenkrise und schließlich der Instabilität des Friedens, die wir – glaube ich – alle spüren. Woran liegt das? Wie kann das sein?

Zunächst einmal sieht es eigentlich ganz vielversprechend aus, denn jetzt haben wir endlich Daten, mit denen wir evidenzbasierte Entscheidungen treffen können. Big Data bietet uns natürlich neue Möglichkeiten. Aber wie wir feststellen müssen, wächst das Datenvolumen schneller als die Verarbeitungskapazität. Es klafft eine Lücke, die immer größer wird. Das bedeutet, wir müssten wissen, welche Daten wichtig sind. Aber wer sagt uns das? Wenn wir die Aufmerksamkeit auf die falschen Daten lenken, dann werden wir in die Irre geführt.

Daneben gibt es noch eine andere Entwicklung: Die Systemkomplexität explodiert noch viel schneller als das Datenvolumen. Das liegt natürlich an den kombinatorischen Möglichkeiten, die entstehen, indem wir Systeme so miteinander vernetzen, dass dadurch neue Systeme entstehen. Das führt letzten Endes dazu, dass alle Daten der Welt nicht reichen, um unsere Systeme – also jedenfalls die komplexen – Top-down zu kontrollieren. Und es braucht einen völlig neuen Ansatz, nämlich den der verteilten Kontrolle.

2.1 Versagen der Top-down-Kontrolle

In der Tat ist es so, dass viele der Probleme, die wir in dieser Welt nicht gelöst haben, aus der Komplexität der Systeme resultieren und aus damit einhergehenden systemischen Instabilitäten. Ein schönes Beispiel, das Sie alle kennen: Der Stau aus dem Nichts. Selbst wenn wir die Gedanken aller Autofahrer lesen könnten, wären sie nicht zu verhindern. Warum kann ich das behaupten? Weil wir mathematische Modelle haben, die uns erläutern, wie und warum diese Staus aus dem Nichts entstehen. Und zwar geschehen sie ab einer gewissen kritischen Dichte, sodass die Abstände zu gering sind, als dass man auf zufällige Schwankungen der Geschwindigkeiten noch rechtzeitig reagieren könnte. Daher schaukeln sich kleine Schwankungen der Geschwindigkeit auf. So entsteht eine Art Dominoeffekt, und am Ende passiert etwas, das keiner wollte: Die Fahrzeuge kommen zum Stehen.

Das ist typisch für systemische Instabilität: Egal, wie viele Daten oder wie viel Technologie wir einsetzen und wie sehr wir uns anstrengen – diese Systeme können außer Kontrolle geraten. Andere Beispiele sind Instabilitäten in Lieferketten oder Booms und Rezensionen – der Stop-and-go-Verkehr der Weltwirtschaft. Ein weiteres Beispiel sind Crowd Disasters wie jenes während der Love Parade 2010. Obwohl da keiner die Absicht hat, jemanden umzubringen, passiert es – weil die Situation außer Kontrolle gerät. Oder denken Sie an die Tragödien der Allgemeingüter: Wir wollen sicherlich nicht die Meere zum Umkippen bringen, trotzdem überfischen wir sie. Ähnliche Probleme kennen wir aus anderen Umweltbereichen. Weitere Beispiele sind soziale Konflikte und Revolutionen.

Die Frage ist: Warum passiert das alles? Warum kriegen wir das nicht in den Griff? Der Grund sind Kaskaden-Effekte: Eine kleine, lokale Störung kann das gesamte System durcheinanderbringen. Beispiel: Die Finanzkrise. Nachdem die Großbank Lehman Brothers Pleite gegangen war, hat es im weiteren Verlauf hunderte andere Banken erwischt, und das kostete letzten Endes hunderte von Milliarden.

Wie können wir solche Systeme beherrschen? Überraschenderweise braucht es nicht mehr Power, sondern mehr Weisheit. Wir kennen dies von unserem Körper. Auch dabei handelt es sich um ein komplexes dynamisches System, und wir wissen: Mehr Medizin hilft nicht mehr, sie kann den Körper vergiften. Wir müssen genau wissen, welche Medizin wir wann in welcher Dosis nehmen. Ebenso ist das mit unserer Gesellschaft. Top-down-Kontrolle funktioniert in der Gesellschaft nicht gut genug. Man kann die Gesellschaft nicht steuern wie einen Bus. Die größten Sicherheitsgewinne im Bereich der Flugsicherheit wurden nicht durch bessere Technologie erzielt, sondern indem man eine neue Betriebskultur einführte, nämlich dass die Copiloten die Entscheidungen der Piloten in Frage stellen durften. Genauso wird die Katastrophe in Fukushima nicht etwa als Naturkatastrophe eingeschätzt, sondern als menschliches Versagen. Auch dort hat man die Vorgaben von oben akzeptiert, ohne zu widersprechen. Das war offensichtlich ein Fehler.

Ein anderes aktuelles Beispiel: 5.000 Überwachungskameras und 100.000 Sicherheitsleute waren nicht genug, um die Sicherheit in Minā bei Mekka zu gewährleisten – weit über 1.000 Menschen kamen dort im September 2015 bei einer Massenpanik während der traditionellen Pilgerfahrt „Hadsch“ tragisch ums Leben. Das heißt, der Überwachungsstaat wird keine Sicherheit garantieren können. Wir benötigen hier einen völlig neuen Ansatz.

2.2 Bottom-up-Organisation versus Top-down-Regulierung

Wie gehen wir also mit diesen Herausforderungen um? Klassischerweise gibt es zwei Ansätze: – Der Bottom-up-Ansatz – beruht auf der Idee, dass sich die Gesellschaft selbst organisieren könnte. Jeder macht das, was er für das Richtige hält, dann sollte das zum Besten der Wirtschaft und Gesellschaft sein. Die Vorstellung ist, dass dies so funktioniert, wie bei einem Vogelschwarm, einer

Ameisenkolonie oder einem Bienenstock. Das kann ganz wunderbar funktionieren, wie von einer „unsichtbaren Hand“ gesteuert, aber manchmal scheint sie leider nicht zur Stelle zu sein. Es entstehen dann Tragödien der Allgemeingüter – zum Beispiel Umweltverschmutzung oder Finanzkatastrophen – und das bedeutet, dass wir ein System nicht einfach sich selbst überlassen können, denn es wird nicht unbedingt immer von selbst das Beste tun.

Deswegen – das ist der Top-down-Ansatz – kommt der Staat ins Spiel und stellt Leitplanken auf, weil er Regulierung als erforderlich betrachtet. Jedes Jahr werden hunderte oder tausende neue Gesetze beschlossen. Aber auch das ist nicht die Lösung. Stattdessen enden wir in Überregulierung. Wir bräuchten eigentlich mehr Innovationen, aber die Manager beklagen sich, dass sie in ihrer Tätigkeit zu stark behindert werden. Ganz nebenbei gesagt ist unser überreguliertes System nicht mehr bezahlbar. Alle Industrienationen – vielleicht mit der Ausnahme der Schweiz – sind völlig überschuldet und haben heute bereits Schulden in der Höhe von 100 bis 200 Prozent des jährlichen Bruttosozialprodukts. Kein Mensch hat jemals gesagt, wie man das je wieder zurückzahlen soll – ein völlig ungelöstes Problem. Und deswegen benötigen wir einen neuen Ansatz.

2.3 Big Data und Künstliche Intelligenz

Da kommen natürlich diese ganzen Daten, die jetzt verfügbar werden, wie gerufen. Innerhalb von einer Minute gibt es 700.000 Google-Anfragen und 500.000 Facebook-Posts. Wenn wir einkaufen oder wenn wir uns fortbewegen, hinterlässt das ebenso Datenspuren. Big Data häuft sich an. Und die Leute sagen: Das ist das Öl der Zukunft.

Man kann damit sicherlich viel Geld machen, aber man kann auch andere schöne Sachen damit anstellen, beispielsweise die Welt neu vermessen. Und zwar zum Beispiel mit einem Smartphone, das wir alle in der Tasche tragen. Mit Hilfe von Daten können wir besser verstehen, wie sich internationale Spannungen ausbreiten – etwa, wie der Irak-Krieg im Laufe der Zeit die gesamte Region destabilisiert hat. Epidemische Ausbreitung ist mittlerweile viel besser verstanden und bis zu einem gewissen Grad auch antizipierbar. Auch die Verbreitung von Wissen ist natürlich von großem Interesse. Wir können heutzu-

tage die Ausbreitung von einzelnen wissenschaftlichen Konzepten und Ideen nachvollziehen und visualisieren, sogar die Ausbreitung von Kultur über tausende von Jahren. Alleine aus Geburts- und Todesdaten kann man unglaublich viel herauslesen.

Die Frage ist also: Was können wir sonst noch alles mit diesen Daten tun? Chris Anderson (2008) behauptete: Es naht das Ende der Theorie; der Überfluss an Daten macht die wissenschaftliche Herangehensweise überflüssig. Dadurch entstand die Vorstellung, wir könnten irgendwann alles wissen, was auf dieser Welt passiert – in Echtzeit. So, als hätten wir eine Kristallkugel. Könnten wir damit sogar voraussagen, was in Zukunft passiert? Und manch einer stellt sich die Frage: Könnte man die Welt wie ein wohlwollender Diktator oder wie ein weiser König regieren und optimieren? Hier ist Skepsis angebracht, denn Big Data ist keineswegs das universelle Tool, für das es viele halten. Big Data enthüllt oft nicht die Ursache der scheinbaren Muster und Zusammenhänge in den Datenbergen. Wenn wir in den Himmel blicken, dann sehen wir Sternbilder, aber aus wissenschaftlicher Sicht haben diese Muster keine Bedeutung. Oder schaut man sich die Anzahl der Serienkiller pro Einwohner in verschiedenen Ländern an, dann scheint sie mit dem Schokoladenkonsum zu wachsen. Wenn das wirklich der Fall wäre, dann würde man in der Schweiz sehr gefährlich leben. Aber offensichtlich hat das weiter nichts zu bedeuten.

Ein anderes Problem, das man bei der Big-Data-Analyse hat, ist es, gute und schlechte Risiken voneinander zu trennen. Versicherungen machen das gerne bei ihren Klienten und die Sicherheitsbehörden möchten gerne herauslesen: Wer ist ein Terrorist, wer ist ein guter Bürger? Aber leider Gottes kann man das oft nicht so klar voneinander trennen. Daher gibt es einerseits Fehlalarme wie gerade in Hannover oder München und andererseits übersehene Risiken wie in Boston oder Paris, und nebenbei auch das Problem der Diskriminierung. Denn wenn wir zum Beispiel die Ernährung heranziehen, um zu bestimmen, wie viel jemand für seine Versicherung bezahlen soll, dann würden wir wahrscheinlich nebenbei, ohne dass es beabsichtigt ist, verschiedene Tarife für Männer und Frauen haben, aber auch für Christen, Juden und Muslime. Sicherlich wäre das eine Diskriminierung, die zu vermeiden wäre.

Wir brauchen also etwas Besseres als Big Data. Hier könnte man nun an künstliche Intelligenz denken. In der Tat ist es so, dass nicht nur die Datenmen-

gen und die Prozessorleistungen explodieren, sondern ebenso die künstliche Intelligenz. Innerhalb von fünf bis 40 Jahren – die Schätzungen divergieren hier ein wenig – werden Computer die Fähigkeiten des menschlichen Gehirns erreichen und überschreiten. Wir haben bereits gesehen, dass intelligente Maschinen besser Schach spielen. Wir wissen, dass sie viele Arbeiten besser und billiger erledigen. Bald werden sie vielleicht auch die besseren Autofahrer sein. Sie sind oft besser in der Beantwortung von Fragen und vielleicht auch bald die besseren Ärzte.

Lange Zeit hat künstliche Intelligenz keine Fortschritte gemacht, aber heutzutage wird sie nicht mehr Zeile für Zeile programmiert, sondern diese Systeme entwickeln sich von selbst. Roboter können lernen. Sie könnten auch andere Roboter bauen, klügere Roboter. Das heißt, sie vermehren sich bzw. sie könnten es zumindest. Und so können sie sich auch weiterentwickeln – eine Roboterevolution sozusagen. Insofern lautet die Frage: Wären superintelligente Maschinen möglich? Und da sind die entscheidenden Stichworte: *cognitive computing* und *deep learning*.

Bis vor kurzem hat man davon noch nicht viel gehört, aber heute ist es ein ganz großes Thema. Und man muss sich fragen: Warum werden jetzt alle bei dem Thema Superintelligenz so nervös? Merkwürdigerweise gerade im Silicon Valley. Elon Musk sagte etwa: „Ich denke, wir müssen wirklich sehr vorsichtig sein mit künstlicher Intelligenz. Es könnte die größte existenzielle Bedrohung der Menschheit sein." (McFarland 2014) Er steht mit dieser Auffassung nicht allein. Bill Gates (2015) meinte zum Beispiel: „Ich bin im Camp derjenigen, die besorgt sind über diese Entwicklung." Und Steve Wozniak, der Apple-Mitbegründer, sagte: „Computer werden uns überholen, keine Frage. Aber werden wir leben wie Götter? Oder werden wir so etwas sein wie Haustiere? Oder wie Ameisen, die man achtlos zertritt? Das kann ich Ihnen nicht sagen." (Smith 2015)

Sicherlich, Superintelligenz-Forschung ist überall auf dem Weg, nicht nur im Silicon Valley. Insbesondere wird auch in China an einem China Brain Project gearbeitet. Baidu, die Suchmaschine, verwendet Nutzerdaten und lässt sie „lernen". Es wird versucht, die einzelnen Bürger gewissermaßen auswendig zu lernen und prognostizierbar zu machen. Im Grunde genommen könnte man denken, dass diese digitalen Doubles uns irgendwann bei den Entscheidun-

gen, die zu treffen sind, ersetzen. Zum Beispiel, dass sie einmal für uns wählen. Die Frage ist: Wer will das? Und wie würden eigentlich diese superintelligenten Maschinen benutzt?

2.4 Skinner-Box und China-Modell

Das Stichwort ist die „kybernetische Gesellschaft". Schon vor Jahrzehnten gab es Ansätze in diese Richtung. Chile war das erste Land, das sich regelmäßig die Produktionsdaten der einzelnen Fabriken melden lies, um Über- bzw. Unterproduktion zu vermeiden. Aber es gab noch den „Störfaktor Mensch", der letzten Endes unberechenbar war. Das hat die Wissenschaftler beschäftigt, und einige meinen nun: Ja, auch diesen Störfaktor kann man eliminieren. Man kann Menschen berechenbar und steuerbar machen.

Dies basiert auf der Theorie von Skinner, bei diesen Experimenten bei denen Tiere wie Ratten, Tauben oder Hunde durch Anreize oder Bestrafung konditioniert wurden. Die Idee ist nun, dass man dies auch auf den Menschen übertragen könnte. Heutzutage leben wir selber in einer Art Skinner-Box – und wir sind die Versuchskaninchen. Wir leben nämlich in einer Filter-Bubble, sind also in einer Welt aus personalisierter Information gefangen. Jeder von uns sieht jetzt die Welt unterschiedlich, so wie man sie uns präsentiert – auf unserem Computer bzw. auf unserem Smartphone. Und mit solchen personalisierten Informationen kann man unsere Entscheidungen beeinflussen, ohne dass dies die Betroffenen merken. Sie denken, das sei ihre Entscheidung, tatsächlich handelt es sich aber um eine Form der Manipulation. Und das ist der eigentliche Grund, warum all diese Daten über uns gesammelt werden. Natürlich muss Terrorismus bekämpft werden. Aber hauptsächlich geht es um die Manipulation und Steuerung unseres Verhaltens und somit ganzer Gesellschaften.

Damit stellt sich die Frage: Würden wir irgendwann bestraft, wenn wir uns nicht entsprechend dieser Vorgaben verhalten? Wenn die Skinner-Box das Vorbild ist, dann lautet die Antwort: Ja, genau das würde passieren! Wie könnte das geschehen? Mit personalisierten Preisen.

Wenn Sie das jetzt für übertrieben halten, dann suchen Sie ein wenig im Internet. Wir sind so weit, dass China jeden seiner Bürger bewertet. Jeder be-

kommt ein bestimmtes Punktekonto, einen Citizen Score. Der hängt nicht nur davon ab, ob man seine Kredite pünktlich zurückbezahlt, sondern auch davon, was man im Internet anklickt, ob man die richtige Gesinnung hat und was die Freunde tun. Dies entscheidet dann darüber, welche Konditionen man beim nächsten Kredit bekommt, ob man einen bestimmten Job erhält oder ein Visum, um ins Ausland zu reisen. Und ähnliche Dinge sind mittlerweile auch in westlichen Ländern auf dem Weg. Das Stichwort – wir haben erst kürzlich darüber gelesen – ist *Karma Police*. Sehen Sie einmal nach bei *The Intercept*, dann sehen Sie die aktuellen Entwicklungen. Auf US-Flughäfen haben wir das schon seit einiger Zeit, dort werden Sie eingeschätzt, ob Sie möglicherweise gefährlich sind: Wenn Sie gähnen, wenn Sie lachen, wenn Sie sich die Haare kämmen oder irgendwie nervös wirken, dann gibt es Minuspunkte (Winter und Currier 2015). Das ist natürlich erschreckend, und obwohl es nicht richtig funktioniert, ist das Verfahren trotzdem weiter im Einsatz.

Das bringt uns zu der Schlussfolgerung, dass die Gefahr besteht, dass wir mehr oder weniger alles verlieren könnten, was wir innerhalb von Jahrzehnten und Jahrhunderten aufgebaut haben. Ich werde das gleich noch etwas näher zeigen. Unsere Freiheit und Selbstbestimmung sind in Gefahr, unsere Menschenwürde (wenn wir gläsern sind, dann haben wir keine), die Unschuldsvermutung (im Grunde genommen ist heute jeder verdächtig, auch derjenige, der nichts angestellt hat), Fairness, Gerechtigkeit, die Möglichkeit, seine eigenen Ziele zu verfolgen, glücklich zu werden. Pluralismus und Demokratie sind in Gefahr, und meiner Meinung nach auch Sicherheit und Frieden.

Die Frage ist: Müssen wir das hinnehmen? Ist das die natürliche Entwicklung der Geschichte? Ist Demokratie vielleicht veraltet? Gehen wir einmal gedanklich diese Überlegung durch, denn sie ist höchst wichtig dafür, nun zu entscheiden, was eigentlich das Richtige ist.

Manche mögen denken: Wäre das schön, wenn wir die Zeiten Ludwigs des XIV. noch hätten, wenn die Französische Revolution nicht passiert wäre, dann könnten wir doch viel schneller entscheiden, alles wäre viel effizienter. Wir könnten ein Einkaufszentrum hier hinstellen und eine Stadt da und einen Flughafen dort. Das Ganze ist unter der Bezeichnung „China-Modell“ bekannt. Und viele denken, bei den Wachstumsraten, die China hat, müssten wir das auch machen. Wie sollten wir sonst im globalen Wettbewerb bestehen?

Aber auch wenn wir Superintelligenz hätten, würden manchmal Fehler passieren. Davor schützt uns auch alle Macht nicht. Deshalb gibt es diese Shoppingmalls, wo niemand einkaufen geht, und Geisterstädte, in denen keiner wohnen möchte. Und es gibt Smog, der die bewohnten Städte fast schon unbewohnbar macht, Katastrophen wie die Explosionskatastrophe in Tianjin und schließlich auch die Meltdowns, die wir kürzlich an den asiatischen Finanzmärkten gesehen haben. Alle Macht, die der chinesische Präsident und der Parteiapparat dort haben, nützt also nichts, um diese Probleme in den Griff zu bekommen. Das heißt, dieses Herrschaftsmodell funktioniert auch nicht so gut, wie man lange gedacht hatte.

Aber warum funktioniert es eigentlich nicht? Es hört sich doch plausibel an, dass der Apfel gesünder ist als die Schokolade und dass man den Leuten daher einen Anstoß geben sollte, den Apfel zu essen anstelle der Schokolade. Aber leider bekommen Äpfel nicht allen Menschen gut. Ich wäre beinahe einmal an einem Apfel gestorben. Wenn Sie zu Ihrem Arzt gehen, sagt der vielleicht: Nüsse sind gesund. Aber wir wissen alle: Es gibt Allergiker, die beim Verzehr von Nüssen einen lebensgefährlichen anaphylaktischen Schock bekommen. Genau genommen gibt es nichts, das für alle gut ist. Das müssen wir einsehen!

Folglich könnten wir auch viele Fehler machen. Vielleicht würden wir mehr schlechte als gute Entscheidungen treffen, wenn man bedenkt, dass nur 38 Prozent aller Studien in der Psychologie reproduziert werden konnten. Das heißt, die empirische Basis, auf die wir uns abstützen müssten, ist gar nicht so solide, wie man oft denkt. Deswegen empfiehlt auch jeder Ernährungsratgeber etwas anderes, vor allem, wenn Sie das über die Jahrzehnte vergleichen. Die Vorstellung, die Krankenkasse oder der Staat könnten uns sagen, was gut für uns ist, halte ich für irrig.

2.5 Veränderungen in Ökonomie und Politik

Ich gebe zu, unser Verhalten ist vorhersehbarer als gedacht. Es gibt Firmen wie Recorded Future, die behauptet, 90 Prozent unserer Tagesabläufe voraussagen zu können. Wir sind eben Gewohnheitstiere, wir haben unseren Zyklus. Jede Woche ist ähnlich gestaltet, zumindest bei vielen Menschen. Und trotzdem können Interaktionen alles ändern. Sie kennen das: Irgendwann begegnen Sie

einem Menschen, Sie verlieben sich. Das verändert Ihr Leben, und wenn Sie Politiker sind, vielleicht auch das Leben der ganzen Nation. Vielleicht ändert es den Lauf der Geschichte. Das heißt, in komplexen dynamischen Systemen gibt es grundsätzliche diese Begrenzung der Vorhersagbarkeit.

Wir haben dazu Experimente im Labor gemacht. Unser Modell konnte 96 Prozent aller individuellen Entscheidungen korrekt voraussagen! Trotzdem ist es so, dass das Gesamtergebnis völlig daneben lag. Wenn man jedoch Zufall zu unserem Modell hinzu addierte, das Modell also auf der individuellen Entscheidungsebene weniger genau machte, lieferte es überraschenderweise viel bessere Gesamtvoraussagen. Wir müssen unsere Vorstellungen von komplexen System also völlig überdenken.

Ganz nebenbei bemerkt steht unsere Gesellschaft vor riesigen Herausforderungen, die alles andere als voraussagbar sind und wahrscheinlich auch nur sehr begrenzt kontrollierbar. Elon Musk (2014) hat zum Beispiel getwittert: „Superintelligenz ist potenziell gefährlicher als Nuklearwaffen." Was könnte er damit gemeint haben?

Die digitale Revolution bringt die Zerstörung der Art und Weise, wie unsere Wirtschaft und Gesellschaft bisher funktionierten. Gewissermaßen wird kein Stein auf dem anderen bleiben. Zum Beispiel ändert sich die Art und Weise, wie wir einkaufen (heutzutage natürlich viel im Internet), wie wir produzieren (zunehmend mit 3D-Druckern), wie wir uns bewegen werden (mit Autos, die ohne menschlichen Fahrer auskommen) oder wie wir Güter transportieren (mit Drohnen). Auch die Forschung verändert sich. Big Data Analytics wird die vierte Säule der Forschung. Ebenso wird sich das Erziehungs- und Bildungssystem ändern, beispielsweise durch Massive Open Online Courses (MOOCS); plötzlich könnten wir Millionen von Menschen gleichzeitig ausbilden. Ich will nicht sagen, dass dies die beste Möglichkeit der Ausbildung ist, aber all diese Dinge passieren jetzt. Auch die gesamte Ökonomie und Politik werden sich verändern, sogar der Krieg – durch die Möglichkeiten von Cyberwar.

Lassen Sie mich ein paar Beispiele geben: Uber fordert gerade die gesamte Taxibranche heraus. Meiner Meinung nach werden sie auch noch das gesamte Weltlogistiksystem umwälzen. Airbnb fordert die gesamte Hotelbranche heraus. Dann gibt es heutzutage 3D-Drucker für Häuser, das schockiert die Bau-

branche. Ein chinesischer Bauunternehmer erstellte gerade ein sechzigstöckiges Hotel innerhalb von drei Wochen. Sein Ziel ist es, das höchste Gebäude der Welt innerhalb von einer Woche zu bauen. Möglich, dass er es schafft. Außerdem haben wir plötzlich eine virtuelle Währung namens Bitcoin, das fordert die Banken heraus. Sind sie überhaupt noch notwendig, fragen sich auch die Bankmanager mittlerweile. Blockchain soll aus der Sicht bestimmter Leute die Basis für eine Neuorganisation der Gesellschaft sein. Sie meinen im Prinzip, dass Politik und Staat abgeschafft gehören, dass alles nur noch zwischen Individuen ausgehandelt werden solle. Durch die neuen Technologien wird sich also alles fundamental verändern.

Wir stehen jedenfalls vor einer neuen Ökonomie. Unsere Ökonomie hat sich schon mehrfach transformiert: erst von einer Agrargesellschaft zur Industriegesellschaft, dann von der Industrie- zur Servicegesellschaft. Und jetzt kommt schließlich eine neue Wirtschafts- und Gesellschaftsform auf, nämlich die digitale Gesellschaft. Das ist natürlich nur eine Bezeichnung, die Gesellschaft selbst ist nicht digital.

Das geht damit einher, dass voraussichtlich innerhalb der nächsten zehn bis 20 Jahre etwa 50 Prozent der heutigen Jobs durch Computer, durch Algorithmen oder durch Roboter übernommen werden. Das wird natürlich die Gesellschaft unglaublich stark herausfordern. Ausgerechnet bei den jungen Menschen, die eigentlich besser mit diesen neuen Technologien umgehen können müssten, ist die Arbeitslosigkeit besonders hoch, in manchen Ländern liegt sie sogar schon über 50 Prozent. Und das ist in der Tat eine Bedrohung für den sozialen Frieden in Europa. Es gibt nur noch vier Länder, in denen junge Menschen noch ausreichend Arbeit finden: Deutschland, Norwegen, Österreich und die Schweiz.

Es sieht so aus, als stünde Europa der Kollaps bevor. Ich hoffe zwar, er wird nicht passieren, aber es ist allerhöchste Zeit, dass wir die richtigen Maßnahmen ergreifen, solange wir noch Geld und Zeit haben, um hoffentlich unbeschadet in dieses Zeitalter einzutreten. Denn all diese eben erwähnten Transformationen in der Vergangenheit gingen leider nicht reibungslos vonstatten, sondern es gab Finanz- und Wirtschaftskrisen, Revolutionen und Kriege. Nun, Finanz- und Wirtschaftskrisen haben wir ja bereits, jetzt wollen wir wenigstens die Revolutionen und Kriege vermeiden – und das ist schwierig genug. Denn

wir könnten sehr leicht in die Situation kommen, wie ich gleich noch erläutern werde, unsere heutige Wirtschaftsform und die Demokratie zu verlieren. Und die Frage ist: Sind wir bereits auf diesem Pfad, oder kriegen wir noch die Kurve, indem wir Kapitalismus und Demokratie neu erfinden und sie mit neuen Technologien – konkret mit dem Internet der Dinge – glücklich miteinander verheiraten?

Wenn Sie das für übertrieben halten, dann möchte ich doch einige Artikel aus Publikationen, die als seriös gelten, in Erinnerung rufen. *The Economist* titelte zum Beispiel: „Wealth without workers, workers without wealth", Henrik Müller (2015) in *Spiegel Online*: „Der Kapitalismus funktioniert nicht mehr", Wolfgang Uchtarius (2011) schreibt in der Zeit: „Der Kapitalismus in der Reichtumsfalle" – diese Artikel hatten wir vor zehn Jahren so noch nicht. „Is Democracy Dead?", fragt Tony Blair (2014) in der *New York Times*. „Die Demokratie – ein Auslaufmodell", schreibt Richard Herzinger (2014) in der *Welt*. Das muss einem schon Angst machen, und wir müssen uns die Frage stellen: Ist die Demokratie wirklich ein Auslaufmodell oder brauchen wir sie doch noch? Hat sie eine Zukunft, wenn wir sie mit einem Upgrade, sozusagen mit einer Frischzellenkur neu beleben?

3 Neue Argumente

Bis vor kurzem war in bestimmten Kreisen die Idee verbreitet, die Probleme der Welt ließen sich durch Top-down-Kontrolle, durch eine zentralisierte Technologie, lösen, die letzten Endes unsere Entscheidungen steuern würde. Ich empfehle Ihnen dazu das Buch „Die Herrschaftsformel" von Kai Schlieter.

Ich glaube, der Grund, warum wir so erfolglos darin waren, die Überwachungsgesellschaft infrage zu stellen, war, dass wir nicht verstanden haben, was wirklich dahinter steckt. Die Politik wollte das Beste, sie wollte die Welt kontrollierbar machen, und wir haben oft mit Grundsätzen der Demokratie argumentiert: Das ist doch nicht vereinbar mit dem Grundgesetz und so weiter und so fort. Aber wenn man bereits zu dem Schluss gekommen ist, die Demokratie sei ein

Auslaufmodell und man brauche etwas anderes, dann ziehen all diese Argumente nicht. Die Argumentation muss aus der Perspektive der zukünftigen Gesellschaft erfolgen.

Ich habe an einem Buch gearbeitet, „The Automation of Society is Next: How to Survive the Digital Revolution" (Helbing 2015), das in dieser Weise argumentiert. Ich hoffe, dass wir jetzt endlich auf dem richtigen Weg sind. Unsere Gesellschaft wird sich transformieren, das hatte ich vorher schon gesagt, und sie wird hoffentlich von einer Raupe zu einem schönen Schmetterling.

Wo geht es hin? Ich glaube, dass das Stichwort Aufklärung – in diesem Fall die digitale Aufklärung – wirklich im Mittelpunkt stehen muss; „Medienkompetenz", wie man das hier nennt. Und dass wir uns aus dem befreien müssen, was manche Leute als „digitale Leibeigenschaft" oder „Feudalismus 2.0" beschrieben haben. Das bedeutet: Die Entscheidungshoheit wieder an Individuen, an verschiedene Institutionen zurückzugeben, aber unterstützt durch digitale Technologien, digitale Assistenten, die es uns erlauben, zwischen verschiedenen Zielen auszuwählen und uns bei der Umsetzung und Erreichung dieser Ziele so gut wie möglich unterstützen.

3.1 Ein globaler Ansatz für globale Probleme

Wir kommen nun also zu neuen Ansätzen, und die Frage ist: Wie sollten wir eigentlich Computerpower in Zukunft benutzen? Da ist wirklich entscheidend, dass wir Systeme, insbesondere komplexe Systeme, besser verstehen. In der Tat ist es so, dass Google Flu Trends[2] lange als Paradebeispiel für das Big-Data-Paradigma galt. Dann stellte sich heraus, dass es gar nicht so gut funktioniert, und dass es heutzutage bessere Ansätze gibt, die mit wesentlich weniger Daten arbeiten. Wenn man berücksichtigt, dass sich Krankheiten ausbreiten, indem Leute von A nach B reisen und von B nach C, wenn man also das Flugverkehrsaufkommen in ein Modell einspeist, dann wird plötzlich die Ausbreitung von Epidemien vorhersagbar. Und das funktioniert wesentlich besser als ein reiner Big-Data-Ansatz. Das heißt, Modelle helfen uns zu entscheiden, wie wir Daten anschauen müssen. Erst dann werden diese Daten nützlich für uns.

2 Siehe unter: https://www.google.org/flutrends/about/ (Zugriff 17. Januar 2016).

Es gibt Modelle für viele Phänomene, für Fußgänger, für Crowd Disasters, für den Verkehr, für wirtschaftliche Booms und Rezessionen, für den Ausfall von Power Grids, für die Zuverlässigkeit der Gasversorgung, aber auch für Dinge, die wirklich schwierig zu verstehen sind: nämlich für soziales Verhalten, für Koordination, für Kooperation, für die Ausbreitung von Kriminalität, für die Entstehung von moralischem Verhalten, sozialen Präferenzen oder sozialen Normen, aber auch für die Entstehung von Konflikten. Es gibt die Idee, man könnte doch diese verschiedenen Modelle zusammenfügen und auf diese Art und Weise besser verständlich machen, was eigentlich in unserer Welt passiert. Das wäre dann so ähnlich wie bei der Wettervorhersage: Am Anfang sind die Modelle noch nicht sehr gut, aber im Laufe der Zeit würden sie immer besser und immer nützlicher werden. Aber der Knackpunkt ist: Um die Welt zu verstehen, brauchen wir weniger Daten als wir denken, aber mehr Zusammenarbeit und verschiedene Perspektiven. Es erfordert also Interdisziplinarität und einen globalen Ansatz, eine globale Anstrengung, um globale Probleme anzugehen. Viele Probleme sind heutzutage global. Die FuturICT Initiative umfasst tatsächlich Sozial-, Natur- und Ingenieurwissenschaftler aus über 30 Ländern. Diese Community ist eigentlich startklar und könnte sofort loslegen – es fehlt nur noch der Startschuss.

3.2 Wir brauchen kollektive Intelligenz

Um mit der irrsinnigen Geschwindigkeit, in der sich unsere Welt verändert, Schritt zu halten, brauchen wir mehr Partizipation. Das ist auch der Grund, warum Stichworte wie Crowd Sourcing, Crowd Funding, Collective Intelligence, Citizen Science etc. plötzlich so wichtig werden. Vieles spricht für eine internationale Kooperation, und man kann diese auch so gestalten, dass sie mit Wettbewerb vereinbar ist, sofern wir Mechanismen einführen, die auf Reputation, Qualifikation und Verdiensten beruhen. Aber entscheidend ist, dass wir lernen, wie wir die besten Ideen und das beste Wissen zusammenführen.

Kollektive Intelligenz ist wirklich das, was wir benötigen, um die Komplexität der Welt doch einigermaßen zu verstehen. Das Interessante dabei ist: Nicht der beste Ansatz, der klügste Kopf oder der größte Supercomputer gewinnt, sondern die Diversität, die Kombination von verschiedenen Perspektiven – das ist zum Teil sehr überraschend und zeigt uns den Weg in die Zukunft. In

der Tat weiß man, dass die diversifiziertesten Ökonomien die erfolgreichsten sind. Das gleiche gilt für Innovation – die passiert dort, wo es am meisten Freiheit und Diversität gibt.

Wie können wir diese kollektive Intelligenz nun also erreichen? Wie können wir der Demokratie eine Frischzellenkur verpassen? Ich sprach vorhin von den digitalen Assistenten. In diesem Zusammenhang werden Online Deliberation Platforms (geeignete Debattenplattformen) wichtig werden, wo alle Argumente auf den Tisch kommen, wo sie sortiert werden, und wo sie dann auf wenige verschiedene Perspektiven kondensiert werden, sodass sie in einem politischen Moderationsprozess integriert werden können. Die zwei oder drei besten integrierten Lösungen würde man weiter verfolgen. Unter Umständen macht es Sinn, in verschiedenen Regionen unterschiedliche Lösungen umzusetzen, denn Diversität ist wichtig für Innovation und kollektive Intelligenz, aber auch für die Resilienz unserer Gesellschaft.

Nun, was braucht es, damit diese kollektive Intelligenz gedeihen kann? Man braucht unabhängige Entscheidungsprozesse und Diversität, man braucht vertrauenswürdige Informationssysteme und man muss Manipulation vermeiden. Ich bin im Übrigen gegenüber künstlicher Intelligenz nicht negativ eingestellt; ich glaube, dass letztlich die Menschen einfach Bestandteile eines globalen Netzwerkes von Intelligenzen sein werden. Darunter werden auch künstliche Intelligenzen sein, und sie werden zur kollektiven Intelligenz beitragen.

3.3 Eine Welt aus Ideen

Lange Zeit dachte ich, ich würde mein Leben damit verbringen, mehr und mehr und immer bessere Modelle zu entwickeln. Doch dann kam ich zum Schluss, dass die Welt sich innerhalb der nächsten zwei bis drei Jahrzehnte so dramatisch transformieren wird, dass sie völlig anders aussehen wird. Es macht also keinen Sinn, eine Welt zu beschreiben, die bald Vergangenheit sein wird. Die Frage ist folglich: Wie bereiten wir uns auf das vor, was da kommen wird?

Wir müssen über die neuen organisatorischen Prinzipien der Welt nachdenken. Sie wird nach anderen Regeln funktionieren, und das braucht Mechanismus-

und System-Design. Wenn wir mit den Modellen, die ich vorher genannt habe, die Kräfte verstehen, die den sozialen und ökonomischen Prozessen zugrunde liegen, dann können wir diese Kräfte auch für uns einsetzen. Wir würden dann nicht gegen Windmühlen laufen und sie zu bekämpfen versuchen, sondern wir würden sie für uns nutzen, so wie wir in der Physik und im Ingenieurwesen gelernt haben, die Kräfte der Natur für uns zu nutzen.

Natürlich ist es so, dass die richtigen Regeln, die es braucht, nicht unbedingt diejenigen sind, die sich die einzelnen Teilhaber der Gesellschaft wünschen, sondern es sind natürlich diejenigen, die die gewünschten Ergebnisse produzieren. Wir werden sehen, dass hier Selbstorganisation eine wichtige Rolle spielt.

Es ist wichtig zu realisieren, dass wir mehr und mehr Zeit in virtuellen Welten, in Informationswelten, verbringen werden und dass die Zukunft dadurch immer immaterieller wird. Sie wird immer mehr ein Ideenkonstrukt – eine Welt, die aus Ideen aufgebaut ist. Natürlich brauchen wir weiterhin Wohnungen und Nahrung, das ist klar, aber wir verbringen einfach immer mehr Zeit in diesen Welten. Wir bauen jetzt digitale Kopien dieser Welt, und warum nicht auch völlig andere digitale Welten, in denen andere Wirtschafts- und Gesellschaftsformen ausprobiert werden können? Und in der Tat, das beginnt auch bereits.

Dieser Umstand, dass die Welt mehr und mehr aus Ideen kreiert wird, ist auch der Grund, warum wir Bits in echten Geldwert umwandeln können. Sie kennen sicherlich aus Ihrer Kindheit die Geschichte, in der aus Stroh Gold gesponnen wird. Jeder hat davon geträumt und natürlich hat es nicht funktioniert. Jetzt plötzlich hat es Bitcoin möglich gemacht.

Welche Gesellschaften werden führend sein? Diejenigen, die verstehen, wie Information funktioniert und wie man sie am besten nutzt. Information sperrt man nicht wie Gold in einen Tresor. Information ist oft ein vergängliches Gut, sie veraltet schnell. Das Besondere an der Information ist aber, dass wir sie so oft teilen können wie wir wollen, letzten Endes ist dies unsere Entscheidung, und dass wir sie auf Milliarden verschiedene Möglichkeiten verwenden können. Die digitale Ökonomie ist kein Nullsummenspiel. Es ist so, dass nicht einer etwas abgeben muss, damit der andere mehr davon haben kann – Im Gegenteil! Informationen teilen macht Informationen sogar oft wertvoller.

Nun wäre die nächste Frage: Wie können wir diese 50 Prozent an neuen Jobs ersetzen, die wir bald verlieren werden? Wenn 50 Prozent der Volkswirtschaft wegfallen, müssen wir die halbe Volkswirtschaft neu erfinden. Klassischerweise hat man das meiste Geld mit Rationalisierung gemacht – „Economies of scale". Jetzt brauchen wir ein ergänzendes Modell, und dieses ist das Modell der Co-Kreation, also der Zusammenarbeit. Es geht nicht mehr darum, dass man versucht, alles selber zu machen, sondern es geht um Interaktion, um Zusammenarbeit, um Synergieeffekte. Dann kommen wir weg von diesem Paradigma der linearen Innovation, wo alle zwei Jahre ein neues Automodell zum Verkauf gebracht wird. Stattdessen wird exponentielle Innovation möglich.

Interoperabilität ist hier das Stichwort. Je mehr Services, je mehr Produkte es gibt, desto mehr werden möglich – wenn wir es nur zulassen. Es ist unsere Entscheidung, so ein Informations-, Innovations- und Produktions-Ökosystem zu bauen. Die beste aller Welten ist diejenige, die für alle Menschen funktioniert und zu der alle beitragen können. Partizipation ist wirklich entscheidend.

Wir können lernen, soziales Kapital zu bilden. Damit haben wir aber immer noch Schwierigkeiten. Vertrauen zum Beispiel ist unglaublich wichtig, ein immaterieller Wert, der die Grundlage für unsere Gesellschaft ist. Jetzt wird es langsam möglich, soziales Kapital zu visualisieren und seine Grundlage zu verstehen. Und vor allen Dingen können wir sozialen und ökonomischen Wert von kulturellen Erfolgsprinzipien ableiten. Das ist ein wichtiger Punkt, denn genau an diesen kulturellen Verwerfungslinien, also dort, wo verschiedene Kulturen aufeinander treffen, wo wir Schwierigkeiten haben, miteinander zurechtzukommen, werden neue Produkte und Services entstehen.

Jede Kultur basiert auf tausenden von verborgenen Erfolgsgeheimnissen; die saugen wir durch unsere Erziehung in uns auf. In vielen Fällen können wir es nicht explizit formulieren, aber würden wir es können, dann könnten wir auch all diese Erfolgsprinzipien auf neue Art und Weise miteinander verbinden. Ich nenne es das „Cultural Genome Project". Dabei ist es wichtig, dass wir kulturelle Diversität haben. Jetzt müssen wir nur lernen, mit dieser Diversität umzugehen und sie in einen Vorteil zu verwandeln. Dazu brauchen wir digitale Assistenten, die uns unterstützen, die Diversität zu verstehen und zu bewältigen. Und in der Tat gibt es bereits erste Beispiele, beispielsweise die Echtzeitübersetzung: Sie laden sich eine App herunter, sprechen in Ihr Telefon in einer

Sprache hinein, auf der anderen Seite kommt es in einer anderen Sprache heraus – wunderbar! Wir könnten auch Apps bauen, um uns vor Situationen zu warnen, die zu unserem Schaden wären, um Situationen zu identifizieren, die wir in unseren Vorteil verwandeln können, und die uns dabei helfen, neuen Wert zu generieren. In diesem Zusammenhang sind sozio-inspirierte Technologien sehr wichtig.

3.4 Was zu tun ist

Dadurch, dass diese Welt mehr und mehr aus Ideen besteht, wird Moral – wie wir auch bei VW gesehen haben – wieder viel wichtiger. Es ist entscheidend, zu verstehen, dass Power Vertrauen erfordert, und Vertrauen erfordert wiederum Transparenz. Und wir brauchen geteilte Werte, damit unsere Welt funktioniert. Es ist also kein Wunder, dass der Papst die Agenda 2030 der Vereinten Nationen offiziell eingeläutet hat, das hat man mit Bedacht gemacht.

Das Wichtigste ist, dass wir positive Externalitäten vergrößern, negative verringern und für eine faire Kompensation sorgen. Das ermöglicht Interoperabilität und Ko-Evolution. Wir können verschiedene Dinge tun, damit wir auf einen besseren Weg kommen, weg von diesem Feudalismus 2.0 und hin zu einer innovativen, kreativen Welt, mit der wir diese verschiedenen Herausforderungen besser bewältigen können

- Digitale Aufklärung fördern,
- dezentralisierte Design- und Kontrollelemente (Modularität) einführen,
- Möglichkeiten zur Partizipation schaffen,
- informationelle Selbstkontrolle ermöglichen,
- Transparenz erhöhen für mehr Vertrauen,
- Informationsqualität verbessern, Verzerrungen reduzieren,
- nutzerkontrollierte Informationsfilter ermöglichen,
- sozioökonomische Diversität schützen,
- Interoperabilität fördern,
- Koordinationstools und digitale Assistenten bauen,
- kollektive Intelligenz fördern,
- Externalitäten messen (und damit handeln),
- multi-dimensionalen Wertetausch unterstützen,
- lokale Feedback-Schleifen ermöglichen!

Wenn wir das tun, dann werden wir bald eine nachhaltigere, eine resilientere und effizientere Gesellschaft haben. Resiliente Systemdesigns sind gerade in Zeiten des Umbruchs wichtig, wenn wir nicht wissen, was im Einzelnen auf uns zukommt. Da ist es entscheidend, dass wir eben diesen Gordischen Knoten zerschneiden. Modulare Designs und verteilte Kontrolle sind wichtig. Da gibt es heutzutage völlig neue Möglichkeiten – digitale Assistenten und neue Organisationsformen –, wo nicht mehr alles top-down organisiert ist, sondern wo Top-down- und Bottom-up-Ansätze auf innovative Art und Weise zusammenwirken.

3.5 Das Internet der Dinge als Bürgernetzwerk

Wie bewältigen wir Globalität? Sie muss mit lokalen Interaktionsprinzipien kombiniert sein, damit wir die Destabilisierung, die wir zurzeit sehen, überwinden. Wenn wir das nicht tun, dann wird unsere Welt fragmentieren, und das würde nichts Gutes bedeuten. Wir müssen lernen, die unsichtbare Hand zum Funktionieren zu bringen, müssen lernen, wie Selbstorganisation funktioniert, denn das Besondere an komplexen System ist, dass sie sich selbst organisieren. Aber wir können die Interaktion, welche die Grundlage dieser Selbstorganisation ist, auf eine Art und Weise verändern, die das Ergebnis so beeinflusst, dass die Strukturen, Eigenschaften und Funktionalitäten entstehen, die wir gerne hätten. Wir können also tatsächlich die Kräfte, die unserer Gesellschaft und Wirtschaft zugrunde liegen, für uns nutzen, indem wir die richtige Art von Feedback-Effekten auf lokaler Ebene einführen. Das erfordert aber eine Art multidimensionales Austausch- oder Finanzsystem. Das haben wir heutzutage noch nicht, wir müssen es erst bauen.

Aber mit dem Internet der Dinge können wir jetzt eigentlich all diese Sachen umsetzen. Wir können Externalitäten messen, die früher einfach nicht messbar waren, und Feedbackeffekte erzeugen, sodass sich die Prozesse besser koordinieren. Dafür braucht es ein technisches System, an dem wir bereits arbeiten. Dieses nennt sich Nervousnet und nutzt letzten Endes Smartphones und all jene Sensoren, die in ihnen eingebaut sind, aber von uns im Moment nicht aktiv genutzt werden. Das könnten wir aber tun, wir könnten die Smartphones miteinander vernetzten, und wir könnten die Daten verwenden, um kollektive Messprozesse durchzuführen. Zum Beispiel könnten wir mit den Da-

ten der Beschleunigungssensoren Erdbeben detektieren und dann Warnungen an unsere Freunde, Kollegen, Bekannten und Verwandten senden lassen.

Entscheidend ist bei einem solchen System natürlich, dass es ein System ist, dem wir vertrauen können. Dies erfordert informationelle Selbstkontrolle. Deswegen geben wir Ihnen so viele Steuermöglichkeiten wie möglich. Insbesondere können Sie entscheiden, welche Sensoren Sie aufschließen wollen und ob Sie die Daten, die dann erzeugt werden, für sich selber behalten wollen oder ob Sie sie teilen möchten. Wir denken auch an einen Datenstore, also eine Art Datenpostfach für jeden, wo Sie einstellen können, wer welche Art von Daten für wie lange und für welchen Zweck benutzen darf.

Das Wichtigste ist wirklich, dieses Internet der Dinge als Bürgernetzwerk zu betreiben, um eine Mitmachgesellschaft zu ermöglichen. Dann werden viele Dinge möglich, nicht nur Echtzeitmessungen, mehr Bewusstsein für die Probleme in unserer Welt und mehr wissenschaftliche Einsichten, sondern eben auch die Selbstorganisationsfähigkeit von vielen Prozessen und kollektive Intelligenz. Zum Beispiel können wir diese lästigen Staus, über die wir am Anfang gesprochen haben, überwinden. Wir haben Fahrerassistentensysteme entwickelt, die auf dezentralisierte Art und Weise den Verkehr stabilisieren, die Kapazität erhöhen. Selbst wenn nur 20 Prozent aller Autos damit ausgestattet sind, hat das schon einen Effekt. Ähnlich könnten wir das Stop-und-go-Phänomen der Weltwirtschaft, die Rezessionen, ausbügeln, sogar mit dezentralisierten Ansätzen. Auch die Selbststeuerung von Ampeln funktioniert viel besser als die zentralisierte Steuerung, die wir heutzutage haben. Sie bringt eine rund 30-prozentige Verbesserung, und zwar für die verschiedensten Verkehrsteilnehmer; sie geht also nicht zu Lasten bestimmter Bevölkerungsgruppen. Auch die Umwelt wird entlastet. Ähnlich können Industrie 4.0, Smart Grids und vieles mehr von dezentralisierten Prinzipien profitieren. Solche Ansätze kann man jetzt auch im Bereich von sozialen Systemen anwenden. Es gibt zum Beispiel verschiedene soziale Mechanismen, welche die Kooperation und Selbstorganisation in unserer Gesellschaft unterstützen können. Reputationssysteme sind nur ein Beispiel.

3.6 Die Gesellschaft ist keine Maschine

Damit komme ich zum Schluss. Die digitale Gesellschaft, samt der Ökonomie 4.0, braucht aus meiner Sicht mehrere öffentliche Informationssysteme. Ein planetares Nervensystem wie Nervousnet wäre zum Beispiel nützlich, um Externalitäten zu messen und Feedbackeffekte zu ermöglichen. Dafür braucht es außerdem ein multidimensionales Austauschsystem, das für alle zugänglich sein muss. Zusätzlich sind digitale Assistenten und Informationsplattformen zur Unterstützung kollektiver Intelligenz nötig. Dies alles würde nicht Top-down umgesetzt, sondern es könnte alles auf verteilten Ansätzen basieren. Dies ist auch für das Thema Security wichtig. Insofern haben wir uns die Gesellschaft der Zukunft nicht wie eine riesige zentral gesteuerte Maschine vorzustellen, sondern als Ko-Evolution von vielen weitgehend autonomen Prozessen, die durch Berücksichtigung der Externalitäten koordiniert werden.

Das hat Vorteile für die Politik, die Wirtschaft und für jeden Einzelnen. Deswegen sollten wir das nun angehen. Zu den Vorteilen gehört die massive Verbesserung der Effizienz durch Selbstorganisation. Der Ansatz ist auch perfekt mit Demokratie und unternehmerischer Freiheit vereinbar. Aber im Unterschied zu heute würden wir durch die Berücksichtigung der Externalitäten mehr Rücksicht auf die Umwelt nehmen, während Kooperation gefördert und Konflikte reduziert würden. Also, worauf warten wir noch? Warum machen wir das nicht einfach zusammen?

Danksagung

Ich danke Christopher Albrodt vom Institut für Medien- und Kommunikationspolitik für die Anfertigung dieses Transkripts und Fabian Granzeuer vom selben Institut für die freundliche Nachdruckgenehmigung.

Literatur

Anderson, Chris. 2008. The end of theory: The data deluge makes the scientific method obsolete. *Wired* (23. Juni). http://www.wired.com/2008/06/pb-theory/ (Zugriff: 3. März 2016).

Blair, Tony. 2014. Is democracy dead?: Tony Blair: for true democracy, thr right to vote is not enough. *The New York Times* (4. Dezember). http://www.nytimes.com/2014/12/04/opinion/tony-blair-is-democracy-dead.html?_r=1 (Zugriff: 3. März 2016).

Gates, Bill. 2015. Eintrag bei reddit – Hi reddit, I'm Bill Gates and I'm back for my third ama. ask me everything. *reddit.com.* https://www.reddit.com/r/IAmA/comments/2tzjp7/hi_reddit_im_bill_gates_and_im_back_for_my_third/ (Zugriff: 3. März 2016).

Google. Google Flu Trends Data. https://www.google.org/flutrends/about/ (Zugriff: 7. April 2016).

Helbing, Dirk. 2015. *The automation of society is next: How to survive the digital revolution;* Version 1.0. North Charleston, SC: Createspace. https://www.researchgate.net/publication/281348054_The_Automation_of_Society_is_Next_How_to_Survive_the_Digital_Revolution_Preprint_version_v0_for_comment_only_not_for_distribution (Zugriff: 3. März 2016).

Helbing, Dirk, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari und Andrej Zwitter. 20015. Digitale Demokratie statt Datendiktatur: Big Data, Nudging, Verhaltenssteuerung: Droht uns die Automatisierung der Gesellschaft durch Algorithmen und künstliche Intelligenz? Ein gemeinsamer Apell zur Sicherung von Freiheit und Demokratie. *Spektrum der Wissenschaft* (17. Dezember). http://www.spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933 (Zugriff: 3. März 2016).

Helbing, Dirk und Steven Bishop. 2012. *FuturICT project summary.* FuturICT. Global computing for our complex world. http://futurict.inn.ac/wp-content/uploads/2015/06/FuturICT_5p_Project-Summary-WITH-LOGOS.pdf (Zugriff: 3. März 2016).

Herzinger, Richard. 2014. Ist die liberale Demokratie ein Auslaufmodell? *Die Welt* (9. November). http://www.welt.de/debatte/kommentare/article134154197/Ist-die-liberale-Demokratie-ein-Auslaufmodell.html (Zugriff: 3. März 2016).

McFarland, Matt. 2014.Elon Musk: With artificial intelligence we are summoning the demon. *The Washington Post* (24. Oktober). https://www.washingtonpost.com/news/innovations/wp/2014/10/24/elon-musk-with-artificial-intelligence-we-are-summoning-the-demon/ (Zugriff: 3. März 2016).

Musk, Elon. 2014. Twitter-Account. Eintrag: 2. August 2014, 19 Uhr 33 Minuten. https://twitter.com/elonmusk/status/495759307346952192 (Zugriff: 3. März 2016).

Müller, Henrik. 2015. Müllers Memo: Der Kapitalismus funktioniert nicht mehr. *Der Spiegel* (12. April). http://www.spiegel.de/wirtschaft/wachstum-der-weltwirtschaft-der-kapitalismus-ist-kaputt-a-1028098.html (Zugriff: 3. März 2016).

Smith, Paul. 2015. Apple co-founder Steve Wozniak on the Apple Watch, electric cars and the surpassing of humanity. *Financial Review* (23. März). http://www.afr.com/technology/apple-cofounder-steve-wozniak-on-the-apple-watch-electric-cars-and-the-surpassing-of-humanity-20150320-1m3xxk (Zugriff: 3. März 2016).

Uchatius, Wolfgang. 2011. Kapitalismus in der Reichtumsfalle. *Die Zeit* (10. November). http://www.zeit.de/2011/46/Kapitalismus (Zugriff: 3. März 2016).

United Nations. 2015. *Global follow-up and review of the 2030 Agenda for sustainable development.* United Nations Department of Economic and Social Affairs. Division for Sustainable Development. https://sustainabledevelopment.un.org/hlpf/follow-up (Zugriff: 3. März 2016).

Winter, Jana und Cora Currier. 2015. Exclusive: TSA's secret behavior checklist to spot terrorists. *The Intercept* (27. März). https://theintercept.com/2015/03/27/revealed-tsas-closely-held-behavior-checklist-spot-terrorists/ (Zugriff: 3. März 2016).

O. A. 2014. Wealth without workers, workers without wealth. *The Economist* (4. Oktober). http://www.economist.com/news/leaders/21621800-digital-revolution-bringing-sweeping-change-labour-markets-both-rich-and-poor (Zugriff: 3. März 2016).

Der Verbraucher als Datenlieferant

Rechtliche Aspekte von „smarten“ Produkten

Barbara Kolany-Raiser

DOI 10.15501/978-3-86336-912-5_3

Abstract

Die Entwicklung der letzten Jahre zeigt, dass immer mehr Produkte „smart“ werden – das Fitnessarmband animiert uns zu mehr Bewegung, der Kühlschrank bestellt eigenständig Lebensmittel nach. Für diese vom Verbraucher generierten Daten interessieren sich beispielsweise Krankenkassen, die den Kauf von Fitnessarmbändern subventionieren und Bonusprogramme einrichten. Neben dem datenschutzrechtlichen Aspekt soll es auch um vertragliche und haftungsrechtliche Fragestellungen rund um die „smarten“ Geräte gehen.

Besonderer Dank für die Mitarbeit geht an die studentischen Hilfskräfte Clara Berrisch, Sandra Dittmer und Lucas Werner.

1 Einleitung

Nach einer im April 2015 durchgeführten Umfrage des Meinungsforschungsinstitutes Forsa, die im Auftrag der Verbraucherzentrale Bundesverband erfolgte, sind 81 Prozent der befragten Verbraucherinnen und Verbraucher der Meinung, dass ihnen aus der Sammlung und Auswertung persönlicher Daten durch Unternehmen im Netz mehr Nachteile als Vorteile erwachsen (vzbv 2015). Viele Daten entstehen dadurch, dass der Kunde selbst sogenannte Smart Devices wie zum Beispiel Smartphones, Smartwatches oder Fitnessarmbänder verwendet, um damit Daten über seine Vitalwerte, seine Ernährung oder sein Schlafverhalten zu sammeln. Dies spiegelt den Trend der Selbstüberwachung zur Selbstoptimierung wider. Die zunehmende Vernetzung von Gegenständen sowohl im geschäftlichen als auch im privaten Bereich birgt aber gleichzeitig enorme Herausforderungen – insbesondere für das Recht.

2 Vertragliche Fragestellungen

Für die vertragliche Einordnung beim Kauf smarter Produkte ist zunächst der Begriff des typengemischten Vertrags von Bedeutung. Darunter versteht man Verträge, bei denen Elemente unterschiedlicher Vertragstypen vorliegen.

Dem Käufer kommt es beim Kauf eines intelligenten Kühlschranks oder einer Smartwatch nicht allein darauf an, die klassischen Funktionen eines Kühlschranks oder einer Uhr zu nutzen, sondern auch die „intelligenten“ Zusatzdienste in Form der serverbasierten Dienste[1] in Anspruch nehmen zu können. Neben den kaufvertraglichen Elementen stellt sich die Frage, wie diese Dienstvertragsmerkmale einzuordnen sind.

1 Der Kühlschrank erinnert z. B. an das Verfallsdatum der Lebensmittel, macht Rezeptvorschläge und schickt Einkaufslisten an das Smartphone.

Wie Solmecke und Vondrlik feststellen, fehlt es im Normalfall an einer ausdrücklichen Regelung für diesen für das smarte Produkt notwendigen Serverdienst. Dies gilt sowohl für den Verkauf von smarten Produkten in Großmärkten als auch beim Onlinevertrieb. (Solmecke und Vondrlik 2013, 756) Unklar ist vor allem, inwiefern von einer stillschweigenden Willenserklärung hinsichtlich des Abschlusses eines Dienstvertrages ausgegangen werden kann.

Für das Vorliegen einer stillschweigenden Willenserklärung ist der Erklärungsgehalt eines objektiven Betrachters zum Zeitpunkt des Vertragsabschlusses maßgeblich. Sowohl im Großmarkt als auch im Falle des Onlineshops handelt es sich bei den ausgestellten und beworbenen Waren um kein verbindliches Angebot. Vielmehr soll der Kunde dazu aufgefordert werden, sein Kaufangebot abzugeben. Ein Kaufangebot wird vom Kunden durch das Auf-das-Kassenband-Legen der Ware oder durch das Abschicken einer Bestellung im Onlineshop abgegeben. Die Vertragsannahme erfolgt durch den Verkäufer (Busche 2016, Rn. 11, 12), entweder ausdrücklich oder stillschweigend durch Übersendung der Ware an den Käufer oder durch das Kassieren des Personals. Der objektive Erklärungsgehalt des vom Käufer abgegebenen Angebotes wird dabei wesentlich durch die sowohl in den Verkaufsräumen als auch im Onlineshop vorhandene Werbung beeinflusst. Der Käufer soll doch gerade zu den in der Werbung dargestellten Bedingungen dem Verkäufer ein Angebot unterbreiten. Wird der serverbasierte Dienst in der Werbung für das smarte Produkt mitbeworben, ist davon auszugehen, dass der Kunde neben dem Erwerb des Eigentums an diesem smarten Produkt auch die Verwendung dieser Zusatzdienste anstrebt und er daher mit seinem Antrag auch den Betrieb des Serverdienstes als Vertragsbestandteil ansieht. (Solmecke und Vondrlik 2013, 756)

Hier stellt sich die Frage, inwieweit der Verkäufer für die serverbasierte Leistung einzustehen hat. Dem Verkäufer ist das offensichtliche Interesse des Kunden an diesem Serverdienst bekannt. Denn auch wenn der Käufer eine Einmalzahlung für den Kaufpreis leistet, kann daraus für ihn nicht geschlossen werden, dass der Verkäufer sich nicht zur Erbringung des Serverdienstes verpflichten möchte (Solmecke und Vondrlik 2013, 755). Daher müsste der Verkäufer die Kundschaft darauf hinweisen, dass er rechtlich nicht für diesen Dienst einstehen will.

Beim Erwerb eines Fitnessarmbandes ist der Zusatzdienst in Form von Pulsmesser und Bewegungstracker der eigentliche Grund für den Kauf des Produktes, weshalb hier davon auszugehen ist, dass der Kaufvertrag in Kombination mit dem serverbasierten Zusatzdienst abgeschlossen werden soll. Dabei ist es unerheblich, ob der Verkäufer den Dienst selbst betreibt oder dieser durch einen Dritten betrieben wird.

Bei unserem Beispiel des smarten Kühlschranks bestehen verschiedene server- und internetbasierte Nutzungsmöglichkeiten. Manche Modelle erlauben nicht nur die Nutzung von Diensten des Herstellers, sondern auch offener Plattformen Dritter.[2] Internetdienste für die laufenden Bestellungen oder andere Funktionen können insofern auch durch vom Verkäufer unabhängige Anbieter erbracht werden. Zudem verbleibt dem Kühlschrank auch ohne zusätzliche serverbasierte Dienste die eigenständige und hauptsächliche Funktion, Lebensmittel zu kühlen und aufzubewahren. Daher ist in diesem Fall davon auszugehen, dass im Kaufrecht und nicht im Dienstvertragsrecht der Schwerpunkt des Vertrages liegt (Bräutigam und Klindt 2015, 1138).

Nachdem geklärt ist, dass der Verkäufer für die Erbringung des serverbasierten Dienstes einstehen muss, stellt sich die Frage der Dauer dieser Leistungspflicht. Es ist anzunehmen, dass die Vertragsparteien bei Kenntnis der Rechtslage auch eine Regelung über die Vertragsdauer getroffen hätten.[3] Da das smarte Produkt ohne den intelligenten Zusatzdienst einen wesentlichen Teil seiner Funktionen einbüßt und damit erheblich an Wert verliert, dürfte dem Verbraucher an einer möglichst langen Vertragsdauer gelegen sein. Auch für den Verkäufer ist eine möglichst lange Vertragsdauer erstrebenswert, wenn er eine Strategie der intensiven Kundenbindung verfolgt. Wichtig ist für den Kunden neben der langen Vertragsdauer jedoch auch die Festschreibung eines Kündigungsverzichtes durch den Verkäufer, da andernfalls eine jederzeitige

2 So beispielsweise Samsungs RF4289, auf dem neben hauseigenen Funktionen wie Samsungs „Grocery Manager App“ auch Dienste wie „Twitter“ oder „Evernote“ genutzt werden können.

3 Zur Auslegung des Vertrages siehe § 157 BGB.

Kündigung des Dienstvertrages durch den Verkäufer möglich wäre.[4] Da es keine allgemeingültige Regelung für die Festlegung einer Mindestleistungsdauer gibt, empfiehlt sich die Orientierung an der Verjährungsfrist, die bei Sachmängeln zwei Jahre gemäß § 438 Abs. 1 Nr. 3 BGB beträgt (Solmecke und Vondrlik 2013, 757).

3 Haftungsrechtliche Fragestellungen

Durch die Einstellung des Serverdienstes wird der smarte Gegenstand entweder komplett funktionslos oder verliert einen Teil seiner Gebrauchsfähigkeit. Dies führt zu einer Wertminderung gegenüber einem Smartprodukt mit funktionsfähigem Serverdienst. Zu klären ist daher, inwieweit dem Käufer Ansprüche aus der vertraglichen oder deliktischen Haftung gegenüber dem Verkäufer erwachsen können.

3.1 Vertragliche Haftung

Durch Abschluss der vertraglichen Vereinbarung wird – wie gezeigt – zum einen die Pflicht, den serverbasierten Dienst zu betreiben, begründet. Zum anderen können aus dem Nichtbetrieb aber auch weitere Ansprüche, wie zum Beispiel Nacherfüllungs- oder Schadensersatzansprüche, erwachsen.

4 Vgl. §§ 620 Abs. 2 i.V.m. 621 Abs. 5 BGB. Solmecke und Vondrlink haben dabei eine Liste von Kriterien erstellt, die bei der Festlegung der Leistungsdauer berücksichtigt werden sollten. So spielt neben dem Äquivalenzinteresse des Käufers auch die Erwartung des Käufers in Bezug auf die Einstellung des Serverdienstes sowie der Produktzyklus oder auch die Preisgestaltung des Produktes oder dessen Funktionsfähigkeit ohne den Serverdienst eine Rolle.

3.1.1 Ansprüche aus Kaufvertrag/Kaufrechtliche Gewährleistung

Sofern ein Sachmangel vorliegt, d. h. die Ist- von der Sollbeschaffenheit abweicht, kommen Gewährleistungsansprüche in Betracht. Beim Fitnessarmband wäre die Sollbeschaffenheit das Funktionieren der smarten Trackingdienste. Wenn diese nicht mehr funktionieren, weicht die tatsächliche, also die Istbeschaffenheit, negativ von der Sollbeschaffenheit ab.

Zwar würden unsere Beispielsprodukte, d. h. der smarte Kühlschrank wie auch das Fitnessarmband, zweifellos durch Einstellung des Serverbetriebes eine wertbildende Eigenschaft verlieren, was grundsätzlich einem Sachmangel entspräche. Dieser Mangel entsteht regelmäßig jedoch erst mit der Einstellung des Serverbetriebes, d. h. erst nach Übergabe des jeweiligen Produktes und somit auch erst nach dem Gefahrübergang.[5] Da im Zeitpunkt des Gefahrübergangs die vereinbarte Beschaffenheit gegeben ist, kann der Käufer keine Gewährleistungsansprüche geltend machen.

Eine Ausnahme gilt jedoch für Verbrauchsgüterkäufe, also Verträge, die zwischen einem Verbraucher und einem Unternehmer über den Kauf einer beweglichen Sache zustande kommen, vgl. § 474 Abs. 1. BGB. Absatz 1 dieser Norm erweitert den Anwendungsbereich des Verbrauchsgüterkaufs explizit auf Verträge, bei denen neben dem Kauf der beweglichen Sache auch die Erbringung einer Dienstleistung Teil des Vertrages wird. Für diese Verträge gilt mitunter die Vorschrift des § 476 BGB. Danach wird vermutet, dass die Sache bereits bei Gefahrübergang mangelhaft war, sofern sich der Mangel innerhalb von sechs Monaten nach Gefahrübergang zeigt. Der Europäische Gerichtshof hat in seinem Urteil vom 4. Juni 2015[6] die Position des Verbrauchers zusätzlich

5 Hierunter versteht man den Zeitpunkt, in dem das Risiko einer Verschlechterung oder der Verlust einer Sache vom Schuldner auf den Gläubiger übergeht.

6 EuGH, Urteil vom 6. Juni 2015, Rs. C-497/13. http://curia.europa.eu/juris/document/document.jsf?text=&docid=164727&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 (Zugriff: 23. November 2015).

dahin gehend gestärkt, dass die Vermutung nicht nur in zeitlicher,[7] sondern auch in sachlicher Hinsicht wirkt. Der Verbraucher braucht folglich innerhalb der ersten sechs Monate nach Gefahrübergang nur noch zu beweisen, dass überhaupt ein Mangel vorliegt. Dies ist insbesondere dann von Vorteil, wenn sich nicht nachweisen lässt, ob der Mangel auf unsachgemäße Bedienung zurückzuführen ist oder ob er schon vor Gefahrübergang vorlag und sich nur zu einem späteren Zeitpunkt gezeigt hat.

Jedenfalls im Bereich des Verbrauchsgüterkaufs kann das kaufrechtliche Gewährleistungsrecht somit für Ansprüche des Käufers eröffnet sein.

3.1.2 Ansprüche aus Dienstvertrag

Beim Dienstvertrag[8] besteht die vertraglich geschuldete Leistung in der ordnungsgemäßen Erbringung der vereinbarten Dienstleistung – für unsere Beispiele wären dies die serverbasierten Dienste. Im Dienstvertragsrecht gibt es, anders als im Kaufrecht, kein eigenes Gewährleistungsrecht, sondern es gilt das allgemeine Leistungsstörungsrecht der §§ 280 ff. BGB.

Durch das Leistungsstörungsrecht wird der Empfänger einer nicht ordnungsgemäßen Leistung umfassend geschützt. Einerseits werden ihm Schäden ersetzt, die direkt daraus resultieren, dass er die Leistung eben nicht oder nicht ordnungsgemäß erhält, andererseits werden ihm Schäden ersetzt, die an seinem restlichen Vermögen dadurch entstehen, dass die Sache nicht ordnungsgemäß ist. Letzteres wäre zum Beispiel der Fall, wenn aufgrund eines Fehlers am smarten Kühlschrank weitere Küchengegenstände oder sich im Kühlschrank befindliche Lebensmittel beschädigt werden.

Wird der serverbasierte Dienst eines Fitnessarmbands eingestellt, ist die Leistung nicht mehr ordnungsgemäß. Der Verkäufer kann sich nach den obigen

---

7 So nämlich die ständige Rechtsprechung des BGH, erstmals in der „Zahnriemen“-Entscheidung vertreten. BGH, Urteil vom 2. Juni 2004, Az. VIII ZR 329/03 („Zahnriemen-Entscheidung“). https://openjur.de/u/197445.html (Zugriff: 23. November 2015).

8 Geregelt in den §§ 611 ff. BGB.

Ausführungen Schadenersatzansprüchen wegen Nicht- oder nicht vertragsgemäßer Leistung ausgesetzt sehen. (Solmecke und Vondrlik 2013, 758)

Wenn aufgrund technischer Probleme die Erbringung des Dienstes unmöglich wird, stellt sich die Frage, ob der Käufer Schadenersatzansprüche gegen den Vertragspartner geltend machen kann (Solmecke und Vondrlik 2013, 758). Erhält das Produkt aufgrund der Störungen keine Antwort mehr vom Server, kann dies dazu führen, dass die smarten Dienste ausfallen. Das Fitnessarmband würde in der Konsequenz aufhören zu tracken beziehungsweise die Ergebnisse nicht speichern können. Oder der Kühlschrank würde nicht mehr selbstständig den Bedarf ermitteln sowie Lebensmittel auf deren Haltbarkeit überprüfen.

Die Frage ist, was der Käufer in einem solchen Fall ersetzt bekommt. Grundsätzlich ist der Geschädigte bei Eintritt eines Schadens so zu stellen, wie er stünde, wenn das schädigende Ereignis ausgeblieben wäre (Oetker 2015, Rn. 18). Der Schaden beträgt somit den Wertverlust, den das Produkt durch die Einstellung des serverbasierten Dienstes erleidet. Konkret bedeutet dies, dass der Wert des Kühlschranks mit und ohne den serverbasierten Dienst verglichen werden muss (Solmecke und Vondrlik 2013, 758). Dies gilt unabhängig davon, ob die Nutzbarkeit des Gegenstands völlig oder nur teilweise aufgehoben wird.

3.2 Deliktische Haftung

Ungeachtet möglicher vertraglicher Ansprüche ist zu prüfen, ob auch Schadenersatzansprüche gemäß § 823 Abs. 1 BGB entstanden sein könnten. Schadenersatzpflichtig ist hiernach, wer bedeutende Rechte oder Rechtsgüter[9] eines anderen widerrechtlich verletzt, wenn letzterem dadurch ein Schaden entsteht.

Da die meisten Anspruchsvoraussetzungen einzelfallbezogen sind, soll hier vor allem auf das Kriterium der Rechtsverletzung eingegangen werden.

9 Geschützt werden vor allem Eigentum, Besitz und weitere Rechte, nicht aber das Vermögen.

Als verletztes Recht kommt insbesondere das Eigentum in Betracht. Eine Eigentumsverletzung liegt immer dann vor, wenn in die Befugnisse des Eigentümers nach § 903 BGB eingegriffen wird. Mögliche Beeinträchtigungen sind die Verletzung der Sachsubstanz, der Entzug der Sache oder die Beeinträchtigung ihrer Nutzungs- und Gebrauchsfähigkeit (Staudinger 2014, Rn. 12). Bei letzterem ist die Abgrenzung zu einem Vermögensschaden, der nach § 823 BGB gerade nicht ersetzt wird, umstritten. Wird die Nutzung einer Sache beeinträchtigt, ohne dass überhaupt körperlich auf sie eingewirkt wird, kommt es nach der Rechtsprechung auf die Intensität der Nutzungsbeeinträchtigung an. Eine Eigentumsverletzung wird daher bejaht, soweit die Verwendungsfähigkeit einer Sache praktisch aufgehoben wird. Geht es dagegen nur um eine bestimmte Verwendungsmöglichkeit, die das Einsatzpotential der Sache nicht erschöpft, liegt keine Verletzung vor (Wagner 2014, Rn. 180).

In Bezug auf smarte Produkte würde dies bedeuten: Fällt ein serverbasierter Dienst aus, muss geprüft werden, ob die Gebrauchs- und Nutzungsfähigkeit beeinträchtigt ist. Für das Fitnessarmband lässt sich wohl nach allen Meinungen eine erhebliche Intensität der Beeinträchtigung und somit eine Eigentumsverletzung bejahen.

Bezüglich des Kühlschranks, der infolge des Dienstausfalls keine Haltbarkeitsdaten mehr anzeigt, muss eine differenziertere Betrachtung erfolgen. Festzuhalten ist nämlich, dass der Kühlschrank auch bei Ausfall des Zusatzdienstes seine Kernaufgabe – die Kühlung seiner Inhalte – weiterhin erfüllt. Der serverbasierte Dienst fällt der Rechtsprechung nach lediglich unter eine Verwendungsmodalität, die das verbleibende Einsatzpotenzial des Geräts unberührt lässt. Die Literatur kommt zu unterschiedlichen Ergebnissen. Ein hinreichender Intensitätsgrad an Beeinträchtigung kann wohl nicht angenommen werden. Jedoch ist es durchaus denkbar, dass der Marktwert der Sache dadurch herabgesetzt wird, was einigen für eine Eigentumsverletzung genügen würde.

4 Datenschutzrechtliche Fragen

Wie eingangs schon ausgeführt, werden durch smarte Produkte wie Fitnessarmbänder, Smartwatches oder andere Wearables Daten über die Herzfrequenz, den Blutdruck, die zurückgelegten Schritte und die Gesamtaktivität des Trägers sowie Standortdaten gesammelt. Häufig geht die Nutzung von Wearables mit der Installation von Gesundheitsapps auf Smartphones oder Tablets einher, die den Nutzer zu mehr sportlicher Betätigung animieren sollen. Die technischen Möglichkeiten, sich im Zuge einer Selbstoptimierung und Motivation selbst zu überwachen und zu kontrollieren, sind vielfältig. Diese Daten stehen dabei nicht bloß dem Träger oder Nutzer der Geräte zum persönlichen Feedback zur Verfügung, sondern ermöglichen es auch, den Herstellern umfangreiche Nutzerprofile zu erstellen. Zudem haben einige (gesetzliche) Krankenkassen die Beliebtheit von digitalen Fitnessangeboten erkannt und bieten neben Apps, digitalen Ärzteführern und Onlinekursen auch Zuschüsse für den Erwerb von Pulsmessern, Selftrackern u. a. digitalen Fitnessgeräten an. So gewährt zum Beispiel die AOK-Nordost ihren Versicherten jedes zweite Jahr einen Zuschuss von fünfzig Prozent der Kosten oder bis zu 50 Euro beim Erwerb eines dieser Produkte. Sie bietet ihren Versicherten zudem seit dem 1. Januar 2015 ein AOK-Gesundheitskonto, in dem verschiedenste Gesundheitsleistungen im Jahr mit bis zu 270 Euro bezuschusst werden können (AOK 2015). Bislang setzen die Krankenkassen jedoch nur auf Bezuschussungen – eine Weiterleitung persönlicher Daten an die Krankenkasse findet zurzeit (noch) nicht statt (Bohsem 2015). Im System der gesetzlichen Krankenkassen ist das Bonussystem nicht neu und vielen durch die Bonushefte bekannt. Die neuen Anreizsysteme werden dabei in bereits bestehende andere Bonusprogramme integriert. Die Versicherten sollen dabei zu einer gesünderen Lebensweise animiert werden.

Am 17. Juli 2015 ist das Gesetz zur Stärkung der Gesundheitsförderung und Prävention in Kraft getreten.[10] Nach § 65a PrävG sollen die Krankenversicherungen in ihren Satzungen ausdrücklich festlegen, unter welchen Bedingungen ihre Versicherten Anspruch auf einen Bonus haben. Durch die Bezu-

10 Gesetz zur Stärkung der Gesundheitsförderung und Prävention (Präventionsgesetz – PrävG), BGBl 1368/2015 I Nr. 31.

schussung von Wearables, Fitnessapps und digitalen Sportkursen kommt es nämlich zu einer indirekten Subvention für Bewegungstrainings. Gerade weil die durch die Verwendung dieser Geräte entstehenden Daten bislang noch nicht an die Versicherungen übermittelt werden, stellt sich die Frage, ob sich Bonuszahlungen und niedrigere Prämien auf Dauer rechtfertigen lassen, wenn eine gesündere Lebensweise der verwendenden Versicherten nicht überprüft wird. (Dams 2014) Derzeit ist es den gesetzlichen Krankenkassen jedoch nur unter den in § 284 Abs. 1 SGB V abschließend aufgeführten Fällen erlaubt, personenbezogene Daten ihrer Versicherten zu erheben. Dabei ist die Erhebung der Daten auch an das strenge Kriterium der Erforderlichkeit gebunden. Es muss ein bestimmbarer Zweck vorliegen, damit die Daten gesammelt werden dürfen. Ist dies nicht gegeben, ist das Sammeln der Daten unzulässig, sodass die Verarbeitung der gewonnenen Daten unzulässig wäre. Da die bereichsspezifischen Vorschriften des SGB V den allgemeinen Vorschriften des Bundesdatenschutzgesetzes (BDSG) vorgehen, ist eine Einwilligung von Patienten nicht möglich. (Peters 2015, Rn. 6,10)

Bei privaten Versicherungen können die Versicherten der Erhebung ihrer personenbezogenen Daten durch das Versicherungsunternehmen vertraglich zustimmen. Bei der DKV können Versicherte sich den Kauf eines Fitnessarmbands oder auch einer Smartwatch mit einem Beitrag von fünfzig Euro fördern lassen. Dieses Angebot bezieht sich allerdings nur auf bestimmte Tarife. (Berres und Weber 2015) Einen Schritt weiter geht die Generali: Für 2016 plant der Konzern die Einführung seiner Vitality-Produkte in Deutschland, Österreich und Frankreich. Neben Innovationen in der Krankenversicherung sind auch Produkte für die Lebens- und Berufsunfähigkeitsversicherung geplant. Dabei soll der Versicherte zu Beginn das Gesundheits- und Fitnessniveau ermitteln und sich dann Ziele setzen, bei deren Erreichung Punkte vergeben werden. Um Gutscheine und Rabatte zu bekommen, werden Punkte für ärztliche Vorsorgetermine, aber auch für Fitness, Bewegung und den Einkauf von gesunden Lebensmitteln vergeben. (Generali 2015) Da Generali Kooperationen mit Sportartikelherstellern und anderen Firmen plant, sind auch Rabatte für Wearables denkbar (Berres und Weber 2015).

Die Anwendbarkeit des BDSG auf die durch das „self-tracking“ erhobenen Daten ergibt sich aus § 1 Abs. 2, BDSG, der die Anwendung des Gesetzes auf die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten festlegt.

Durch das Gerät werden die Daten über den Puls, die Herzfrequenz oder andere Bewegungsdaten sowohl erhoben als auch verarbeitet – und zwar in Form der Speicherung und Aufbereitung für den Nutzer. Unstrittig ist, dass es sich bei den durch die Wearables erhobenen Daten um personenbezogene Daten handelt, da nach § 3 Abs. 1 BDSG personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person sind. Einzelangaben über persönliche Verhältnisse sind jene, die der Identifizierung der Person dienen, worunter auch Angaben zum Gesundheitszustand fallen (Franzen 2016, Rn. 2). Daten über den Gesundheitszustand einer Person sind dabei besonders sensible Angaben über eine Person und fallen daher unter § 3 Abs. 9 BDSG.

Normadressat ist die verantwortliche Stelle. Nach § 3 Abs. 7 BDSG ist das jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Wird eine Fitnessapp von einer gesetzlichen Krankenkasse oder einer Versicherung angeboten, so ist diese als verantwortliche Stelle anzusehen. Auch wenn die personenbezogenen Daten nicht von der Krankenkasse oder Versicherung selbst verarbeitet werden, sondern durch eine andere Stelle im Auftrag der Krankenkasse oder Versicherung, trägt diese die Verantwortung für den Umgang mit den personenbezogenen Daten und die Einhaltung der gesetzlichen Vorgaben. (Dammann 2014, Rn. 224 ff.) Die damit einhergehenden Kontroll- und Sorgfaltspflichten ergeben sich aus § 11 BDSG: Wird für den technischen Betrieb der App ein Clouddienst eingesetzt, so muss die Krankenkasse oder Versicherung darauf achten, dass die Datenverarbeitung nicht in den USA stattfindet, da das Safe Harbor Abkommen[11] durch das Urteil des Europäischen Gerichtshofs[12] für ungültig erklärt wurde, weil es keinen adäquaten Daten-

11 Das Safe Harbor Abkommen war eine Vereinbarung zwischen der EU und den USA in Bezug auf die Übermittlung personenbezogener Daten in die USA. Das Abkommen basierte auf einer Entscheidung der Europäischen Kommission aus dem Jahr 2000. Grundsätzlich verbietet die Europäische Datenschutzrichtlinie eine Datenübermittlung an Staaten mit einem geringeren Datenschutzniveau, zu welchen die USA zählen. Durch das Safe Harbor Abkommen wurde ein Verfahren entwickelt, welches den Unterzeichnern des Abkommens dennoch einen Datentransfer ermöglichte. Für mehr Informationen vgl. BDFI unter http://bit.ly/1j5Ddjr.

12 EuGH, Urteil vom 6. Oktober 2015, C-362/14. Maximilian Schrems v. [Irish] Data Protection Commissioner, Fn.106. http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=DE (Zugriff: 23. November 2015).

schutz für die Datenübertragung zwischen Europa und den USA sicherstellt. Im Februar 2016 haben sich die EU-Kommission und die Vereinigten Staaten auf ein neues Abkommen zur transatlantischen Übermittlung von Daten für kommerzielle Zwecke geeignet (sog. EU-US Privacy Shield). Das neue Abkommen soll die Grundrechte europäischer Bürger schützen, indem es strengere Datenschutzauflagen für US-Unternehmen vorsieht, den Zugriff der US-Behörden auf personenbezogene Daten begrenzt und Beschwerdemöglichkeiten für EU-Bürger bereithält. (Europäische Komission 2016).

Die Tatsache, dass Versicherungen wie die Generali international operieren, steht der Anwendung des deutschen BDSG nicht entgegen. Der Anknüpfungspunkt ist die deutsche Niederlassung der Versicherung.[13]

Für die Anwendbarkeit des BDSG ist es unerheblich, ob die Daten vom Betroffenen selbst oder einem Dritten stammen oder für welchen Zweck sie erhoben wurden (Dammann 2014, Rn. 4). Beim Datenschutzrecht handelt es sich um ein sogenanntes Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten grundsätzlich verboten ist, sofern nicht die Einwilligung des Betroffenen vorliegt oder eine Rechtsvorschrift dies erlaubt (Scheja und Haag 2013, Rn. 74).

Durch die Einwilligung wird der Umgang mit den personenbezogenen Daten legitimiert. Sie muss vor Beginn der Datenverarbeitung erteilt worden sein. Eine nachträgliche Genehmigung stellt keine Einwilligung dar, wodurch die Verarbeitung der personenbezogenen Daten unzulässig bleibt (Simitis 2014, Rn. 29). Außerdem muss sie freiwillig erteilt werden und sich auf den konkreten Umgang mit den Daten beziehen, weshalb der Betroffene über den Zweck der Erhebung, Verarbeitung oder Nutzung der Daten sowie den geplanten Umfang der Datenerhebung in Kenntnis gesetzt werden muss. Ist der konkrete Umfang noch unklar, besteht die Pflicht, den Betroffenen über alle

13 Vgl. § 1 Abs. 5 BDSG, die Anwendbarkeit des deutschen Datenschutzrechts knüpft primär an den Sitz der verantwortlichen Stelle. Hier gilt insoweit das Recht des Ortes, wo die Daten erhoben, verarbeitet oder genutzt werden. Sofern die tätige Stelle im Inland eine Niederlassung besitzt, greift allerdings wieder das Territorialitätsprinzip, sodass das deutsche Datenschutzrecht anwendbar ist. Dies gilt auch im Falle von rechtlich selbstständigen Tochtergesellschaften ausländischer Unternehmen (vgl. von Lewinski 2014, Rn. 52).

in Betracht kommenden Möglichkeiten und die daraus resultierenden Folgen zu informieren. Dementsprechend umfangreich können die für eine wirksame Einwilligung notwendigen Informationen ausfallen. Da es sich bei den durch Wearables erhobenen Daten nicht selten um besonders sensible Daten nach § 3 Abs. 9 BDSG handelt, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen. Aufgrund des im Datenschutzrecht geltenden Grundsatzes der Zweckbindung müssen die Daten gelöscht werden, sobald der festgelegte Zweck für die Datenerhebung erreicht wurde.

Die Einwilligung des Betroffenen bedarf nach § 4 Abs. 1 S. 3 BDSG der Schriftform und muss von ihm eigenhändig unterzeichnet werden. Das Schriftformerfordernis dient dem Schutz des Betroffenen vor übereilter und unbedachter Äußerung. Nach § 126a BGB ist eine elektronische Einwilligung möglich, sofern sie eine elektronische Signatur aufweist.[14]

Soll die Erhebung und Verarbeitung der Daten im Rahmen eines geplanten Anreizsystems wie jenem der Generali erfolgen, so muss dem Schriftformerfordernis Genüge getan werden und sich die Einwilligung explizit auf die Erhebung und Verarbeitung der durch die Fitnessarmbänder oder Apps erhobenen Gesundheitsdaten beziehen.[15]

Das BDSG ist gem. § 1 Abs. 3 subsidiär gegenüber bereichsspezifischen Regelungen, wie den datenschutzrechtlichen Vorschriften des Telemediengesetzes (TMG). Dieses findet stets Anwendung, wenn es sich bei dem Dienst um ein Telemedium handelt. Nach § 1 Abs. 1 TMG sind dies elektronische Informa-

14 Nach der Rechtsprechung des BGH ist eine Einwilligung auch im Rahmen von Allgemeinen Geschäftsbedingungen möglich, sofern sie besonders hervorgehoben ist. Dadurch ist dann eine gesonderte Unterschrift nicht notwendig (vgl. Payback-Urteil und Happy-Digits-Urteil). Dies gilt jedoch nicht für AGBs im elektronischen Geschäftsverkehr, mangels Schriftlichkeit. BGH, Urteil vom 16. Juli 2008, Az. VIII ZR 348/06 („Payback-Urteil"). http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=45162&linked=urt&Blank=1&file=dokument.pdf (Zugriff: 23. November 2015). BGH, Urteil vom 11. November 2009, Az. VIII ZR 12/08 („Happy Digits-Urteil"). https://www.jurion.de/Urteile/BGH/2009-11-11/VIII-ZR-12_08 (Zugriff: 23. November 2015).

15 Die Erhebung und Verarbeitung von personenbezogenen Daten durch Versicherungen ist nicht von der Privilegierung der Forschung nach § 4a Abs. 2 BDSG erfasst.

tions- und Kommunikationsdienste mit Ausnahme von Telekommunikation und Rundfunk. Während Telekommunikation auf die reine Übertragung von Signalen abzielt, kommt es bei Telemedien dagegen auf eine Inhaltsleistung an. Für die Anwendung muss zumindest eine Inhaltsleistung angeboten werden, wie dies bei den Wearables der Fall ist und es muss ein sogenanntes Anbieter-Nutzer-Verhältnis nach § 11 TMG bestehen. Stehen Berufs- oder dienstliche Zwecke für die Datennutzung im Vordergrund, ist das TMG nicht anwendbar. Bei den hier zu untersuchenden Diensten besteht gerade ein klassisches Anbieter-Nutzer-Verhältnis zwischen dem Verbraucher, der zum Beispiel die Trackingdienste nutzt, und dem Betreiber oder Hersteller, der die Dienste anbietet.

Neben den wichtigsten datenschutzrechtlichen Grundsätzen aus dem BDSG kennt das TMG spezielle Erlaubnistatbestände, in denen der Datenumgang ausnahmsweise erlaubt ist. Dabei wird zwischen Bestandsdaten (§ 14 TMG) und Nutzungsdaten (§ 15 TMG) unterschieden.

Bestandsdaten sind personenbezogene Daten des Nutzers, die während der gesamten Durchführung des Vertrags über die Nutzung eines Telemediums erforderlich sind, also insbesondere Kontakt- und Bankdaten. Bei Trackingdaten handelt es sich um Daten, die nach Vertragsschluss erst durch die Inanspruchnahme der Dienste erhoben werden, sodass es sich gerade nicht um Bestandsdaten handelt. Geht es jedoch um die Kopplung des Trackers mit einem Bonusprogramm wie Generali dies plant, dann ist die Erhebung von Kontaktdaten erforderlich, um eine Zurechnung der Daten zum Nutzer des Wearables zu ermöglichen.

„Nutzungsdaten“ sind erforderlich, um die Inanspruchnahme der Dienste zu ermöglichen und abzurechnen. Dabei werden auch solche Daten erfasst, die während oder durch die Nutzung entstehen (Spindler und Nink 2015, Rn. 2). Nutzungsdaten sind etwa Angaben über die vom Nutzer in Anspruch genommenen Dienste oder die Dauer der Benutzung. Sie müssen von den Inhaltsdaten abgegrenzt werden, auf die in Ermangelung spezieller Regelungen des TMG das BDSG anzuwenden ist. Inhaltsdaten sind im Gegensatz zu Nutzungsdaten gerade nicht zur Inanspruchnahme des Dienstes notwendig. Vielmehr sind sie Daten, die durch einen Telemediendienst übermittelt werden, um die Leistungs- und Rechtsverhältnisse zu erfüllen (Spindler und Nink 2015, Rn. 3).

Es muss somit festgestellt werden, ob die von den Wearables erhobenen Daten als Nutzungs- oder als Inhaltsdaten zu qualifizieren sind, um sie dementsprechend dem Anwendungsbereich eines datenschutzrechtlichen Gesetzes zuordnen zu können. Dabei muss zwischen den Trackingdaten und solchen, die notwendig sind, um die Trackingdaten an ein Bonusprogramm zu koppeln, unterschieden werden. Die von den Wearables erhobenen Trackingdaten betreffen je nach Gerät Gesundheitsdaten wie Puls- und Blutdruck oder messen die sportliche Aktivität mithilfe von Geodaten. Die Erhebung dieser Daten hat den Zweck, die vertraglich vereinbarte Leistung, namentlich die Erbringung der Trackingdienste, zu erfüllen. Somit handelt es sich um Inhaltsdaten, sodass die datenschutzrechtlichen Sonderbestimmungen der §§ 11–15a TMG keine Anwendung finden und auf die allgemeinen Regelungen des BDSG zurückgegriffen werden muss.[16] Bei der Erhebung von Gesundheitsdaten im Rahmen von Bonusprogrammen müssen zusätzlich solche Daten erhoben werden, mithilfe derer der Nutzer identifiziert und seinen Trackingdaten zugeordnet werden kann. In diesem Fall würden Bestands-, Inhalts- und Nutzungsdaten erhoben werden, auf die zum einen das TMG als auch das BDSG anwendbar sind. Die Einwilligung kann nach § 13 Abs. 2 TMG auch in elektronischer Form erfolgen, sofern sichergestellt ist, dass der Betroffene die Einwilligung bewusst und eindeutig erteilt hat, dies protokolliert wurde, der Inhalt der Einwilligung jederzeit abrufbar ist und dem Betroffenen die jederzeitige Möglichkeit zum Widerruf der Einwilligung offen steht.

Die Einwilligung nach § 13 Abs. 2 TMG bezieht sich aber nur auf die Bestands- und Nutzerdaten. Da für die Verwendung von Wearables im Rahmen von Bonuspunkteprogrammen von Versicherungen auch gerade die Inhaltsdaten relevant sind, da sich aus ihnen der Nachweis der sportlichen Betätigung ergibt, ist das Schriftformerfordernis des § 4a Abs. 1 S. 3 BDSG einzuhalten. Wurde nur eine elektronische Einwilligung eingeholt, so ist diese zwar für die Bestands- und Nutzungsdaten wirksam, in Bezug auf die Inhaltsdaten aber liegt

16 In Ausnahmefällen sind Inhaltsdaten doch unter § 15 TMG zu fassen, vgl. hierzu Spindler/Nink, Rn. 7.

eine unwirksame Einwilligung vor[17], sofern sie nicht mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist.[18]

Durch die Verwendung von Fitnessapps und Wearables will der Nutzer sich zu mehr Bewegung motivieren. Werden die von den Geräten erhobenen Daten im Rahmen von Bonusprogrammen oder zur Senkung von Versicherungstarifen an Versicherer übertragen, trägt der Nutzer zur Schaffung seines Gesundheitsscores bei. Hier besteht die Gefahr von zukünftigen Versicherungstarifen nach dem Modell „pay-as-you-live", wie sie bereits bei Autoversicherungen existieren (sogenannte Pay-as-you-drive-Tarife) (Fromme 2015; Kfz-Versicherungen 2015). Nicht umsonst hat die Bundesdatenschutzbeauftragte vor unbedachtem Umgang mit den Gesundheitsdaten zur Erzielung kurzfristiger finanzieller Vorteile gewarnt und die Frage aufgeworfen, ob der Gesetzgeber den Schutz, der gesetzlich Versicherten gewährt wird, auch Versicherten von privaten Kassen gewähren sollte (Voßhoff 2015).

5 Fazit

Beim Verkauf von smarten Produkten muss mehr Transparenz für den Verbraucher geschaffen werden. Der Verbraucher muss Klarheit über die Person seines Vertragspartners und die Laufzeit des internetbasierten Zusatzdienstes haben. Nur so kann er vor einem plötzlichen Wertverlust oder der völligen Unbrauchbarkeit des smarten Produktes geschützt werden.

Der Verbraucher muss klar über die Risiken aufgeklärt werden, bevor er sich dazu entschließt, seine durch Fitnessapps oder Wearables gesammelten Gesundheitsdaten an Krankenversicherungen weiterzuleiten. Gerade weil Algorithmen Korrelationen finden und Prognosen bilden, die auf den ersten Blick

17 Vgl. Simitis§ 4a Rn. 33 ff. Wird die Schriftform der Einwilligung nach § 4a Abs. 1 S. 3 BDSG nicht eingehalten, ist die Einwilligung wegen des Formmangels nichtig nach § 125 BGB.

18 Vgl. § 126a BGB.

nicht sichtbar sind, ist die Frage, inwieweit der Verbraucher die Folgen der Nutzung seiner Daten durch seine Versicherung abschätzen kann.

Der Verbraucher kann bei Vorliegen einer unzulässigen Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten einen Schadensersatzanspruch nach § 7 BDSG geltend machen. Problematisch ist zum einen, dass der Betroffene zuerst einmal davon Kenntnis erlangen muss, was sich aufgrund der häufigen Intransparenz der Datenerhebungs- und Datenverwendungsvorgänge als schwierig erweisen dürfte. Zum anderen muss er den Nachweis eines konkreten Schadens erbringen.

Verstöße gegen Datenschutzbestimmungen dürfen für die Unternehmen nicht mehr Gewinn bringen, als an Bußgeld bezahlt werden muss. Eine Erhöhung der Geldstrafe würde dazu führen, dass auch marktbeherrschende Unternehmen spürbar getroffen werden und sich die Sanktionswirkung entfalten kann.

Literatur

AOK-Nordost. 2015. *Aok.* https://www.aok.de/nordost/leistungen-service/aok-gesundheitskonto-248715.php (Zugriff: 20. November 2015).

Berres, Irene und Nina Weber. 2015. Zuschuss für Wearables: Die Kasse trainiert mit. *Spiegel Online* (7. August). http://www.spiegel.de/gesundheit/ernaehrung/apple-watch-und-co-was-soll-die-krankenkasse-bezuschussen-a-1046835.html (Zugriff: 20. November 2015).

Bohsem, Guido. 2015. Zuschuss für die Apple-Watch. *Sueddeutsche.de.* (6. August). http://www.sueddeutsche.de/wirtschaft/aok-bonus-fuer-apple-watch-1.2596338 (Zugriff: 20. November 2015).

Bräutigam, Peter und Thomas Klindt. 2015. Industrie 4.0, das Internet der Dinge und das Recht. *Neue Juristische Wochenschrift* 68, Nr. 16, 1137–1141.

Busche, Jan. 2016. § 145, Rn. 11, 12. In: *Münchener Kommentar zum BGB*, hg. von Hans Jürgen Säcker und Roland Rixecker. 7. Auflage. München: Beck.

Dammann, Ulrich. 2014. § 3 BDSG, Rn. 4, 224 ff. In: *Bundesdatenschutzgesetz*, hg. von Spiros Simitis. 8. Auflage. Baden-Baden: Nomos.

Europäische Kommission. 2016. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. Europe-

an Commission Press Release Database (2. Februar). http://europa.eu/rapid/press-release_IP-16-216_en.htm (Zugriff: 8. April 2016).

Franzen, Martin. 2016. § 3 BDSG, Rn. 2. In: *Erfurter Kommentar zum Arbeitsrecht*, hg. von Rudi Müller-Glöge, Ulrich Preis und Ingrid Schmidt. 16. Auflage. 2016. München: Beck.

Fromme, Herbert. 2015. Billigere Autoversicherung dank Blackbox. *Sueddeutsche.de (*20. Mai). http://www.sueddeutsche.de/auto/telematik-tarife-bei-kfz-versicherungen-viel-ueberwachung-fuer-ein-bisschen-ersparnis-1.2486679 (Zugriff: 23. November 2015).

Generali, Deutschland. Vitality. 2015. http://www.generali-deutschland.de/online/portal/gdinternet/de/content/311198/1150478 (Zugriff: 20. November 2015).

KFZ-Versicherungen. 2015. Pay as you drive (PAYD). *Kfz-Versicherungen*. http://www.kfz-versicherungen.com/ratgeber/pay-as-you-drive/ (Zugriff: 23. November 2015).

Lewinski, Kai. 2014. § 1 BDSG Rn. 52. In: *Auernhammer BDSG – Kommentar zum Bundesdatenschutzgesetz*, hg. von Martin Eßer und Philipp Kramer. 4. Auflage. München: Beck.

Oetker, Hartmut. 2015. § 249, Rn. 18. In: *Münchener Kommentar zum BGB*, hg. von Hans Jürgen Säcker und Roland Rixecker. 7. Auflage. München: Beck.

Peters, Karl. 2015. § 284, Rn. 6,10. In: *Kasseler Kommentar zum Sozialversicherungsrecht*, hg. von Stephan Leitherer. 86. Ergänzungslieferung – Stand 06/2015. München: Beck.

Pilkington, Katie. 2013. Samsung‘s RF4289HARS smart fridge has room to grow. *Cnet.com*. 23. September. http://www.cnet.com/products/samsung-rf4289hars-refrigerator-series/ (Zugriff: 20. November 2015).

Scheja, Gregor und Christian Haag. 2013. Teil 5 Datenschutzrecht, Rn. 74. In: *Münchener Anwaltshandbuch IT-Recht*, hg. von Andreas Leupold und Silke Glossner. 3. Auflage. München: Beck.

Simitis, Spiros. 2014. § 4a BDSG, Rn. 29, 33 ff. 2014. In: *Bundesdatenschutzgesetz*, hg. von Spiros Simitis. 8. Auflage. Baden-Baden: Nomos.

Solmecke, Christian und Simon-Elias Vondrlik. 2013. Rechtliche Probleme bei Produkten mit serverbasierten Zusatzdiensten – Was passiert, „wenn der Kühlschrank keine Einkaufsliste mehr schreibt…“. *MultiMedia und Recht* 16, Nr. 12, 755–760.

Spindler, Gerald und Judith Nink. 2015. § 15 TMG, Rn. 2, 3. In: *Kommentar zum Recht der elektronischen Medien*, hg. von Gerald Spindler und Fabian Schuster. 3. Auflage. München: Beck.

Staudinger, Ansgar. 2014. § 823, Rn. 12. In: *BGB Handkommentar*, hg. von Reiner Schulze, 8. Auflage. Baden-Baden: Nomos.

vzbv (Verbraucherzentrale Bundesverband). 2015. Big Data: Verbraucher befürchten Nachteile durch Profilbildung. Pressemitteilung 4. Mai. *vzbv.de*. http://www.vzbv.de/pressemitteilung/big-data-verbraucher-befuerchten-nachteile-durch-profilbildung (Zugriff: 30. Oktober 2015).

Wagner, Gerhard. 2014. § 823, Rn. 180, 184. In: *BGB Handkommentar*, hg. von Reiner Schulze et al. 8. Auflage. Baden-Baden: Nomos.

Sicherheit der Verbraucher in vernetzten Fahrzeugen

Kerstin Lemke-Rust

DOI 10.15501/978-3-86336-912-5_4

Abstract

Dieser Beitrag betrachtet den Stand der Entwicklung bei der Vernetzung von Fahrzeugen aus Sicht der IT-Sicherheit. Etablierte Kommunikationssysteme und Verkehrstelematikanwendungen im Automobil werden ebenso vorgestellt und diskutiert wie auch zukünftige Kommunikationstechnologien Car-2-Car und Car-2-X. IT-Sicherheit im Automobil ist ein schwieriges Feld, da es hier um eine Integration von neuen innovativen Anwendungen in eine hochkomplexe bestehende Fahrzeugarchitektur geht, die zu keinen neuen Gefährdungen für die Fahrzeuginsassen führen darf. Zudem bleibt die Funktionsweise dieser Anwendungen mit ihren Auswirkungen auf das informationelle Selbstbestimmungsrecht oft intransparent. Die abschließende Diskussion gibt Handlungsempfehlungen aus Sicht der Verbraucher.

1 Einleitung

Das moderne Automobil ist bereits heutzutage ein hoch komplexes IT-System, das mit vielfältigen externen Kommunikationsschnittstellen für Verkehrstelematikanwendungen ausgestattet ist (vgl. Abbildung 1). Diese Kommunikationsschnittstellen dienen dazu, extern verfügbare Informationen in dem Fahrzeug zu erhalten oder Informationen, die im Fahrzeug generiert werden, über eine vorhandene Funktechnologie mit einer festen Infrastruktur auszutauschen.

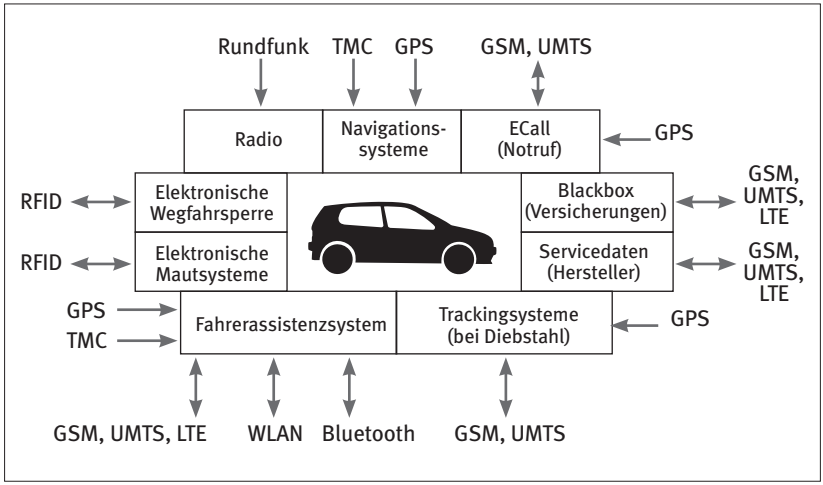


Abbildung 1: Funk basierte Kommunikationsschnittstellen eines modernen Automobils. Eigene Darstellung.

Altbewährt ist der Rundfunkempfang im Auto. Radios ermöglichen den Fahrzeuginsassen so den Empfang von Verkehrsnachrichten und Unterhaltungsprogrammen.

Seit Mitte der 1990er-Jahre sind elektronische Wegfahrsperren eingeführt worden, um die Fahrzeuge stärker gegen Diebstahl zu schützen. Bei der Wegfahrsperre startet der Motor erst, wenn das Motorsteuerungsgerät die Echtheit des Zündschlüssels im Zündschloss durch ein kryptografisches Protokoll ve-

rifiziert hat. Die verwendete Funktechnologie ist eine RFID (Radio Frequency Identification) Technik, die auf induktiver Kopplung im Abstand von einigen Zentimetern zwischen Zündschloss und Zündschlüssel basiert.

Mit RFID-Technik basierend auf elektromagnetischer Rückstrahlkopplung können Kommunikationsreichweiten bis zu 100 Metern erzielt werden. Hiermit funktionieren elektronische Mautsysteme, die zwischen einer Bordeinheit im Automobil und fest installierten Barken an Straßen oder mobilen Kontrollfahrzeugen Nachrichten zur Bezahlung der Maut austauschen.

Für den Fahrzeugführer brachten die Navigationssysteme einen Durchbruch bei der individuellen Routenführung mit sich. Die Navigationssysteme empfangen Nachrichten des globalen satellitengestützten Positionsbestimmungsdiensts GPS (Global Positioning System) und des Funknachrichtendiensts TMC (Traffic Message Channel). Während der Fahrt ist kein Informationsfluss aus dem Auto an Hintergrundsysteme möglich. Es gibt jedoch einen Rückkanal zum Hersteller des Navigationsgeräts, sobald das Navigationsgerät an das Internet angeschlossen ist, beispielsweise wegen einer Aktualisierung der Software oder des Kartenmaterials. Hierbei können im Navigationsgerät gespeicherte Fahrtrouten und auch gefahrene Geschwindigkeiten an den Hersteller übertragen werden (Fahn 2013). Navigationssoftware auf einem Smartphone ist aus Datenschutzsicht wesentlich kritischer, da hierdurch direkt eine Verknüpfung mit persönlichen Daten möglich ist und eine Kommunikationsverbindung zum Anbieter der Navigationssoftware bei Verfügbarkeit einer Internetanbindung geöffnet werden kann (Fahn 2013).

Fahrerassistenzsysteme verfügen neben GPS und TMC über Mobilfunkschnittstellen GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System) oder LTE (Long Term Evolution). Ferner nutzen Fahrerassistenzsysteme die Funktechnologien Wireless LAN (WLAN) und Bluetooth mit einer Kommunikationsreichweite von zehn bis 100 Metern. Teilweise sind auch weitere Technologien verbaut wie Ultraschall und Kameras, die dem Fahrer beispielsweise als Einparkhilfe dienen können. Diese Fahrerassistenzsysteme unterstützen den Fahrer bei der Fahrzeugführung, beispielsweise durch eine Warnung vor kritischen Situationen. Ferner bieten sie Komfortfunktionen wie eine Freisprecheinrichtung und die Einbindung von persönlicher Informationstechnik (Smartphones etc.) in das Automobil an.

Weitere Anwendungen benötigen einen Kommunikationskanal, auf dem Fahrzeugdaten direkt an Hintergrundsysteme verschickt werden können und das Fahrzeug auch von Hintergrundsystemen kontaktiert werden kann. Hierfür wird typischerweise Mobilfunk genutzt. Trackingsysteme dienen dazu, ein gestohlenes Fahrzeug mittels GPS auf Anfrage zu lokalisieren. Servicedatensysteme dienen zum bi-direktionalen Austausch von Kommunikationsdaten mit dem Fahrzeughersteller. Über diese Schnittstelle kann der Hersteller auch neue Software oder neue Konfigurationsdaten beispielsweise für personalisierte Fahrwerkseinstellungen in das Fahrzeug einspielen. Sogenannte Blackboxes werden von der Versicherungswirtschaft zunehmend in Fahrzeuge eingebaut, um das Fahrerverhalten analysieren zu können, sofern ein Versicherungsnehmer hierzu seine Einwilligung gegeben hat. Am 28. April 2015 hat das EU-Parlament beschlossen, dass das vom Nutzer nicht deaktivierbare eCall Notrufsystem ab April 2018 werksseitig in alle neuen Fahrzeuge eingebaut werden muss, um bei einem Unfall automatisiert einen Notruf über den Mobilfunk durch das Fahrzeug auszulösen (European Commission 2015). Zusätzliche Dienste, die das fahrzeugseitig eingebaute System von eCall nutzen, sind optional vorgesehen (Das Europäische Parlament und der Rat der Europäischen Union 2015).

Daneben gibt es weitere Anwendungen, zum Beispiel in der Verkehrsflussanalyse, die sich die Verfügbarkeit von Bluetooth und vermutlich zukünftig auch von WLAN in den Fahrzeugen zunutze machen. Durch an den Straßen positionierte Bluetooth Scanner werden ausgesendete individuelle MAC (Media Access Control) Adressen der in den Fahrzeugen vorhandenen Bluetooth-Geräte empfangen. Durch die Zeitdifferenz des Empfangs von derselben MAC Adresse an zwei räumlich entfernten Scannern kann die Durchschnittsgeschwindigkeit berechnet werden.

1.1 Autohersteller vs. Internetfirmen

Anwendungen der Fahrerassistenz und Mehrwertdienste im Automobil wecken auch die Begehrlichkeiten von großen Internetfirmen wie Google und Apple nach Integration ihrer Smartphone-Technologie in das Automobil. Die Automobilhersteller streben dagegen an, ihre Kunden durch neue digitale Angebote an sich zu binden (Schwan 2015). Aufmerksamkeit erregte kürzlich die Mel-

dung, dass Porsche nur die iPhone-Integration mit Apples CarPlay unterstützt, nicht aber Android Auto (Becker 2015). Grund hierfür sei Googles Forderung nach umfangreichen Fahrzeugdaten. Die Automobilhersteller Audi, BMW und Porsche erwägen aktuell, Sensordaten aus ihren Fahrzeugen für den dazugekauften Kartendienst „Here“ von Nokia zu öffnen (siehe dpa und axk, 2015), Kartendaten werden als eine Schlüsseltechnologie bei der zukünftigen Entwicklung von vernetzten und selbstfahrenden Autos eingeschätzt.

2 IT-Sicherheit im Automobil

2.1 Safety vs. Security

Sicherheit hat in der deutschen Sprache zwei Bedeutungen: funktionale Sicherheit (Safety) und Angriffssicherheit (Security). Funktionale Sicherheit gewährleistet, dass ein System unter allen normalen Betriebsbedingungen funktioniert und keine unzulässigen Zustände annimmt (Eckert 2014). Funktionale Sicherheit schützt damit vor zufälligen Fehlerzuständen, die in dem normalen Betrieb auftreten können. Angriffssicherheit schützt Systeme vor intelligenten Angreifern, die Sicherheitsfunktionen überwinden oder umgehen können, und damit das System und die zu schützenden Ressourcen angreifbar machen. Der Grad der Angriffssicherheit ist proportional zu den Aufwänden, die ein Angreifer investieren muss, um Sicherheitsmaßnahmen außer Kraft zu setzen.

Beide Bedeutungen der Sicherheit sind fundamental bei der Entwicklung von Automobilen. Primäres Ziel ist der Schutz der Unversehrtheit von Fahrzeuginsassen im Falle von Unfällen oder zufälligen Störungen der IT-Systeme im Automobil. Als Beispiel für ein funktionales Sicherheitssystem sei der Airbag genannt, der im Falle eines Zusammenstoßes automatisch auslöst, um den Aufprall der Fahrzeuginsassen abzubremsen. Die elektronische Wegfahrsperre als Beispiel für ein IT-Sicherheitssystem verhindert ein einfaches Kurzschließen am Zündschloss durch eine kryptografische Authentifikation zwischen Zündschlüssel und Motorsteuerung.

Funktionale Sicherheitsfunktionen können durch funktionale Tests unter realistischen Einsatzbedingungen geprüft werden. Schwieriger ist die Prüfung des Grads der Angriffssicherheit, hierzu bedarf es einer Schwachstellenanalyse.

2.2 Kommunikationssicherheit im Automobil

In vernetzten Automobilen findet Kommunikation statt –

- zwischen einem Fahrzeug und einem Hintergrundsystem (1:1),
- zwischen einer stationären straßenseitigen Systemeinheit (ggf. verbunden mit einem Hintergrundsystem) und mehreren Fahrzeugen (1:n) sowie
- zukünftig auch untereinander zwischen mehreren Fahrzeugen (m:n), die sich zufällig innerhalb der Kommunikationsreichweite befinden und sogenannte Ad-Hoc Netze bilden. (Siehe Abschnitt 3.)

Informationen, die über Netzwerke gesendet werden, sind diversen Bedrohungen ausgesetzt. Dies ist in Abbildung 2 illustriert.

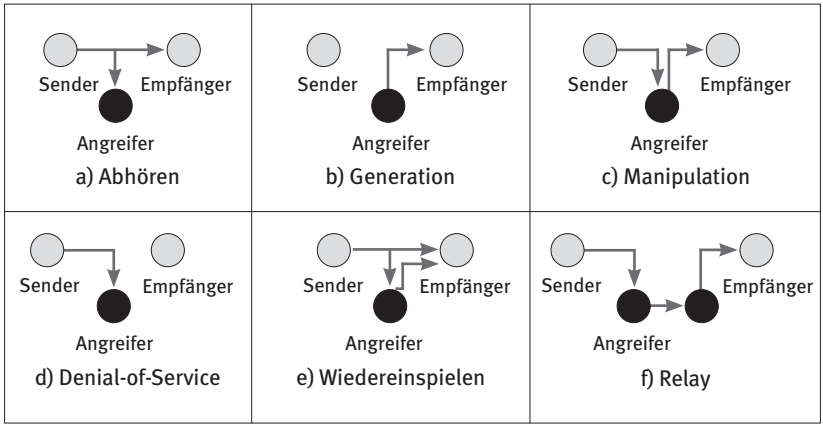


Abbildung 2: Angriffe auf Kommunikationssysteme. Eigene Darstellung.

Es handelt sich hierbei um
a) das Abhören von Informationen,
b) die Generierung neuer Informationen durch den Angreifer,
c) die Manipulation der Informationen auf der Kommunikationsstrecke,
d) das Unterdrücken der Weiterleitung von Informationen (Denial-of-Service),
e) das Wiedereinspielen aufgezeichneter Informationen durch den Angreifer zu einer späteren Zeit (Replay) und
f) das Weiterleiten der Informationen an einen entfernten Ort (Relay). Diese Bedrohung ist spezifisch für Funknetze mit begrenzter Reichweite, bei denen implizit angenommen wird, dass die Kommunikationspartner sich innerhalb der Kommunikationsreichweite eines Funknetzes befinden.

In der Netzwerksicherheit existieren kryptografische Sicherungsmaßnahmen zu den oben genannten Angriffen a) auf die Vertraulichkeit, b) auf die Authentizität und c) auf die Integrität.

Durch Verschlüsselung kann das Abhören der Informationen auf der Netzwerkschnittstelle unterbunden werden und Vertraulichkeit von Informationen erreicht werden. Zur Verschlüsselung können symmetrische oder asymmetrische Verfahren eingesetzt werden. Bei symmetrischen Verfahren müssen die Kommunikationspartner über einen gemeinsamen geheim zuhaltenden Schlüssel verfügen. Bei asymmetrischen Verfahren besteht jeder Schlüssel aus einem öffentlichen und privaten Teil, wovon nur der öffentliche an die Kommunikationspartner herausgegeben wird. Symmetrische Verfahren sind wesentlich performanter als asymmetrische Verfahren, diese Tatsache muss bei dem Design von zeitkritischen Anwendungen berücksichtigt werden.

Das Generieren von Informationen durch unautorisierte Angreifer sowie die Manipulation von gesendeten Informationen kann durch kryptografische Authentifikationsverfahren wie den Message Authentication Code (MAC) oder mittels einer digitalen Signatur detektiert werden. Während der MAC auf der symmetrischen Kryptografie beruht und die Verteilung von geheimen symmetrischen Schlüsseln erfordert, ist die digitale Signatur ein asymmetrisches Verfahren, bei der der Signaturersteller über den privaten Schlüssel verfügt und alle Empfänger den dazugehörigen öffentlichen Schlüssel brauchen.

Diese kryptografischen Verfahren sind sowohl vom Sender als auch vom Empfänger anzuwenden. Insbesondere bedeutet dies, dass die Kommunikationspartner über das erforderliche Schlüsselmaterial verfügen müssen. Der Einsatz von universellen symmetrischen Schlüsseln, die an alle Fahrzeuge ausgegeben werden, ist im automobilen Kontext nicht empfehlenswert, da ein Angreifer diesen Schlüssel nur aus einer Komponente eines Fahrzeugs extrahieren muss, um danach das gesamte System kompromittieren zu können. Bei 1:1 oder 1:n Kommunikationen kann der gemeinsame symmetrische Schlüssel vom Hintergrundsystem aus einem Masterschlüssel unter Verwendung einer Identität des Fahrzeugs abgeleitet werden, die Fahrzeuge erhalten damit einen individuellen Schlüssel. In automobilen Ad-Hoc Netzen ist ein solches Verfahren der Schlüsselableitung nicht möglich, es bleibt damit die asymmetrische Verschlüsselung und die digitale Signatur. Beides erfordert einen Austausch von Zertifikaten einer vertrauenswürdigen Zertifikatsstelle, um Man-in-the-Middle-Angriffe, bei denen sich der Angreifer aktiv in die Kommunikation einbindet, möglichst zu unterbinden. Bei Verwendung der asymmetrischen Verschlüsselung muss der Austausch von Zertifikaten vor der Verschlüsselung von Informationen verfolgen.

Die Angriffe d), e) und f) sind generell schwierig abzuwehren. Denial-of-Service Angriffen, beispielsweise durch Störsender, und damit dem Verlust der Verfügbarkeit kann entgegengewirkt werden, wenn Kommunikationssysteme redundant ausgelegt werden bzw. mehrere Kommunikationswege für eine Nachricht in einem Ad-Hoc Netzwerk vorgesehen sind. Das Wiedereinspielen von Nachrichten kann durch kryptografische Protokolle mit frischen Zufallszahlen, die von beiden Protokollteilnehmern erzeugt werden, erkannt werden. Diese Protokolle sind bei zeitkritischen Rundfunk-Nachrichten an viele Empfänger jedoch nicht geeignet. Alternativ kann angestrebt werden, die Uhrzeit aller Kommunikationsparteien zu synchronisieren und die Uhrzeit des Senders kryptografisch als Teil der Informationen zu sichern. Gegenmaßnahmen gegen Relay-Angriffe bedürfen einer möglichst genauen Ortsbestimmung des Senders und des Empfängers, die als Teil der gesendeten Information kryptografisch zu sichern und vom Empfänger zu prüfen ist.

2.3 Eingebettete Sicherheit im Automobil

2.3.1 Fahrzeug-internes Netzwerk

In einem Automobil der Luxusklasse gibt es heutzutage zwischen 70 und 120 Steuergeräte mit zusammen über 100 Millionen Zeilen Software Code (von Stokar 2015). Diese Steuergeräte sind in dem Fahrzeug über ein Controller Area Network (CAN) Bussystem vernetzt. Die Kommunikation zwischen Steuergeräten auf dem Fahrzeug-internen Bus ist im Regelfall nicht mit kryptografischen Maßnahmen geschützt. Wenn ein Angreifer Zugriff auf diesen Fahrzeug-internen Bus erlangt, so kann er praktisch alle Steuergeräte kontrollieren. In die Fahrzeuge ist werksseitig eine On-Board-Debugschnittstelle OBD2 eingebaut, mit der Hersteller und Werkstätten die Funktionsfähigkeit der einzelnen Steuergeräte prüfen und neue Software aufspielen können. Diese Schnittstelle OBD2 öffnet aber auch für Angreifer mit physischem Zugang zum OBD2 mannigfaltige Wege, sich in das Fahrzeug-interne Netzwerk einzuklinken und Steuergeräte neu zu konfigurieren oder zu programmieren.

Eine noch größere Bedrohung ergibt sich, wenn Angreifer ohne direkten Zugang auf das Fahrzeug in der Lage sind, sich Zugriff auf den Fahrzeug-internen Bus zu verschaffen und Nachrichten in das Fahrzeug schicken zu können. Die Machbarkeit solcher externen Angriffe ist bereits in Checkoway et al. (2011) demonstriert worden: Die Autoren entdeckten Schwachstellen in der Implementierung von Kommunikationssystemen, die durch Nutzung von CD-Spieler, Bluetooth-Schnittstellen und Mobilfunkschnittstellen ausgenutzt werden konnten. Die Autoren stellen fest, dass jede dieser entdeckten Schwachstelle es Ihnen erlaubte, volle Kontrolle über den Fahrzeug-internen Bus zu erlangen. Hohe Aufmerksamkeit in der Öffentlichkeit erregte die Meldung vom Sommer 2015, dass es Hackern in den USA gelungen ist, einen Jeep Cherokee über das Internet fernzusteuern (Eikenberg 2015; Miller und Valesek 2015). Hierfür verwendeten sie das Uconnect System, über das Fahrzeuge per Mobilfunk aus dem Internet erreichbar sind. Die Hacker konnten demonstrieren, dass eine Fernsteuerung von sicherheitsrelevanten Fahrzeugteilen wie Bremsen, Beschleunigung und teilweise auch von der Lenkung möglich ist.

2.3.2 Sicherheitsrelevante Komponenten

Durch den zunehmenden Einbau von Sicherheitsmechanismen in Hardware- und Softwarekomponenten in das Automobil wird die Resistenz dieser Steuergeräte gegen Implementierungsangriffe durch Angreifer mit physischem Zugriff wichtig. Hier lässt sich sagen, dass im Automobil überwiegend Standard-Mikrocontroller verbaut werden, die keine speziellen intrinsischen Hardware-Sicherheitsfunktionen mitbringen. Ein solcher spezieller Schutz wird wichtig, sobald kryptografische Schlüssel oder andere sensitive Konfigurationsdaten gespeichert werden. Implementierungsangriffe und Sicherheitsmaßnahmen zur Härtung von Komponenten und zum Schutz der kryptografischen Schlüssel und sensitiven Daten werden in Lemke et al. (2006) vorgestellt.

3 Zukünftige Technologien der Car-2-Car Kommunikation

Die nächste Generation von Kommunikationssystemen im Fahrzeug hat das Ziel, Nachrichten zwischen Fahrzeugen auszutauschen. Dies ist ein Teilbereich der intelligenten Transportsysteme (ITS). Bei den Kommunikationsnetzen handelt es sich um Ad-Hoc-Netze, die durch Fahrzeuge, die sich zufällig innerhalb der Kommunikationsreichweite des Senders befinden, gebildet werden. Die beteiligten Kommunikationspartner wechseln. Man unterscheidet

- Car-to-Infrastructure bzw. Infrastructure-to-Car (C2X) und
- Car-to-Car (C2C) Kommunikation

Bei der C2X Kommunikation kommuniziert das vorbeifahrende Fahrzeug mit einer festen Infrastruktur, deren Funkstationen stationär an einer Straße installiert sind. Bei C2C kommunizieren zwei oder mehrere Fahrzeuge während der Fahrt.

Beteiligte Entitäten an der C2C/C2X Kommunikation sind die entsprechend mit ITS-Systemen ausgerüsteten Fahrzeuge, stationäre ITS-Funkstationen an

der Straße und ITS-Hintergrundsysteme, die Nachrichten mit den stationären ITS-Funkstationen typischerweise über eine Mobilfunkverbindung austauschen (vgl. Abbildung 2). Die ITS-Funkstationen kommunizieren über eine WLAN-Funkverbindung mit den Fahrzeugen. Jedes Fahrzeug agiert auch als ein Router und kann Nachrichten so zu weiter entfernten Fahrzeugen übertragen, (vgl. CAR 2 CAR o. D.).

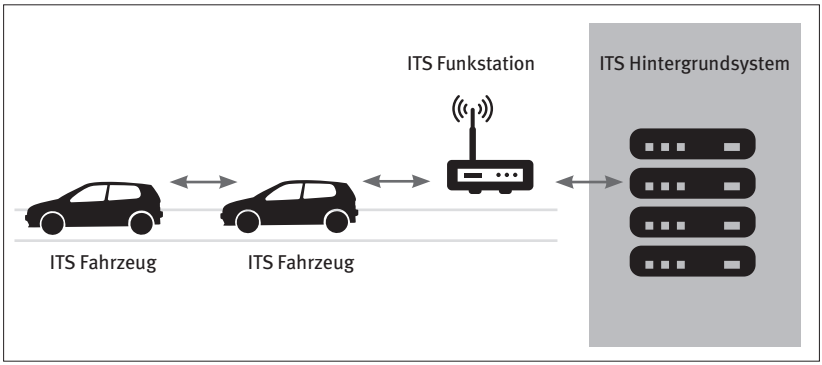


Abbildung 3: C2C/C2X System. Eigene Darstellung.

Die Ziele bei der Einführung von C2C/C2X sind die Erhöhung der Verkehrssicherheit, die Verbesserung des Verkehrsflusses und die Bereitstellung weiterer Mehrwertdienste. In den letzten Jahren gab es zu intelligenten Transportsystemen bereits Standardisierungsarbeiten durch ETSI und große Forschungsprojekte, die an der Realisierung gearbeitet haben. Dieser Artikel stützt sich überwiegend auf die öffentlich verfügbaren Informationen aus den kürzlich beendeten Projekten PRESERVE (www.preserve-project.eu) und simTD (www.simtd.de) ab.

Das Projekt PRESERVE benennt sicherheitssensitive Anwendungsfälle von hoher Relevanz: die Einsatzfahrzeugwarnung, das elektronische Bremslicht, Warnungen bei einem liegen gebliebenen Fahrzeug, Stauwarnungen, Gefahrenwarnungen, Kreuzungswarnungen, Verkehrsinformationen und Routenempfehlung, lokale Verkehrsflussdaten, Baustellenwarnungen, Ampelphasenassistenz, Verkehrszeichenwarnungen und Kollisionswarnungen (PRESERVE Konsortium 2014, 19 f.).

3.1 Sicherheits- und Datenschutzanforderungen

Aufgrund der Diversität von Anwendungsfällen ergeben sich je nach Anwendungsfall spezielle Bedrohungen und daraus resultierende Sicherheits- und Datenschutzanforderungen. Potenzielle Angreifer auf ein C2C/C2X Kommunikationssystem sind autorisierte Nutzer, die sich einen Vorteil in dem System verschaffen möchten, oder auch externe Angreifer, die das System sabotieren und dadurch autorisierte Nutzer auch gefährden können. Angreifer können die Kommunikationsnachrichten mitschneiden, generieren, manipulieren, einspielen oder weiterleiten und für das Senden von eigenen Nachrichten eine manipulierte oder gestohlene Identität verwenden.

3.1.1 Beispiel: Sicherheitsanforderungen für die Einsatzfahrzeugwarnung

Ein relevanter Anwendungsfall ist die Einsatzfahrzeugwarnung, die ein Einsatzfahrzeug zusätzlich zu Blaulicht und Martinshorn per Funk an andere Verkehrsteilnehmer sendet. Die gesendeten Informationen der Einsatzfahrzeugwarnung sind an alle Verkehrsteilnehmer adressiert, Vertraulichkeit der gesendeten Daten ist nicht erforderlich. Die wesentliche Bedrohung liegt darin, dass unberechtigte Fahrzeuge diese Einsatzfahrzeugwarnung generieren könnten, um sich eine freie Fahrt auf Kosten der anderen Verkehrsteilnehmer zu verschaffen. Dieser Bedrohung kann durch Verwendung und Prüfung eines Authentizitätsnachweises in der Nachricht entgegengewirkt werden. Damit ergibt sich die Sicherheitsanforderung, dass das Einsatzfahrzeug seine Nachricht der Einsatzfahrzeugwarnung signiert, und die anderen Verkehrsteilnehmer diese Signatur der Nachricht prüfen müssen, bevor sie auf diese Nachricht reagieren. Insbesondere muss unzweifelhaft aus der digitalen Signatur hervorgehen, dass es sich um ein autorisiertes Einsatzfahrzeug handelt. Eine weitere ähnlich gelagerte Bedrohung liegt darin, dass Angreifer eine von ihnen mitgeschnittene Einsatzfahrzeugwarnung selbst erneut senden (Replay). Da es sich um ein Wiedereinspielen einer echten Nachricht handelt, muss dieser Bedrohung durch Einbeziehung von Zeit- und Ortsdaten in die Signatur einer Einsatzfahrzeugmeldung entgegengewirkt werden. Hieraus ergibt sich die Sicherheitsanforderung, dass das Einsatzfahrzeug seine geografische Position und die aktuelle Zeit zum Zeitpunkt der Generierung der Nachricht als

Teil der Nachricht signieren muss und dass die anderen Verkehrsteilnehmer auch diese geografische Position und Uhrzeit mit der eigenen Position und Uhrzeit vergleichen müssen. Da eine Synchronisation der Uhren und Positionsdaten in verschiedenen Fahrzeugen schwer umsetzbar ist und damit gewisse Toleranzen in C2C/C2X Anwendungen vorgesehen werden müssen, ist davon auszugehen, dass in einem zeit- und ortsnahen Kontext von einem Angreifer wieder eingespielte authentische Nachrichten („Echos“) zumindest teilweise nicht erkannt werden können.

3.1.2 Datenschutzanforderungen vs. Zurechenbarkeit

Da C2C/C2X ein komplexes System darstellt, ist es aus Systemsicht wichtig, vermeintliche Angriffe analysieren zu können und Verursacher ausfindig zu machen. Dies erfordert fahrzeugseitig eine Speicherung von Ereignissen und einen Mitschnitt der gesendeten und empfangenen Nachrichten, die regelmäßig oder bei Bedarf an Hintergrundsysteme übertragen werden können.

Sicherheitsanforderungen nach Speicherung von Nachrichten stehen Datenschutzanforderungen an das Selbstbestimmungsrecht der Fahrer gegenüber. Die zentrale Bedrohung des Datenschutzes ist die Erstellung von Bewegungsprofilen des Fahrers durch das Hintergrundsystem oder durch Dritte. Eine weitere Bedrohung entsteht, wenn der Aufenthaltsort des Fahrzeugführers in Echtzeit abfragbar ist („Hotlisting“). Daraus ergibt sich als primäre Anforderung des Datenschutzes, die Identität des Fahrers eines Fahrzeugs gegenüber anderen Verkehrsteilnehmern und Dritten anonym zu halten und eine Verkettung von gesendeten Nachrichten des Fahrzeugs zu dem Fahrer zu verhindern. Ein abgeschwächtes Sicherheitsziel der Anonymität ist die Pseudonymität, bei der die Identität eines Einzelnen nur von einer hierfür autorisierten Stelle im Gesamtsystem offengelegt werden kann.

Es gilt einen Kompromiss zwischen den Anforderungen des Datenschutzes nach Schutz des Einzelnen gegenüber dem Systembetreiber oder Dritten und der IT-Sicherheit nach Schutz des Systems gegenüber Einzelnen oder externen Angreifern zu finden. Eine Lösung ist die kurzzeitige Verwendung von Pseudonymen, deren Konzeption im Folgenden erläutert wird.

3.1.3 Ausgabe von Pseudonymen durch eine PKI

Das Vertrauen zwischen Sender und Empfänger kann durch eine Public-Key-Infrastruktur (PKI) aufgebaut werden (vgl. PRESERVE Konsortium 2014, 83f. und Ullmann 2015). Hierzu bedarf es einer Wurzel-Zertifizierungsstelle (Root CA), die als Vertrauensanker dient. Unter der Root CA ist eine Long-Term CA (LTCA) und eine Pseudonym CA (PCA) vorgesehen. Von der LTCA erhält jedes Fahrzeug ein Langzeit-Zertifikat, mit dem es sich in kurzen Zeitabständen wiederholt von der PCA Zertifikate mit einem Pseudonym ausstellen lassen kann. Durch Pseudonym-Zertifikate wird der Fahrzeugführer geschützt vor einer lang andauernden Aufzeichnung seiner Bewegungsdaten durch Dritte. Die Erstellung von Bewegungsprofilen wird dadurch auf die Zeit limitiert, in der ein Fahrzeug dasselbe Pseudonymzertifikat nutzt. Von dem Betreiber der PKI kann allerdings die Identität des Fahrzeugführers, der ein bestimmtes Pseudonym nutzte, aufgedeckt werden. In PRESERVE Konsortium (2014, 83 f.) ist vorgesehen, dass in diesem Prozess die LTCA integriert sein muss, so dass die PCA nicht die Langzeit-Identität des Fahrzeugs kennt und die LTCA nicht die ausgegebenen Pseudonyme. Andere Verfahren, bei denen ein direkter Datenaustausch zwischen ausgegebenem Pseudonym und Langzeit-Identität in der PKI umgesetzt wird, werden auch in PRESERVE Konsortium (2014, 86) diskutiert.

3.2 Machbarkeit von sicherer Car-2-Car Kommunikation

In vielen Anwendungsfällen der C2C/C2X Kommunikation gibt es die Vorgabe von kritischen zeitlichen Restriktionen. Beispielsweise nennt das PRESERVE Projekt eine Latenzzeit von weniger als 100 ms für die Einsatzfahrzeugwarnung (PRESERVE Konsortium 2014, 23).

In dem Projekt simTD (www.simtd.de) unter dem Konsortialführer Daimler AG wurde ein Feldversuch zur C2C/C2X Technologie mit 120 Fahrzeugen und mehr als 100 fest installierten Funkstationen durchgeführt. Jedoch fand dieser Versuch aus Performancegründen ohne kryptografische Sicherheitsmaßnahmen statt, da sich herausgestellt hat, dass die simTDHardware nicht in der Lage war, die geforderte Anzahl eingehender Nachrichten kryptografisch zu bearbeiten (SIMTD Konsortium 2013, 130). Dies hat zur Folge, dass sämtliche Sicherheitsanforderungen, die kryptografische Verfahren erfordern, in diesem Feldtest

außer Acht gelassen wurden. Ein Feldtest für C2C/C2X Technologie ohne Einsatz von kryptografischen Verfahren wird als sehr fragwürdig bewertet.

Das EU-Projekt PRESERVE (www.preserve-project.eu) unter der Konsortialführerschaft der Universität Twente, Niederlande, hat sich zum Ziel gesetzt, ein sicheres und skalierbares C2C/C2X Subsystem für realistische Szenarien zu entwickeln. Unter anderem wurde das Ziel verfolgt, ein performantes Hardware Sicherheitsmodul zu entwickeln. Das PRESERVE Projekt arbeitet mit Elliptischer Kurvenkryptographie (ECC), AES und SHA-2. Nach Moser (2015) konnte die Machbarkeit der Performanzanforderungen von 1.000 ECC-Verifikationen in dem PRESERVE Projekt nachgewiesen werden. Der speziell entwickelte PRESERVE ASIC benötigt 3,4 ms für eine ECC-Signaturverifikation bei einer Taktrate von 160 MHz, auf dem PRESERVE ASIC stehen 6 Kerne parallel zur ECC-Verifikation zur Verfügung, so dass pro Sekunde 1760 ECC Verifikationen durchführbar sind. Ein Feldtest mit diesem Hardware Sicherheitsmodul hat in dem Projekt PRESERVE nicht stattgefunden.

Ein länderübergreifender ITS-Feldversuch befindet sich aktuell in Vorbereitung (http://www.c-its-korridor.de). In einem Dreiländerprojekt mit den Niederlanden, Deutschland und Österreich sollen auf den Autobahnen von Rotterdam über Frankfurt nach Wien (a) die Warnung vor Tagesbaustellen und (b) ein verbessertes Verkehrsmanagement der Fahrzeugdaten mit erprobt werden.

3.3 Schwierigkeiten und offene Probleme

3.3.1 Mensch-Maschine Schnittstelle zum Fahrzeugführer

Aus den bisherigen Forschungsarbeiten ist noch nicht offensichtlich, wie Fahrzeugführer über eingehende Nachrichten informiert werden und ob ein Fahrzeugführer über eine Benutzerschnittstelle in die Lage versetzt werden soll, Warnungen an andere Fahrzeuge zu generieren. Dies ist für jede C2C/C2X Anwendung festzulegen. Der Empfang von ITS-Warnungen darf nicht zu einer automatisch eingeleiteten Reaktion des Fahrzeugs an Bremsen oder Lenkung führen. Letztendlich bleibt der Fahrzeugführer in der Verantwortung, auf ITS Warnungen angemessen zu reagieren.

3.3.2 Langwierige Einführung

Bei der Einführung von C2C/C2X Kommunikation ist in den Anfangsjahren nur ein Bruchteil aller Fahrzeuge mit der entsprechenden Technik werksseitig ausgestattet. Die volle Funktionalität von C2C/C2X kann erst nach vielen Jahren erreicht werden.

3.3.3 Verwaltung der Zertifikate und Komponenten

Es gibt neuartige funktionale Anforderungen an die vorgesehene PKI. Die PCAs müssen mehrmals täglich neue Pseudonym-Zertifikate an alle Fahrzeuge mit C2C/C2X Technologie ausgeben, damit die Pseudonyme wirksam sind gegen eine Erstellung von Bewegungsprofilen. Es sind organisatorische Maßnahmen für den Zertifikatsrückruf vorzusehen, zum Beispiel wenn ein Fahrzeug infolge eines Unfalls verschrottet wird, und es sind Maßnahmen empfehlenswert, die den Lebenszyklus von bordseitig eingebauten C2C/C2X Einheiten von der Inbetriebnahme bis zu ihrer Zerstörung nachvollziehen.

3.3.4 Länderübergreifende PKI

Es ist zu erwarten, dass PKIs zur C2C/C2X Kommunikation in jedem Land aufgebaut werden müssen. Erfahrungsgemäß ist eine Harmonisierung von länderübergreifenden PKIs schwierig. Dies ist aber erforderlich, damit auch Verkehrsteilnehmer aus anderen Ländern, die die technischen Voraussetzungen für die C2C/C2X Kommunikation mitbringen, aktiv an dem Ad-Hoc Netz der Fahrzeuge teilnehmen können.

3.3.5 Angriffssicherheit der ITS Funkstationen

Sobald ITS-Funkstationen an der Straße Masterschlüssel oder private Signaturschlüssel von ITS-Anwendungen enthalten, können sie zu einem Angriffsziel von kriminellen Organisationen werden. Es sind entsprechende Schutzmaßnahmen gegen Kompromittierung des Schlüsselmaterials und gegen Manipulationen und Sabotage zu entwickeln und umzusetzen (Ullmann et al. 2015).

4 Handlungsempfehlungen

Es ist festzustellen, dass es sich bei dem Thema dieses Beitrags um ein hoch-komplexes Feld handelt. Die folgenden Handlungsempfehlungen decken aus Sicht der Autorin wichtige Teilaspekte ab, sie erheben aber keinen Anspruch auf Vollständigkeit.

4.1 Verfügbarkeit des Fahrzeugs

Sicherstellung der Primärfunktionen: Priorität für die Verbraucher hat die Aufrechterhaltung der Fahrtüchtigkeit des Fahrzeugs. Diese Primärfunktionen wie Motorsteuerung, Lenkung und Bremsanlage dürfen nicht durch Störungen oder Angriffe von bordseitigen Verkehrstelematikeinrichtungen beeinflusst werden können. Eine bereits bekannte Maßnahme, die hierzu weiterverfolgt werden sollte, ist die spezielle Abschirmung von Steuergeräten, die für Primärfunktionen zuständig sind, von dem übrigen Fahrzeug-Bussystem (Szerwinski 2014).

Jahrzehntelanger Betrieb von Fahrzeugen: Gegenüber klassischer IT-Technik, in der Hardware- und Softwarekomponenten nur wenige Jahre zum Einsatz kommen und danach durch Nachfolger ausgetauscht werden, haben wir es in der Automobilindustrie mit jahrelangen Vorlaufzeiten bis zur Produktionsreife und zusätzlich mit einer jahrzehntelangen Nutzung der Fahrzeuge im Feld zu tun. Ein großes Problem, was mit der Langlebigkeit von Komponenten einhergeht, ist die Wartung der Software- und auch der Hardwarekomponenten. Aus Verbrauchersicht ist es wünschenswert, Hardwarekomponenten über viele Jahre wartbar und Original-Ersatzteile verfügbar zu halten. Zudem sind Softwarestände für vielfältige Modelle aktualisierbar zu halten. Es ist wünschenswert, wenn ein Austausch von Hardwarekomponenten im Fahrzeug infolge von neueren Entwicklungen in den Spezifikationen möglichst vermieden werden kann.

Werkstätten: Aus Kostensicht ist es wünschenswert, dass auch freie Werkstätten weiterhin Reparaturen am Fahrzeug und an bordseitigen Telematikeinrich-

tungen durchführen können. Dies erfordert, dass freie Werkstätten auch die erforderlichen Handbücher und Tools zur Fehlerdiagnose und Zugang zu Originalersatzteilen und Software-Updates erhalten. Es ist aber auch festzuhalten, dass Werkstätten durch den OBD2-Zugang sehr einfach Manipulationen an Steuergeräten zum Schaden der Verbraucher durchführen können. Es ist damit wichtig, die Vertrauenswürdigkeit von Werkstätten und ihren Mitarbeitern durch unangemeldete und unabhängige Expertentests zu überprüfen.

Schutz vor Plagiaten: Gefälschte Ersatzteile haben üblicherweise keine vergleichbaren Prüfverfahren durchlaufen wie originale Ersatzteile. Der Einbau dieser Plagiate in die Fahrzeuge kann damit zu einer Bedrohung für die Fahrzeuginsassen werden, wenn funktionale Sicherheitsanforderungen nicht erfüllt sind. Plagiate können zudem zum Aushebeln von Sicherheitsmechanismen in Fahrzeugen eingesetzt werden. Hier sind organisatorische und technische Verfahren zu entwickeln und durchzusetzen, die die Detektion von Plagiaten seitens des Herstellers, in der Lieferkette, in den Werkstätten oder auch durch den Verbraucher ermöglichen.

Schadsoftware im Automobil: Für die Zukunft ist zu erwarten, dass Schadsoftware auch in das Auto Einzug hält, sobald Anwendungen großflächig ausgerollt werden, in denen kriminelle Organisationen einen Gewinn durch softwareseitige Manipulationen der Fahrzeug-internen Komponenten auf Kosten der Verbraucher erzielen können. Entfernung von persistenter Schadsoftware ohne komplette Neuinstallation des Betriebssystems ist bereits bei PCs ein sehr schwieriges Problem, das entsprechende Expertise erfordert. Auf einer komplexen Fahrzeug-IT mit Dutzenden von eingebetteten Steuergeräten gestaltet sich das Problem noch um Größenordnungen schwieriger, sodass zur Entfernung von persistenter Schadsoftware eine komplette Neuinstallation der Software zu empfehlen ist.

Kosten-Nutzen-Analyse bei jeder C2C/C2X Anwendung: Aus Verbrauchersicht ist es wichtig, dass vor einer Pilotierung einer C2C/C2X Anwendung eine positive Kosten-Nutzen-Betrachtung von unabhängigen Experten erfolgt ist. Aufgrund der Vielzahl von möglichen Anwendungen und den damit verbundenen zusätzlichen Kosten für den Fahrzeugeigner sollte eine Fokussierung auf wenige Anwendungen mit nachgewiesenem Nutzen für die Sicherheit der Verkehrsteilnehmer stattfinden.

4.2 Datenschutz

Kontrolle der Verbraucher über personenbezogene Fahrzeugdaten: Es wird dringend empfohlen, der unkontrollierbaren direkten Übertragung von personenbezogenen Informationen aus bordseitigen Komponenten, wie es aktuell zum Beispiel bei den Blackboxes der Versicherungen der Fall ist, Einhalt zu gebieten. Denkbar ist ein Ansatz, bei dem die bordseitige Komponente die Fahrzeugdaten lokal akkumuliert und die detaillierten im Fahrzeug erhobenen Daten – wie zum Beispiel erfasste Fahrtstrecken, Geschwindigkeiten, Beschleunigungen und Bremsvorgänge – löscht. Ein Datenübertrag sollte dann auf die Sendung eines Ergebnisberichts über einen längeren Zeitraum beschränkt werden. Der Fahrzeugführer ist darüber zu informieren, welche Daten an die Versicherung übersandt werden. Der Fahrzeugführer sollte berechtigt werden, den Datentransfer zu stoppen. Auch Anwendungen wie eCall und Trackingsysteme, die typischerweise vom Fahrzeugführer nicht deaktivierbar sind, haben die technische Möglichkeit, jederzeit bei Verfügbarkeit eines Mobilfunknetzes den aktuellen Aufenthaltsort des Fahrzeugs abzufragen (Hotlisting). Dies stellt praktisch eine Verwanzung des Fahrzeugs dar, die als eine starke Einschränkung des informationellen Rechts auf Selbstbestimmung zu werten ist. Bezüglich dieser Art von Anwendungen sollte eine Deaktivierbarkeit seitens des Fahrzeugführers zukünftig vorgesehen werden, so wie es auch bei Smartphones der Fall ist. Die Erstellung von Bewegungsprofilen eines Fahrzeugs ist möglich, sobald aus diesem Fahrzeug ein Gerät mit einer eindeutigen Identität sendet. Dies ist aktuell bei den Verkehrsflussanalysen mit Bluetooth den meisten Verbrauchern vermutlich nicht bewusst. Bei C2C/C2X ist es aus Datenschutzsicht empfehlenswert, an das Fahrzeug direkt einen Satz von mehreren Pseudonymen-Zertifikaten herauszugeben, aus denen das Fahrzeug sich für einen gewissen Zeitraum zufällig bedienen kann.

Definition von Datenschutzanforderungen: Der Gesetzgeber, die Wirtschaft und die Verbraucher sind gefordert, Datenschutzanforderungen für die vorhandenen und neuen Verkehrstelematikanwendungen zu definieren. Die korrekte Umsetzung in Fahrzeugkomponenten, straßenseitigen Funkstationen und Hintergrundsystemen ist mit Hilfe von unabhängigen Gutachtern zu prüfen, bevor eine Zulassung erteilt wird.

4.3 Offene Spezifikationen und Benutzerdokumente

Bereitstellung umfangreicher Informationen für den Verbraucher: Zu jeder Verkehrstelematikanwendung sollten umfangreiche Informationen an die Verbraucher herausgegeben werden. Diese Informationen können unterschiedliche Zielgruppen adressieren und damit im Detailgrad variieren. Die Verbraucher sollten letztendlich selbst entscheiden, bis zu welchem Detailgrad sie sich mit den vorgesehenen Verfahren auseinandersetzen möchten. Die bereitgestellten Informationen sollten es einem Verbraucher mit technischer Expertise ermöglichen, die Details der Protokolle und Schnittstellen der Verkehrstelematikanwendung zu analysieren.

4.4 IT-Sicherheit

Etablierte kryptografische Algorithmen: In der Vergangenheit sind in Fahrzeugen oft proprietäre, geheim gehaltene kryptografische Verfahren genutzt worden, die in den letzten Jahren durch teilweise aufwendiges Reverse-Engineering von Forschern in Erfahrung gebracht wurden und danach direkt aufgrund vorhandener Schwachstellen in den Kryptoverfahren, der Schlüsselgenerierung oder der Implementierung teilweise katastrophal gebrochen werden konnten. Beispielsweise sei hier die Veröffentlichung (Verdult et al. 2015) genannt, in der die Wegfahrsperre Megamos analysiert worden ist. Diese Wegfahrsperre wurde in vielen Fahrzeugmodellen unterschiedlicher Fahrzeughersteller in den Jahren 2000 bis 2011 verbaut und galt bisher als sicher, im Gegensatz zu den bereits gebrochenen Konkurrenzsystemen DST40, Keeloq und Hitag2 (Gleich 2015). Volkswagen hatte diese Veröffentlichung im Jahr 2013 auf dem USENIX Symposium 2013 gerichtlich verhindern lassen, die Veröffentlichung geschah damit erst zwei Jahre später (Gleich 2015). Es ist damit dringend anzuraten, dass die Verkehrstelematikanwendungen zukunftsfähige etablierte kryptografische Verfahren nach dem Stand der Technik nutzen. Dies bezieht auch den Wechsel auf vertrauenswürdigere elliptische Kurvenparameter wie beispielsweise die Brainpool-Kurven bei C2C/C2X Anwendungen ein (Ullmann et al. 2015). Es ist dringend zu empfehlen, Klartextnachrichten wie etwa SMS (Short Message Service) aus den Verkehrstelematikanwendungen komplett zu eliminieren und eine Ende-zu-Ende Verschlüsselung durchgängig einzuführen.

IT-Sicherheitsnachweise seitens der Hersteller: Da technische Schwachstellen von den Herstellern bisher oft geheimgehalten werden konnten, sind sie auch den Strafverfolgungsbehörden und den Gerichten vermutlich unbekannt. Der Verbraucher kann damit zum Beispiel beim Autodiebstahl schnell zu Unrecht in den Verdacht geraten, mit kriminellen Organisationen kooperiert zu haben. Das Vertrauen in die Verkehrstelematikanwendungen ist für die Verbraucher und die Gesellschaft insgesamt entscheidend. Durch die Offenlegung von Schnittstellen und durch Schwachstellenanalysen der Software- und Hardwarekomponenten durch unabhängige IT-Sicherheitsexperten können potentielle Angriffswege erkannt und anschließend unterbunden werden. So kann insgesamt ein höheres Sicherheitsniveau erreicht werden.

Definition von IT-Sicherheitsanforderungen: Der Gesetzgeber, die Wirtschaft und die Verbraucher sind gefordert, geeignete Sicherheitsanforderungen und technische Richtlinien für die vorhandenen und neuen Verkehrstelematikanwendungen zu definieren. Die Sicherheitsanforderungen sollten – je nach der Bedrohungslage der konkreten Anwendung durch kriminelle Organisationen – ein mittleres bis hohes Sicherheitsniveau anstreben. Die korrekte Umsetzung in Fahrzeugkomponenten, straßenseitigen Funkstationen und Hintergrundsystemen sollte mit Hilfe von unabhängigen IT-Sicherheitsexperten im Rahmen einer Zertifizierung geprüft werden, bevor eine Zulassung erteilt wird.

Literatur

Becker, Leo. 2015. Bericht: Porsche setzt auf CarPlay statt Android Auto wegen Datenschutzbedenken. *Mac & i* (6. Oktober). http://www.heise.de-2839133 (Zugriff: 1. März 2016).

Bißmeyer, Norbert, Sebastian Mauthofer, Jonathan Petit, Mirko Lange, Martin Moser, Daniel Estor, Michel Sall, Michael Feiri, Rim Moalla, Marcello Lagana und Frank Kargl. 2014. *V2x security architecture v2,* hg. von Norbert Bißmeyer. Version 1.0. Preserve 31. Januar 2014. https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.3-V2X_Security_Architecture_V2.pdf.

CAR 2 CAR (CAR 2 CAR Communication Consortium). o. D. https://www.car-2-car.org/ (Zugriff: 1. März 2016).

Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner und Tadayoshi Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. *USENIX Security* (10.–12. August).
(10.–12. August). http://www.autosec.org/pubs/cars-usenixsec2011.pdf
Eckert, Claudia. 2014. *IT-Sicherheit*. 9. Auflage. Berlin: De Gruyter Oldenbourg.
Eikenberg, Ronald. 2015. Hacker steuern Jeep Cherokee fern. *heise Security* (22. Juli).http://www.heise.de/-2756331 (Zugriff: 1. März 2016).
Das Europäische Parlament und der Rat der Europäischen Union. 2015. *Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigungen zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG*. Amtsblatt der Europäischen Union. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R0758&from=EN (Zugriff: 1. März 2016).
European Commission. 2015. *eCall: Time saved = lives saved*. http://ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved (Zugriff: 1. März 2016).
Fahn, Christian. 2013. Ich weiß, wo du gestern vor einem Jahr warst. *Donaukurier* (6. August). http://www.donaukurier.de/nachrichten/digital/datenschutz/datenschutztipps/Datenschutz-Digital-Ich-weiss-wo-du-gestern-vor-einem-Jahr-warst;art267994,2801060 (Zugriff: 1. März 2016).
Gleich, Clemens. 2015. VW-Wegfahrsperren: Volkswagen-Hack endlich veröffentlicht. *heise online* (13. August). http://www.heise.de-2778632 (Zugriff: 2. März 2016).
Kannenberg, Axel. 2015. Autobauer prüfen Daten-Freigabe aus vernetzten Fahrzeugen für ihren Kartendienst Here. *heise online* (7. Dezember). http://www.heise.de/-3033589 (Zugriff: 1. März 2016).
Lemke, Kerstin, Christof Paar und Marko Wolf. 2006. *Embedded Security in Cars*. Heidelberg: Springer VS.
Miller, Charlie und Chris Valesek. 2015. *Remote exploitation of an unaltered passenger vehicle.* http://illmatics.com/Remote%20Car%20Hacking.pdf
Moser, Martin. E-Mail Nachricht an Autorin, 30. Oktober 2015.

Schwan, Ben. 2015. Gegen Apple und Co.: Autobauer wollen „direkte Schnittstelle“ zum Kunden behalten. *Mac & i* (9. November). http://heise.de/-2911839 (Zugriff: 2. März 2016).

Stokar, Rudolf von. 2015. Warum die Autoindustrie neue Software Updates braucht. Herausforderung beim Update von ECUs. *Elektroniknet.de*. http://www.elektroniknet.de/automotive/tools/artikel/117489/1/ (Zugriff: 2. März 2016).

Stotz, Jan Peter, Norbert Bißmeyer, Frank Kargl, Stefan Dietzel, Panos Papadimitratos und Christian Schleiffer, Hg. 2011. *Security requirements of VSA*. Version 1.1. Preserve Juni 2011. https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.1-Security%20Requirements%20of%20Vehicle%20Security%20Architecture.pdf.

Szerwinski, Robert. 2014. *Security in the automotive domain*. CAST Workshop Mobile and Embedded Security. (22. Mai).

Ullmann, Markus, Christian Wieschebrink und Dennis Kügler. 2015. Public key infrastructure and crypto agility concept for intelligent transportation systems. Proceedings VEHICULAR, in: *IARIA* 2015, 14–19.

Wenzel, Andreas, Hrsg. 2013. *Sichere intelligente Mobilität. Testfeld Deutschland: Deliverable D5.5, TP5-Abschlussbericht – Teil B-3 – Technische Bewertung* Version 1.0. SIMTD Konsortium. (9. Dezember). http://www.simtd.de/index.dhtml/object.media/deDE/8118/CS/-/backup_publications/Projektergebnisse/simTD-TP5-Abschlussbericht_Teil_B-3_Technische_Bewertung_V10.pdf.

Verdult, Roel, Flavio D. Garcia und Baris Ege. 2015. *Dismantling megamos crypto: wirelessly lockpicking a vehicle immobilizer*. Supplement to the Proceedings of the 22nd USENIX Security Symposium 2013.

Smart Grid

Chancen und Risiken für Verbraucher

Ulrich Greveler

DOI 10.15501/978-3-86336-912-5_5

Abstract

Im November 2015 wurde ein Gesetzesentwurf zur Digitalisierung der Energiewende beschlossen. Erneut ist damit eine Debatte um den Rollout von Smart Metern (digitalen Stromzählern) aufgeflammt. Bisher nutzen private Haushalte elektromechanische Stromzähler, die händisch abgelesen werden und keine flexible Tarifierung erlauben. Die künftigen Zähler sollen den Weg für die Digitalisierung des gesamten Stromnetzes ebnen. Das dabei entstehende Smart Grid kann bei einem regionalen Überangebot an elektrischer Energie durch Nutzung von steuerbaren Geräten einen Ausgleich vornehmen. Stromkunden bezahlen dann über variable Tarife weniger für die verbrauchte Kilowattstunde: Geräte schalten sich flexibel dazu und stabilisieren die Nachfrage. Die zu erhebenden Daten sind sehr sensibel und können Rückschlüsse auf Lebensgewohnheiten oder identifizierbare Aktivitäten zulassen. Der Gesetzesentwurf berücksichtigt zwar Hinweise, die aus Fachdiskussionen und wissenschaftlichen Untersuchungen stammen und die Schwachstellen bei vorhandenen Smart Meter-Infrastrukturen aufzeigen; es bleibt jedoch zweifelhaft, ob die zwangsweise Digitalisierung der Stromverbrauchsmessung Verbrauchern Vorteile bringt, die den Risiken und Kosten angemessen gegenüber stehen.

Ein erweiterter Abstract dieses Beitrages ohne Handlungsempfehlungen wurde vorab auf der Plattform „SciLogs.de – Tagebücher der Wissenschaft“, *„Zwangsdigitalisierung der Stromverbraucher oder sinnvolle Regulierung?“* publiziert.

1 Hintergrund

Mit dem vom Bundeskabinett im November 2015 beschlossenen Gesetzesentwurf zur Digitalisierung der Energiewende hat die Debatte um Sinn oder Unsinn eines flächendeckenden Rollouts von Smart Metern (digitalen Stromzählern, siehe Abbildung 1) erneut an Intensität gewonnen. Das Gesetz soll im ersten Quartal des Jahres 2016 vom Bundestag beschlossen und im Bundesrat beraten werden. Der Zeitplan könnte aber noch modifiziert werden, da sich starke Widerstände abzeichnen.

Abbildung 1: Smart Meter. Quelle: EVB Energie AG. Bildquelle: https://de.wikipedia.org/wiki/Intelligenter_Z%C3%A4hler#/media/File:Intelligenter_zaehler-_Smart_meter.jpg. CC BY-SA 3.0.

Die Modernisierung des Energienetzes aufseiten des Verbrauchers[1] würde nach Inkrafttreten des Gesetzes erheblich beschleunigt werden. Bisher nutzen

1 *Verbraucher* grenzt sich hier auch gegen den Begriff Stromverbraucher ab, der über Disziplingrenzen uneindeutig ist, da er sich je nach Kontext sowohl auf Geräte als auch auf Personen beziehen kann.

private Haushalte fast ausschließlich elektromechanische Stromzähler (sogenannte Ferraris-Zähler, siehe Abbildung 2), die händisch abgelesen werden und – abgesehen von Tag-Nacht-Strom-Tarifen im Umfeld von Elektrospeicherheizungen – keine zeit- oder lastabhängige Tarifierung erlauben. Die digitalen Zähler sollen die alten Stromzähler ablösen und damit den Weg für die Digitalisierung des gesamten Stromnetzes ebnen.

2 Digitalisierung und stabile Netze

Verbraucherschützer laufen Sturm gegen die „Zwangsdigitalisierung durch die Kellertür" (VZBV 2015) und werfen der Regierung vor, Verbraucher zur Preisgabe von Daten zu zwingen, während Vertreter des Bundesministeriums für Wirtschaft und Energie (BMWi) auf erneuerbare Energien hinweisen, die über digitale Zähler besser in den Strommarkt integriert werden können, was letztlich auch für private Verbraucher von großem Nutzen sei.

Eine technisch-wirtschaftliche Motivation für einen massenhaften Rollout von digitalen Stromzählern liegt darin, dass die verstärkte Nutzung erneuerbarer Energien zu einer stärker fluktuierenden Stromerzeugung führt und damit die Netze, die Angebot und Nachfrage stets regional in Waage halten müssen, destabilisiert werden. Das Stromangebot soll zukünftig mit einer ebenfalls schwankenden Nachfrage synchronisiert werden, um die Netzinfrastruktur effizient nutzen zu können und Netzinstabilitäten zu vermeiden. Aus granularen Verbrauchsdaten und über Netzsensoren lassen sich Netzzustandsdaten gewinnen, die zur Stabilisierung des Stromnetzes verwendet werden. Dann kann zukünftig bei einem Überangebot an elektrischer Energie durch Nutzung von steuerbaren Geräten ein Ausgleich vorgenommen werden.

Besteht ein Überangebot an Strom, soll der zeitnahe Verbrauch incentiviert werden, um Nachfrage zu schaffen. Die Kunden bezahlen dann über variable Tarife weniger für die verbrauchte Kilowattstunde (kWh): Waschmaschinen, Kühlschränke, Trockner und Spülmaschinen („weiße Ware") schalten sich innerhalb gewisser Freiheitsgrade (zum Beispiel Temperaturgrenzen bei Kühl-

truhen, Nachtzeit bei Geschirrspülern und Wäschetrocknern) flexibel dazu, zudem können Elektrofahrzeuge mit hoher Batteriekapazität genau dann geladen werden, wenn die Nachfrage anderer Verbraucher sinkt, um eine stabile Nachfrage nach elektrischer Energie zu erzielen. Die Steuerung von „Stromfressern“ wie Nachtspeicherheizungen und Wärmepumpen durch ein intelligentes Stromnetz ergänzt das Konzept eines selbst-stabilisierenden Netzes (Smart Grid) über die Einbeziehung elektrischer Verbraucher.

Abbildung 2: Zweitarifzähler mit Rundfunksteuerempfänger für Tag- und-Nacht-Tarif. Quelle: KMJ. CC BY-SA 3.0. http://www.scilogs.de/datentyp/zwangsdigitalisierung-stromverbraucher-regulierung/.

3 Kollidierende Interessen

Die Debatte gewinnt dadurch weiter an Schärfe, dass Interessen der Verbraucher in Bezug auf Datenschutz und Datensicherheit ihrer Energieverbrauchsdaten – und damit der Schutz ihrer Privatsphäre – mit energiepolitischen Zielen kollidieren, die eine Modernisierung und Digitalisierung des Stromnetzes im Zuge der Energiewende ebenfalls im Sinne dieser Verbraucher als gesellschaftliches Interesse vorsehen. Ein Ausgleich der Interessen ist nur eingeschränkt möglich, da der Zustimmungsvorbehalt der betroffenen Bürgerinnen und Bürger aufgehoben werden soll, um einen technischen Fortschritt zu erzwingen.

Der Gesetzgeber muss hier eine politische Entscheidung treffen: Welches Interesse ist in der Post-Snowden-Ära höher zu bewerten? Das Interesse der Stromkunden, Ihr Recht auf informationelle Selbstbestimmung nicht aufzugeben, oder das Interesse der Stromkunden, an einem modernen Energienetz zu partizipieren, das (sofern die formulierten Ziele erfüllt werden können) eine stabile, nachhaltige und kostengünstige Versorgung garantiert? Die Entscheidung dürfte den Abgeordneten nicht leicht fallen, denn es gibt gut begründete Zweifel, dass das Gesetz die hochgesteckten Ziele tatsächlich erfüllen wird. Neben den zuvor genannten Verbraucherinteressen gibt es kommerzielle Interessen seitens der Netzbetreiber und Gerätehersteller: Wenn der Gesetzgeber den Rollout der Geräte erzwingt, winkt ein planungssicheres Milliardengeschäft, ohne dass die Endverbraucher erst mühsam von der Sinnhaftigkeit der digitalen Zähler in ihren Kellern überzeugt werden müssen. Die Bereitschaft, freiwillig einen digitalen Zähler anzuschaffen und einbauen zu lassen, ohne für diese Entscheidung belohnt zu werden, dürfte für den Großteil der Haushalte als gering angenommen werden.

4 Personenbezogenheit und Sensibilität der Daten

Die von Smart Metern erhobenen Daten zum Stromverbrauch stellen wie alle auf einen Haushalt bezogenen Verbrauchsdaten (beispielsweise Gas, Wasser, Wärme) grundsätzlich personenbezogene Daten dar. Das Recht auf informationelle Selbstbestimmung wird tangiert, wenn Stromverbrauchsdaten gemessen, übermittelt oder verarbeitet werden. Beim Datenschutzrecht wird von einem Verbot mit Erlaubnisvorbehalt ausgegangen. Die Erlaubnis kann durch Rechtsvorschrift oder Einwilligung des Betroffenen erfolgen. Der Gesetzesentwurf schafft hier also notwendige Rechtsvorschriften, um ohne die Einwilligung der Endverbraucher Eingriffe in das Recht auf informationelle Selbstbestimmung vorzunehmen.

Ob die aus dem Gesetzesentwurf erwachsende Duldungspflicht der Verbraucher angemessen ist, ist angesichts des erheblichen Grundrechtseingriffs verfassungsrechtlich umstritten, denn die freie Wahl des Messstellenbetreibers allein mildert diesen Eingriff nur in äußerst schwacher Weise ab. Die Umsetzung variabler Tarife wäre auch über andere technische Infrastrukturen denkbar, womit der angestrebte Zweck der Duldungspflicht möglicherweise durch mildere, gleich wirksame Mittel erreicht werden könnte (vgl. Schneidewind 2015). Eine Verfassungsbeschwerde könnte sich auf diesen Schwachpunkt in der Gesetzesbegründung beziehen und anstreben, die Regelung über das Bundesverfassungsgericht zu Fall zu bringen.

Während der Personenbezug der erhobenen Daten unstrittig und bei den beteiligten Akteuren bekannt ist, geht die Wahrnehmung der Sensibilität der erhobenen Daten auseinander. Eine Auswertung von Metering-Daten erlaubt deutlich präzisere Einblicke in die Privatsphäre als nur eine Feststellung, welche Energiemenge eine Person (oder ein Haushalt) verbraucht. Abhängig von der Auflösung der Daten können Rückschlüsse auf Lebensgewohnheiten (zum Beispiel Anwesenheitszeiten, siehe Abbildung 3) oder identifizierbare Aktivitäten (etwa kochen, duschen, schlafen) vorgenommen werden (Molina-Markham et al. 2010).

So können beispielsweise bei einer Messauflösung von 15 Minuten folgende Lebensgewohnheiten einer im Haushalt lebenden Person ermittelt werden (Müller 2010):

- Zu welcher Uhrzeit geht sie zu Bett?
- Zu welcher Uhrzeit steht sie auf?
- Gibt es nächtliche Toilettenbesuche?
- Wie häufig wird gekocht?
- Wann verlässt sie das Haus, wann kehrt sie zurück?
- Verändern sich die Lebensgewohnheiten (Nachwuchs, Besuch)?

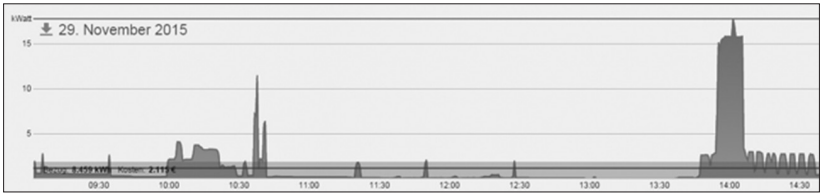


Abbildung 3: Visualisierung des Stromverbrauchs eines Smart Meters, Privathaushalt. Eigene Darstellung.

Bei feingranularen Daten (Aufzeichnung in Sekundenintervallen) steigt die Sensibilität der Daten weiter an. Eine vom Autor dieses Beitrages gegründete Arbeitsgruppe an der Fachhochschule Münster zeigte bereits 2012, dass bei der Verarbeitung von hoch aufgelösten Energieverbrauchsdaten Rückschlüsse auf Bewegungsverhalten im Haushalt – bis hin zur Identifizierung von eingeschalteten Fernsehprogrammen oder abgespielten Videofilmen aufgrund der Abhängigkeit des Energieverbrauchs von Bildschirmhelligkeitswerten – möglich sind (Greveler, Justus und Löhr 2012a). Letztlich kann über die Identifizierung aller elektrischen Geräte und ihrer Parameter (Greveler und Justus, Löhr 2012b) der gesamte persönliche Lebensbereich, soweit er sich im Haushalt abspielt, rekonstruiert werden, und Einblicke bis in die Intimsphäre werden möglich wie zum Beispiel die Feststellung, welche Filme im Haushalt abgespielt werden oder ob Besuch hereingelassen wurde (vgl. Greveler 2014).

Über die Analysemöglichkeiten der erfassten Daten hinaus wurden bei der ersten Generation in Deutschland verbauter Smart Meter (2011) schwerwie-

gende Mängel bei der Implementierung des Gateways (das die Datenübertragung vornimmt) durch Untersuchungen der zuvor genannten Arbeitsgruppe festgestellt: So wurden bei in Privathaushalten verbauten Smart Metern die Energieverbrauchsdaten unverschlüsselt und nicht signiert übertragen, womit elementare Grundsätze von Datenschutz und Datensicherheit verletzt wurden. Diese Tatsache wog umso schwerer, dass vertraglich vom Anbieter zugesichert wurde, dass die Übertragung nur verschlüsselt erfolge. Die Umsetzung dieser Vereinbarung war schlicht vergessen worden.

5 Welchen Verbraucherschutz und welchen Zwang bei der Einführung sieht das neue Gesetz vor?

Der Gesetzesentwurf berücksichtigt augenscheinlich Hinweise, die aus Fachdiskussionen und wissenschaftlichen Untersuchungen stammen und die Schwachstellen bei vorhandenen Smart Meter-Infrastrukturen aufzeigten. Es wird auch deutlich, dass die nachgewiesene Sensibilität von granularen Stromverbrauchsdaten von den Gesetzesautoren berücksichtigt wurde. Die Duldungspflicht erstreckt sich allein auf Daten, die viertelstündlich erhoben und innerhalb der häuslichen Infrastruktur gespeichert werden. Diese Daten sind zwar granulare Energieverbrauchsdaten und lassen Rückschlüsse auf Lebensgewohnheiten und Anwesenheitszeiten zu, sie sind jedoch nicht feingranular und verwischen daher Informationen, die bis in die Intimsphäre reichen können.

Zudem wurden im Vorfeld der Formulierung des Gesetzes fachliche Anforderungen gesammelt, die im Auftrage des BMWi vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam mit Branchenvertretern, der Bundesdatenschutzbeauftragten und Beauftragten der Länder, der Bundesnetzagentur und der Physikalisch-Technischen Bundesanstalt erarbeitet wurden. Im Einzelnen lassen sich folgende zentralen Punkte feststellen:

- Schutzprofile und technische Richtlinien zur Gewährleistung von Datenschutz und Sicherheit werden nun verbindlich. Damit dürfen unsichere Gateways nicht mehr eingesetzt werden und ein drohender Wildwuchs bei technischen Realisierungen von Datenschutzanforderungen wird frühzeitig beendet.
- Zu sendende Daten werden vom Smart Meter-Gateway verschlüsselt und signiert. Damit werden elementare Standards bei der Durchsetzung von Datensicherheit festgeschrieben.
- Gesetzlich erzwungen wird „nur", dass standardmäßig 15-Minutenwerte im Messsystem vorhanden sind. Diese werden aber nicht notwendigerweise übertragen. Die gespeicherten Werte könnten beispielsweise für die Visualisierung des Stromverbrauchs genutzt werden, um dem Verbraucher hausintern Energiekosteneinsparpotenziale aufzuzeigen. Unklar bleibt, wie zukünftig ein behördlicher Zugriff auf diese im Messsystem gespeicherten Daten erfolgen könnte, etwa im Zuge von Ermittlungsverfahren oder bei strafprozessualer Durchsuchung. Eine behauptete häusliche Anwesenheit seitens eines Tatverdächtigen könnte durch Auswertung der Daten widerlegt oder mindestens begründet angezweifelt werden.
- Ob Daten übertragen werden, regeln die Vorschriften des dritten und vierten Teils des Gesetzesentwurfs. Es darf, soweit der Verbraucher keinen variablen Tarif vereinbart hat und keine steuerbaren Geräte betrieben werden, standardmäßig nur ein Wert pro Abrechnungsjahr nach außen übertragen werden. Für die meisten Haushalte wird die Infrastruktur daher keine Änderung im Hinblick auf die zu Abrechnungszwecken übermittelte Information bewirken.
- Zugeordnete technische Richtlinien des BSI sehen Sicherheitsanforderungen an das Smart Meter-Gateway, das Sicherheitsmodul und die Administration des Gateways vor. Zudem werden kryptografische Vorgaben formuliert und eine Schlüsselinfrastruktur (PKI) wird vorgezeichnet. Die Richtlinien und Vorgaben sind dabei umfassend, vergleichsweise streng und gehen insbesondere hinsichtlich der Komplexität über die aus Sicht der Datenschützer formulierten Erwartungen hinaus. Dies ist dadurch zu erklären, dass intelligente Stromnetze als zukünftige, kritische Infrastruktur gesehen werden, deren Schutz besondere Priorität genießt.
- Eine Preisobergrenze von hundert Euro pro Jahr wird für Haushalte mit einem Verbrauch von bis zu 10.000 kWh pro Jahr, festgelegt; diese Grenze sinkt auf sechzig Euro bei Verbrauchern mit weniger als 6.000 kWh pro Jahr (diesen Jahresverbrauch unterschreiten beispielsweise die meisten 4-Per-

sonen-Haushalte) und über weitere Zwischenschritte bis auf 23 Euro pro Jahr für Haushalte mit einem Jahresstromverbrauch unter 2.000 kWh (etwa energiesparsame Singlehaushalte).
- Die Einbaupflicht beginnt zwar bereits 2017 (ab 10.000 kWh pro Jahr) aber erst 2020 für „normale“ private Haushalte, die in der Regel 10.000 kWh deutlich unterschreiten.

Datenschutzrisiken verbleiben hierbei aufseiten der Daten verarbeitenden Stellen, die granulare Verbrauchsdaten speichern (beispielsweise um für Kunden variable Tarife abzurechnen). Sollte es hier zu einem Entweichen von Stromverbrauchsdaten aufgrund unzureichender Schutzmaßnahmen oder erfolgreicher Hackerangriffe oder einer missbräuchlichen Nutzung innerhalb der berechtigten Stelle kommen, wäre der Eingriff in die Privatsphäre der Stromkunden kaum zu unterschätzen.

6 Hohe Kosten und hoher Aufwand für einmal jährlich Stromablesen?

Nach Umsetzung des Rollouts der digitalen Zähler beginnend 2020 werden die meisten Haushalte noch keine steuerbaren Geräte (wie zum Beispiel Elektrofahrzeuge mit kompatiblen Batteriesteuerungen) besitzen und abseits des bereits heute stellenweise praktizierten Tag- und Nachtstromtarifs keine variablen Stromtarife nutzen. Es ist kurzfristig kein solches Angebot erkennbar, das für eine ebenfalls derzeit noch nicht feststellbare Nachfrage vorhanden wäre. Ein im Privathaushalt verbautes Smart Meter-Gateway wird dann zunächst gemäß gesetzlicher Vorgaben nur einmal jährlich den zur Rechnung fälligen Verbrauchswert übertragen, der dann – diese Erleichterung sollte nicht verschwiegen werden – nicht mehr händisch abgelesen werden muss. Jährlichen Kosten von 60 Euro wird zudem die grundsätzliche, technische Möglichkeit gegenüberstehen, sich eine Visualisierungskomponente zuzulegen, die den Stromverbrauch viertelstündlich darstellt, um das eigene Verhalten anpassen zu können (siehe Abbildungen 4 und 5).

Darüber hinaus entfallen für einige Verbraucher das Selbstablesen und die oft als lästig empfundene telefonische Durchgabe des Jahresverbrauchs per Sprachcomputer. Die Enttäuschung über diese Vorteile dürfte bei vielen Verbrauchern angesichts der Kosten aber groß sein.

Abbildung 4: Statistische Auswertung über Smart Meter-Messstellenbetreiber discovergy, Privathaushalt. Eigene Darstellung (CC BY-SA 3.0).

7 Warum wird die Digitalisierung erzwungen?

Sieht man einmal vom häufig benannten aber bisher nicht belegten Generalverdacht ab, dass eine erfolgreiche Lobbyarbeit von Geräteherstellern das Gesetzesvorhaben beschleunigt haben könnte, lässt sich auch ein nachvollziehbares politisches Ziel identifizieren. Mit der Zwangseinführung versucht die Bundesregierung, ein „Henne-Ei-Problem“ bei der Etablierung einer bisher fehlenden technischen Infrastruktur zu lösen: Solange es keine attraktiven variablen Stromtarife und keine nützlichen steuerbaren Geräte gibt, werden nur wenige, von digitaler Technik per se begeisterte Verbraucher einen Smart Meter auf eigene Kosten einbauen lassen. Umgekehrt fehlen aber die wirtschaftlichen Anreize für Hersteller und Netzbetreiber, neuartige Geräte zu

entwickeln, zertifizieren zu lassen und auf den Markt zu bringen, die dann verbraucherseitig vom intelligenten Stromnetz gesteuert werden und über variable Stromtarife Kosten senken können, wenn diese Geräte nicht bundesweit mit vorhandenen Smart Metern interoperabel kommunizieren können.

Mit der verpflichtenden Einführung intelligenter und interoperabler Messsysteme wird sich diese Ausgangslage ändern. Es werden stufenweise in jedem Haushalt Messsysteme existieren, die viertelstündig ermittelte Stromverbrauchsdaten in ihren Datenspeichern vorhalten und die über definierte Schnittstellen zu kompatiblen und zertifizierten Geräten verfügen. Dies schafft die Grundlage eines Marktes für Geräte, Systeme und Tarifvertragsmodelle im Umfeld eines Smart Grids, die auf diesen Daten operieren können und Netzauslastung und Kosten sowohl für Verbraucher als auch für Energielieferanten und Netzbetreiber optimieren helfen.

Dass der Verbraucher diese Weiterentwicklung des Stromnetzes zum großen Teil selbst finanziert, ist eine politische Entscheidung, die naturgemäß hart umstritten ist. Die sogenannte EEG-Umlage zur Förderung der Stromerzeugung aus erneuerbaren Energiequellen sorgte bereits in der jüngeren Vergangenheit für zusätzliche Kosten im zweistelligen Milliardenbereich, die über die Stromrechnung an die Verbraucher weitergegeben wurden. Die Jahresgebühren für Smart Meter werden hier noch zusätzlich eine weitere Preissteigerung für alle Haushalte bewirken, die keine Kostenersparnis in mindestens der Höhe einer Jahresgebühr realisieren können.

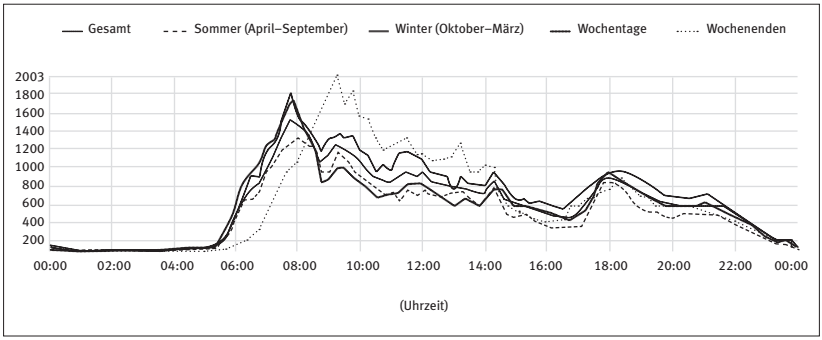


Abbildung 5: Lastprofil, generiert aus Metering-Daten über Messstellenbetreiber discovergy, Privathaushalt. Eigene Darstellung (CC BY-SA 3.0).

7.1 Legt die Energiewende eine Zwangsdigitalisierung des Netzes aus wissenschaftlich-technischer Sicht nahe?

Eine Analyse publizierter Fachbeiträge mit der Absicht Argumente pro Digitalisierung des Stromzählers zu finden, führt rasch zum Ergebnis, dass es zwar vielfältige technologische und wissenschaftlich-technische Ansätze gibt, ein zukünftiges Smart Grid zu gestalten und auszubauen, jedoch zum gegenwärtigen Zeitpunkt keine sinnvollen Prognosen zu einer Entwicklung des Netzes in den Folgejahren nach einem Smart Meter-Rollout existieren. Dies ist dadurch begründet, dass es kaum verlässliche Einschätzungen zum Ausbau des Stromnetzes selbst (zum Beispiel Realisierung von Nord-Süd-Trassen und großen Energiespeichern), zur zukünftigen Rolle regionaler Energieversorger, zum Einsatz neuartiger technologischer Innovationen beim Netzausbau und zum Verbraucherverhalten selbst gibt. Mit anderen Worten: Wir wissen heute noch nicht, ob die zukünftige Metering-Infrastruktur tatsächlich wesentlich zur Stabilisierung und Auslastung der Stromnetze führen wird. Es gibt weitere wirkungskonkurrierende technologische Ansätze: Es werden wesentliche Effekte von intelligenten Stromspeichern und Hochspannungs-Gleichstrom-Übertragungs-Leitungen erwartet, die Wind- und Solarenergie dort zeitversetzt bereitstellen, wo die Nachfrage am Größten ist. Zudem können regionale Stromerzeuger und vermaschte Netze bereits heute zunehmend flexibler auf Lastspitzen reagieren. Ob die Steuerung der weißen Ware und der Batterien von Elektrofahrzeugen zukünftig erhebliche positive Effekte auf die Netzstabilität haben wird, lässt sich nicht allein auf Basis aktueller Daten zur Stromenergienutzung vorhersagen. Ebenso wenig ist heute bekannt, ob Verbraucher zukünftig allein aufgrund einer verbesserten Visualisierung ihres Verbrauchs die Stromabnahme merklich senken werden. Lediglich das kurzfristige Potenzial der Kostenersparnis seitens der Verbraucher lässt sich anhand der aktuellen Strommarktdaten abschätzen: Experten bezweifeln bei diesen Abschätzungen, dass das Einsparpotenzial die Jahreskosten der Smart Meter übersteigen wird (Liebe et al. 2015). Auch das deutsche Elektrohandwerk kritisiert in einer Pressemitteilung vom 24. November 2015, dass sich die zwangsweise einzuführenden digitalen Stromzähler nicht bei allen Verbrauchern lohnen werden.

Seitens des Bundesministeriums für Wirtschaft und Energie werden hohe Erwartungen an das Gesetz geknüpft: „Intelligente Messsysteme können nicht nur den Stromverbrauch messen, steuern und kommunizieren (…). Sie [sind

ein] Allround-Talent, um Energiekosten zu senken und Effizienz und Komfort zu steigern“ (BMWi 2015). Sollte das Gesetz diese hohen Erwartungen nicht erfüllen, werden die Verbraucherschützer mit der Aussage, dass für die meisten Haushalte keine Vorteile aufgrund des Rollouts entstehen, recht behalten. Die privaten Haushalte werden dann weniger zu ihrem Glück gezwungen, als dass sie nur zusätzliche Kosten und Datenschutzrisiken werden tragen müssen.

8 Handlungsempfehlungen

Da im Rahmen der Schriftenreihe, in der dieser Beitrag erscheint, die Formulierung konkreter Handlungsempfehlungen vorgesehen ist, werden nun unter Bezugnahme auf die im vorherigen Abschnitt dargestellte Ausgangssituation Empfehlungen an die verbraucherpolitischen Akteure abgeleitet. Die Empfehlungen verlassen dabei teilweise den Bereich der rein sachlich-neutralen Bewertung, da hier auch eine Abwägung der politischen Interessen der Beteiligten (Datenschutzinteressen vs. Netzausbau-Interesse) erfolgt, die sich nach Auffassung des Autors nicht neutral aus den Fakten folgern lässt.

8.1 Opt-Out-Recht in Betracht ziehen: Um Verbraucher werben!

Die vorgesehene Zwangseinführung wird viel Porzellan zerschlagen, weil die betroffenen Verbraucher auf diesem Wege nur die Kosten und Risiken wahrnehmen, während die Chancen, die eine Digitalisierung bietet, kaum noch gewürdigt werden. Der Gesetzgeber sollte eine Anpassung des Gesetzes prüfen, die ein Opt-Out für private Haushalte vorsieht, um zu einer Freiwilligkeit der Einführung zurückzukehren.

Statt eines gesetzlichen Zwangs könnte eine Kampagne, die die konkreten Vorteile einer Umstellung auf digitale Stromzähler benennt, die einforderbare Garantien in Bezug auf die Wirkung formuliert und die eine sanfte Umstellung ohne granulare Datenspeicherung vorsieht, die Verbraucher „mitnehmen“ und

zu Vorreitern der Energiewende machen. Diese Kampagne könnte mit Finanzierungshilfen, die die Kosten in der Anfangsphase (zum Beispiel die ersten fünf Jahre), in der – in Ermangelung entsprechender tariflichen Angebote und steuerbaren Geräte – wenig bis keine Vorteile realisiert werden, verbunden werden.

8. 2 Visualisierung der Energiekosten und Verhaltensänderung erleichtern!

Die in den Messsystemen gespeicherten Daten liegen für den Großteil der Verbraucher brach, weil diese weder variable Tarife nutzen, noch eine Auswertung der Daten zur Optimierung des persönlichen Energieverbrauchs vornehmen können. Eine Verpflichtung der Partei, die den Einbau der digitalen Zähler vornehmen lässt, zum Anbieten einer kostenlimitierten, ohne Internetverbindung operablen und einfach zuhause installierbaren Lösung zur Visualisierung der Daten inkl. automatisierter Energieberatung (etwa über die Identifikation stromhungriger Geräte) würde helfen, den Schatz an Daten für die Betroffenen zu bergen, ohne eine Datenübertragung sensibler Daten nach außen vorzunehmen. Dies könnte auch über leihweise für einen begrenzten Zeitraum überlassene Geräte geschehen, die von Energieberatern ausgegeben werden.

8.3 Technologiekosten nur auf die Verbraucher umlegen, die profitieren!

Der Gesetzesentwurf sieht zwar feste Obergrenzen für die Kosten der Digitalisierung der Messsysteme vor, diese sind aber recht hoch, wenn sie in Relation zu erwarteten Einsparpotenzialen betrachtet werden. Um eine Belastung der Verbraucher mit zusätzlichen Energienebenkosten zu verhindern, könnten die Kosten den tatsächlichen Einspareffekten zugeordnet werden. Wer also tatsächlich variable Stromtarife nutzt, könnte über einen anteiligen Beitrag, der aus der Differenz zum Normaltarif errechnet wird, belastet werden, so dass ein Umlageverfahren etabliert wird, dass diejenigen, die überproportional viele Kosten sparen, stärker belastet. Verbraucher, die keine Vorteile über das digitale Messsystem realisieren, müssen dann auch keine zusätzlichen Kosten tragen.

8.4 Konsequenzen bei Datenschutzverstößen festschreiben!

Energieverbrauchsdaten stellen äußerst sensible personenbezogene Daten dar. Erhebliche Datenschutzrisiken verbleiben aufseiten der Daten verarbeitenden Stellen, die granulare Verbrauchsdaten speichern, um beispielsweise variable Tarife abzurechnen. Bei Datenschutzverstößen sollte hierbei eine Haftungsregelung greifen, die über die Androhung von fixen Bußgeldern hinausgeht und in Relation zum angerichteten Schaden steht. Ein Ansatz könnte darin bestehen, die Verbraucher von Ansprüchen zur Bezahlung des Stromverbrauchs bei variablen Tarifen freizustellen, wenn es Datenschutzverstöße gegeben hat. Mit anderen Worten: Wer unter einer „Datenpanne" zu leiden hat, muss den Strom im betroffenen Verbrauchsjahr nicht mehr bezahlen. Auf diese Weise würde eine starke anbieterseitige Motivation geschaffen, mit den granularen Stromverbrauchsdaten sorgsam umzugehen, sie frühzeitig zu pseudonymisieren und diese Daten unmittelbar nach dem Abrechnungsvorgang zu löschen.

Literatur

BMWi (Bundesministerium für Wirtschaft und Energie). 2015. *Intelligente Messsysteme als wichtiger Baustein der Energiewende*. Faktenblatt des Bundesministerium für Wirtschaft und Energie, Stand September 2015. http://www.bmwi.de/BMWi/Redaktion/PDF/F/faktenblatt-digitalisierung-energiewende,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

Greveler, Ulrich, Benjamin Justus und Dennis Löhr. 2012a. Forensic content detection through power consumption. In*: IEEE International Workshop on Security and Forensics in Communication Systems, 6759–6763*. Ottawa: IEEE Computer Society Press.

— 2012b. Identifikation von Videoinhalten über granulare Stromverbrauchsdaten. In: *Sicherheit 2012 – Sicherheit, Schutz und Zuverl*ässigkeit, *7.–9. März 2012, Darmstadt. Konferenzband der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)*, hg. von Neeraj Suri und Michael Waidner, 35–45. GI Proceedings, 195. Bonn: Gesellschaft für Informatik. http://subs.emis.de/LNI/Proceedings/Proceedings195/P-195.pdf.

Greveler, Ulrich. 2014. Smart Meter: Strom sparen – Daten verschwenden? In: *Der gläserne Verbraucher: Wird Datenschutz zum Verbraucherschutz?* hg. von Christian Bala und Klaus Müller. Beiträge zur Verbraucherforschung, Bd. 1, 83–92. Düsseldorf: Verbraucherzentrale NRW. http://verbraucherzentrale.nrw/bzv1.

Liebe, Andrea, Stephan Schmitt und Matthias Wissner. 2015. *Quantitative Auswirkungen variabler Stromtarife auf die Stromkosten von Haushalten*. WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH. Kurzstudie 11. November 2015. http://zap.vzbv.de/ceoba83d-8d69-4aed-bbc3-af50e58fdf59/Auswirkungen-variabler-Stromtarife-auf-Stromkosten-Haushalte-WIK-vzbv-November-2015.pdf

Molina-Markham, Andrés, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet und David Irwin. 2010. Private memoirs of a smart meter. In: *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for energy-efficiency in building, hg. von Antonio Ruzzelli, 61–66.* BuildSys '10. New York: ACM. doi:10.1145/1878431.1878446.

Müller, Klaus J. 2010. Gewinnung von Verhaltensprofilen am intelligenten Stromzähler. In: *Datenschutz und Datensicherheit* 34, Nr. 6: 359–364. doi:10.1007/s11623-010-0107-2.

Schneidewindt, Holger. 2015. Ist der Smart Meter-Zwang verfassungswidrig? In: *Phasenprüfer – Der Blog für Energiepolitik* (Blog). (24. September). http://phasenpruefer.info/ist-smart-meter-zwang-verfassungswidrig/ (Zugriff: 29. Februar 2016).

vzbv (Verbraucherzentrale Bundesverband e.V.). 2015. Smart Meter-Einbau: Zwangsdigitalisierung durch die Kellertür: Pressemitteilung des Bundesverbands der Verbraucherzentralen und Verbraucherverbände (22. September). http://www.vzbv.de/pressemitteilung/smart-meter-einbau-zwangsdigitalisierung-durch-die-kellertuer (Zugriff: 29. Februar 2016).

Der digital verführte, ahnungslose Verbraucher

Verbraucherpolitisches Handeln bei wachsenden Manipulationsmöglichkeiten des Verbraucherinteresses durch unkontrollierbare Datenauswertung der Unternehmen

Michael Schleusener und Sarah Hosell

DOI 10.15501/978-3-86336-912-5_6

Abstract

2015 nutzten rund 79 Prozent der deutschsprachigen Bevölkerung ab 14 Jahre insgesamt rund zwei Stunden pro Tag das mobile Internet via Smartphones oder Tablets. Dabei ist das Smartphone als „der Spion in der Hosentasche" fähig, eine Vielzahl von Daten über seinen Träger zu sammeln. Durch deren Auswertung lassen sich mit bestimmten Wahrscheinlichkeiten Aussagen über individuelle Charaktereigenschaften, Emotionen aber auch Verhaltensprognosen treffen. Dies ermöglicht Unternehmen, Menschen hinsichtlich ihrer Bedürfnisse zu manipulieren. Neu ist, dass der Verbraucher die Datenbasis selbst liefert sowie das zunehmende Ausmaß der Auswertung und die undurchsichtige Verwendung dieser Daten. Die Bedrohung für den Verbraucher entsteht, wenn er glaubt, aus freiem Willen eine Entscheidung getroffen zu haben. Dieser Beitrag zeigt: wie der Verbraucher dabei einer Kontrollillusion unterliegt; welche Heuristiken Verbraucher im Umgang mit der Preisgabe persönlicher Daten entwickelt haben; inwiefern Verbraucher von dieser Entwicklung profitieren können; welche Implikationen es für den Verbraucherschutz gibt.

Der Artikel ist eine überarbeitete Version von Michael Schleusener und Sarah Stevens (2015, siehe Seite 129).

1 Herausforderung durch zunehmende Manipulations- und abnehmende Schutzmöglichkeiten

79 Prozent der Deutsch sprechenden Onlinenutzer nutzen das mobile Internet täglich und verweilen dabei rund 160 Minuten darin (ARD/ZDF Onlinestudio 2015). Der Smartphone- oder Tablet-PC-Besitz ist von rund der Hälfte im Jahr 2014 auf 70 Prozent in 2015 angestiegen. Dabei nutzen vor allem die bis 30-Jährigen und die 30- bis 49-Jährigen mit höherem Einkommen das mobile Internet. Die Unterschiede zwischen Frauen und Männern sind dabei marginal (kaufDA Studie 2014). Diese zunehmende Verwendung mobiler internetfähiger Endgeräte befähigt Unternehmen, Daten vielfältigster Weise über die Verwender zu sammeln. Das Datensammeln und -auswerten an sich ist nicht neu: Kreditkartenunternehmen oder Versicherungen sammeln seit geraumer Zeit Daten und werten diese auch aus (Demandowsky 2010). Jedoch wurde dies bisher vergleichsweise grob gemacht, indem Bedürfnisse von Verbrauchern auf Segmentebene und nicht auf Individualebene ermittelt und adressiert wurden. Neu sind die zunehmende Intransparenz, das Ausmaß und die Geschwindigkeit, mit der Daten gesammelt, ausgewertet oder weiterverkauft werden. Verbraucher können nicht mehr nachvollziehen, welche Daten über sie und über ihr Verhalten digital erfasst, gespeichert und ggf. ausgewertet werden. Darüber hinaus erzeugen Unternehmen durch die Kombination von Daten systematisch neue Daten und Erkenntnisse, bei denen nicht einmal mehr die Herkunft oder die letztendlichen Eigentumsverhältnisse dieser Daten geklärt werden kann (Reiners und Suckfüll 2013), womit die Rechte der Betroffenen möglicherweise ausgehebelt werden. Das Weitergeben und der Weiterverkauf sind ebenso intransparent wie die Schlüsse, die über den einzelnen Verbraucher auf dieser Datenbasis gefällt werden.

Die folgende Abbildung 1 stellt zunächst dar, aus welchen Quellen die Daten kommen (innerer Ring). Es wird deutlich, dass heute neben den für den Verwender sichtbar erhobenen Daten (zum Beispiel bei Bezahlung, Kauf oder Internetsuche) sehr viele Daten ohne Wahrnehmung des Verbrauchers (etwa

Standort, Vitalzustände) für Dritte verfügbar sind. Bei den selbst offerierten Daten kann noch angenommen werden, dass diese zumindest grundsätzlich einer Steuerung durch den Verbraucher unterliegen. Für sensorerfasste Daten gilt dies nur noch bedingt und die daraus abgeleiteten Daten und Erkenntnisse können vom Verbraucher überhaupt nicht mehr kontrolliert werden. Dies führt zu einer abnehmenden Souveränität und damit steigender Verletzbarkeit der Verbraucher.

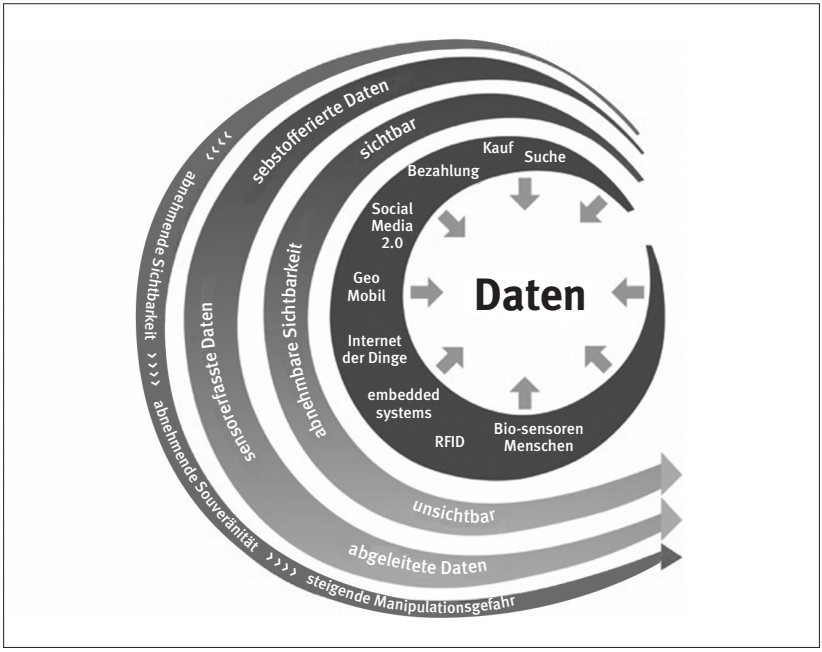


Abbildung 1: Quellen und Sichtbarkeit von Daten. Eigene Darstellung.

Im Rahmen des diesem Beitrag zugrunde liegenden Forschungsprojektes wurde eine Vielzahl von Gesprächen mit führenden Experten aus Politik, Wirtschaft und Wissenschaft geführt.

Die Experten sind sich darin einig, dass alle Arten von Datenverknüpfungen denkbar sind und, sofern technisch möglich, auch realisiert werden respektive teilweise bereits real sind. Des Weiteren herrscht Einigkeit darüber, dass diese

Entwicklung sich fortsetzen und die Informationstechnologie das Leben weiter durchdringen wird. Dies bedeutet mehr Geräte im Alltag, mehr Vernetzung, mehr Automatisierung sowie mehr „Embedded Systems“ und somit letztlich mehr Quellen, aus denen Daten gewonnen werden können.

Aus technischer Perspektive sind aus den Expertengesprächen die Dimensionen Transparenz (Intransparenz) und Schnelligkeit der aktuellen Entwicklung hervorzuheben, da diese beiden Aspekte beim Verbraucher zur Verwirrung und zur Unsicherheit führen. Besonders ist die Aussage zu erwähnen, dass die Datensouveränität der Bürger von Experten bereits als verloren eingeschätzt wird. Als Begründung wird dafür die Unsichtbarkeit des Sammelns, Auswertens und Kombinierens von Daten genannt. Die Bedrohung durch Datendiffusion wird von den Experten als steigend eingeschätzt. Sicher ist, dass die schnelle technologische Entwicklung bereits jetzt bewirkt, dass Gesetzgeber und Datenschützer dieser immer hinterher laufen. Die Anzahl der unbewussten Situationen für den Verbraucher steigt, unabhängig von einer möglichen positiven oder negativen Wirkung.

Durch den Einbezug von individuellen Kriterien wie Alter, Geschlecht, ethnischer oder religiöser Zugehörigkeit, Armut oder den Gesundheitszustand besteht die Gefahr der Diskriminierung oder gar des Ausschlusses von bestimmten Angeboten (Christl 2014). Neben diese soziodemografischen Daten treten durch die einfache Beobachtbarkeit von Verhaltensdaten, wie aufgesuchte Orte oder angewählte Webseiten sowie den Aktivitäten auf diesen Seiten, eine Vielzahl von Verhaltensdaten, die weitaus relevantere Erkenntnisse über die Verbraucher liefern.

Durch die individuelle Datenauswertung ergibt sich für den Verbraucher das Problem, dass etwaige Schwächen oder Vorlieben der Verbraucher durch Unternehmen gezielt genutzt werden können, um latente Wünsche und Bedürfnisse jedes einzelnen Verbrauchers zu wecken. Die tatsächlichen Wahlmöglichkeiten des Einzelnen können dadurch eingeschränkt werden. Dies beginnt bei der Selektion von Angeboten, die jeder einzeln bekommt, beispielsweise im Sinne einer Preisdiskriminierung wie es manche Reiseanbieter online machen, die Preise für Nutzer eines Apple-Gerätes um bis 13 Prozent (Müller 2014) anheben, und endet nicht bei lebensentscheidenden Fragen in den Bereichen Finanzen, Krankenversicherung oder Arbeitsplatz. Für Verbraucher

mit „riskanten“ Verhaltensweisen können in Zukunft höhere Versicherungsprämien anfallen. Bei einigen Autoversicherungen gibt es bereits seit Anfang 2014 die Möglichkeit der Mitnahme einer Blackbox, die das Fahrverhalten aufzeichnet. Auf Basis dieser Daten kann der Versicherungsnehmer bei entsprechender Fahrweise Rabatt auf die Versicherung erhalten. (Plusminus-Sendung 2014) Eine Datenökonomie in dieser Form ist nicht nur vor dem Hintergrund des Bundesdatenschutzgesetzes (BDSG), sondern auch vor dem Hintergrund des „Allgemeinen Gleichbehandlungsgesetzes“ (AGG) in allen Belangen zu hinterfragen. Das Allgemeine Gleichbehandlungsgesetz, als Umsetzung einer europarechtlichen Vorgabe, „verhindert oder beseitigt Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität“ (Wikipedia 2016).

Letztlich wird die Bedeutung des Themas weiter zunehmen. Die Position des Verbraucherschutzes ist dabei eher defensiv und hat bei den gegebenen strukturellen Rahmenbedingungen (Gesetzgebung, Geschwindigkeit verwaltungsbezogener Prozesse im Vergleich zu den Prozessen der Technologieentwicklung und der Internetunternehmen) kaum noch eine Chance, obwohl sie wesentlich wichtiger geworden ist.

2 Bedrohungsszenario – oder gibt es auch Vorteile?

Die konventionelle Werbung bearbeitet klassisch den Massenmarkt oder bestimmte Marktsegmente. Produktinformationen für Verbraucher auf Basis der Auswertung persönlicher Daten sind jedoch maßgeschneidert auf die individuellen Bedürfnisse der Person. Im Vergleich zur konventionellen Werbung, wo der Versuch der Manipulation für den Verbraucher offenkundig ist, wird es bei der maßgeschneiderten Ansprache schwieriger, den Manipulationsversuch zu erkennen. Folglich nimmt ein Verbraucher seine getroffene Entscheidung auf Basis von manipulierten Daten als eine Entscheidung aus freiem Willen wahr

zugunsten des Manipulierenden. Daten treten somit als neuer Produktionsfaktor auf – neben den bisherigen Produktionsfaktoren Arbeit, Kapital und natürliche Ressourcen.

Derzeit kann zum Beispiel beim Eintritt in eine private Krankenversicherung eine Gesundheitsprüfung durchgeführt werden, die möglicherweise dazu führt, dass ein Verbraucher mit Vorerkrankungen keine Versicherung erhält oder einen teureren Tarif bezahlen muss als ein vermeintlich gesunder Verbraucher. Im Hinblick auf die beschriebene Datenökonomie würden Versicherer eine bestimmte Menge an auswertbaren Daten voraussetzen, um preiswertere Angebote zu machen. Daraus folgend würde es für gesunde oder reiche Verbraucher ein anderes Internet mit anderen Angeboten geben als für Kranke oder Arme (Christl 2014). Versucht ein Verbraucher, sich und seine persönlichen Daten durch die Verweigerung einer entsprechenden Geräte- oder Programmnutzung zu schützen, würde dies auch nicht helfen, da ein zu geringer Datenpool über einen Verbraucher automatisch zu einer negativen Risikoeinschätzung führen würde. Die Frage ist, zu welchem Zeitpunkt der „Tipping Point“ erreicht ist, an dem die Bedrohung für den Verbraucher größer wird, wenn er keine Daten preisgibt.

Neben dem beschriebenen Bedrohungsszenario gibt es bereits Vorteile für den Verbraucher durch die Preisgabe persönlicher Daten: Die auf Basis der ausgewerteten Daten individuell auf den Verbraucher zugeschnittenen Informationen können für den Verbraucher insofern nützlich sein, da er nicht zunächst irrelevante Informationen von relevanten trennen muss, was eine Zeitersparnis für den Verbraucher bedeuten dürfte. Darüber hinaus ist Informationsselektion mit Aufwand bei der Hirnleistung verbunden. Möglicherweise sind manche Verbraucher gar nicht in der Lage, diese kognitive Leistung aufzubringen oder wollen diese nicht aufbringen und sind dankbar für eine Reduktion durch Auswertung ihrer persönlichen Daten durch Dritte.

So können durch Käufergemeinschaften im Internet Preisvorteile erzielt werden, die ein einzelner Verbraucher alleine nicht erhalten würde. Verbraucher erlauben beispielsweise Tageszeitungen im Internet, durch die Verknüpfung ihrer Daten personalisierte und damit von den Werbetreibenden hoch bezahlte Werbung zu schalten. Damit legen sie die finanzielle Basis für ein „kostenloses“, nicht mit Geld zu bezahlendes, Angebot, das sie sich sonst nicht alle

leisten könnten beziehungsweise würden. Das bedeutet, ein Zugang wird erst durch das Bezahlen mit Daten möglich.

Die im Rahmen der Untersuchung befragten Experten sagen, der Nutzen für den Verbraucher sei so groß, dass die Kosten der Datenpreisgabe wenig Gewicht haben. Außerdem ist die Preisgabe von persönlichen Daten meist mit indirekten Folgen behaftet, während der Nutzen für den Verbraucher direkt erkennbar ist. Auch ökonomisch gesehen ist die Auswertung von Daten nicht ausschließlich negativ zu sehen. Von den Experten wurden sowohl positive als auch negative Beispiele skizziert. Als positiv wurden der Einsatz zur Verbrechensbekämpfung sowie die Vorhersage und Analyse von Staus genannt; als negativ wurde die Manipulationsmöglichkeit des freien Willens durch Vorhersage von konsumrelevanten Verhaltensweisen auf Basis von persönlichen Daten genannt.

Des Weiteren gibt es Verbraucher, die verführt werden wollen. „Der Mensch möchte gar nicht nachdenken, sondern er will verführt werden!“ (Thinius und Untiedt 2013) Letztlich liegt es im Interesse der Verbraucher, dass ihre latenten Bedürfnisse geweckt und befriedigt werden, um ein erfülltes Leben zu haben. Auf diesen grundsätzlichen Aspekt soll an dieser Stelle jedoch nicht weiter eingegangen werden.

3 Untersuchungsdesign zur Wahrnehmung des Bedrohungsszenarios

Unter Berücksichtigung der dargestellten Ergebnisse der Expertenbefragung wurden Dimensionen der Bedrohung (im Weiteren: Eskalationsstufen) entwickelt, um diese im Rahmen einer Fokusgruppenuntersuchung einzusetzen. Die Stufen unterscheiden sich in der Menge und der Art der gesammelten Daten. Auf jeder höheren Stufe werden mehr Daten gesammelt und verwendet, um dem Verbraucher entsprechende Angebote zu offerieren. Die folgende Abbildung stellt diese Stufen im Überblick dar.

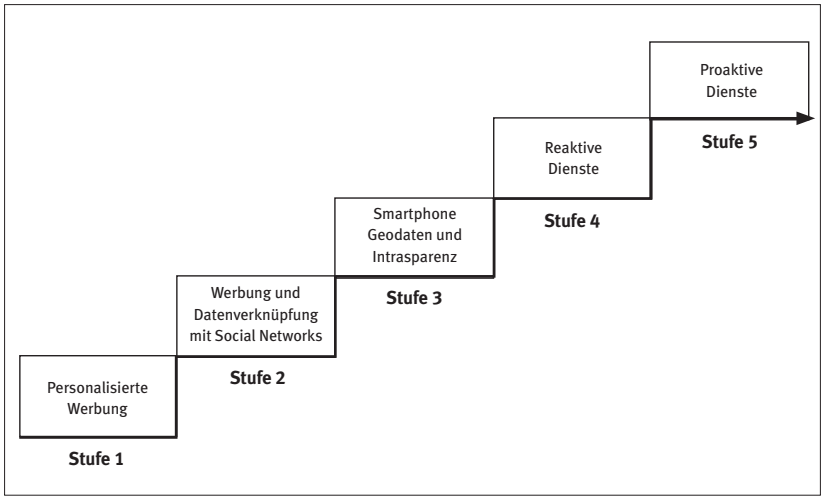


Abbildung 2: Eskalationsstufen. Eigene Darstellung.

Auf der ersten Stufe steht die personalisierte Werbung im Internet. Dabei werden Daten aus dem Surfverhalten von Verbrauchern gesammelt und darauf aufbauend auf Vorlieben und Bedürfnisse geschlossen. Darüber hinaus werden diese gesammelten Daten mit sogenannten statistischen Zwillingen kombiniert, um so dem Verbraucher passgenauer relevante Werbeinhalte zu zeigen. Daraus wird versucht, dem Verbraucher beim Surfen im Internet möglichst relevante Werbeinhalte zu präsentieren.

Auf Stufe zwei steht die Werbung in Kombination mit Daten aus Social Networks. Dabei wird auf selbst offerierte Daten zurückgegriffen, um dem Verbraucher personalisierte Werbung zu zeigen. Außerdem werden dabei „Likes" und andere Aktivitäten auf sozialen Netzwerken berücksichtigt.

Die dritte Stufe fügt Daten aus mobilen Netzwerken hinzu. Daraus entstehen zwei Dimensionen: zum einen die Dimension „Geodaten", die Standortinformationen verwendet; zum anderen die Dimension „Transparenz", die deutlich macht, dass die Verwendung von Standortinformationen für den Verbraucher zumeist nicht direkt merkbar ist.

Auf der vierten Stufe stehen die reaktiven Dienste. Damit sind Dienste gemeint, die auf unterschiedliche Datenquellen zurückgreifen (zum Beispiel Standortinformationen, Daten aus Social Networks oder Informationen über das Surfverhalten), und diese auswerten, um dem Verbraucher auf Anfrage konkrete Angebote und Antworten zu liefern. Als Beispiel kann hier die Software Siri von Apple dienen. Der Verbraucher kann Siri konkrete Fragen stellen, zum Beispiel „Wo ist die nächste Tankstelle?". Diese Software versorgt sich automatisch mit den benötigen Informationen wie Standort usw., um dem Verbraucher eine Antwort liefern zu können.

Im Gegensatz zu reaktiven Diensten wird bei den proaktiven Diensten auf Stufe fünf vom Verbraucher keine Information mehr angefordert. Stattdessen werten diese Dienste Gewohnheiten von Verbrauchern aus, um unaufgefordert konkrete Angebote zu offerieren. Ein Beispiel ist die Augmented-Reality-Software „Wikitude" (Wikipedia 2015). Vor dem Hintergrund der eingangs beschriebenen Ubiquität von Smartphones und deren Nutzung sind die Möglichkeiten, die mit diesen Geräten realisiert werden können, bei der Entwicklung der Eskalationsstufen zentral mit eingeflossen.

Es wird nun vermutet, dass mit steigender Anzahl von verknüpften Daten die Akzeptanz aus Verbrauchersicht sinkt. Da den Verbrauchern der Umfang der jeweils zugrunde liegenden Datensammelei nicht bewusst ist, wird den Teilnehmern der Fokusgruppenuntersuchung die Vorgehensweise der Unternehmen auf jeder Stufe bzw. zu jeder Maßnahme zunächst erläutert und an einem Beispiel dargestellt.

4 Der Verbraucher im Bann der Kontrollillusion

Das Ziel der Fokusgruppengespräche war damit, anhand der Eskalationsstufen herauszufinden, an welcher Stelle für den Verbraucher die Grenzen der von ihm tolerierten Datensammlung überschritten werden und er sich klar manipuliert fühlt. In Anlehnung an das Papier „Der vertrauende, der verletzliche oder der verantwortungsvolle Verbraucher? Plädoyer für eine differenzierte Strategie in der Verbraucherpolitik“ (Micklitz et al. 2015), in dem unterschiedliche Strategien für unterschiedliche Verbraucher propagiert werden, wurden die Gespräche mit drei heterogenen Gruppen konzipiert. In Gruppe 1 befanden sich junge, online-affine Probanden, gut gebildet und über einen mobilen Zugang zum Internet verfügend. Der Anteil von Frauen und Männern sollte gleich verteilt sein, Computerexperten sollten nicht darunter sein.

Gruppe 2 beinhaltet junge, online-aktive Probanden mit einfachem Bildungsniveau. In Gruppe 3 sind ältere Probanden, die auch online aktiv sind sowie stationär einkaufen, durchaus ein Smartphone nutzen, jedoch keine Computerexperten sind. Jede Gruppe bestand aus sechs bis acht Teilnehmern.

Kern der Fokusgruppengespräche war die Diskussion der jeweiligen Eskalationsstufe. Diese wurde in zwei Schritten durchgeführt: Die erste Einschätzung erfolgte auf Basis des individuell vorhandenen Wissens beziehungsweise der individuellen Annahmen bezüglich der vom Unternehmen genutzten Daten. In einem zweiten Schritt wurde den Probanden mit Hilfe von Beispielen und Live-Demonstrationen deutlich gemacht, wie und wo Daten erhoben werden und welche Auswirkungen dies auf die von ihnen wahrgenommene Darbietung von Angeboten hat.

Für die hier folgende Auswertung soll aber die erste Einschätzung des Bedrohungspotenzials im Mittelpunkt stehen. Diese Einschätzung erfolgte zunächst durch eine graphisch durch die betreffende Person selbst dargestellte Einschätzung, die anschließend in der Gruppe diskutiert wurde.

Die Ergebnisse sind in einer vereinfachten Form dargestellt:

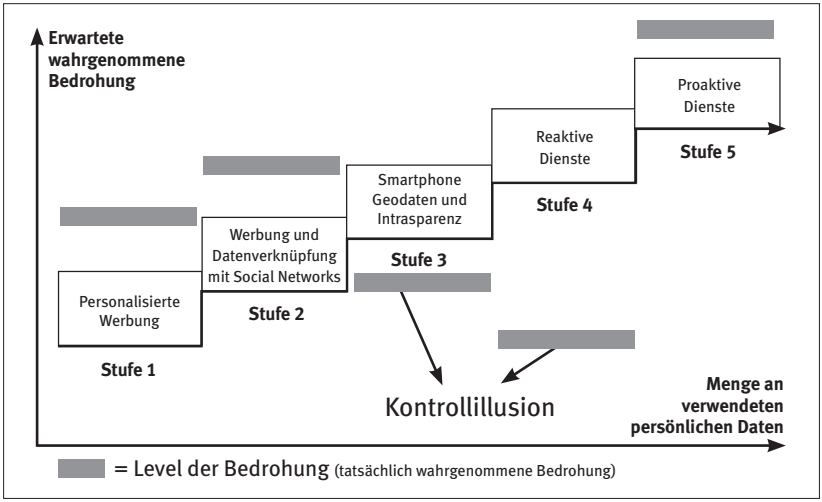


Abbildung 3: Wahrgenommene Bedrohung und Kontrollillusion. Eigene Darstellung.

Wie erwartet steigt in den ersten beiden Stufen mit zunehmender Menge der vom Anbieter verwendeten Daten die vom Verbraucher wahrgenommene Bedrohung an. Kommen Daten, auch standortbezogene, aus der eigenen Smartphone-Nutzung hinzu, dann fällt diese überraschenderweise wieder. Die Verbraucher haben einerseits das Gefühl, die Kontrolle über die Verwendung der Standortdaten zu haben, indem die GPS-Funktionalität des Gerätes ein- bzw. ausgeschaltet werden kann. Gleichzeitig ist nicht bewusst, dass auch über andere Mechanismen (zum Beispiel WLAN Ortung) der Standort ermittelt werden kann. Ferner ist die Vielzahl an gesammelten Daten in der jeweiligen Nutzungssituation nicht präsent, da der Nutzer nur einmal bei der Installation einer Anwendung (App) zugestimmt hat, dass diese Anwendung Daten sammelt bzw. bestimmte Funktionen des Telefons nutzt. Damit deutet sich bereits in dieser Stufe das fundamentale Dilemma bzw. die Kontrollillusion an. „Die *Kontrollillusion* (engl. *illusion of control*) ist die menschliche Tendenz zu glauben, gewisse Vorgänge kontrollieren zu können, die nachweislich nicht beeinflussbar sind.“ (Langer 1975) Weil der Verbraucher meint, die Situation kontrollieren zu können, wird er umso anfälliger für Manipulationen durch die Anbieterseite.

Noch deutlicher wird dies bei den reaktiven Diensten. Da der Verbraucher diese selbst anfordert, ist er der Meinung, dass er die Ergebnisse entsprechend steuern kann. Dies ist jedoch nicht der Fall, da für die Bereitstellung dieser Dienste gerade Daten und Informationen genutzt werden, die von den Systemen aus unterschiedlichen Quellen zusammengetragen wurden. Damit erfährt auch dieser Level mit seiner größeren Menge an verwendeten Daten eine Unterschätzung der wahrgenommenen Bedrohungslage und damit der möglichen Manipulation des Verbraucherinteresses. Auch hier bewirkt die Kontrollillusion, dass der Verbraucher sogar noch anfälliger wird für Manipulationen, da er der Ansicht ist, die erhaltenen Ergebnisse selbst angefordert bzw. herbeigeführt zu haben. Es ist somit die Suggestion eines freien Willens, der jedoch längst vom Anbieter beeinflusst wird. Mit Bezug auf das Papier „Der vertrauende, der verletzliche oder der verantwortungsvolle Verbraucher?“ kann trotz bewusst unterschiedlicher Zusammensetzung der Fokusgruppen keine konkrete Aussage über unterschiedlich agierende Verbrauchergruppen mit unterschiedlichen Schutzbedarfen getroffen werden.

Zusammenfassend lässt sich festhalten, dass Dinge, die die Verbraucher selbst anfragen und damit vermeintlich steuern können, eine deutlich höhere Akzeptanz aufweisen als solche, wo die Anbieter ihrerseits Vorschläge machen. Der Übergang kann schleichend sein und die Anbieter könnten sich diesen Effekt zunutze machen, wenn sie dem Verbraucher die Ausübung seines freien Willens suggerieren.

5 Nutzenüberlegungen bei der Zustimmung zur Datennutzung

Im Rahmen der Fokusgruppengespräche wurde weiterhin untersucht, wie sich Nutzer verhalten, wenn sie neue Anwendungen (Apps) auf ihren mobilen Endgeräten, insbesondere Smartphones, installieren. Im Rahmen eines solchen Installationsvorgangs fragen Apps in der Regel den Anwender nach seiner Zustimmung, bestimmte Daten und Funktionen des Gerätes nutzen zu dürfen.

Wird diese Zustimmung verweigert, dann kann die entsprechende Anwendung nicht verwendet werden. Eine differenzierte Vergabe von Zugriffsrechten ist zumindest bei standardmäßigen Android-Geräten sowie auch iOS-Geräten nicht vorgesehen; das heißt, dass entweder allen Nutzungsanfragen zugestimmt wird oder die App nicht funktioniert. Nach dem Installationsvorgang wird der Nutzer nicht mehr gefragt oder merkt auch nicht mehr, welche Aktivitäten die App gerade durchführt.

Häufig fallen damit der positive Nutzen einer App zum Installationszeitpunkt und mögliche, spätere Datenübermittlungen mit potenziell negativen Folgen zeitlich deutlich auseinander. Unter diesen negativen Folgen sollen an dieser Stelle mögliche Manipulationen des Verbraucherinteresses – und damit zunächst nicht gewünschter, ressourcenraubender Konsum – verstanden werden. Die Folgen einer Nutzung von Apps mit anschließender Konsumentenmanipulation sind damit nicht transparent und können den Nettonutzen dieser App negativ werden lassen. In der folgenden Abbildung wird dies schematisch dargestellt:

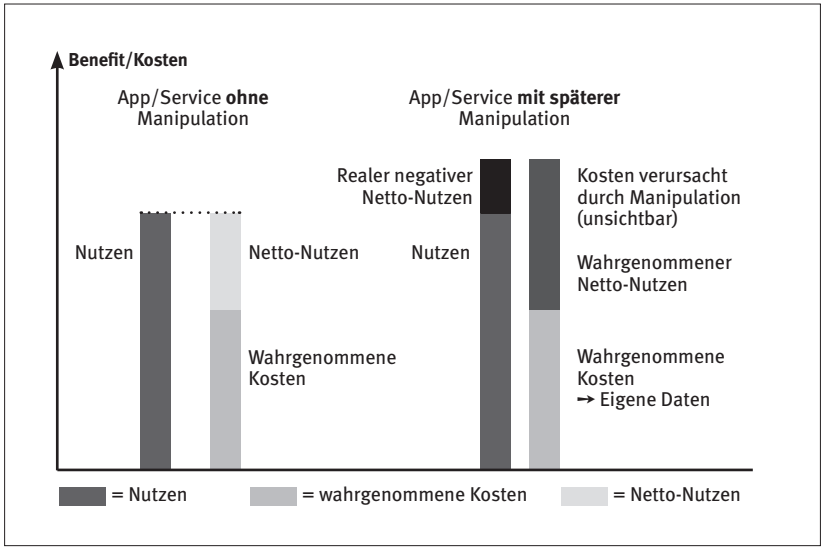


Abbildung 4: Kosten-/Nutzenbetrachtung von Apps mit und ohne Manipulation. Eigene Darstellung.

Auf der linken Seite steht eine App oder ein Internetservice, der nicht später Daten nutzt, um das Verbraucherinteresse zu manipulieren. Hier entsprechen die wahrgenommen Kosten den tatsächlichen Kosten, sodass der Netto-Nutzen richtig eingeschätzt wird. Auf der rechten Seite beispielhaft ein Angebot, bei dem die tatsächlichen Kosten höher sind als die Kosten, die bei der Installation der App wahrgenommen werden. Die tatsächlichen Kosten sind höher, da sie die nur durch Manipulation erzeugten Konsumausgaben einschließen, die ohne die spätere manipulative Wirkung der Werbung nicht getätigt worden wären. Insofern nimmt der Verbraucher einen positiven Netto-Nutzen wahr, obwohl dieser tatsächlich negativ ist. Zu dieser nicht durchschaubaren späteren Verhaltensabsicht des App-Anbieters (Hidden Intention) kommt die Tatsache des zeitlichen Auseinanderfallens der negativen und positiven Nutzenkomponenten dazu und führt zu einer Fehlentscheidung.

So überwiegen die Verlockungen und Vorteile der Angebote (Kaufen übers Netz, Nutzung sozialer Netzwerke, interessante Apps), die ganz konkret sind, die möglichen Bedenken, die Kunden haben könnten. Dazu kommt, dass sich durch Netzeffekte der Nutzen bestimmter Services und Apps permanent durch die steigende Nutzerzahl erhöht, etwa bei sozialen Netzwerken oder Messenger-Diensten. Gerade bei im sozialen Kontext relevanten Medien wirkt die damit verbundene Zugehörigkeit oder eben Abwesenheit in unmittelbar auf der persönlichen Beziehungsebene wichtigen sozialen Gruppen so stark, dass eine sehr hohe Toleranzschwelle gegenüber möglichen negativen Effekten besteht. Der faktische gesellschaftliche Ausschluss einer Person, die am Nachrichtenstrom ihrer unmittelbaren Peergroup nicht partizipiert, ist ein enormer Druck und führt dazu, mögliche Bedenken zu ignorieren.

Dazu kommt, dass die positiven Nutzenkomponenten sofort, d. h. direkt nach der Installation bzw. Anmeldung wirken. Bedenken hinsichtlich zeitlich nachgelagerter, negativer Effekte, die noch dazu recht abstrakt sind, haben demgegenüber kein Gewicht. Dies gilt umso mehr, als dass diese aufgrund ihres verdeckten und manipulativen Charakters nicht oder nur selten als solche erkannt werden und kaum ursächlich einem früheren, nutzengetriebenen Verhalten zugerechnet werden.

6 Heuristik zur Datenfreigabe durch die Verbraucher

Im Rahmen der Fokusgruppengespräche wurde weiterhin diskutiert, wie die Verbraucher sich in einer Entscheidungssituation über die Zustimmung zur Datenfreigabe für Apps verhalten. Es wurde deutlich, dass dies zwar situationsabhängig ist, sich aber dennoch unterschiedliche Entscheidungsprozesse je nach Nutzungsverhalten identifizieren lassen. Abbildung 5 zeigt in einem Überblick das mögliche Nutzungsverhalten in Verbindung mit den jeweiligen Entscheidungsprozessen. Dabei wird vielfach ein komplexer extensiver Entscheidungsprozess durch eine möglichst vereinfachende Heuristik ersetzt:

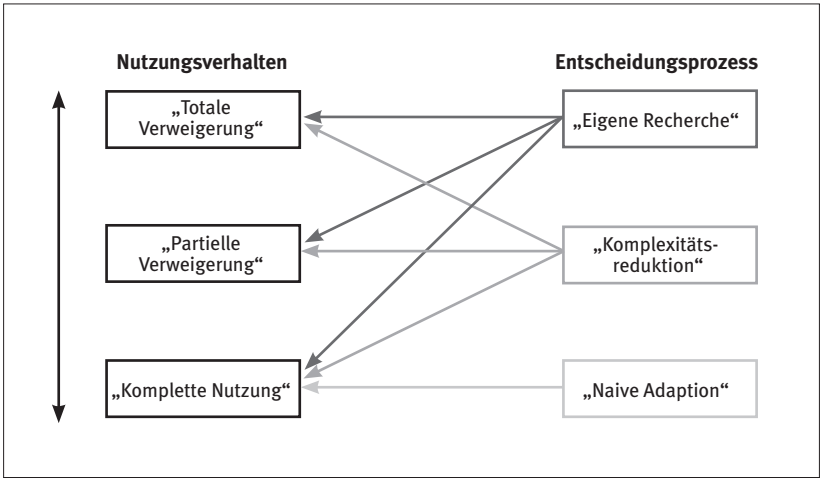


Abbildung 5: Heuristiken der Verbraucher. Eigene Darstellung.

Bei der totalen Verweigerung verzichten Verbraucher bewusst auf den Nutzen von Apps, wenn sie dafür beispielsweise den Zugriff auf das eigene Telefonbuch oder die Standortinformationen freigeben müssten. Des Weiteren werden Dienstleistungen mit scheinbar zwielichtigen Nutzungsbedingungen nicht aktiviert/verwendet. Basis einer solchen Entscheidung kann eine eige-

ne Recherche sein, bei der sich herausgestellt hat, dass der Schaden durch die betreffende App größer als der zu erwartende Nutzen ist. Häufiger jedoch dürfte dieses Nutzungsverhalten Ergebnis einer heuristischen Komplexitätsreduktion sein, bei der pauschal die Berechtigung für die Nutzung bestimmter Smartphone-Funktionen und – Daten verweigert wird, ohne weitere detaillierte Nutzenüberlegungen anzustellen.

Aus Sicht des Verbraucherschutzes scheint diese Vorgehensweise zunächst wünschenswert zu sein. Doch bei genauerer Betrachtung wird der Verbraucher zwar vor möglicher Manipulation geschützt, gleichzeitig aber auch von den positiven Wirkungen einer Nutzung ausgeschlossen, und dies möglicherweise grundlos, wenn die Entscheidung beispielsweise auf einer einfachen, komplexitätsreduzierenden Heuristik beruht. Beispielsweise könnte im Ergebnis ein Verbraucher auf die Nutzung einer App zum Benzinpreisvergleich verzichten, die ihm nicht einmal später durch Manipulation schaden will. Dies kann er durch Anwendung der einfachen, komplexitätsreduzierenden Heuristik jedoch nicht erkennen und zahlt so möglicherweise mehr für sein Benzin als nötig. Diese Folge wäre sicherlich nicht im Sinne des Verbraucherschutzes.

„Partielle Verweigerung“: Diese Methode beinhaltet das teilweise Abschalten von Funktionen respektive das bewusste Einschalten für den Moment, in dem die Funktion für die Erreichung des Nutzens benötigt wird. Zum Beispiel wird für den Einsatz des Routenplaners auf dem Smartphone für die Zeit der Nutzung die Ortung aktiviert und im Anschluss daran wieder deaktiviert. Dabei ist zu erwarten, dass dieses Verhalten vornehmlich das Ergebnis eigener Recherchen sein wird, da eine differenzierte Entscheidung und auch aktive Umsetzung der Funktionseinschränkungen einen erhöhten kognitiven Aufwand erfordert. Letztlich kommt der Verbraucher bei diesem Nutzungsverhalten in den Genuss der positiven Nutzenkomponenten, ohne allzu große negative Konsequenzen fürchten zu müssen.

Schließlich wurde in den Fokusgruppengesprächen deutlich, dass teilweise die Verbraucher auch unreflektiert (d. h. naiv) allen Bedingungen zustimmen und so jeweils Apps unbeachtlich ihres Datensammlungs- und Manipulationspotenzials nutzen. Diese Verbraucher realisieren den vollen positiven Nutzen der Apps, eröffnen gleichzeitig aber die weitesten Möglichkeiten der datenbasierten Manipulation. Ein solches Verhalten kann selbstverständlich auch das

Ergebnis einer gezielten Recherche wie auch auf Basis einer komplexitätsreduzierenden Heuristik entstanden sein.

Die Verbraucher werden zwischen den einzelnen Entscheidungsprozessen und damit auch beim Nutzenverhalten springen. Der Umfang der jeweils herangezogenen Informationen zur Entscheidungsfindung bzw. der Einsatz einer komplexitätsreduzierenden Heuristik wird davon abhängig gemacht, wie groß der Nutzen der App ist und wie wahrscheinlich das Eintreten der wahrgenommenen negativen Konsequenzen ist. So wird das Entscheidungsverhalten bei einem einfachen Daddel-Spiel eines unbekannten Entwicklers aus dubioser Quelle und mit der Anfrage nach umfangreichen Rechten versehen wesentlich weniger komplex sein und schneller zu kompletter Ablehnung führen als beispielsweise bei der Bewertung einer Benzinpreisübersicht eines Telekommunikationsanbieters mit direktem ökonomischen Nutzen. Die Fahrplan-App der Deutschen Bahn wird vermutlich bei hohem wahrgenommenem Nutzen aufgrund des offensichtlich vertrauenswürdigen Anbieters nur eine wenig komplexe Beurteilung erfahren. Damit wird deutlich, dass die Vorgehensweise bei der Beurteilung in vielen Fällen situationsbezogen ist.

Aufbauend auf diesen empirisch aus den Gruppengesprächen abgeleiteten Heuristiken und Verhaltensmustern sollen abschließend Maßnahmen für die Verbraucherpolitik entwickelt werden.

7 Implikationen für den Verbraucherschutz

Das dargestellte Nutzungsverhalten und die entsprechenden Entscheidungsprozesse bieten eine erste Grundlage für die Entwicklung von Implikationen für den Verbraucherschutz. Eine Zuordnung und einen Überblick gibt die folgende Abbildung, die anschließend näher erläutert wird:

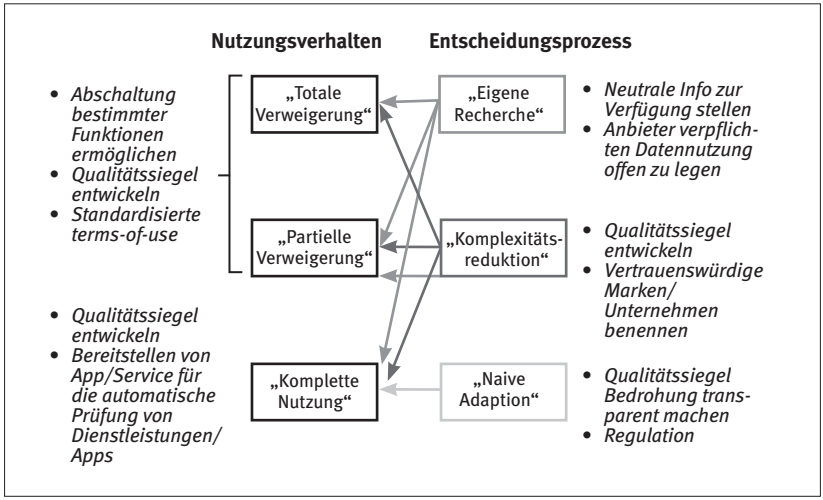


Abbildung 6: Implikationen für den Verbraucherschutz. Eigene Darstellung.

Es bestehen sowohl Ansatzpunkte für Maßnahmen bei unterschiedlichem Nutzungsverhalten wie bei den Entscheidungsprozessen.

Wie beschrieben kann eine totale Verweigerung der Nutzung auch zu ökonomischen Nachteilen führen, wenn das Manipulationspotenzial falsch eingeschätzt wird. Hier kann der Verbraucherschutz darauf hinwirken, dass bestimmte Funktionen abschaltbar gestaltet sein müssen und damit eine totale Verweigerung unnötig wird. Die Entwicklung von Qualitätssiegeln und standar-

disierten Nutzungsbedingungen mit entsprechenden, vor unberechtigter und manipulativer Datenverwendung schützenden Regelungen kann ebenfalls hilfreich sein. Dies gilt auch für den Fall der kompletten Nutzung eines Angebotes ohne Einschränkungen. Apps und Services, die sich den Regeln des Verbraucherschutzes unterwerfen, erlauben ein uneingeschränktes Nutzungsverhalten. Darüber hinaus wäre es denkbar und empfehlenswert, direkt bei der Bewertung von Apps/Services anzusetzen und durch den Verbraucherschutz eine eigene App entwickeln zu lassen, die im Moment des Installationsvorgangs einer gerade heruntergeladenen App deren Datennutzungsverhalten analysiert und unter Umständen mit Rückgriff auf entsprechende Informationen der Verbraucherschutzstellen eine Empfehlung ausgibt, ob die zur Nutzung anstehende App installiert werden soll oder nicht. Sollten damit Verbraucher von der Nutzung von Apps abgehalten werden, ohne die Gründe zu verstehen und zu teilen, kann dies allerdings auch zu Reaktanzen gegenüber der Verbraucherschutz-App und dem Verbraucherschutz selbst führen.

Auf der anderen Seite lässt sich mit weiteren und teilweise auch denselben Maßnahmen die Entscheidungsfindung der Verbraucher verbessern. Diejenigen Verbraucher, die den kognitiven Aufwand nicht scheuen, können über die Bereitstellung von neutralen Informationen erreicht werden. Dieser bislang häufig präferierte Weg setzt allerdings ein erhebliches kognitives Engagement der Verbraucher voraus, das sicherlich nur in wenigen Fällen beobachtet werden kann. Zur weiteren Unterstützung der eigenen Verbraucherrecherche könnten Anbieter über den Gesetzgeber verpflichtet werden, bestimmte Informationen zur Datennutzung offen zu legen. Letztlich ist bei allen diesen Maßnahmen eine gewisse Skepsis über ihre Wirkung angebracht, da sie eine aufwändige Form der Entscheidungsfindung voraussetzen.

Die Entwicklung von Vertrauenssiegeln („Bedingungen geprüft durch die Verbraucherzentrale“) und die Benennung vertrauenswürdiger Anbieter kommt der Trägheit der Konsumenten entgegen und folgt eher einer Vorgehensweise wie bei der Nutzung von komplexitätsreduzierenden Heuristiken.

Das Verhalten der naiven Adaption kann wiederum dadurch beeinflusst werden, dass versucht wird, die Bedrohung transparent und damit relevant zu machen. Dies wäre der Versuch, die naive Adaption in Richtung eines weniger naiven Verhaltens zu verschieben. Es ist fraglich, ob dies gelingen kann.

Wenn dies nicht der Fall ist, könnte noch eine weitergehende Regulierung der Datennutzung helfen, da anschließend auf Verbraucherseite eine weitere Auseinandersetzung mit der Problematik nicht mehr erforderlich ist. Allerdings ist hier wiederum die anfangs erwähnte unterschiedliche Geschwindigkeit von Wirtschaft/Technologie in der Umsetzung neuer Anwendungen auf der einen Seite sowie von Politik und Verwaltung auf der anderen Seite zu beachten, sodass eine echte, zeitnahe Regulierung eher unwahrscheinlich erscheint.

Literatur

AGOF (Arbeitsgemeinschaft Online Forschung e.V.) 2014. *Internet facts 2014-05.*: https://www.agof.de/download/Downloads_Internet_Facts/Downloads_Internet_Facts_2014/Downloads_Internet_Facts_2014-05/05-2014_AGOF%20internet%20facts%202014-05.pdf.

ARD/ZDF. 2015. *Internetnutzung unterwegs: Nutzungsfrequenz Internet unterwegs 2011 bis 2015*. Onlinestudie. http://www.ard-zdf-onlinestudie.de/index.php?id=527 (Zugriff: 2. März 2016).

Christl, Wolfie. 2014. *Kommerzielle digitale Überwachung im Alltag: Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data: Internationale Trends, Risiken und Herausforderungen anhand ausgewählter Problemfelder und Beispiele.* Studie im Auftrag der Bundesarbeitskammer Wien. Cracked Labs. Institut für Kritische Digitale Kultur. http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf.

Demandowsky, Maximilian von. 2010. Kreditkarteninformationen. Firmen sagen Ehescheidungen voraus. *Der Tagesspiegel* (8. Juni). http://www.tagesspiegel.de/weltspiegel/kreditkarteninformationen-firmen-sagen-ehescheidungen-voraus/1854194.html (Zugriff: 3. März 2016).

kaufDA Studie. 2014. *Studie zum Thema „Zukunft und Potenziale von standortbezogenen Diensten für den stationären Handel". Repräsentative Verbraucherbefragung der Hochschule Niederrhein mit Unterstützung des Handelsverbands Deutschland (HDE).* Berlin. http://www.bonial.de/zukunft-und-potenziale-von-standortbezogenen-diensten-fur-den-stationaren-handel/ (Zugriff: 3. März 2016).

Langer, Ellen J. 1975. The illusion of control. *Journal of Personality and Social Psychology* 32, Nr. 2: 311–28. doi:10.1037/0022-3514.32.2.311.

Markowetz, Alexander, Konrad Błaszkiewicz, Christian Montag, Christina Switala, und Thomas E. Schlaepfer. 2014. Psycho-informatics: Big Data shaping modern psychometrics. *Medical Hypotheses* 82, Nr. 4 (April 2014): 405–11. doi:10.1016/j.mehy.2013.11.030.

Micklitz, Hans-W., Andreas Oehler, Michael-Burkhard Piorkowsky, Lucia A. Reisch und Christoph Strünck. 2010. *Der vertrauende, der verletzliche oder der verantwortungsvolle Verbraucher? Plädoyer für eine differenzierte Strategie in der Verbraucherpolitik: Stellungnahme des Wissenschaftlichen Beirats Verbraucher- und Ernährungspolitik beim BMELV.* Berlin, Dezember. http://www.bmel.de/SharedDocs/Downloads/Ministerium/Beiraete/Verbraucherpolitik/2010_12_StrategieVerbraucherpolitik.pdf?__blob=publicationFile.

Müller, Peter. 2014. Mac-User sollen im Web häufig teurere Angebote erhalten. *web.de Magazin* (11. Dezember). http://web.de/magazine/digital/mac-user-web-haeufig-teurere-angebote-30271328 (Zugriff: 2. März 2016).

Plusminus-Sendung. 2014. „http://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/ndr/2014/blackbox-102.htm“ -boerse/plusminus/sendung/ndr/2014/blackbox-102.htm (Zugriff: 16. Januar 2015).

Reiners, Wilfried und Hanns Suckfüll. 2013. *Datensouveränität im Rahmen einer Personal Data* In: *Economy.* APDE – Association for Personal Data Economy. München, Juli. http://www.apde-org.eu/media/pdf/Recht%20der%20Datensouveraenitaet%20DE_2.pdf.

Schleusener, Michael und Sarah Stevens. 2015. Der digital verführte, ahnungslose Verbraucher: Verbraucherpolitisches Handeln bei wachsenden Manipulationsmöglichkeiten des Verbraucherinteresses durch unkontrollierbare Datenauswertung der Unternehmen. *Working Papers des KVF NRW,* Nr. 1. Juni. Düsseldorf: Verbraucherzentrale NRW/Kompetenzzentrum Verbraucherforschung NRW. doi:10.15501/kvfwp_1.

Thinius, Jochen und Jan Untiedt. 2013. *Events – Erlebnismarketing für alle Sinne – Mit neuronaler Markenkommunikation Lebensstile inszenieren.* Wiesbaden: Springer Gabler.

Presse- und Informationsamt der Bundesregierung. 2014. Hightech-Strategie. Der Spion in der Hosentasche. *bundesregierung.de.* http://www.bundesregierung.de/Content/DE/Artikel/2014/09/2014-09-16-hts-smartphone.html (Zugriff: 3. März 2016).

Wikipedia. 2016. Allgemeines Gleichbehandlungsgesetz. http://de.wikipedia.org/wiki/Allgemeines_Gleichbehandlungsgesetz (Zugriff: 3. März 2016).
Wikipedia. 2015. Wikitude. http://de.wikipedia.org/wiki/Wikitude (Zugriff: 3. März 2016).

Zusammenfassende Thesen

Kompetenzzentrum Verbraucherforschung NRW

DOI 10.15501/978-3-86336-912-5_7

1 Thesen zur Ausgangssituation und zum Handlungsbedarf für Forschung und Politik

These 1.1 Die Digitalisierung einer Vielzahl von Lebens- und Wirtschaftsbereichen führt zu grundlegenden Veränderungen in der Konsumlandschaft.

Die Digitalisierung verändert die Art und Weise wie wir miteinander kommunizieren, wie wir uns über Produkte und Dienstleistungen informieren, wie wir konsumieren und wie wir am wirtschaftlichen Leben partizipieren. Auch entstehen neue Produkte, Dienstleistungen und Märkte. Hierbei handelt es sich oft um Plattformmärkte („two-sided markets"). Diese sind dadurch charakterisiert, dass es a) Intermediäre gibt und dass b) zwei komplementäre und voneinander unabhängige Nutzergruppen existieren, die beide davon profitieren, dass sich möglichst viele Akteure auf der Plattform engagieren. So ermöglichen es Angebote der Sharing Economy beispielsweise, dass Menschen viel einfacher als bisher ihre Fahrzeuge, Wohnungen oder Werkzeuge miteinander teilen. Nicht alle dieser Angebote sind als neu einzustufen. Lesezirkel, Mitfahrzentralen oder Bibliotheken gab es auch schon früher. Allerdings machen es die IT-gestützten Systeme für Privatpersonen wesentlich einfacher, Ressourcen zu teilen. Sie machen das „Matching" einfacher und helfen, das Vertrauensproblem über Reputationsmechanismen zu überwinden.

These 1.2 Diese Veränderungen sind aus verbraucherpolitischer Perspektive als ambivalent zu bewerten.

Auf der einen Seite sind diese Veränderungen für Verbraucher als positiv zu bewerten. So hat die Digitalisierung den Wettbewerb in vielen Bereichen tendenziell intensiviert, Preisvergleiche einfacher gemacht und Märkte vergrößert (etwa dadurch, dass die Markteintrittsbarrieren für Unternehmen niedriger geworden sind oder weil der grenzüberschreitende Handel einfacher geworden ist). Auf der anderen Seite gibt es jedoch auch negative Entwicklungen etwa hinsichtlich des Schutzes der Privatsphäre von Verbraucherinnen und Verbrauchern, der Datensicherheit, der Urheberrechte oder hinsichtlich einer möglichen Diskriminierung von Verbraucherinnen durch Scoring-Verfahren. Die Digitalisierung und Big Data-Anwendungen führen insbesondere dazu, dass Wirtschaftsakteure viel mehr Daten über Verbraucherinnen und Verbraucher erheben und auswerten als es vielen Verbraucherinnen und Verbrauchern

bewusst ist. Hierdurch wird eine Profilbildung ermöglicht. Die mit der Profilbildung verbundenen Gefahren sind besonders groß, wenn personenbezogene Daten erhoben werden. Allerdings können auch Daten, die ursprünglich keinen Personenzug hatten, durch Kombination mit anderen Daten zu personenbezogenen Daten werden. – Besonders bei Wearables (wie Armbanduhren, Fitnessarmbändern, intelligenten Textilien, Hörgeräten und Brillen) können sehr sensible Daten erhoben werden.

These 1.3 Diese ambivalenten Veränderungen führen zu neuen gesellschaftlichen Fragen und alte Fragen werden im neuen Licht diskutiert.

Diese als ambivalent einzustufenden Veränderungen werfen eine Vielzahl von alt-bekannten und neuen Fragen auf:

- *Auswirkungen auf den Wettbewerb:* Befördern das Internet und neue digitale Dienste zumindest langfristig auch eine Monopolisierung oder zumindest eine wachsende Konzentration?
- *Schutz der Privatsphäre:* Wie kann die Privatsphäre der Verbraucherinnen und Verbraucher im digitalen Zeitalter gewahrt werden? Wie können Verbraucherinnen und Verbraucher dazu befähigt werden, sich selbstbestimmt in der digitalen Welt zu bewegen – wie müssen Einwilligungen hierzu weiterentwickelt werden? Welche Anforderungen müssen an Scoring-Verfahren gestellt werden, um sicherzustellen, dass von ihnen keine Diskriminierung ausgeht oder dass fehlerhafte Daten verwendet werden?
- *Auswirkungen der Digitalisierung auf besondere Bevölkerungsgruppen:* Führt die Digitalisierung zu prekären Arbeitsverhältnissen? Profitieren verschiedene Verbrauchergruppen unterschiedlich stark von der Digitalisierung? Wer sind die Gewinner, wer die Verlierer?
- *Gesamtgesellschaftliche Auswirkungen:* Führen diese Entwicklungen zu einer zunehmenden Individualisierung und damit auch zu einer Entsolidarisierung? Kann die Digitalisierung einen Beitrag leisten, Steuerhinterziehung – etwa durch den bargeldlosen Zahlungsverkehr – zu erschweren?
- *Sharing Economy:* Bedarf es für die Sharing Economy an spezifischen Regulierungen?

2 Aktuelle Thesen aus Wissenschaft und Forschung

These 2.1 Aus ökonomischer Sicht sind die Auswirkungen der Digitalisierung auf Verbraucherinnen und Verbraucher schwierig pauschal zu beurteilen.

Die Auswirkungen der Digitalisierung auf Verbraucherinnen und Verbraucher sind schwieriger zu bewerten als auf „traditionellen" Märkten. Denn auf der einen Seite profitieren Verbraucherinnen und Verbraucher etwa von großen Plattformen, auf denen möglichst viele Anbieter und Käufer vertreten und aktiv sind. Auf der anderen Seite entstehen jedoch gerade durch diese Größe Abhängigkeiten und Ausbeutungsgefahren. Es besteht eine Gefahr für eine aus Verbrauchersicht als kritisch zu beurteilende Monopolisierung.

These 2.2 Die IT nimmt in Fahrzeugen einen immer höheren Stellenwert ein. Hierdurch können neue Dienste zur Verfügung gestellt werden. Gleichzeitig wächst jedoch auch die Gefahr für die Integrität der Fahrzeuge.

Fahrzeuge werden immer vernetzter. Hierbei ist zwischen einer Car-to-Infrastructure (C2X) und einer Car-to-Car (C2C) Kommunikation zu unterscheiden. Mithilfe der Vernetzung sollen etwa die Verkehrssicherheit erhöht (z. B. Warnung vor herannahenden Rettungsfahrzeugen oder langsamen Fahrzeugen) und aktuelle Verkehrsflussinformationen und Mehrwertdienste bereitgestellt werden. Allerdings bergen diese neuen Kommunikationsmöglichkeiten Einfallstore für Angriffe. Hierbei sind unterschiedliche Angriffsszenarien zu unterscheiden: Abhören, Denial of Service (DoS), Manipulation, Generation, Wiedereinspielen und Relay. Für diese Angriffsmöglichkeiten existieren Gegenmaßnahmen. Allerdings steht eine konsequente Umsetzung dieser Gegenmaßnahmen vor einer Reihe von Herausforderungen: So setzen diese sehr performante IT-Systeme voraus, es muss die lange Lebensdauer von Pkw berücksichtigt werden (mehr als 20 Jahre) und es müssen länderübergreifende Lösungen entwickelt werden. Diese Hürden müssen in den kommenden Jahren überwunden werden. Grundsätzlich ist in der zukünftigen Entwicklung dafür Sorge zu tragen, dass Fahrzeuge auch bei Störungen in der Telematik fahrtüchtig sind, dass eine lange Lebensdauer der Hardware-Komponenten gegeben ist, dass die Soft- und Hardwarekomponenten integer sind, dass Schadsoftware im Auto erkannt und entfernt werden kann, dass es verifizierte

Software-Updates gibt und dass sicherheitsrelevante Komponenten im fahrzeuginternen Netzwerk speziell abgeschirmt sind.

These 2.3 Smart Meter bieten für Verbraucherinnen und Verbraucher grundsätzlich viele sinnvolle Einsatzmöglichkeiten. Allerdings können über diese Technologie auch tiefgreifende Einblicke in die Lebensgewohnheiten gewonnen werden. Solange die Missbrauchsmöglichkeiten nicht minimiert sind, werden Verbraucherinnen und Verbraucher dieser Technologie nicht vertrauen.

Die Bundesregierung hat sich das Ziel gesetzt, Smart Meter zu fördern. Durch deren Einsatz sollen Fluktuationen im Stromnetz abgefedert werden, Verbrauchern eine Möglichkeit gegeben werden, Energie gezielter zu sparen und einen besseren technischen Support zu erhalten. Allerdings können die gewonnenen Daten, wenn es sich um feingranular erhobene Daten handelt, auch für eine Profilbildung missbraucht werden. So können bei einer missbräuchlichen Verwendung auf der Grundlage der Stromverbrauchsdaten, sehr intime Rückschlüsse über Lebensgewohnheiten gewonnen werden. Auch könnten die Smart Grids Ziel von „Hacker-Angriffen" sein. Diese Angriffe könnten zu verfälschten Stromverbrauchsdaten führen oder Ausfälle von Netzsegmenten provozieren. Solche Ausfälle könnten in benachbarte Netze kaskadieren. Trotz dieser Gefahren werden Anforderungen der Datenschutzaufsichtsbehörden, die das Missbrauchsrisiko der Daten verringern sollen, heute oft nicht erfüllt. Der Erfolg eines großflächigen Rollouts dieser Technologie wird jedoch davon abhängen, dass der Datenschutz in die Technik integriert wird und dass die Datensicherheit auch bei den Grids ernst genommen wird.

These 2.4 Bürgernetzwerke und partizipative Systeme stellen Möglichkeiten dar, die Souveränität der Verbraucherinnen und Verbraucher in einer digitalen Welt zu schützen.

Auf die Herausforderungen der Digitalisierung kann durch Bürgernetzwerke und partizipative Systeme reagiert werden. Durch solche dezentralen, von Bürgerinnen und Bürger getragenen Netzwerke, kann eine Vielzahl gesellschaftlicher Fragen adressiert werden. Gleichzeitig kann die Privatsphäre der Nutzer etwa vor Datenmissbrauch oder vor ungerechtfertigten Bewertungen geschützt werden. In diesem Sinn kann die Souveränität der Verbraucherinnen

und Verbraucher durch einen kollektiven und partizipativen Ansatz gestärkt werden.

These 2.5 Untersuchungen deuten darauf hin, dass Verbraucherinnen und Verbraucher ihre Selbstkontrollmöglichkeiten hinsichtlich der Nutzung von Daten tendenziell überschätzen.

Digitale Technologien ermöglichen neue Arten von Diensten. Hierzu zählen personalisierte Werbung, Werbung und Datenverknüpfung mit Social Networks, Smartphone Geodaten, reaktive und proaktive Dienste. Die Menge der verwendeten personenbezogenen Daten steigt bei diesen Diensten an. Eine Forschungsarbeit zeigt, dass die Befragten proaktive Dienste, Werbung und Datenverknüpfung mit sozialen Netzwerken und personalisierte Werbung als am bedrohlichsten wahrnehmen. Überraschenderweise werden reaktive Dienste und Smartphone Geodaten im Vergleich nicht so bedrohlich wahrgenommen. Bei diesen beiden Diensten fallen die tatsächliche und die erwartete Bedrohung auseinander. Ein Erklärungsansatz für dieses Auseinanderklaffen ist die Kontrollillusion der Befragten. Das heißt, sie nehmen (fälschlicherweise) an, die Anwendungen besser kontrollieren zu können als es tatsächlich der Fall ist.

3 Implikationen für die Verbraucherpolitik und Verbraucherforschung

These 3.1 Da digitale Produkte und Dienstleistungen zumeist grenzüberschreitend angeboten werden, bedarf es eines zumindest europaweit einheitlichen Datenschutzrechtsrahmens.

Digitale Angebote werden zumeist grenzüberschreitend angeboten. Um sicherzustellen, dass zumindest in der Europäischen Union gleiche Verbraucherschutzstandards und ein Level Playing Field für Anbieter existieren und die Datenschutzgesetze auch einheitlich durchgesetzt werden, muss die Datenschutzgrundverordnung in diesem Jahr erfolgreich verabschiedet werden. Hierbei dürfen zentrale Konzepte wie die der Zweckbindung, Datensparsamkeit, einer freiwilligen und informierten Einwilligung, Privacy by Design und

Privacy by Default sowie ein wirkungsvolles Durchsetzungsregime nicht verwässert werden.

These 3.2 Über den Rechtsrahmen hinaus existieren noch weitere Ansätze für den Verbraucherschutz, die weiterentwickelt werden sollten.

Rechtliche Schritte allein reichen jedoch nicht aus. Daher sollte auch beim Nutzungsverhalten der Verbraucherinnen und Verbraucher angesetzt werden. Der Verbraucherschutz könnte verbessert werden, indem Verbraucherinnen und Verbraucher die Möglichkeit erhalten, bestimmte Funktionen abzuschalten; Qualitätssiegel könnten entwickelt werden, die auf einen datensparsamen Umgang mit Daten hinweisen; auch könnten standardisierte Terms of Use oder Apps für eine automatische Prüfung von Dienstleistungen entwickelt werden. Um Entscheidungsprozesse zu vereinfachen, könnten vertrauenswürdige Marken/Unternehmen ausgezeichnet werden. Auch sollten Bedrohungen transparenter gemacht werden. Hierbei ist es wichtig, die Medienkompetenzen zu stärken.

These 3.3 Weil die Digitalisierung ambivalente Auswirkungen hat, ist eine inter- und transdisziplinäre Forschung wichtig.

Da die Auswirkungen der Digitalisierung auf die Verbraucherinnen und Verbraucher sehr ambivalent sind, sollte auf Initiative und mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) eine Forschungsinfrastruktur für die gesellschaftlichen, politischen und ökonomischen Folgen der Digitalisierung und Informatisierung geschaffen werden. In der Forschung käme es darauf an, interdisziplinär und transdisziplinär zu forschen. Auch muss wegen stark divergierender Nutzerpräferenzen etwa zu Fragen des Datenschutzes sichergestellt werden, dass Nutzererwartungen und -einstellungen in der Forschung berücksichtigt werden. Daher ist ein Instrumentenmix in der Forschung wichtig: angefangen bei der Szenarienbildung, über Expertendelphi, Expertenworkshops, Fokusgruppen, Bürgerkonferenzen und Umfragen bis hin zu Fachtagungen.

Autorinnen und Autoren

Dr. Christian Bala ist wissenschaftlicher Mitarbeiter des Kompetenzzentrums Verbraucherforschung NRW (KVF NRW) der Verbraucherzentrale Nordrhein-Westfalen e. V. und Lehrbeauftragter an der Fakultät für Sozialwissenschaft der Ruhr-Universität Bochum.

Prof. Dr. Ulrich Greveler lehrt Informatik an der Fakultät für Kommunikation an der Hochschule Rhein-Waal in Kamp-Lintfort.

Prof. Dr. Dirk Helbing ist Professor für Computational Social Science an der Fakultät für Geistes-, Sozial- und Staatswissenschaften sowie Partner der Fakultät für Informatik an der ETH Zürich.

Prof. Dr. Sarah Hosell ist Professorin für Wirtschafts- und Medienpsychologie an der HMKW (Hochschule für Medien, Kommunikation und Wirtschaft), Campus Köln.

Dr. Barbara Kolany-Raiser ist wissenschaftliche Mitarbeiterin am Institut für Informations-, Telekommunikations- und Medienrecht (ITM) – Zivilrechtliche Abteilung der Westfälischen Wilhelms-Universität und Projektkoordinatorin des Projekts ABIDA (Assessing Big Data).

Prof. Dr. Kerstin Lemke-Rust lehrt angewandte Informatik mit Schwerpunkt auf Informationssicherheit an der Hochschule Bonn-Rhein-Sieg, Sankt Augustin.

Prof. Dr. Michael Schleusener ist Professor für Betriebswirtschaftslehre, insbesondere Marketing am Fachbereich Wirtschaftsingenieurwesen der Hochschule Niederrhein, Krefeld und Leiter des eWeb Research Centers an der Hochschule Niederrhein.

Wolfgang Schuldziniski ist Vorstand der Verbraucherzentrale Nordrhein-Westfalen e. V.

Impressum

Verbraucherzentrale Nordrhein-Westfalen e. V.
Mintropstraße 27, 40215 Düsseldorf
Telefon: (02 11) 38 09-0, Telefax: (02 11) 38 09-235
www.verbraucherzentrale.nrw

Die „Beiträge zur Verbraucherforschung“ werden von Dr. Christian Bala (für das Kompetenzzentrum Verbraucherforschung NRW) und Wolfgang Schuldzinski (für die Verbraucherzentrale Nordrhein-Westfalen e. V.) herausgegeben.

Die in diesem Band versammelten Beiträge geben die Meinung und die wissenschaftlichen Erkenntnisse der Autorinnen und Autoren wieder und müssen nicht mit den Meinungen und Positionen des KVF NRW, der Verbraucherzentrale NRW e. V., des MKULNV und des MIWF übereinstimmen.

Das KVF NRW ist ein Kooperationsprojekt der Verbraucherzentrale NRW e. V. mit dem Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz (MKULNV) und dem Ministerium für Innovation, Wissenschaft und Forschung (MIWF) des Landes Nordrhein-Westfalen.

verbraucherzentrale Nordrhein-Westfalen

Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur und Verbraucherschutz des Landes Nordrhein-Westfalen

Ministerium für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen

Kontakt:
Verbraucherzentrale Nordrhein-Westfalen e. V.
Kompetenzzentrum Verbraucherforschung NRW (KVF NRW)
Mintropstraße 27, 40215 Düsseldorf, Telefon: (02 11) 38 09-0
E-Mail: verbraucherforschung@verbraucherzentrale.nrw
www.verbraucherforschung-nrw.de

Lektorat:	Heike Plank
Redaktion:	Kathrin Velewald und Corinna Koch
Gestaltung:	typocepta, Köln
Gestaltungskonzept:	punkt8, Braunwald+Walter GbR, www.punkt8-berlin.de.
Druck:	rewi Druckhaus, Wissen

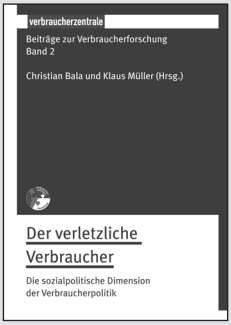
Redaktionsschluss: März 2016

Die Schriftenreihe **„Beiträge zur Verbraucherforschung“**

Band 1: Der gläserne Verbraucher

Konsum und Überwachung | Die Privatsphäre des Verbrauchers – ein Luxusgut? | Datenschutz und Cloud Computing aus Verbrauchersicht | Smart Meter: Strom sparen – Daten verschwenden? | Der gläserne Patient – Chance oder Risiko? | Bitcoin – Anonym Einkaufen im Internet?

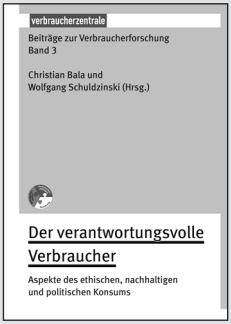
1. Auflage 2014, 128 Seiten



Band 2: Der verletzliche Verbraucher

Verletzliche Verbraucher oder Haushalte | Formen der Patientenbeteiligung | Young Professionals in der Finanzberatung | Energiearmut: Wer sind die verletzlichen Verbraucher? | Suffizienz als Anknüpfungspunkt für ein nachhaltiges Handeln des verletzlichen Verbrauchers | Der verletzliche Verbraucher im E-Commerce

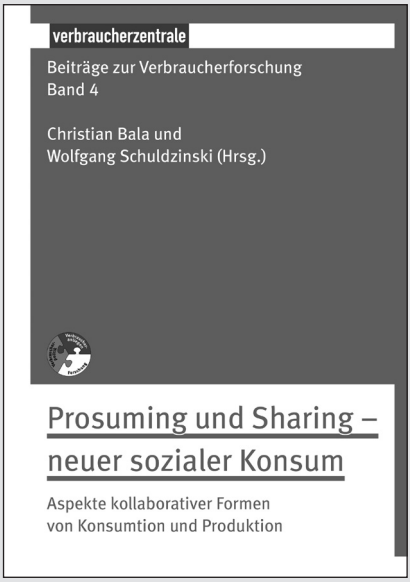
1. Auflage 2014, 160 Seiten



Band 3: Der verantwortungsvolle Verbraucher

Vom Verbraucher zum Change Agent | Konsumentenbefragungen zum Thema „Fair Trade“ und „Bio“ an Hochschulen in Nordrhein-Westfalen | „KlimaHaushalte“ erproben CO_2-arme Routinen im Alltag | Neues Dachlabel für nachhaltig erzeugte Lebensmittel | Energielabel – Fluch oder Segen für Verbraucher?

1. Auflage 2015, 136 Seiten



Band 4: Prosuming und Sharing – neuer sozialer Konsum

Neue Formen kooperativen Wirtschaftens | Alternative Konsumformen als Herausforderungen für die Verbraucherpolitik | Carsharing – ein Beitrag zu nachhaltiger Mobilität | Sharing Information – Warum wir Informationen über Online-Medien teilen | Share Economy jenseits des WWW | Genossenschaftliche Prosumermodelle

1. Auflage 2016, 184 Seiten

www.vz-ratgeber.de | www.verbraucherforschung-nrw.de
Jetzt kostenfrei als E-Book oder als Printversion (zzgl. Versandkosten)