WISO DISKURS

10/2019

Positionspapier

SICHERHEIT, SELBSTBESTIMMUNG, FAIRNESS UND TEILHABE

Handlungsempfehlungen für eine Verbraucherpolitik im digitalen Wandel

FRIEDRICH EBERT STIFTUNG

Die Friedrich-Ebert-Stiftung

Die Friedrich-Ebert-Stiftung (FES) wurde 1925 gegründet und ist die traditionsreichste politische Stiftung Deutschlands. Dem Vermächtnis ihres Namensgebers ist sie bis heute verpflichtet und setzt sich für die Grundwerte der Sozialen Demokratie ein: Freiheit, Gerechtigkeit und Solidarität. Ideell ist sie der Sozialdemokratie und den freien Gewerkschaften verbunden.

Die FES fördert die Soziale Demokratie vor allem durch:
- politische Bildungsarbeit zur Stärkung der Zivilgesellschaft;
- Politikberatung;
- internationale Zusammenarbeit mit Auslandsbüros in über 100 Ländern;
- Begabtenförderung;
- das kollektive Gedächtnis der Sozialen Demokratie mit u. a. Archiv und Bibliothek.

Die Abteilung Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung

Die Abteilung Wirtschafts- und Sozialpolitik verknüpft Analyse und Diskussion an der Schnittstelle von Wissenschaft, Politik, Praxis und Öffentlichkeit, um Antworten auf aktuelle und grundsätzliche Fragen der Wirtschafts- und Sozialpolitik zu geben. Wir bieten wirtschafts- und sozialpolitische Analysen und entwickeln Konzepte, die in einem von uns organisierten Dialog zwischen Wissenschaft, Politik, Praxis und Öffentlichkeit vermittelt werden.

WISO Diskurs

WISO Diskurse sind ausführlichere Expertisen und Studien, die Themen und politische Fragestellungen wissenschaftlich durchleuchten, fundierte politische Handlungsempfehlungen enthalten und einen Beitrag zur wissenschaftlich basierten Politikberatung leisten.

Für diese Publikation ist in der FES verantwortlich

Dr. Robert Philipps ist in der Abteilung Wirtschafts- und Sozialpolitik verantwortlich für den Gesprächskreis Verbraucherpolitik.

Positionspapier

SICHERHEIT, SELBSTBESTIMMUNG, FAIRNESS UND TEILHABE

Handlungsempfehlungen für eine Verbraucherpolitik im digitalen Wandel

Dr. Robert Philipps, Prof. Dr. Christian Thorun, Dr. Julius Rauber und Dr. Sara Elisa Kettner (Redaktion)

Mitglieder der Projektgruppe:

Inge Blask MdL > verbraucherpolitische Sprecherin der SPD-Landtagsfraktion NRW
Dr. Wolfgang Gründinger > Bundesverband Digitale Wirtschaft, European Digital Leader des World Economic Forum
Rita Hagl-Kehl MdB > Parlamentarische Staatssekretärin im BMJV
Yannick Haan > iRights.Lab GmbH, Mitglied der Medien- und netzpolitischen Kommission beim SPD-Parteivorstand
Marion Jungbluth > Mobilitätsexpertin
Dr. Robert Philipps > Leiter Gesprächskreis Verbraucherpolitik der Friedrich-Ebert-Stiftung
Sarah Ryglewski MdB > verbraucherpolitische Sprecherin der SPD-Bundestagsfraktion
Carmen Sinnokrot > Vorstandsmitglied des Forums Netzpolitik der SPD Berlin, Referentin SPD-Bundestagsfraktion (AG Recht und Verbraucherschutz)
Dr. Aleksandra Sowa > Buchautorin, Gesellschaft für Informatik e.V., Grundwertekommission der SPD und Senior Manager bei PwC GmbH WPG
Volkmar Stein > Sprecher Forum Netzpolitik der SPD Berlin (Referent Bundesministerium für Wirtschaft und Energie)
Wolfgang Teves > Referatsleiter im Bundesministerium der Justiz und für Verbraucherschutz
Prof. Dr. Christian Thorun > Geschäftsführer ConPolicy, Institut für Verbraucherpolitik
Marin Yotov > wissenschaftlicher Mitarbeiter von PStS Rita Hagl-Kehl MdB

Folgende Expert_innen haben ihre Expertise im Rahmen von Workshops und Hintergrundgesprächen eingebracht. Die FES dankt ihnen sehr herzlich für ihr Engagement:

Andre Berends > Europäische Kommission
Lina Ehrig > Verbraucherzentrale Bundesverband
Achim Klabunde > Berater beim Europäischen Datenschutzbeauftragten
Henry Krasemann > Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Julia Krüger > netzpolitik.org und wissenschaftliche Mitarbeiterin von MdB Saskia Esken
Prof. Marian Margraf > Freie Universität Berlin
Diego Naranjo > European Digital Rights
Paul Nemitz > Europäische Kommission
Michael Neuber > Bundesverband digitale Wirtschaft
Frederick Richter > Stiftung Datenschutz
Teemu Ropponen > MyData Initiative
Dr. Christoph Schmon > Bureau Européen des Unions de Consommateurs (BEUC)
Eva Sinkovic > Europäische Kommission
Prof. Gerald Spindler > Universität Göttingen
Dr. Claus-Dieter Ulmer > Deutsche Telekom
Prof. Christiane Wendehorst > Universität Wien
Lennart Wetzel > Microsoft Deutschland

Dieses Positionspapier wurde auf Grundlage von Beratungen einer Projektgruppe der Friedrich-Ebert-Stiftung erstellt. Die Inhalte des Papiers stellen nicht zwingend und in allen Punkten die Meinung jedes Mitglieds der Projektgruppe dar. Die Teilnehmenden haben als Privatpersonen an diesem Projekt mitgewirkt. Die FES dankt ihnen sehr herzlich für ihr Engagement.

INHALT

1

EINLEITUNG UND ZUSAMMENFASSUNG

Die Digitalisierung verändert nicht nur unser Konsumverhalten, sondern transformiert ganz grundlegend unseren Alltag als Verbraucher_innen. Produkte der Haushaltselektronik, Kinderspielzeuge oder Entertainment-Geräte werden intelligenter und sind immer häufiger durchgehend mit dem Internet verbunden. Parallel dazu entwickeln sich neuartige Dienstleistungen wie Sprachassistenzanwendungen, Chatbots und Robo-Advice-Systeme, die etwa in der Anlageberatung genutzt werden. Diese neuen Produkte und Dienstleistungen erweitern zwar unsere Konsummöglichkeiten und gehen auch häufig mit einem erhöhten Komfort einher. Gleichzeitig werfen diese grundlegenden Transformationen für die Verbraucherpolitik neue wichtige Fragen auf. Sie lassen sich in drei wesentlichen Themenfeldern bündeln:

- **Sicherheit**: Ein zentrales Ziel der Verbraucherpolitik besteht darin, die Sicherheit von Produkten zu gewährleisten, damit Verbraucher_innen vor Gefahren für ihre Gesundheit geschützt sind. Es stellt sich jedoch die Frage, ob die bestehenden Schutzvorschriften des Produktsicherheits- und Haftungsrechts, die in Zeiten entwickelt wurden, als Produkte noch nicht smart waren, zeitgemäß sind oder ob sie weiterentwickelt werden müssen.
- **Selbstbestimmung**: Im Zuge der Digitalisierung basieren immer mehr Geschäftsmodelle sowie Produkte und Dienstleistungen auf der Verarbeitung von personenbezogenen Daten. Diese Daten ermöglichen eine Personalisierung von Angeboten. Sie stellen gleichzeitig jedoch ein Risiko dar, wenn Verbraucher_innen zunehmend durchleuchtet und gläsern werden. Für die Verbraucherpolitik ergibt sich daraus die Frage, wie sich künftig gewährleisten lässt, dass das Grundrecht auf informationelle Selbstbestimmung auch in einer immer weitreichenderen digitalen und vernetzten Welt effektiv verwirklicht werden kann.
- **Fairness und Teilhabe**: Verfahren der künstlichen Intelligenz (KI) stellen eine digitale Schlüsseltechnologie dar und sind vielseitig einsetzbar. Doch auch hier stellt sich die Frage, wie Verbraucherpolitik dafür sorgen kann, dass KI-Verfahren fair und nachvollziehbar eingesetzt werden. Ebenso muss sichergestellt werden, dass alle gesellschaftlichen Gruppen von diesen Verfahren profitieren.

Der hier vorliegende Bericht gibt als Antwort auf diese Fragen konkrete verbraucherpolitische Empfehlungen. Sie wurden durch eine Projektgruppe erarbeitet, die sich auf Einladung der Friedrich-Ebert-Stiftung im Jahr 2018 mit diesen grundsätzlichen Herausforderungen für die Verbraucherpolitik befasst hat. Die Gruppe bestand aus Vertreter_innen ganz unterschiedlicher Organisationen und veranstaltete mehrere Expertenworkshops zu den oben genannten Themen. Die wichtigsten Empfehlungen lauten:

1. In einigen Bereichen ist es notwendig, das **bestehende Recht fortzuentwickeln** und an die heutigen Realitäten der Digitalwirtschaft anzupassen.

   - Es sollte ein **umfassendes IT-Produktsicherheitrecht für vernetzte Produkte** auf europäischer oder nationaler Ebene geschaffen werden. Hier sollten insbesondere Mindestsicherheitsstandards bezüglich Verschlüsselung, Authentisierung und einer Pflicht des Herstellers zur Bereitstellung von Updates festgelegt werden.
   - Um ökonomische Anreize zur Erhöhung des IT-Sicherheitsniveaus zu schaffen und Verbraucher_innen im Schadensfall zu kompensieren, sollten die **Haftungsregeln** auf die Höhe der Zeit gebracht werden. So sollte der **Schadensbegriff** im **Produkthaftungsgesetz** auch Persönlichkeitsrechtsverletzungen umfassen und der **Produktbegriff** um Software erweitert werden. Bei autonomen Systemen sollte explizit eine **Gefährdungshaftung der Hersteller** eingeführt werden. Diese Gefährdungshaftung könnte überdies mit einer **Zwangsversicherung** (plus Haftungsdeckel) für die Hersteller kombiniert werden.
   - Der Hersteller sollte verpflichtet werden, für die üblicherweise zu erwartende Lebensdauer des Produktes **Updates** zur Gewährleistung der IT-Sicherheit bereitzustellen. Zudem sollte die Verpflichtung bestehen, die Verbraucher_innen darüber zu informieren, wie lange das Produkt konkret mit Updates versorgt wird.

- Zur Verbesserung der **informationellen Selbstbestimmung** sollte die Bundesregierung Vorschläge für **Piktogramme** entwickeln und diese verbindlich machen und Maßnahmen umsetzen, damit **Datenschutzerklärungen maschinenauslesbar** werden. Zudem sollte ein **Regulierungsrahmen für Datentreuhänder** geschaffen werden, um deren Unabhängigkeit und Neutralität sicherzustellen.
- Um **Fairness und Teilhabe bei künstlicher Intelligenz** und automatisierten Entscheidungen zu gewährleisten, sind gesetzliche Regelungen zu schaffen, die die **Transparenz** für Verbraucher_innen sicherstellen, **Diskriminierung** ausschließen, die **Individualisierung von Preisen** beschränken und die **Aufsicht** stärken.
- Insbesondere sollte die Bundesregierung den unterschiedlichen bereits existierenden sektoralen **Behörden** die **Kompetenzen** geben, KI-basierte Entscheidungen in dem jeweiligen Wirtschaftsbereich auf Rechtmäßigkeit zu überprüfen und ggf. einzuschreiten. Überdies sollte eine **Digitalagentur** im Sinne eines Kompetenzzentrums geschaffen werden, um Kompetenzen in diesem Bereich zu bündeln und um andere Behörden in ihrer Arbeit zu unterstützen.
- Anbieter sollten Verbraucher_innen über den **Einsatz KI-basierter Verfahren** informieren, solange diese eine Verbraucherrelevanz haben. Auch sollten Verbraucher_innen die wesentlichen Merkmale, auf deren Basis sie gescort werden, sowie deren Gewichtung auf verständliche und nachvollziehbare Weise offengelegt werden.

2. Damit Recht nicht nur auf dem Papier steht, muss Sorge dafür getragen werden, dass es auch effektiv im kollektiven Verbraucherinteresse durchgesetzt wird – sei es durch staatliche oder private Akteure. Die **Rechtsdurchsetzung** ist für einige der neuen Herausforderungen jedoch unzureichend aufgestellt. Mangelnde Zuständigkeiten sowie unzureichende fachliche Kompetenzen und Ressourcen bei Aufsichtsbehörden und Verbraucherorganisationen sind nur einige der Beispiele, die einem effektiven Vollzug derzeit in der digitalen Welt entgegenstehen.

   - Um die **Rechtsdurchsetzung** im Bereich der IT- und Produktsicherheit zu verbessern, sollten die zuständigen **europäischen und nationalen Aufsichtsbehörden** (Enisa, BSI, KBA, BNETZA) in ihren Kompetenzen, Mandaten und Ressourcen gestärkt werden.
   - Die Länder sollten die Haushaltsmittel für die **Datenschutzbehörden** und zivilgesellschaftlichen **Verbraucherschutzverbände** aufstocken. Zudem sollten Maßnahmen umgesetzt werden, um die aufsichtsrechtlichen Kompetenzen im Datenschutz, die aktuell auf 16 Bundesländer und den Bund verteilt sind, zu bündeln. Eine solche Bündelung sollte über einen **Staatsvertrag** zwischen den Ländern umgesetzt werden.
   - Zur Gewährleistung von **Fairness und Teilhabe bei künstlicher Intelligenz** und automatisierten Entscheidungen sollte die Bundesregierung die existierenden sektoralen **Behörden** mit einer Kompetenz ausstatten, KI-basierte Entscheidungen auf Rechtmäßigkeit zu überprüfen und ggf. einzuschreiten. Auch sollte sie eine **Digitalagentur** schaffen, die die sektoralen Behörden im Sinne eines Kompetenzzentrums in ihrer Arbeit unterstützt.

3. Die Digitalisierung ermöglicht es der Verbraucherpolitik, neue Wege zu gehen. Ansätze, die den **Verbraucherschutz durch Technik** voranbringen, sollten deshalb viel systematischer als bislang gefördert werden. Digitale Technologien können etwa dafür genutzt werden, die Teilhabe zu fördern oder Kosten zu senken. Auch können viele Risiken, die mit der Digitalisierung einhergehen, durch den Einsatz digitaler Technologien abgemildert werden.

   - Schlüsseltechnologien zur Förderung der Selbstbestimmung wären zum einen **Privacy Enhancing Technologies wie Anonymisierungs- und Pseudonymisierungsverfahren** sowie **Privacy Bots**, die es Verbraucher_innen erleichtern, ihre informationelle Selbstbestimmung im digitalen Alltag zu behaupten. Auf der anderen Seite zählen hierzu auch **Personal Information Management Systems (PIMS)**, bei denen unabhängige Intermediäre das Datenmanagement im Auftrag der Verbraucher_innen übernehmen. Die Bundesregierung sollte solche Ansätze fördern und rechtliche Mindeststandards für PIMS setzen, um deren Unabhängigkeit und Neutralität zu gewährleisten.
   - Im Bereich der künstlichen Intelligenz sollte die Bundesregierung **Open-Data-Ansätze fördern**, um es gemeinwohlorientierten Organisationen zu ermöglichen, KI-basierte Ansätze zu entwickeln und in den Markt zu bringen.

4. Gerade aufgrund der hohen Entwicklungsgeschwindigkeit und des globalen Kontextes, in denen digitale Produkte und Dienstleistungen entwickelt und angeboten werden, ist es entscheidend, dass **Unternehmen ihrer digitalen gesellschaftlichen Verantwortung konsequent nachkommen**.

   - Dies bedeutet etwa, dass Unternehmen bereits im Design ihrer Produkte wichtige **Prinzipien wie die des Privacy, Security und Ethics by Design und by Default** mitberücksichtigen. Auch beinhaltet dies, dass Unternehmen Ansätze nutzen, um komplexe Datenschutzerklärungen verständlicher zu machen (etwa durch Piktogramme oder eine einfache Sprache), oder indem sie Privacy Enhancing Technologies in den Markt bringen, die den Selbstdatenschutz der Verbraucher_innen fördern. Es gilt daher, den Diskurs zur **Corporate Digital Responsibility** zu fördern und Schrittweise verbindlich zu machen.

5. Die **Verbraucherforschung** ist auszubauen, insbesondere um verbraucherschützende Technologien zu fördern und

zu entwickeln. Hierzu gehören Ansätze im Bereich des Datenschutzes und der Differential Privacy, der einfach zu nutzenden Ende-zu-Ende-Verschlüsselung sowie zu den oben genannten Designprinzipien.

6. Die **Verbraucherbildung** muss mit der Digitalisierung Schritt halten, sodass Verbraucher_innen überhaupt erst über die notwendigen Kompetenzen verfügen, die neuen technischen Entwicklungen beurteilen zu können und sie verantwortungsvoll zu nutzen.

2

PRODUKTSICHERHEIT IN DER DIGITALEN WELT

Ob beim Kauf von Lebensmitteln, Spielzeug oder einem neuen Haushaltsgerät – Verbraucher_innen müssen darauf vertrauen können, dass die angebotenen Produkte sicher sind und keine Gefahr für ihre Gesundheit darstellen. Die Produktsicherheit stellt dementsprechend ein Kernanliegen der Verbraucherpolitik dar.

Um die Produktsicherheit und Kompensation im Schadensfall zu gewährleisten, existiert in Deutschland eine Reihe gesetzlicher Regelungen. Das Produktsicherheitsgesetz (ProdSG) sowie eine Vielzahl nachgelagerter Produktsicherheitsverordnungen für unterschiedlichste Produkte definieren wesentliche Sicherheitsanforderungen. Sicherheitsgütesiegel wie das GS-Zeichen (geprüfte Sicherheit) dokumentieren, dass ein Produkt den Anforderungen entspricht. Wenn Verbraucher_innen durch ein fehlerhaftes Produkt geschädigt werden, greift gegenüber dem Hersteller die Produzentenhaftung – auch deliktische Produzentenhaftung genannt (geregelt in § 823 BGB). Demnach ist der- oder diejenige zu Schadensersatz verpflichtet, der oder die vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines oder einer anderen widerrechtlich verletzt. Überdies können aus der Verletzung einer Norm des Produktsicherheitsgesetzes Haftungsansprüche aus dem Deliktsrecht resultieren. Das Produkthaftungsgesetz (ProdHaftG) sieht ferner eine verschuldensunabhängige Haftung der Hersteller bei fehlerhaften Produkten vor. Diese sogenannte Gefährdungshaftung tritt ein, wenn Gesundheit oder Eigentum von Verbraucher_innen durch ein fehlerhaftes Produkt geschädigt werden. Gegenüber dem Hersteller können zudem vertragliche Ansprüche aus einem Garantieversprechen bestehen. Vor allem aber existiert gegenüber dem oder der Verkäufer_in die Gewährleistung bzw. Mängelhaftung. Diese greift in dem Fall, in dem ein_e Verkäufer_in gegen seine bzw. ihre vertragliche Pflicht verstößt und statt einer einwandfreien Ware eine mangelhafte Ware liefert.

Historisch gesehen sind diese Produktsicherheits- und Haftungsvorschriften für Probleme der physischen bzw. technischen Sicherheit (Brandgefahr, verschluckbare Kleinteile oder Stromschlag) entwickelt worden, aber nicht für solche der IT-Sicherheit bzw. der Sicherheit in der vernetzten Welt. Sicherheitsprobleme bei neuen technischen Entwicklungen sind mit den bisherigen rechtlichen Regelungen daher nicht in jedem Fall ausreichend adressiert und werden von Unternehmen bisher nicht genügend beachtet. Das betrifft immer mehr ursprünglich analoge Produktgruppen wie Kinderspielzeuge, Haushaltsgeräte, ebenso wie Autos oder Medizinprodukte, die inzwischen digitalisiert, also mit softwarebasierten, neuen Funktionalitäten ausgestattet, vernetzt und gegebenfalls internetfähig gemacht werden. Zudem entstehen ganz neue Produktgruppen, digitale Sprachassistenzsysteme etwa.

Mit der Digitalisierung und Vernetzung von Produkten steigt auch deren Anfälligkeit für Funktionsstörungen und IT-Sicherheitslücken. Für Verbraucher_innen können diese Anfälligkeiten erhebliche negative Auswirkungen haben. Sie reichen von Ausspähungen bzw. Verletzungen des Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung über Einbußen der Funktionalität bis hin zu Vermögensschäden (zum Beispiel durch Datenverlust) oder – im Extremfall – Gefahren für Leib und Leben, etwa wenn ein vernetztes Fahrzeug nicht ordnungsgemäß funktioniert.

Die intensive Marktdurchdringung steht bei vielen dieser vernetzbaren und vernetzten Produktgruppen aber noch bevor (eco/Arthur D. Little 2017). Dadurch bietet sich die Chance, potenzielle Fehlentwicklungen frühzeitig zu identifizieren und Handlungsoptionen für mehr Sicherheit in der digitalen Welt rechtzeitig zu entwickeln. Auch die Bundesregierung sieht die Handlungsnotwendigkeit, wenn sie im Koalitionsvertrag ankündigt, das Produktsicherheitsrecht zu novellieren und eine gewährleistungsähnliche Herstellerhaftung zu prüfen, um die IT-Sicherheit in verbrauchernahen Produkten zu erhöhen.

2.1 EIN GROSSES SPEKTRUM AN DIGITALEN UND VERNETZTEN PRODUKTEN ENTSTEHT

Die Bandbreite verbrauchernaher Produktgruppen, die digitalisiert und vernetzt werden, ist sehr groß. So gibt es etwa für das Smarthome vernetzte Entertainment-Geräte (intelligente

Lautsprecher, Smart-TVs, Spielkonsolen, Kinderspielzeug oder Gesellschaftsspiele), vernetzte Haushaltsgeräte (Mikrowellen, Kühlschränke oder Waschmaschinen) oder vernetzte Regelungs- und Sicherheitsinstrumente (Thermostate, Stromzähler, Lampen, Schlösser oder Überwachungskameras). Insgesamt wird erwartet, dass die Anzahl an Smarthome-Systemen in der Europäischen Union von 12 Millionen im Jahr 2017 auf 30 Millionen im Jahr 2019 ansteigen wird (Deutsche Telekom/Qivicon 2015).

Auch für die Nutzung außerhalb der eigenen vier Wände gibt es vernetzte Produkte, beispielsweise Smartwatches oder Fitness-Tracker. In Nischenmärkten existiert auch bereits vernetzte Kleidung, bei der zum Beispiel über einen Chip in der Jacke das Smartphone gesteuert wird (Horizont 2017). Vernetztes Werkzeug wiederum kann mithilfe des Smartphones gefunden werden (THIS Magazin 2017). Expert_innen sehen auch ein großes Potenzial im Bereich der vernetzten Mobilität und hier insbesondere beim vernetzten Auto. Es wird erwartet, dass im Jahr 2035 zwischen 28 und 48 Millionen autonome Fahrzeuge produziert werden (Oliver Wyman Analysis 2015). Dadurch entsteht ein großes Potenzial an neuen vernetzten Diensten und Anwendungen rund um das „Connected Car" (Süddeutsche Zeitung 2017).

2.2 DAS ENGAGEMENT VON UNTERNEHMEN IN DIE IT-SICHERHEIT IST OFT UNZUREICHEND

Neben vielen Erleichterungen und Vorteilen, die das Internet der Dinge (IoT) mit sich bringt – z. B. einer zentralen Steuerung der vernetzten Geräte von einem beliebigen Ort aus –, gibt es aber auch eine Reihe von Problemen bezüglich der IT-Sicherheit, die durch die Digitalisierung und Vernetzung entstehen. Viele Hersteller von internetfähigen oder vernetzbaren Geräten sehen IT-Sicherheit bislang nicht als wichtiges Kriterium für die Verkaufschancen eines Produkts an. Laut einer Studie von Crisp Research im Auftrag von TÜViT aus dem Jahr 2017 befinden zwei Drittel der befragten Unternehmen, dass die Produktperformance und der Preis im Zweifelsfall wichtiger als die IT-Sicherheit sind (TÜViT/Crisp Research 2017). Zudem sind viele Hersteller bisher analoger Produkte im Bereich IT-Sicherheit unerfahren, mit der Konsequenz, dass IT-Sicherheit nicht von Anfang an bei der Produktentwicklung mitgedacht wird (Kettner et al. 2018a). Deshalb werden Sicherheitsupdates häufig nicht ausreichend und zeitnah angeboten, wodurch entdeckte Sicherheitslücken nicht schnell genug geschlossen werden können (BSI 2017). Außerdem sind viele Schnittstellen unzureichend gesichert und verschlüsselt: Sie werden häufig nicht mit Passwörtern geschützt und wenn, sind die Passwörter häufig zu einfach („1111", „1234" usw.), was Kriminellen potenzielle Cyberangriffe erleichtert (BSI 2017). Auch werden die Bedürfnisse, Verhaltensweisen und technischen Fähigkeiten der Benutzer_innen, die für eine adäquate Umsetzung von IT-Sicherheitszielen oft essenziell sind, nicht ausreichend in der Produktentwicklung berücksichtigt (Margraf/Pfeiffer 2015).

2.3 UNZUREICHENDE IT-SICHERHEIT KANN GRAVIERENDE FOLGEN FÜR DIE VERBRAUCHER_INNEN HABEN

Die beschriebenen Sicherheitsmängel können bei vernetzten Produkten fatale Folgen haben. Über sogenannte Man-in-the-Middle-Angriffe kann beispielsweise in die Kommunikation zwischen zwei Geräten oder Systemen eingedrungen werden, um die gesendeten Signale und Nachrichten abzuhören oder zu verändern (BSI 2016). Kriminelle können dadurch persönliche Daten stehlen und für illegale Zwecke – von unerlaubter Werbung bis hin zum Identitätsdiebstahl – missbrauchen oder aber die Funktionen der vernetzten Geräte manipulieren. Dies kann nicht nur zu finanziellen und materiellen Schäden führen – wie bei einem Einbruch durch das Hacken eines vernetzten Türschlosses oder bei Applikationen mit Bezahlfunktion. Auch körperliche Schäden sind zu befürchten, wenn etwa das automatische Bremssystem eines vernetzten Autos manipuliert (Frankfurter Allgemeine Zeitung 2017) oder eine Attacke auf vernetzte Herzschrittmacher durchgeführt (Spiegel Online 2017) wird.

Vernetzte Geräte können auch illegal genutzt werden, ohne dass es die Betroffenen merken. So können vernetzte Geräte beispielsweise durch Kriminelle gekapert und in einem sogenannten Botnetz zusammengeführt werden. Durch solche Botnetze können wiederum großangelegte Cyberangriffe auf Unternehmen oder staatliche Institutionen durchgeführt werden. Im Jahr 2017 sollten etwa bei einem Angriff auf 1,25 Millionen Kund_innen der Deutschen Telekom deren Router in das Botnetz Mirai integriert werden, um dem Konkurrenten eines liberianischen Telekommunikationsunternehmens zu schaden (t3n 2018).

Laut Meinung von Expert_innen werden für solche Angriffe zukünftig vermehrt technisch einfache Geräte mit CPU und Internetanschluss (wie z. B. Saugroboter) genutzt, da sie im Vergleich zu herkömmlichen Produkten wie Computer oder Router oftmals schlecht gesichert und relativ einfach zu hacken sind (C't 2018).

2.4 RECHTLICHER SCHUTZ DER VERBRAUCHER_INNEN IST LÜCKENHAFT

Eine unzureichende IT-Sicherheit von vernetzten Geräten kann also zu gravierenden Schäden für die Verbraucher_innen führen, und aktuell bestehen solche ausreichenden Schutzvorschriften leider nicht.

2.4.1 RECHTLICHE VORGABEN ZUR IT-SICHERHEIT BEI VERNETZTEN PRODUKTEN

Das im Jahr 2015 in Kraft getretene IT-Sicherheitsgesetz bezieht sich insbesondere auf IT-Systeme der Wirtschaft, vor allem bei kritischen Infrastrukturen wie etwa der Strom- und Wasserversorgung sowie große Krankenhäuser. Die Sicherheit vernetzter verbrauchernaher Produkte wird hier bisher jedoch weitgehend ausgeklammert. Zwar enthalten einschlägige EU-Richtlinien (EU-Funkanlagenrichtlinie, EU-Niederspannungsrichtlinie) und das sie umsetzende Produktsicherheitsgesetz mit diversen sektoralen Verordnungen Vorgaben

zur IT- und Datensicherheit. Diese sind jedoch sehr allgemein gehalten[1] und zudem bisher weder durch delegierte Rechtsakte noch durch den Stand der Technik wiedergebende Normen unterlegt.

2.4.2 HAFTUNG UND KOMPENSATION BEI FEHLERHAFTEN VERNETZTEN GERÄTEN

Auch die Haftungsregeln bei fehlerhaften IoT-Geräten sind unzureichend. In der Konsequenz führt das dazu, dass Unternehmen keine wirksamen Anreize haben, in die IT-Sicherheit ihrer Produkte zu investieren. Aus rechtlicher Sicht gilt es, zwischen drei verschiedenen Arten von Schäden und deren Folgen für die Nutzer_innen vernetzter Produkte zu unterscheiden:

Erstens können Schäden an Gesundheit und Eigentum von Verbraucher_innen entstehen. Wird etwa ein Türschloss, das über einen Cloud-Service gesteuert wird, gehackt und hierdurch ein Einbruch ermöglicht, entstehen Schäden am Eigentum (durch Einbruchsschäden und Diebstahl) und gegebenenfalls auch Personen- bzw. Körperschäden.

Schadensersatzansprüche gegenüber dem oder der Verkäufer_in wegen Schäden nicht am Vertragsgegenstand selbst scheiden in der Regel aus juristischen Gründen aus, weil hierfür zum Beispiel die Kenntnis des Verkäufers oder der Verkäuferin von der nicht sicheren Software Voraussetzung ist. Darüber hinaus ist die rechtliche Einordnung des Vertrages (Kaufvertrag, Dienstvertrag, Mietvertrag oder typengemischter Vertrag?) bei vernetzten Geräten und intelligenten Techniksystemen und der daraus resultierenden Verbraucherrechte oft nur juristischen Expert_innen möglich.

Auch Ansprüche gegen den Hersteller greifen häufig nicht. So ist höchstrichterlich nicht geklärt, ob Software, die Cloud-basiert bereitgestellt wird, überhaupt ein Produkt im Sinne des § 2 ProdHaftG darstellt. Für Eigentumsschäden gilt zudem ein Selbstbehalt in Höhe von 500 Euro. Ein Produkt muss im Übrigen nur beim Inverkehrbringen dem Stand der Technik entsprechen; später erkannte Sicherheitslücken führen daher nicht zu Haftungsansprüchen auf der Grundlage des Produkthaftungsgesetzes. Eine ausdrückliche Verpflichtung zur Lieferung von Updates gegenüber dem Hersteller besteht nicht. Nach aktueller Rechtslage können Verbraucher_innen in einem solchen Fall wohl weder den Händler noch die Hersteller des Türschlosses oder den Cloud-Software-Dienstleister haftbar machen.

Zweitens können für Verbraucher_innen Schäden durch den Verlust oder den Missbrauch von Daten entstehen. Beispiele hierfür sind etwa das Löschen von Urlaubsfotos oder der Diebstahl und die Veröffentlichung von intimen Fotos. Hier besteht das Problem, dass solche immateriellen Schäden nicht vom geltenden Produkthaftungsgesetz erfasst und andere Haftungsmöglichkeiten (vertraglich oder deliktisch) fast nie gegeben oder durchsetzbar sind (Spindler 2007a).

Drittens können für Verbraucher_innen Vermögensschäden entstehen. IoT-Geräte bestehen aus Hard- und Softwarekomponenten. Die Software kann in das Gerät eingebaut sein, aber auch als externes Zusatzangebot (z. B. Steuerungs-App) für die Nutzung eine wichtige Bedeutung haben. Wenn der Anbieter der Software etwa seinen Betrieb einstellt, kann das IoT-Produkt seine Funktionsfähigkeit einbüßen oder zumindest wichtige Nutzungsmöglichkeiten verlieren. Auch kann es sein, dass der Softwareanbieter keine Updates mehr zur Verfügung stellt, sodass Sicherheitslücken nicht geschlossen werden. Eine Folge hiervon ist, dass das Produkt an Wert verliert. Da es wegen der Vielzahl von Vertragsverhältnissen bei vernetzten Produkten jedoch oft unklar ist, wer letztlich Anspruchsgegner des Verbrauchers oder der Verbraucherin ist (Hersteller der Hardware, der Softwarehersteller aufgrund des Abschlusses einer Endnutzervereinbarung oder der Händler), stehen Verbraucher_innen oft vor einem Durchsetzungsproblem. Im Ergebnis ist die Wahrscheinlichkeit groß, dass sie auf dem Schaden sitzen bleiben (Wendehorst 2017).

2.5 HANDLUNGSEMPFEHLUNGEN

Um die IT-Sicherheit bei vernetzten Produkten zu erhöhen, sollten sowohl (1) technische als auch (2) rechtliche sowie (3) informatorische Maßnahmen ergriffen werden.

(1) Security by Design konkretisieren und in Normen und Standards verankern

Viele Gefahren von vernetzten Geräten wären zu minimieren, wenn Grundsätze und Designprinzipien der IT-Sicherheit von den Herstellern eingehalten würden. So sollte bspw. das „Minimalprinzip" berücksichtigt werden: Die Komplexität des jeweiligen Betriebssystems ist an der Komplexität der zu erbringenden Leistung orientiert und sollte demnach nicht überdimensioniert sein. Denn mit der Komplexität des Betriebssystems steigt auch die Anzahl potenzieller Fehlerquellen, die Sicherheitslücken darstellen können. So wäre für viele Geräte des IoT grundsätzlich nur ein minimales Betriebssystem ohne zusätzliche Funktionen vonnöten (Margraf 2017). Zudem sollten zusätzliche Produktfeatures wie zum Beispiel Kameras in Smart-TVs standardmäßig deaktiviert sein und Debug- und Testfunktionen entfernt werden, bevor die Geräte auf den Markt kommen (Margraf im Expertenworkshop 2018). Des Weiteren sollte die Update-Fähigkeit von Produkten gewährleistet sein. Auch eine durchgängige Verschlüsselung und Authentisierung im Nutzungsprozess sowie eine Einbindung von relevanten Drittanbietern in das Sicherheitskonzept für das Produkt kann für eine Verbesserung der IT-Sicherheit von vernetzten Produkten sorgen (Margraf 2017).

Die Hersteller sind also aufgefordert, das Prinzip des Security by Design konsequent zu berücksichtigen und IT-Sicherheit schon beim Design der Produkte mitzudenken. Um das verbindlich zu machen, sollten die Maßnahmen produktspezifisch konkretisiert werden und in die Norm- und Standardsetzung der Hersteller einfließen.

---

1 § 3 Abs. 3 EU-Funkanlagenrichtlinie: „Funkanlagen müssen in bestimmten Kategorien oder Klassen so konstruiert sein, dass sie die folgenden grundlegenden Anforderungen erfüllen: […] e) Sie verfügen über Sicherheitsvorrichtungen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden. i) Sie unterstützen bestimmte Funktionen, mit denen sichergestellt werden soll, dass nur solche Software geladen werden kann, für die die Konformität ihrer Kombination mit der Funkanlage nachgewiesen wurde."

(2) Rechtliche Bestimmungen an die digitale Welt anpassen und Absicherung für Verbraucher_innen verbessern

Neben der konsequenten Berücksichtigung von Security by Design sind auch rechtliche Schutzmechanismen für die Verbraucher_innen erforderlich. Dabei sollten einerseits die Anforderungen an die Produktsicherheit ex ante, also vor der Markteinführung eines Produkts, an die Erfordernisse der digitalen Welt angepasst und andererseits durch eine Veränderung bzw. Verschärfung der Haftungsregeln vor allem für Hersteller stärkere Anreize zur Einhaltung bestimmter IT-Sicherheitsstandards geschaffen werden.

(a) Produktsicherheitsrecht

- Es sollte ein umfassendes **IT-Produktsicherheitsrecht** für vernetzte Produkte auf europäischer oder nationaler Ebene geschaffen werden. Hier sollten insbesondere Mindestsicherheitsstandards bezüglich Verschlüsselung, Authentisierung und einer Pflicht des Herstellers zur Bereitstellung von Updates festgelegt werden. Die Update-Pflicht wurde bereits in einer EU-Richtlinie beschlossen und muss nun in nationales Recht umgesetzt werden (Verbraucherzentrale Bundesverband 2019). Das Gesetz sollte zudem je nach Risiko abgestufte Anforderungen enthalten, für bestimmte Produktgruppen gelten und sektorspezifisch anwendbar sein (Heise Online 2017).
- Bestimmte Gefahren müssen ex ante ausgeschlossen werden, weshalb für besonders risikoreiche IT-Produkte und -Anwendungen ein **Zulassungsverfahren in Anlehnung an die Typgenehmigung für automatisierte Fahrsysteme im Fahrzeug** notwendig ist. Ein Zulassungsverfahren ist vor allem für kritische Bereiche relevant, da Schäden in diesen Bereichen lebens- und gesundheitsgefährdend sein können. Zur Vereinfachung des Zulassungsverfahrens könnten auch **Zertifikate** für einzuhaltende Standards genutzt werden, die durch entsprechende Institutionen vergeben werden (Heise Online 2017). Ein erster Schritt in diese Richtung wurde mit dem Rechtsakt zur Cybersicherheit geschaffen, der einen europäischen Zertifizierungsrahmen für IT-Sicherheit von Produkten und Dienstleistungen setzt (Europäische Kommission 2018).
- Zur besseren Erkennbarkeit übergesetzlicher IT-Sicherheitsstandards können die im Cybersicherheitspaket der EU-Kommission vorgeschlagenen **Gütesiegel** entwickelt werden.
- Bestimmte **Informationspflichten** sowie die Einführung **freiwilliger IT-Sicherheitskennzeichen** sind im Entwurf des überarbeiteten IT-Sicherheitsgesetzes geplant (Netzpolitik.org 2019). Ob und in welcher Form diese Ansätze schlussendlich umgesetzt werden, bleibt abzuwarten.

(b) Haftungs- und Gewährleistungsrecht

Die Haftungsfrage kann einen großen Einfluss auf die Sorgfalt der Hersteller und deren Bemühungen zur Umsetzung eines guten IT-Sicherheitsstandards haben. Ökonomische Anreize zur Erhöhung des IT-Sicherheitsniveaus bestehen wie oben gezeigt derzeit aber kaum, weil Ansprüche wegen fehlender IT-Sicherheit entweder nicht bestehen oder schwer durchsetzbar sind.

- Deshalb sollten der **Schadensbegriff im Produkthaftungsgesetz** sowie der Kreis der möglichen Schäden erweitert bzw. an die Notwendigkeiten der digitalen Welt angepasst werden, indem zum Beispiel Persönlichkeitsrechtsverletzungen als Schaden explizit anerkannt werden.
- Zudem sollte der **Produktbegriff im Produkthaftungsgesetz** um Software erweitert werden. Die bisherige Rechtsprechung ist uneindeutig, und es fehlt an einer höchstrichterlichen Aussage hierzu (Spindler 2007a).
- Der Hersteller sollte im Rahmen des **Produkthaftungsgesetzes** nicht nur für die Fehler haften, die zum Zeitpunkt des Inverkehrbringens vorlagen, sondern auch für Fehler, die während der Lebensdauer des Produkts auftreten, etwa indem ein notwendiges Update nicht oder fehlerhaft bereitgestellt wurde.
- Bei autonomen Systemen sollte explizit eine **Gefährdungshaftung der Hersteller** eingeführt werden (Spindler 2007b). Vorbild könnte hierfür das Arzneimittelgesetz sein. Diese Gefährdungshaftung könnte überdies mit einer **Zwangsversicherung** (plus Haftungsdeckel) für die Hersteller kombiniert werden. Dadurch wird zum einen gewährleistet, dass Verbraucher_innen entschädigt werden. Zum anderen werden IT-Sicherheitsrisiken bepreist, wodurch die Hersteller einen Anreiz haben, IT-Sicherheit möglichst gut im Design ihrer Produkte zu berücksichtigen (Spindler 2015).
- **Gewährleistungsansprüche** (Reparatur, Austausch, Kaufpreisminderung, Rücktritt) im Falle eines IT-Sicherheitsmangels sollten auch direkt an den Hersteller gerichtet werden können. Händler_innen können meist nicht erkennen, ob die Betriebssysteme eines vernetzten Gerätes Sicherheitsanforderungen entsprechen; vor allem aber können Hersteller erforderliche Sicherheitsupdates entwickeln und aufspielen. Für die Gebrauchstauglichkeit und IT-Sicherheit von vernetzten Geräten kommt es nicht mehr alleine auf die Fehlerfreiheit des Gerätes zum Kaufzeitpunkt an, sondern Softwareaktualisierungen sind über die Dauer des Produktlebenszyklus notwendig. Daneben sollte auch der oder die Händler_in für das gesamte Leistungsbündel (Produkt, Steuerungs-App, gegebenenfalls Embedded Software) für die Dauer der Gewährleistung einstehen, damit Verbraucher_innen eine_n einheitliche_n Anspruchsgegner_in erhalten.

(c) AGB-Recht

– Die Steuerungssoftware von vernetzten Produkten wird in der Regel auf der Grundlage von AGBs (sogenannten Endnutzervereinbarungen) bereitgestellt. Dass in derartigen AGBs etwa die Bereitstellung von Sicherheitsupdates ausgeschlossen oder dass die datenschutzrechtliche Einwilligungserfordernis umgangen wird, sollte durch eine **Anpassung des AGB-Rechts** – insbesondere der Klauselkataloge §§ 308, 309 BGB – verhindert werden. Das AGB-Recht stellt ein scharfes Schwert dar, da eine nichtige Klausel in den AGBs eines Herstellers automatisch die gesetzlichen Ansprüche z. B. auf Unterlassung oder Schadensersatz für die Verbraucher_innen wiederaufleben lässt (Heise Online 2017).

(d) Versorgung mit Updates und Kennzeichnungspflicht für die Dauer von Updates

– Der Hersteller sollte verpflichtet werden, für die üblicherweise zu erwartende Lebensdauer des Produktes **Updates zur Gewährleistung der IT-Sicherheit** zur Verfügung zu stellen. Zudem sollte die Verpflichtung bestehen, die Verbraucher_innen vor dem Kauf darüber zu informieren, wie lange das Produkt konkret mit Updates versorgt wird. Produkte, für die keine Sicherheitsupdates mehr zur Verfügung gestellt werden, sollten vom Markt genommen werden.

(e) Behördliche Rechtsdurchsetzung

– Um die **Rechtsdurchsetzung** im Bereich der IT- und Produktsicherheit zu verbessern, sollten die zuständigen **europäischen und nationalen Aufsichtsbehörden** (u. a. Enisa, BSI, KBA, BNETZA) in ihren Kompetenzen, Mandaten und Ressourcen gestärkt werden. Zudem sollten die Behörden die Verbraucherinformation und Aufklärung in diesem Themenfeld ausbauen.

(3) Verbraucher_innen für den sicheren Umgang mit vernetzten Produkten befähigen und Forschung vorantreiben

Neben diesen regulatorischen Maßnahmen bedarf es auch informatorischer Maßnahmen. Hierzu zählt insbesondere die **Förderung von Bildungsmaßnahmen** für Nutzer_innen über vernetzte Produkte, deren Gefahren und Selbstschutz. Überdies sollte die Forschungsförderung zu Themen der IT-Sicherheit, insbesondere zur Ende-zu-Ende-Sicherheit und zu den Security-by-Design-Prinzipien, ausgebaut werden.

3

SELBSTBESTIMMUNG IN DER DIGITALEN WELT

Immer mehr Geschäftsmodelle basieren auf der Durchleuchtung und Vermessung von Menschen und deren Verhalten. Personenbezogene Daten sind für diese Art der Datenökonomie essenziell. Viele der auf Daten basierenden Geschäftsmodelle und Anwendungen sind auch für Verbraucher_innen vorteilhaft. Individualisierte Produktempfehlungen oder Suchergebnisse sind beispielsweise nur auf der Grundlage einer personalisierten Datenverarbeitung möglich.

Auf der anderen Seite stellt die zunehmend lückenlose Durchleuchtung auch ein erhebliches Risiko für Verbraucher_innen dar. Sie kann potenziell zur Bedrohung für die freiheitliche, demokratische und solidarische Gesellschaft werden, wenn Menschen manipuliert werden, ein bestimmtes Verhalten durch offenen oder subtilen Druck erzeugt wird oder Teilhabechancen aufgrund eines Datenprofils eingeschränkt werden. Daher ist es wichtig, das Grundrecht auf informationelle Selbstbestimmung durchzusetzen. Hiernach hat jede_r Einzelne das Recht, selbst über die Preisgabe und Verwendung seiner bzw. ihrer personenbezogenen Daten zu entscheiden.

Die Möglichkeiten von Verbraucher_innen, ihr Recht auf informationelle Selbstbestimmung souverän auszuüben, sind in der Praxis jedoch beschränkt: Eine unzureichende Transparenz über Datenverarbeitungsprozesse, fehlende Wahlalternativen oder auch die Überforderung, einen Überblick über die Vielzahl von Datenerhebungen und erteilten Einwilligungen zu behalten, sind Beispiele hierfür. So gaben etwa nur 16 Prozent der Teilnehmenden einer Umfrage an, sich immer ausreichend über die Bedingungen der Datenerfassung und die weitere Verwendung ihrer Daten informiert zu fühlen (Special Eurobarometer 431 2015). Dieses Beispiel zeigt, dass die derzeitige Praxis weit vom Ziel der informationellen Selbstbestimmung entfernt ist.

3.1 RECHTLICHER RAHMEN: EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG

Der rechtliche Rahmen für den Schutz der informationellen Selbstbestimmung wird insbesondere durch die europäische Datenschutzgrundverordnung (DSGVO) geregelt, die im Mai 2018 europaweit anwendbar geworden ist. Sie soll die Prinzipien des Datenschutzes und des Schutzes der informationellen Selbstbestimmung in der digitalen Welt zur Geltung bringen und damit gerade auch die Rechte der Verbraucher_innen stärken.

Im Kern bekräftigt die DSGVO bereits zuvor in Deutschland geltende Prinzipien des Datenschutzes. Gleichwohl enthält sie eine Reihe von Vorgaben, die den Datenschutz weiter verbessern können. Aus Sicht der Verbraucher_innen sind insbesondere die folgenden Vorgaben hervorzuheben:

- Erstens besteht ein wesentliches Ziel der DSGVO darin, Transparenz über Datenverarbeitungen herzustellen. So schreibt Artikel 12 (1) vor, dass der Verantwortliche „geeignete Maßnahmen (trifft), um der betroffenen Person alle Informationen (...) in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln".
- Zweitens setzen Datenverarbeitungen, die über gesetzlich definierte Erlaubnistatbestände hinausgehen, eine Einwilligung voraus. Diese muss eine Reihe von Voraussetzungen erfüllen und insbesondere freiwillig erfolgen.
- Drittens haben Verbraucher_innen eine Reihe von Rechten, die ihre Souveränität auch nach der Datenerhebung wahren sollen („Betroffenenrechte"). Sie haben etwa das Recht auf Auskunft über die über sie erhobenen Daten sowie das Recht, eine Berichtigung oder Löschung von personenbezogenen Daten zu erwirken.
- Viertens wird Datenschutz durch Technikgestaltung („Privacy by Design", z. B. Pseudonymisierung) und durch datenschutzfreundliche Voreinstellungen („Privacy by Default") gefördert. So sollen Unternehmen geeignete Maßnahmen umsetzen, um die personenbezogenen Daten der Betroffenen besser zu schützen oder Daten erst gar nicht zu erheben. Zudem wird das Prinzip der Zweckbindung hochgehalten, wonach Daten in der Regel nur zu einem vorher festgelegten Zweck erhoben und verwertet werden dürfen.
- Fünftens wird der Geltungsbereich durch das Marktortprinzip erweitert und die Durchsetzung der Regeln durch höhere Bußgelder gestärkt.

Durch die DSGVO wurden die Verbraucherrechte im Bereich der Datenverarbeitung gestärkt. Lücken bestehen aber bei der praktischen Umsetzung, weil die Rechte der Verbraucher_innen vielfach faktisch nur unzureichend wirksam werden, wie im Folgenden erläutert wird.

3.2 INFORMATIONELLE SELBSTBESTIMMUNG – IM VERBRAUCHERALLTAG NUR UNZUREICHEND VERWIRKLICHT

Trotz der in der DSGVO festgeschriebenen Bestimmungen kann derzeit von einer tatsächlichen Souveränität der Verbraucher_innen über die Preisgabe und Verwendung ihrer persönlichen Daten im Konsumalltag nicht gesprochen werden. Anspruch und Realität klaffen in sechs wesentlichen Handlungsbereichen weit auseinander.

(1) Unzureichende Transparenz

Verbraucher_innen ist oft nicht klar, wozu Unternehmen ihre Daten verwenden. So geben 68 Prozent der Teilnehmenden einer Umfrage an, dass es ihnen beispielsweise eher schwer fällt, nachzuvollziehen, ob eine Webseite ein personenbezogenes Profil erhebt, und 74 Prozent geben an, dass die Weitergabe ihrer Daten an Dritte eher schwierig festzustellen sei (Kettner/Thorun 2018).

Die Gründe für diesen Mangel an Transparenz und Nachvollziehbarkeit sind vielfältig: So werden Verbraucher_innen von langen Datenschutztexten, die mitunter mehrere Tausend Wörter umfassen, abgeschreckt (Contissa et al. 2018). Die Sprache ist für Verbraucher_innen ohne technische oder juristische Fachexpertise kaum verständlich. Das gilt beispielsweise für Datenschutztexte für E-Payment-Lösungen (Marktwächter Digitale Welt 2017) oder Smarthome-Anwendungen (Kettner et al. 2018a). Die Texte sind häufig unstrukturiert und schwer zu navigieren. Auch sind die relevanten Texte für Verbraucher_innen auf Webseiten oft schwer auffindbar, was zu geringen Leseraten führt (Kettner et al. 2018b; Elshout et al. 2016).

Andererseits müssen die Datenschutztexte nicht nur verständlich, sondern auch juristisch korrekt sein. Hierzu ist präzises Fachvokabular unausweichlich, das bereits an sich für durchschnittliche Rezipient_innen sehr technisch und schwer verständlich ist. Jeder Datenschutztext muss also die schwierige Balance zwischen Verständlichkeit und rechtlicher Korrektheit schaffen.

Ein Transparenzdefizit besteht auch in der Frage, bei welchen Anbietern überhaupt persönliche Daten zu welchem Zweck gespeichert sind. Der Verbraucheralltag im Netz ist durch so viele Interaktionen mit Unternehmen gekennzeichnet, dass die wenigsten Verbraucher_innen einen Überblick haben dürften, wann sie welchen Unternehmen eine Einwilligung für welchen Zweck gegeben haben.

(2) Probleme bei der Einwilligung/Mangel an Wahlfreiheit

Ein weiteres Beispiel dafür, dass die Verbraucherrealität hinter dem gesetzlichen Anspruch zurückbleibt, ist die Freiwilligkeit bei der Einwilligung. So müssen Verbraucher_innen im Alltag oftmals (ungewollt) ihre Daten preisgeben, beispielsweise um sich auf Mietwohnungen zu bewerben oder wenn der oder die Arbeitgeber_in bestimmte Informationen verlangt.

Auch stehen Verbraucher_innen oft vor der Herausforderung, dass sie im Konsumalltag über keine praktikablen Wahlalternativen verfügen. Dies ist insbesondere bei Social-Media- und Plattformangeboten der Fall. Wenn alle Freund_innen einen bestimmten Dienst nutzen und dieser nicht mit anderen Diensten interoperabel ist, ist die Wahlfreiheit für Verbraucher_innen in der Konsumrealität eingeschränkt, auch wenn es theoretisch Wahlalternativen gibt.

(3) Erschwerte Durchsetzung der Betroffenenrechte

Auch bezüglich der Rechteausübung der Verbraucher_innen existieren auf dem Digitalmarkt Hürden. Damit Rechte wie Widerspruch, Berichtigung oder Löschung überhaupt ausgeübt werden können, müssen Datenschutzerklärungen Angaben und Kontaktmöglichkeiten zur verantwortlichen Stelle enthalten. Eine Untersuchung von Smarthome-Anwendungen im Jahr 2018 fand jedoch heraus, dass ein nicht unerheblicher Anteil der Smarthome-Anbieter in den Datenschutzerklärungen keine Kontaktinformationen angibt (Kettner et al. 2018a). So bleibt die Realität derzeit hinter dem Auskunftsanspruch gemäß Art. 15 DSGVO zurück. Selbst wenn formal Kontaktmöglichkeiten gegeben sind, ist die Rechteausübung meist sehr beschwerlich, weil der Interaktionsprozess nicht nutzerfreundlich ausgestaltet ist („Rechteausübung auf einen Klick"). Ebenfalls erschwert wird die Ausübung der Rechte durch den fehlenden Überblick, bei welchen Anbietern und zu welchem Zweck persönliche Daten gespeichert sind.

(4) Datenschutz durch Technikgestaltung erfährt noch nicht die notwendige Bedeutung

Technische Designprinzipien wie die des Privacy by Design und Privacy by Default werden von Unternehmen häufig nicht angemessen umgesetzt. Die Voreinstellung zum Einsatz der Gesichtserkennung beim sozialen Netzwerk Facebook ist beispielsweise by Default ausgewählt. Nutzer_innen müssen aktiv werden, um diese Verarbeitung auszustellen. Ähnlich wenig verbraucherfreundlich gestaltet Amazon die Zugriffsmöglichkeiten des Sprachassistenten Alexa. So stehen keine Einstellungsmöglichkeiten zur Verfügung, die beispielsweise einen Fremdzugriff verhindern oder die Daten von betroffenen Dritten wie minderjährigen Kindern schützen (Alvarez/Rövekamp 2019).

(5) Mangelnde Ausstattung der Datenschutzaufsicht

Aussagen einiger Datenschutzaufsichtsbehörden zufolge sind viele Aufsichtsbehörden derzeit personell nicht ausreichend in der Lage, den gebotenen Informations- und Rechtsdurchsetzungserfordernissen nachzukommen. So gingen im Zuge des Inkrafttretens der DSGVO so viele Bürgerbeschwerden und Unternehmensanfragen ein, wie noch nie zuvor (T-Online 2018).

(6) Verunsicherung der Verbraucher_innen

Die DSGVO hat erhebliche Verunsicherung bei Verbraucher_innen und vielen kleinen und mittleren Unternehmen ausgelöst. Vielerorts verbieten Schulen und Kindergärten beispielsweise Fotos bei Klassenfahrten oder anderen Veranstaltungen, weil sie Angst davor haben, unbeabsichtigt Rechtsverletzungen zu begehen. In der Tat gibt es enorme Graubereiche, die erst gerichtlich geklärt werden müssen, und auch die amtlichen Handreichungen für die Interpretation der Bestimmungen wirken oft eher verwirrend. Dort, wo neben der DSGVO nationale Gesetzgebungskompetenzen verbleiben, sollte die Bundesregierung im Sinne der Verbraucher_innen für Klarheit sorgen.

3.3 LÖSUNGSANSÄTZE UND HANDLUNGSEMPFEHLUNGEN

Wie die Analyse zeigt, bleibt die Verbraucherrealität derzeit oft hinter dem Anspruch der informationellen Selbstbestimmung und den rechtlichen Anforderungen zurück. Um die Defizite abzustellen, sollten die folgenden Lösungsansätze umgesetzt werden, die in drei Handlungsfeldern zusammengefasst werden können.

(1) Vorgaben der DSGVO konsequent im Sinne der Verbraucher_innen um- und durchsetzen und Transparenz steigern

Das informationelle Selbstbestimmungsrecht muss mit Leben gefüllt werden. Die hohen Strafzahlungen für Verletzungen des Datenschutzrechts erzielen dabei bereits heute eine abschreckende Wirkung. Zugleich verfügen die Behörden über ausreichend Spielraum, um bei unbeabsichtigten und geringen Regelverstößen eher beratend als strafend tätig zu werden.

- Um ihrer Funktion der Beratung und Aufsicht effektiver nachkommen zu können, müssen die **Datenschutzbehörden** sowie die **zivilgesellschaftlichen Daten- und Verbraucherschutzverbände** mit den nötigen personellen und finanziellen Ressourcen ausgestattet werden. Die Länder sollten die Haushaltsmittel für die Datenschutzbehörden und zivilgesellschaftlichen Verbraucherschutzverbände daher aufstocken.
- Überdies sollten Schritte umgesetzt werden, um die **aufsichtsrechtlichen Kompetenzen im Datenschutz**, die aktuell auf 16 Bundesländer und den Bund verteilt sind, zu bündeln. Hierdurch könnten sich die Datenschutzaufsichtsbehörden spezialisieren und effektiver agieren. Eine solche Bündelung sollte über einen **Staatsvertrag** zwischen den Ländern umgesetzt werden.
- Zu guter Letzt sollten **Datenschutzzertifikate und Siegel** gefördert werden, insbesondere die Erarbeitung eines einheitlichen Europäischen Datenschutzsiegels nach Artikel 42 (5) DSGVO. Dies ermöglicht es Verbraucher_innen, auf einen Blick eine glaubwürdige Bewertung der Datenverarbeitung eines Unternehmens durch einen unabhängigen Dritten zu erhalten. Eine solche Bewertung durch unabhängige Dritte verringert die Informationskosten für Verbraucher_innen.

(2) Verständlichkeit durch Piktogramme erhöhen

- Ein Bild sagt oft mehr als tausend Worte. Gemäß dieser Erkenntnis sind in Artikel 12 (7) DSGVO **standardisierte Bildsymbole** bereits angedacht und sollen Verbraucher_innen dabei helfen, visuell einen Überblick über die Datenverarbeitungen eines Produkts und einer Dienstleistung zu erhalten. In der Praxis werden diese jedoch noch nicht angewandt. Die Bundesregierung sollte daher Vorschläge für Piktogramme entwickeln und diese verbindlich machen.
- Überdies sollte die Bundesregierung Maßnahmen umsetzen, damit Datenschutzerklärungen und Piktogramme **maschinenauslesbar** werden. Hierdurch würde der Einsatz von Privacy Bots (siehe unten) leichter gemacht. Privacy Bots könnten Verbraucher_innen darin unterstützen, das Ausmaß der Verarbeitung ihrer persönlichen Daten selbstbestimmt zu entscheiden.
- Zu guter Letzt sollten auch **Muster-Datenschutzerklärungen** von den Datenschutzbehörden entwickelt und herausgegeben werden. Diese Muster würden es nicht nur Unternehmen einfacher machen, rechtlich zulässige Datenschutzerklärungen zu verfassen. Sie würden auch die Vergleichbarkeit steigern.

(3) Verbrauchersouveränität durch Technologie fördern

Technologien sollten künftig viel stärker als bislang dafür verwendet werden, die Verbrauchersouveränität zu fördern. Hierzu zählen auf der einen Seite Privacy Enhancing Technologies (PETs) und Privacy Bots sowie auf der anderen Seite Personal Information Management Systems (PIMS). Die Bundesregierung sollte solche Ansätze fördern.

(a) **Privacy Enhancing Technologies**: PETs sind technische Lösungsansätze, die die Datensparsamkeit fördern und es für Verbraucher_innen vereinfachen, Datenverarbeitung zu erkennen und gemäß ihren Präferenzen anzupassen. Dazu zählen bspw. unterschiedliche Anonymisierungs- und Pseudonymisierungsverfahren sowie weitere Mechanismen, die die Integrität und Unverfälschbarkeit von Daten

gewährleisten. So können mit ihrer Hilfe erhobene Daten entweder keiner Person mehr zugeordnet werden, oder ein Identifikationsmerkmal wird durch ein Pseudonym ersetzt. So kann auf die Identität der betroffenen Person nicht oder nur sehr schwer rückgeschlossen werden. Ein Beispiel, das in der Praxis Anwendung findet, ist der Telekom „Enkroder" (Ulmer 2016). Die Bundesregierung sollte PETs fördern und dafür sorgen, dass diese in Normen und Standards aufgegriffen werden. Auch sollte eine De-Anonymisierung grundsätzlich verboten werden, außer in begründeten Ausnahmefällen.

(b) **Privacy Bots**: Die Bundesregierung sollte auch die Entwicklung von Privacy Bots fördern. Wenn maschinenlesbare Datenschutzerklärungen bereitgestellt werden, können Privacy Bots die Datenschutzerklärung für die Nutzer_innen auswerten und so die Lesezeit und Informationsaufwände reduzieren. Das Projekt Platform for Privacy Preferences (P3P) zählt zu den ersten Privacy Bots, das auf maschinenlesbaren Datenschutzerklärungen basiert. Eine Umsetzungsform ist beispielsweise der „Privacy Bird", der nach einer Präferenzabfrage bei den Nutzer_innen einen Abgleich mit den maschinell ausgelesenen Datenschutztexten vornimmt und Nutzer_innen eine Warnung bei ungewollten Verarbeitungen gibt. Eine andere technische Variante der Privacy Bots basiert auf der automatisierten, semantischen Analyse von Datenschutzerklärungen. In dieser Variante ist es nicht zwingend nötig, dass die Datenschutztexte in maschinenlesbarer Form vorliegen – ein trainierter Algorithmus könnte die Aufgabe der Inhaltsextraktion übernehmen. Ein Beispiel für einen deutschsprachigen Privacy Bot, der die Datenschutztexte selbstständig „lesen" kann, ist der vom Bundesministerium für Bildung und Forschung (BMBF) geförderte DATENSCHUTZscanner (2018). Englischsprachige Lösungen sind der „Pribot" (Harkous et al. 2018) und „Claudette" (Lippi et al. 2018). Eine Erweiterung dieser Privacy Bots könnte außerdem der automatische Präferenzabgleich sein, bei dem Verbraucher_innen vorab angeben, dass bestimmte Datenverarbeitungen nicht mit ihren Präferenzen übereinstimmen, und dann durch den Privacy Bot gewarnt werden, sobald ein Dienst diese Datenverarbeitung vornimmt. Bisher ist diese Erweiterung jedoch noch nicht marktfähig umgesetzt worden.

(c) **Personal Information Management Systems**: Der Ansatz Personal Information Management Systems (PIMS) hat zum Ziel, den Nutzer_innen durch die Zwischenschaltung eines Intermediärs mehr Kontrolle über ihren Datenstrom zu ermöglichen. So sollen Nutzer_innen etwa mittels eines Datendashboards oder eines unabhängigen Datentreuhänders in die Lage versetzt werden, die eigenen Daten zu verwalten und gemäß ihren Präferenzen an Anbieter weiterzugeben oder die Nutzung einzuschränken. Über ein Datendashboard könnten Nutzer_innen also selber einstellen, welche personenbezogenen Informationen sich in einem bestimmten Kontext zur Weitergabe eignen und welche nicht. Beispiele für sogenannte Intermediäre und PIMS-Ansätze sind die MyData-Initiative (2018; Horn et al. 2017) sowie Anbieter wie digi.me aus Großbritannien und die Cozy Cloud aus Frankreich. Im Bereich des automatisierten Fahrens hat sich bereits eine Reihe von Unternehmen ins Spiel gebracht, eine Datentreuhänderrolle zu übernehmen. Die Bundesregierung sollte durch Regulierung die Voraussetzung dafür schaffen, dass Datentreuhänder unabhängig, neutral und ohne ein wirtschaftliches Eigeninteresse an der Verwertung der im Auftrag der Verbraucher_innen verwalteten Daten agieren. Hierfür muss bei privaten Akteur_innen insbesondere gewährleistet werden, dass es keine finanziellen oder anderen interessengeleiteten Verflechtungen gibt. Auch müssen eine potenzielle Monopolstellung ausgeschlossen und Koppelungen unterbunden werden. So darf es nicht passieren, dass etwa ein Anbieter seine Kund_innen dazu verpflichtet, mit einem bestimmten Treuhänder zusammenzuarbeiten. Um diese Interessenkonflikte zu umgehen, könnte auch eine öffentlich-rechtliche Ausgestaltung infrage kommen.

Neben diesen drei Handlungsfeldern sollte eine breite Debatte darüber stattfinden, welche Geschäftsmodelle der digitalen Ökonomie mit einer freiheitlichen und solidarischen Gesellschaft vereinbar sind bzw. welche Geschäftsmodelle strukturell Selbstbestimmung verhindern.

4

FAIRNESS UND TEILHABE BEI KÜNSTLICHER INTELLIGENZ UND AUTOMATISIERTEN ENTSCHEIDUNGEN

Technologien der künstlichen Intelligenz sind auf dem Vormarsch. In sozialen Netzwerken oder bei Suchmaschinen sorgen KI-basierte Technologien dafür, dass Inhalte, Angebote und Werbung personalisiert angezeigt werden (Heise Online 2018; Search Engine Land 2015), Chatbots und Robo-Advice-Systeme kommen in der Geldanlageberatung zum Einsatz (Klar 2018), KI-basierte Systeme werden für die Schadensregulierung im Versicherungsbereich genutzt (Microsoft 2017), Roboter unterstützen Pflegebedürftige im Alltag (MDR 2019), auch in der medizinischen Diagnostik sind KI-Anwendungen auf dem Vormarsch (Handelsblatt 2017) und bei selbstfahrenden autonomen Fahrzeugen werden KI-Systeme ebenfalls eingesetzt. Es ist davon auszugehen, dass diese Technologien in den kommenden Jahren immer verbreiteter zur Anwendung kommen werden. So wird für die Automobilindustrie davon ausgegangen, dass im Jahr 2035 zwischen 28 und 48 Millionen autonome Fahrzeuge produziert werden (Oliver Wyman Analysis 2015).

Für die Verbraucherpolitik ist mit diesen rapiden Entwicklungen eine Reihe von Fragen verbunden: Wie kann erreicht werden, dass KI-Technologien Mehrwerte für Verbraucher_innen mit sich bringen und fair und nachvollziehbar eingesetzt werden? Wie kann es gelingen, dass KI inklusiv wirkt und nicht zur Benachteiligung insbesondere von schwächeren Verbrauchergruppen führt? Wie kann die Teilhabe der ganzen Gesellschaft am Nutzen dieser Technologien sichergestellt werden?

Die Relevanz dieser Fragen zeigt sich darin, dass sich Regierungen auf internationaler, europäischer (Europäische Kommission 2019; High-Level Expert Group on Artificial Intelligence 2019) und nationaler Ebene intensiv mit Fragen der KI sowie algorithmischen Entscheidungen befassen. So hat sich die Bundesregierung im Rahmen ihrer „Strategie Künstliche Intelligenz" auf die Fahne geschrieben, die Forschung und den Einsatz von KI in Deutschland voranzutreiben (Die Bundesregierung 2018). Ziel der Bundesregierung ist demnach eine KI, die „unserer Wirtschafts-, Werte- und Sozialstruktur entspricht" (Die Bundesregierung 2018). Überdies hat die Bundesregierung im September 2018 eine Datenethikkommission einberufen. Sie erarbeitet bis Herbst 2019 Leitlinien zum ethischen und verantwortlichen Umgang mit KI (BMI/BMJV 2018). Darüber hinaus hat der Deutsche Bundestag eine Enquete-Kommission eingesetzt, die sich mit den wirtschaftlichen, sozialen und ökologischen Potenzialen und Risiken von KI befasst sowie ethische Richtlinien entwickelt (Deutscher Bundestag 2018).

4.1 DEFINITION UND BESCHREIBUNG

Das Forschungs- und Anwendungsgebiet „künstliche Intelligenz" versucht, menschliches, intelligentes Verhalten, das in der Lage ist, eigenständig Probleme zu lösen und nicht lediglich nach einer vorher festgelegten Routine zu verfahren, auf Maschinen zu übertragen (Fraunhofer-Gesellschaft 2017). Technisch ermöglicht wird dies vor allem durch Algorithmen, in denen mathematische Verfahren angewendet werden. Zwei wichtige Teilbereiche von KI sind das Natural Language Processing (NLP) – Systeme, die Sprache verarbeiten können – sowie das maschinelle Lernen – hierbei lernt eine Maschine, aus Erfahrungsdaten neues Wissen zu generieren und gegebenenfalls Schlussfolgerungen und Handlungen anzupassen (t3n 2017). Verfahren der künstlichen Intelligenz werden häufig für algorithmen-basierte Prognosen und Entscheidungen verwendet – das sogenannte Algorithmic Decision Making (ADM).

Ein zentraler Unterschied wird zwischen „schwacher" KI (Artificial Narrow Intelligence) und „starker" KI (Artificial General Intelligence) gemacht (Searle 1980; Bostrom 1998).[2] Schwache KI kann eigenständig Aufgaben, für die sie entwickelt wurde, lösen und sich dabei selbst verbessern und weiterentwickeln (Fraunhofer-Gesellschaft 2017). Jedoch fehlt es ihr an der Kompetenz zu generalisierenden Transferleistungen sowie Reflexion, wodurch sich starke KI auszeichnet (Fraunhofer-Gesellschaft 2017). Anwendungen, die auf starker KI beruhen, existieren bisher allerdings noch nicht.

2 Es gibt verschiedene Definitionen der Kategorien von KI. Zudem erwähnen einige Kategorisierungen noch eine dritte Kategorie, die Artificial Superintelligence (ASI). Diese Stufe von KI wäre dann intelligenter als der Mensch (siehe z. B. Bostrom 1998).

4.2 CHANCEN UND RISIKEN FÜR VERBRAUCHER_INNEN

Der Einsatz von KI-basierten Technologien bringt für die Verbraucher_innen Chancen und Risiken mit sich. Chancen bestehen in den folgenden Aspekten:

- **Teilhabe** kann beispielsweise bei der Geldanlage erhöht werden, wenn Robo-Advisor es auch einkommensschwächeren Personen ermöglichen, bereits kleinere Summen Geld anzulegen. Auch können es Sprachassistenzsysteme blinden Menschen erleichtern, digitale Dienste, die normalerweise eine Tastensteuerung benötigen, zu nutzen, und hierdurch einen Beitrag zur Inklusion leisten.
- **Menschliche Fehler und Vorurteile** können durch standardisierte automatisierte Prozesse minimiert werden. Hierdurch können grundsätzlich auch die Konsistenz und Nachvollziehbarkeit von Entscheidungen erhöht werden. Das ist dann der Fall, wenn Entscheidungen immer nach den gleichen Vorgaben aufgrund festgelegter Kriterien getroffen werden. So kann „menschliche Willkür" etwa von einzelnen (Anlage-) Berater_innen reduziert werden.
- **Kosten** können gesenkt werden, wenn Leistungen (teil-)automatisiert effizienter und dadurch kostengünstiger erbracht werden.
- **Neue Services** können entwickelt werden, die einen unmittelbaren Verbrauchernutzen spenden wie etwa Sprachassistenzsysteme, mit denen das Smarthome gesteuert werden kann, oder Pflegeroboter.
- **Gemeinwohlinteressen** könnten etwa dadurch gefördert werden, dass Algorithmen, die in Angebots- und Preisvergleichsportalen verwendet werden, Nachhaltigkeitsaspekte konsequent berücksichtigen. Auch können Algorithmen in der Verkehrssteuerung Anwendung finden, wodurch Staus und Emissionen reduziert werden.

Gleichzeitig wird jedoch auch eine Vielzahl von Risiken und Herausforderungen diskutiert. Hierzu zählen:

- **Intransparenz**: Wenn Verbraucher_innen nicht wissen, welche Daten in den KI-Systemen verarbeitet werden und wie Entscheidungen zustande kommen, sind sie den Systemen ausgeliefert. So wichen etwa zwei Chatbots von Facebook bei einem Laborexperiment im Laufe der Zeit vom Standard-Englisch ab, sodass auch die Entwickler_innen die Bots nicht mehr verstanden (Zeit Online 2017). Ein weiteres Beispiel sind Auskunfteien wie die SCHUFA, die Daten über die Kreditwürdigkeit von Verbraucher_innen sammeln. Bei diesen können Verbraucher_innen ihren Scorewert nicht nachvollziehen.
- **Fragen der Verantwortlichkeit**: Bei Entscheidungen, die ein Algorithmus trifft, ist die Frage nach Verantwortlichkeit und Haftung zu stellen. Es muss klar sein, wer die Verantwortung trägt, wenn selbstgesteuerte KI-Systeme Fehler machen, die zu psychischen oder physischen Schäden führen (Spindler 2018). In Deutschland ist durch das Gesetz zur Erlaubnis hoch- und vollautomatisierten Fahrens geregelt, dass bei Softwarefehlern der Hersteller haftet. Ähnliche Vorgaben existieren jedoch nicht für andere Anwendungsfelder.
- **Diskriminierung und Verstetigung von Vorurteilen**: Wenn KI-Systeme zur Bewertung Daten wie das Geschlecht, die Religionszugehörigkeit, ethnische Herkunft oder sexuelle Orientierung heranziehen, kann hiermit rechtswidrige Diskriminierung verbunden sein. Auch können KI-Systeme, je nachdem welche (Trainings-)Daten und Entscheidungsregeln sie verwenden, gesellschaftliche Vorurteile verstetigen (Drösser 2016). Beispielsweise „erlernte" ein intelligenter Chatbot von Microsoft rassistisches Verhalten durch seine Konversationen auf Twitter, wo eine Gruppe versierter Nutzer_innen den Bot gezielt zu rassistischen Reaktionen trainierte (The Guardian 2016).
- **Wettbewerbsverzerrungen und Monopolisierungstendenzen**: Die Qualität von KI-Systemen kann mit der Verfügbarkeit von (Feedback-)Daten steigen. Hierdurch sind die Unternehmen im Vorteil, die jetzt bereits umfangreich Daten erheben und verarbeiten. Zwar hängt die Qualität von KI-Systemen auch von der Qualität der Algorithmen ab, allerdings resultiert aus der Notwendigkeit großer Trainingsdatenbestände eine Gefahr der Monopolisierung.
- **Wirtschaftliche Benachteiligung von Verbraucher_innen**: Algorithmen im Onlinehandel könnten „lernen", die Preissetzung so zu optimieren, dass Unternehmen zu Lasten der Verbraucher_innen möglichst hohe Gewinne erzielen (individualisierte Preise). Ebenfalls möglich wäre es, dass Algorithmen unterschiedlicher Anbieter „lernen", bei der dynamischen Anpassung von Preisen abgestimmt vorzugehen, sodass die Preissetzung im Ergebnis wie eine kartellartige Preisabsprache wirkt.

4.3 LÖSUNGSANSÄTZE UND HANDLUNGSEMPFEHLUNGEN

Die Diskussion zeigt, dass KI-basierte Systeme nicht per se gut oder schlecht sind, sondern dass es von ihrer konkreten Ausgestaltung und ihrem Einsatzfeld abhängt, welche gesellschaftliche Wirkung von ihnen ausgeht. Um einen aus Sicht der Verbraucher_innen fairen und inklusiven Einsatz von KI-basierten Systemen sicherzustellen, sollten die folgenden Handlungsempfehlungen umgesetzt werden. Sie lassen sich dabei in die folgenden drei Handlungsfelder unterteilen.

(1) Potenziale KI-basierter Systeme für den Verbraucherschutz und die Verbraucherbefähigung sowie für die Förderung des Gemeinwohls erforschen und einsetzen

Wie die eingangs genannten Beispiele zu den Chancen zeigen, können KI-basierte Systeme einen Beitrag für ein Mehr an Teilhabe, für die Durchsetzung von Verbraucherrechten sowie für die Erreichung gemeinwohlorientierter Ziele leisten. Dementsprechend sieht die KI-Strategie der Bundesregierung vor, die „Entwicklung von innovativen Anwendungen, die die Selbstbestimmung, die soziale und kulturelle Teilhabe sowie den Schutz der

Privatsphäre der Bürgerinnen und Bürger unterstützen" zu fördern (Die Bundesregierung 2018: 10).

- Hierfür müssen **Forschungsmittel** zur Verfügung gestellt und dafür gesorgt werden, dass **gemeinwohlorientierte Anwendungen in den Markt** kommen. Ein guter Auftakt hierfür stellt eine Richtlinie des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) aus dem Frühjahr 2019 dar. Mit ihr werden Anwendungen künstlicher Intelligenz zur Unterstützung des Verbraucheralltags gefördert (BMJV 2019b).
- Überdies sollten **Open-Data-Ansätze** unterstützt werden. Da Daten die Grundlage für KI-basierte Anwendungen sind und viele gemeinwohlorientierte Organisationen und Unternehmen nicht über die Möglichkeiten verfügen, selbst diese Datenbestände zu generieren, sollten Ansätze umgesetzt werden, die dafür sorgen, dass alle Anbieter, Verbraucher_innen und Aufsichtsbehörden grundsätzlich einen Zugang zu diesen Daten haben.

(2) Mindeststandards konsequent einführen und effektiv durchsetzen

Um Diskriminierung und Entsolidarisierung durch Algorithmen und Scoring zu verhindern, „Social Scoring" abzuwehren und dafür zu sorgen, dass wir auch weiterhin in einer solidarischen Gesellschaft leben, wollen wir die Gefahren von Algorithmen-basierten Entscheidungen und Scoring auf Individuen und Gesellschaft eindämmen, Nachvollziehbarkeit und Transparenz für Verbraucher_innen sicherstellen und unabhängige staatlich-legitimierte Kontrollinstitutionen einführen. Hierfür sind die folgenden konkreten Handlungsempfehlungen von zentraler Bedeutung:

- **Personale Verantwortlichkeit muss weiterhin gelten:** Wenn KI-basierte Systeme eingesetzt werden, ist dafür zu sorgen, dass die Geschäftsleitung in der Pflicht bleibt. Daher müssen KI-basierte Verfahren und Systeme auch weiterhin in eine ordnungsgemäße Geschäftsorganisation eingebettet sein. Hiermit verbunden sind eine angemessene Dokumentation und ein wirksames Kontrollsystem. Die Verantwortung auch für automatisierte Prozesse muss letztlich bei der Leitungsebene der Unternehmen bleiben (BaFin 2018: 175).
- **Nachvollziehbarkeit automatisierter Entscheidungen gewährleisten:** Anwender KI-basierter Systeme müssen dafür Sorge tragen, dass KI-basierte Entscheidungen erklärbar und nachvollziehbar sind. Es darf keine Blackbox geben. So müssen zumindest die Zielsetzung des zugrundeliegenden Modells, die grundlegende Funktionsweise, die eingehenden Merkmale sowie die Entscheidungsparameter nachvollziehbar sein (BaFin 2018: 175). Dies gilt insbesondere für Sektoren, die unter Aufsicht stehen. Denn nur, wenn diese Voraussetzungen vorliegen, hat die Aufsicht überhaupt eine Möglichkeit, rechtzeitig Fehler im Analyseprozess zu erkennen und entsprechend einzuschreiten.
- **Transparenz für Verbraucher_innen sicherstellen:** Anbieter sollten Verbraucher_innen über den Einsatz KI-basierter Verfahren informieren, solange diese eine Verbraucherrelevanz haben. Diesbezügliche allgemeine Vorgaben der Datenschutzgrundverordnung (insb. Art. 13 Abs. 2 lit.f sowie 15 Abs. 1 Buchst. h) sollten konkretisiert werden. Auch sollten Verbraucher_innen die wesentlichen Merkmale, auf deren Basis sie gescort werden, sowie möglichst auch deren Gewichtung auf verständliche und nachvollziehbare Weise offengelegt werden (SVRV 2018: 4).
- **Diskriminierung ausschließen:** Um die Gefahr von Willkür und Diskriminierung bei KI-basierten Entscheidungen zu minimieren, ist eine **Qualitätssicherung** sicherzustellen. Hierfür sollten Qualitätsleitbilder im Zusammenspiel von Wirtschaft, Aufsicht und Verbraucherverbänden erarbeitet werden. Beispielsweise im Rahmen von Folgeabschätzungen sollten sie umgesetzt werden (SVRV 2018: 6). Die Anforderungen des Allgemeinen Gleichbehandlungsgesetzes (AGG) sind konsequent umzusetzen.
- **Individualisierung von Preisen gesetzlich beschränken:** KI-Verfahren, die darauf abzielen, Verbraucherpreise zu individualisieren, sind Grenzen zu setzen. Sollten Unternehmen Preise individualisieren, müssten sie zumindest immer einen Referenzpreis angeben. Hierbei handelt es sich um einen Vergleichspreis, der ohne die Berücksichtigung individueller Merkmale zustande kommt. Auch muss sichergestellt werden, dass eine Individualisierung von Preisen bei Versicherungen (wie Telematiktarifen) nicht dazu führt, dass das Kollektivprinzip ausgehöhlt wird.
- **Aufsicht befähigen und verbessern:** Eine kompetente Aufsicht über KI-basierte Entscheidungen setzt voraus, dass es überhaupt Behörden mit den notwendigen aufsichtsrechtlichen Mandaten gibt und dass diese über die fachlichen Kompetenzen und Fähigkeiten verfügen, eine effektive Kontrolle durchzuführen. Notwendig ist hierfür ein Zusammenspiel unterschiedlicher Disziplinen aus Informatik, Statistik sowie Rechts- und Sozialwissenschaften. Gleichzeitig ist dafür Sorge zu tragen, dass keine Doppel- und Parallelstrukturen aufgebaut werden. Die Bundesregierung sollte deshalb den unterschiedlichen bereits existierenden sektoralen Behörden die Kompetenz geben, KI-basierte Entscheidungen in dem jeweiligen Wirtschaftsbereich auf Rechtmäßigkeit zu überprüfen und gegenbenenfalls einzuschreiten. Überdies sollte eine Digitalagentur im Sinne eines Kompetenzzentrums geschaffen werden, um Kompetenzen in diesem Bereich zu bündeln und um andere Behörden in ihrer Arbeit zu unterstützen (SVRV 2018: 7; Gesellschaft für Informatik 2018: Abschnitt 8.2.2).
- **Rechtliche Voraussetzungen für Reverse-Engineering prüfen:** Um es Aufsicht und Forscher_innen zu ermöglichen, KI-basierte Systeme hinsichtlich ihrer Rechtskonformität zu überprüfen, sollte

die Bundesregierung die rechtlichen Voraussetzungen und Absicherungen dafür schaffen, dass ein KI-System für Aufsichts- und Forschungszwecke nachkonstruiert werden darf (Reverse-Engineering). Die rechtlichen Voraussetzungen sind hierfür derzeit unklar.

- **Allgemeines Bewusstsein für KI-basierte Entscheidungen im Verbraucheralltag schärfen:** Viele Verbraucher_innen sind sich über den Einsatz, die Funktionsweise und die Bedeutung von KI-basierten Entscheidungen nicht bewusst. Daher sollten staatliche Einrichtungen sowie Bildungsträger und Verbraucherorganisationen dazu befähigt werden, Projekte für die Wissens- und Kompetenzvermittlung zu diesem Thema umzusetzen (SVRV 2018: 5).

(3) Digitale Unternehmensverantwortung fördern

In Anlehnung an den Diskurs zur Corporate Social Responsibility (CSR) findet derzeit eine Weiterentwicklung des CSR-Konzepts statt, in dessen Kontext die Verantwortung von Unternehmen für die Auswirkungen der Digitalisierung auf die Gesellschaft betrachtet wird (Thorun et al. 2018). Das Bundesministerium der Justiz und für Verbraucherschutz hat im Jahr 2018 eine CDR-Initiative ins Leben gerufen, um dieses Konzept mit Leben zu füllen (BMJV 2019a).

Hinsichtlich des Einsatzes von KI-basierten Systemen folgt hieraus eine Reihe von Maßnahmen, die über die gesetzlichen Anforderungen hinausgehen und die Unternehmen auf freiwilliger Basis umsetzen sollten. Hierzu zählen:

- Eine konsequente Berücksichtigung von ethischen und rechtlichen Erwägungen im Design von Verfahren, Prozessen und Produkten (Ethics/Compliance by Design). Ethische Prinzipien sollten konkretisiert werden und in die Norm- und Standardsetzung bei KI-Lösungen einfließen.
- Klare Verantwortungsregelungen in Unternehmen.
- Einrichtung von Ethikbeiräten in Unternehmen, um neue Innovationen hinsichtlich ihrer ethischen Verantwortbarkeit zu bewerten.

Unternehmen wie SAP, die Deutsche Telekom oder Google haben sich bereits ethische Leitlinien auferlegt. Fachgemeinschaften wie die Gesellschaft für Informatik haben ausführliche Ethikkodizes entwickelt. Es ist zu begrüßen, dass die Wirtschaft immer stärker ethische Verantwortung zum Kern ihrer Identität macht. Gleichwohl besteht noch ein erheblicher Nachholbedarf.

Abkürzungsverzeichnis

ADM	Algorithmic Decision Making
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
ASI	Artificial Superintelligence
BGB	Bürgerliches Gesetzbuch
BMBF	Bundesministerium für Bildung und Forschung
BNETZA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CSR	Corporate Social Responsibility
DSGVO	europäische Datenschutzgrundverordnung
GS	geprüfte Sicherheit
IoT	Internet der Dinge
KBA	Kraftfahrt-Bundesamt
KI	künstliche Intelligenz
NLP	Natural Language Processing
P3P	Platform for Privacy Preferences
PET	Privacy Enhancing Technology
PIMS	Personal Information Management System
ProdHaftG	Produkthaftungsgesetz
ProdSG	Produktsicherheitsgesetz

Literaturverzeichnis

Article 29 Data Protection Working Party 2017: Guidelines on Transparency under Regulation 2016/679, wp260, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850 (5.7.2018).

Bostrom, Nick 1998: How Long Before Superintelligence?, https://nickbostrom.com/superintelligence.html (20.11.2018).

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) 2018: Big Data trifft auf künstliche Intelligenz: Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen, https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.pdf?__blob=publicationFile&v=3 (13.4.2019).

Bundesministerium der Justiz und für Verbraucherschutz (BMJV) 2015: One-Pager: Muster für transparente Datenschutzhinweise, http://www.bmjv.de/SharedDocs/Downloads/DE/Verbraucherportal/OnePager/11192915_OnePager-Datenschutzhinweise.pdf?__blob=publicationFile&v=3 (5.7.2018).

Bundesministerium der Justiz und für Verbraucherschutz (BMJV) 2019a: Corporate Digital Responsibility (CDR) – Initiative: https://www.bmjv.de/DE/Themen/FokusThemen/CDR_Initiative/CDR_Initiative_node.html (25.4.2019).

Bundesministerium der Justiz und für Verbraucherschutz (BMJV) 2019b: Richtlinie über die Förderung von Vorhaben zur Entwicklung verbraucherbezogenen Forschung und Entswicklung zu „Anwendungen künstlicher Intelligenz zur Unterstützung des Verbraucheralltags (consumer enabling technologies)“ (25.4.2019).

Bundesministerium des Innern, für Bau und Heimat (BMI); Bundesministerium der Justiz und für Verbraucherschutz (BMJV) 2018: Leitfragen der Bundesregierung an die Datenethikkommission, https://www.bmjv.de/SharedDocs/Downloads/DE/Ministerium/ForschungUndWissenschaft/DEK_Leitfragen.pdf;jsessionid=80594E26A47CBF474D0FB66E84E-F65AC.1_cid334?__blob=publicationFile&v=1 (13.4.2019).

Bundesministerium für Wirtschaft und Energie (BMWi); Bundesministerium der Justiz und für Verbraucherschutz (BMJV) 2015: „Mehr Sicherheit, Souveränität und Selbstbestimmung in der digitalen Wirtschaft“: Herausforderungen und Handlungselemente für Gesellschaft, Wirtschaft und Verbraucher, https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/Maßnahmenprogramm_BMJV_BMWi.pdf?__blob=publicationFile&v=2 (5.7.2018).

Bundesamt für Sicherheit in der Informationstechnik (BSI) 2017: G 5.143 Man-in-the-Middle-Angriff, Berlin, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05143.html (11.7.2019).

Bundesamt für Sicherheit in der Informationstechnik (BSI) 2017: Die Lage der IT-Sicherheit in Deutschland 2017, Berlin, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf;jsessionid=1703DA590A297FA3939523178D-7C254C.2_cid369?__blob=publicationFile&v=4 (11.4.2018).

Contissa, Guiseppe; Docter, Koen; Lagioia, Francesca; Lippi, Marco; Micklitz, Hans-W.; Palka, Przemyslaw; Sartor, Giovanni; Torroni, Paolo 2018: CLAUDETTE Meets GDPR Automating the Evaluation of Privacy Policies Using Artificial Intelligence, Study Report, Funded by The European Consumer Organisation (BEUC), http://www.beuc.eu/publications/beuc-x-2018-066_claudette_meets_gdpr_report.pdf (10.7.2018).

Cozy Cloud 2018: Cozy.io: Choose Simplicity, Get Cozy, https://cozy.io/en (10.7.2018).

C’t 2018: Angriff der Kryptogeld-Sauger, https://www.heise.de/ct/ausgabe/2018-9-Krypto-Miner-Ihr-PC-rechnet-fremd-4013390.html (16.4.2018).

DATENSCHUTZscanner 2017: DATENSCHUTZscanner by PrivacyGuard: Ein Forschungsprojekt gefördert vom Bundesministerium für Bildung und Forschung, https://datenschutz-scanner.de/das-projekt (10.7.2018).

Deutscher Bundestag 2018: Drucksache 19/2978: Einsetzung einer Enquete-Kommission „Künstliche Intelligenz: Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“, Berlin.

Deutsche Telekom 2016: Datenschutz – ganz einfach!, https://www.telekom.de/datenschutz-ganz-einfach (10.7.2018).

Deutsche Telekom; Qivicon 2015: Marktanalyse und Wachstumschancen, Bonn, https://www.qivicon.com/assets/PDF/Deutsche-Telekom-QIVICON-Marktanalyse-Smart-Home.pdf (8.5.2018).

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) 2015: Allgemeine Geschäftsbedingungen (AGB) von Kommunikationsdienstleistern (Ergebnisbericht), https://www.divsi.de/wp-content/uploads/2015/10/2015-10-22_DIVSI_AGB-Umfrage_Charts.pdf (5.7.2018).

Die Bundesregierung 2018: Eckpunkte der Bundesregierung für eine Strategie Künstliche Intelligenz, in: Strategie Künstliche Intelligenz der Bundesregierung, Berlin.

Die Welt 2014: Vergreistes Japan setzt in der Pflege auf Roboter, https://www.welt.de/gesundheit/article129502877/Vergreistes-Japan-setzt-in-der-Pflege-auf-Roboter.html (20.11.2018).

Digi.me. 2018: Digi.me: Take Control of the Data Powering Your Digital Life, http://digi.me (10.7.2018).

Drösser, Christoph 2016: Total berechenbar?: Wenn Algorithmen für uns entscheiden, München.

eco – Verband der Internetwirtschaft e. V.; Arthur D. Little 2017: Der deutsche Smart-Home-Markt 2017-2022: Zahlen und Fakten, https://www.eco.de/presse/studie-von-eco-und-adl-smart-home-umsaetze-verdreifachen-sich-bis-2022-auf-43-milliarden-euro (8.5.2018).

Elshout, Maartje; Elsen, Millie; Leenheer, Jorna; Loos, Marco; Luzak, Joasia 2016: Study on Consumers' Attitudes Towards Terms and Conditions (T&Cs): Final Report, Report for the European Commission, Consumers, Health, Agriculture and Food Executive Agency (Chafea) on Behalf of Directorate-General for Justice and Consumers, Amsterdam.

Europäische Kommission 2019: Communication from the Commission: Building Trust in Human-Centric Artificial Intelligence, Brüssel.

Europäische Kommission 2018: Rechtsakt zur Cybersicherheit, https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_de (11.7.2019).

Fischer-Hübner, Simone; Wästlung, Erik; Zwingelberg, Harald (Hrsg.) 2009: UI Prototypes: Policy Administration and Presentation (Version 1), Deliverable D4.3.1 of the EC FP7 Project PrimeLife, http://primelife.ercim.eu/images/stories/deliverables/d4.3.1-ui_prototypes-policy_administration_and_presentation_v1.pdf (10.7.2018).

Fraunhofer-Gesellschaft 2017: Trends für die künstliche Intelligenz, https://www.fraunhofer.de/content/dam/zv/de/publikationen/broschueren/Trends-fuer-die-kuenstliche-Intelligenz.pdf (20.11.2018).

Frankfurter Allgemeine Zeitung 2017: Unsichere Technik: Warnung vor Hackerangriffen auf Autos, http://www.faz.net/aktuell/wirtschaft/unternehmen/allianz-warnt-vor-hackerangriffen-auf-autos-15251834.html (13.4.2018).

Gesellschaft für Informatik 2018: Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen, Berlin.

Gluck, Joshua; Schaub, Florian; Friedman, Amy; Habib, Hana; Sadeh, Norman; Cranor, Lorrie Faith; Agarwal, Yuvraj 201: How Short Is Too Short?: Implications of Length and Framing on the Effectiveness of Privacy Notices, in: Symposium on Usable Privacy and Security (SOUPS), Denver, S. 321–340.

Handelsblatt 2017: Mit Algorithmen zur besseren Diagnose, http://www.handelsblatt.com/my/technik/medizin/kuenstliche-intelligenz-im-krankenhaus-mit-algorithmen-zur-besseren-diagnose/19783458.html?ticket=ST-7152776-bMnKOadjv0TaHJ96Bred-ap4 (20.11.2018).

Harkous, Hamza; Fawaz, Kassem; Lebret, Rémi; Schaub, Florian; Shin, Kang G.; Aberer, Karl 2018: Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning, USENIX Security 2018, Baltimore, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-harkous.pdf (13.4.2019).

Heise Online 2015: Prognose: 250 Millionen vernetzte Autos zum Jahr 2020, https://heise.de/-2528445 (18.4.2018).

Heise Online 2017: Internet der Dinge: Forscher fordern verschärftes Haftungsrecht für vernetzte Produkte, https://heise.de/-3761982 (8.5.2018).

Heise Online 2018: Künstliche Intelligenz: Facebook sagt Nutzerverhalten voraus und verkauft damit Anzeigen; https://www.heise.de/newsticker/meldung/Kuenstliche-Intelligenz-Facebook-sagt-Nutzerverhalten-voraus-und-verkauft-damit-Anzeigen-4024377.html (20.11.2018).

Herbig, Daniel 2018: Gespeicherter Standortverlauf: Bundesregierung rügt Google, in: Heise Online, 28.8.2018, https://www.heise.de/newsticker/meldung/Gespeicherter-Standortverlauf-Bundesregierung-ruegt-Google-4147018.html (13.4.2019).

High-Level Expert Group on Artificial Intelligence 2019: Policy and Investment Recommendations for Trustworthy AI, Brüssel.

Holtz, Leif-Erik Nocun, Katharina; Hansen, Marit 2011: Towards Displaying Privacy Information with Icons: Privacy and Identity Management for Life, http://dl.ifip.org/db/conf/primelife/primelife2010/HoltzNH10.pdf (13.4.2019).

Horizont 2017: Vernetzte Kleidung: Das ist die sprechende Jeansjacke von Google und Levi's, http://www.horizont.net/tech/auftritte-des-tages/Vernetzte-Kleidung-Das-ist-die-sprechende-Jeansjacke-von-Google-und-Levis-161403 (12.4.2018).

Horn, Nikolai; Riechert, Anne; Müller, Christian 2017: Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, Stiftung Datenschutz, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf (10.7.2018).

Kettner, Sara Elisa; Thorun, Christian; Kleinhans, Jan-Peter 2018a: Big Data im Bereich Heim und Freizeit mit Schwerpunkt Smart Living: Status Quo und Entwicklungstendenzen, http://www.abida.de/sites/default/files/Gutachten_HeimUndFreizeit.pdf (5.7.2018).

Kettner, Sara Elisa; Thorun, Christian; Vetter, Max 2018b: Wege zur besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz, ConPolicy – Institut für Verbraucherpolitik, https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf (5.7.2018).

Klar, Thomas 2018: Kundenservice der Zukunft, https://www.computerwoche.de/a/kundenservice-der-zukunft,3545038 (20.11.2018).

Lippi, Marco; Palka, Przemyslaw; Contissa, Guiseppe; Lagioia, Francesca; Micklitz, Hans-W.; Sartor, Giovanni; Torroni, Paolo 2018: CLAUDETTE: An Automated Detector of Potentially Unfair Clauses in Online Terms of Service, https://arxiv.org/pdf/1805.01217.pdf (13.4.2019).

Margraf, Marian 2017: Datenschutz und -sicherheit in einer zunehmend vernetzten Welt, in: Datenschutz und Datensicherheit: DuD Januar 2017, 41 (1), S. 21–23, https://link.springer.com/article/10.1007/s11623-017-0719-x (8.5.2018).

Margraf, Marian; Pfeiffer, Stefan 2015: Benutzerzentrierte Entwicklung für das Internet der Dinge, in: Datenschutz und Datensicherheit 39 (4), S. 246–249, https://link.springer.com/article/10.1007/s11623-015-0404-x (8.5.2018).

Marktwächter Digitale Welt 2017: E-Payment: Wie sicher sind unsere Daten beim Bezahlen im Netz?: Eine Untersuchung der Verbraucherzentralen, https://ssl.marktwaechter.de/sites/default/files/downloads/17-11-14_untersuchungsbericht_e-payment.pdf (5.7.2018).

Mitteldeutscher Rundfunkt 2019: Hilfe in der Pflege: Roboter „Pepper" stellt sich vor, https://www.mdr.de/wissen/pflegeroboter-pepper-100.html (13.4.2019).

Microsoft 2017: Künstliche Intelligenz: Neue Modelle für Versicherungen, https://enterprise.microsoft.com/de-de/articles/industries/insurance/kuenstliche-intelligenz-neue-modelle-fuer-versicherungen (20.11.2018).

MyData 2018: MyData Global Network, https://mydata.org (10.7.2018).

Netzpolitik.org 2019: IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll, https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll (11.7.2019).

Oliver Wyman Analysis 2015: Global Production Forecast for Semi- and Fully Automated Vehicles, http://www.oliverwyman.de/content/dam/oliver-wyman/global/en/files/who-we-are/press-releases/OliverWyman_Graphics_Value%20Pools%20Autonomous%20Driving_EN_16072015_final.pdf (13.4.2019).

Platform for Privacy Preferences (P3P) Project o. J.a: Enabling Smarter Privacy Tools for the Web, https://www.w3.org/P3P (10.7.2017).

Platform for Privacy Preferences (P3P) Project o. J.b: Privacy Bird, http://www.privacybird.org/tour/1_3_beta/tour.html (10.7.2017).

Rott, Peter 2018: Rechtspolitischer Handlungsbedarf im Haftungsrecht, insbesondere für Digitale Anwendungen, Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V., Berlin, https://www.vzbv.de/sites/default/files/downloads/2018/05/04/gutachten_handlungsbedarf_im_haftungsrecht.pdf (9.5.2018).

Sachverständigenrat für Verbraucherfragen (SVRV) 2017: Digitale Souveränität, Gutachten des Sachverständigenrats für Verbraucherfragen, Berlin, http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_Digitale_Souveränität_.pdf (20.11.2018).

Sachverständigenrat für Verbraucherfragen (SVRV) 2018: Verbrauchergerechtes Scoring, Gutachten des Sachverständigenrats für Verbraucherfragen, Berlin, http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Verbrauchergerechtes_Scoring.pdf (31.10.2018).

Search Engine Land 2015: Meet RankBrain: The Artificial Intelligence That's Now Processing Google Search Results, https://searchengineland.com/meet-rankbrain-google-search-results-234386 (20.11.2018).

Searle, John R. 1980: Minds, Brains, and Programs, http://cogprints.org/7150/1/10.1.1.83.5248.pdf (20.11.2018).

Special Eurobarometer 431 2015: Data Protection, https://data.europa.eu/euodp/de/data/dataset/S2075_83_1_431_ENG (10.7.2018).

Spiegel Online 2017: Sicherheitslücke bei Herzschrittmachern: 13.000 deutsche Patienten müssen für Update ins Krankenhaus, http://www.spiegel.de/netzwelt/gadgets/abbott-herzschrittmacher-mit-schwachstelle-13-000-patienten-in-deutschland-betroffen-a-1165555.html (13.4.2018).

Spindler, Gerald 2007a: Gutachten zu Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären im Auftrag des Bundesamts für Sicherheit in der Informationstechnik, Bonn, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2 (8.5.2018).

Spindler, Gerald 2007b: Digitales Produktsicherheitsrecht, Vortrag über mögliche regulatorische Ansatzpunkte für ein Digitales Produktsicherheitsrecht im Bundesministerium der Justiz und für Verbraucherschutz, 5.7.2017, http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/20170704dig_ProduktsicherheitsR.pdf?__blob=publicationFile&v=2 (8.5.2017).

Spindler, Gerald 2015: Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz: Braucht das Recht neue Haftungskategorien?: Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, in: Computer und Recht 31 (12), S. 766–776, https://www.degruyter.com/view/j/cr.2015.31.issue-12/cr-2015-1205/cr-2015-1205.xml (8.5.2017).

Spindler, Gerald 2018: Zukunft der Digitalisierung: Datenwirtschaft in der Unternehmenspraxis, https://der-betrieb.owlit.de/document.aspx/?sUrl=rn%3aroex%5e%5efile%3a%2f%2fR|%2f03%2f02%2f01%2fzsa%2fdb%2f18%2f1%2f181a35dc87152b52d3e662333480aaaf.xml&ref=searchservice&authentication=none (15.1.2018).

Süddeutsche Zeitung 2017: Die Daten eines Autos sind das neue Öl, http://www.sueddeutsche.de/auto/vernetzte-autos-die-daten-eines-autos-sind-das-neue-oel-1.3469344 (12.4.2018).

The Guardian 2016: Tay, Microsoft's AI Chatbot, Gets a Crash Course in Racism from Twitter, https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter (20.11.2018).

THIS Magazin 2017: Bosch setzt auf vernetztes Elektrowerkzeug, http://www.this-magazin.de/artikel/tis_Vernetzte_Werkzeuge_2789600.html (10.4.2018).

Thorun, Christian; Kettner, Sara Elis; Merck, Johannes 2018: Ethik in der Digitalisierung: Der Bedarf für eine Corporate Digital Responsibility, https://library.fes.de/pdf-files/wiso/14691.pdf (13.4.2019).

TNS Emnid; Verbraucherzentrale Bundesverband (vzbv) 2015: Datenschutz: Die Sicht der Verbraucherinnen und Verbraucher in Deutschland, http://www.vzbv.de/sites/default/files/downloads/Datenschutz_Umfrage-Sicht-Verbraucher-Ergebnisbericht-TNS-Emnid-Oktober-2015.pdf (5.7.2018).

T-Online 2018: DSGVO-Beschwerden: Datenschutzbeauftragte klagen wegen Überlastung, https://www.t-online.de/digital/internet/id_83989016/folgen-der-dsgvo-datenschutzbeauftragte-klagen-wegen-ueberlastung.html (30.8.2018).

TÜV Informationstechnik GmbH (TÜViT) 2006: Nachweis der Datenschutzkonformität, https://www.tuvit.de/de/leistungen/datenschutz/trusted-site-privacy (10.7.2018).

TÜV Informationstechnik GmbH (TÜViT); Crisp Research 2017: Security by Design: Die Rolle von IT-Sicherheitsstrategien in der Digitalisierung, https://www.tuvit.de/de/aktuelles/beitraege-white-paper/security-by-design (11.4.2018).

t3n 2017: Was ist eigentlich der Unterschied zwischen AI, Machine Learning, Deep Learning und Natural Language Processing?, https://t3n.de/news/ai-machine-learning-nlp-deep-learning-776907 (20.11.2018).

t3n. 2018: Nach Angriff auf 1,25 Millionen Telekom-Router: Hacker erhält Bewährungsstrafe, https://t3n.de/news/telekom-router-angriff-urteil-842758 (12.4.2018).

Ulmer, Claus D. 2016: Preserving the Utility of Data and Privacy of Individuals: Future of Privacy Forum, https://fpf.org/wp-content/uploads/2016/11/161108-BPS-Ulmer.pdf (10.7.2018).

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) 2014: Datenschutz-Gütesiegel beim ULD, https://www.datenschutzzentrum.de/guetesiegel (10.7.2018).

Verbraucherzentrale Bundesverband 2019: EU verbessert Gewährleistungsrecht für Verbraucher, https://www.vzbv.de/meldung/eu-verbessert-gewaehrleistungsrecht-fuer-verbraucher (11.7.2019).

Wendehorst, Christiane 2017: Besitz und Eigentum im Internet der Dinge, in: Micklitz, Hans-Wolfgang; Joost, Gesche; Reisch, Lucia; Zander-Hayat, Helga (Hrsg.): Verbraucherrecht 2.0: Verbraucher in der digitalen Welt, Baden-Baden, S. 337–414, https://www.nomos-elibrary.de/10.5771/9783845284569-367/besitz-und-eigentum-im-internet-der-dinge (8.5.2018).

Zalando SE 2016: Datenschutz-One-Pager, https://a1276.ztat.net/lpo/zalando/1_cro/2017/02/BIT-129/zalando-onepager.pdf (10.7.2018).

Zeit Online 2017: Eine Sprache macht noch keinen Terminator, http://www.zeit.de/digital/internet/2017-08/kuenstliche-intelligenz-sprache-lernen-facebook-chatbot (20.11.2018).

Impressum:

Friedrich-Ebert-Stiftung
Herausgeberin: Abteilung Wirtschafts- und Sozialpolitik
Godesberger Allee 149, D-53175 Bonn
Fax 0228 883 9202, 030 26935 9229, www.fes.de/wiso

Bestellungen/Kontakt: wiso-news@fes.de

ISBN: 978-3-96250-329-1

Diese Publikation wird aus Mitteln der Franziska- und Otto-Bennemann-Stiftung gefördert.

Titelmotiv: © metamorworks / Adobe Stock
Gestaltungskonzept: www.stetzer.net
Druck: www.bub-bonn.de

ABTEILUNG WIRTSCHAFTS- UND SOZIALPOLITIK

WEITERE VERÖFFENTLICHUNGEN ZUM THEMA

Die Grundversorgung mit Strom und Gas in Deutschland: Potenziale zur Verbraucherentlastung und Handlungsoptionen
WISO DISKURS – 03/**2019**

Das Vorsorgekonto: Basisprodukt für die private Altersvorsorge
WISO DISKURS – 01/**2019**

Verbraucherschutz in der Plattformökonomie
WISO DISKURS – 15/**2018**

Fighting Energy Poverty in Europe: Responses, Instruments, Successes
GOOD SOCIETY – SOCIAL DEMOCRACY #2017 – 2017

Verbraucherdatenschutz in der Digitalisierung: Herausforderungen und Lösungsansätze
WISO DIREKT – 19/**2017**

Wohlfahrts- und Verteilungswirkungen personalisierter Preise und Produkte
WISO DISKURS – 06/**2017**

Digitale Plattformen: Ein neues Handlungsfeld für die Daseinsverantwortung des Staates?
WISO DIREKT – 09/**2017**

Energiearmut bekämpfen: Instrumente, Maßnahmen und Erfolge in Europa
GUTE GESELLSCHAFT – SOZIALE DEMOKRATIE #2017PLUS – 2017

Mehr Mitsprache und Orientierung: Vorschläge für ein nutzerfreundliches und patientenorientiertes Gesundheitssystem
WISO DISKURS – 01/**2017**

Blockchain in der Energiewirtschaft: Schöne neue (digitale) Energiewelt für Verbraucher_innen und Prosumer?
WISO DIREKT – 30/**2016**

Prospects for Consumers in a European Energy Union
GOOD SOCIETY – SOCIAL DEMOCRACY #2017 – 2016

Verbraucherschutz und Verbraucherpolitik im Urteil der Bevölkerung: Eine Repräsentativbefragung der Bevölkerung ab 16 Jahre
WISO DISKURS – 08/**2016**

Rechtsdurchsetzung im Verbraucherdatenschutz: Bestandsaufnahme und Handlungsempfehlungen
GUTE GESELLSCHAFT – SOZIALE DEMOKRATIE #2017PLUS – 2016

Herausforderung Verbraucherdatenschutz in der digitalen Welt
GUTE GESELLSCHAFT – SOZIALE DEMOKRATIE #2017PLUS – 2015

FRIEDRICH EBERT STIFTUNG

Volltexte dieser Veröffentlichungen finden Sie bei uns im Internet unter

www.fes.de/wiso