SVRV Sachverständigenrat für Verbraucherfragen

Digitale Souveränität

Gutachten des Sachverständigenrats für Verbraucherfragen

Juni 2017

Mitglieder des SVRV

Prof. Dr. Lucia Reisch (Vorsitzende)
Professorin für Interkulturelle Konsumforschung und europäische Verbraucherpolitik an der Copenhagen Business School

Dr. Daniela Büchel (stellv. Vorsitzende)
Mitglied der Geschäftsleitung REWE für die Bereiche Human Resources und Nachhaltigkeit

Prof. Dr. Gerd Gigerenzer
Direktor der Abteilung „Adaptives Verhalten und Kognition“ und des Harding-Zentrums für Risikokompetenz am Max-Planck-Institut für Bildungsforschung in Berlin

Helga Zander-Hayat
Leiterin des Bereichs Markt und Recht bei der Verbraucherzentrale Nordrhein-Westfalen

Prof. Dr. Gesche Joost
Professorin für das Fachgebiet Designforschung an der Universität der Künste und Internetbotschafterin der Bundesregierung im Gremium der „Digital Champions“ der EU

Prof. Dr. Hans-Wolfgang Micklitz
Professor für Wirtschaftsrecht am Europäischen Hochschulinstitut in Florenz

Prof. Dr. Andreas Oehler
Professor für Finanzwirtschaft an der Universität Bamberg und Direktor der Forschungsstelle Verbraucherfinanzen und Verbraucherbildung

Prof. Dr. Kirsten Schlegel-Matthies
Professorin für Haushaltswissenschaft an der Universität Paderborn

Prof. Dr. Gert G. Wagner
Professor für Empirische Wirtschaftsforschung und Wirtschaftspolitik an der Technischen Universität Berlin, Vorstandsmitglied des Deutschen Instituts für Wirtschaftsforschung und Max Planck Fellow am MPI für Bildungsforschung

Mitarbeitende des SVRV

Leiter der Geschäftsstelle:
Thomas Fischer, M.A.

Wissenschaftlicher Stab der Geschäftsstelle:
Dr. Irina Domurath, Dr. Christian Groß

Gliederung

Vorwort

Executive Summary

1. Stand der Debatte

2. Konzept: Leitlinien und Handlungsfelder

2.1. Vier Leitlinien: Wahlfreiheit, Selbstbestimmung, Selbstkontrolle, Sicherheit

2.2. Drei Handlungsfelder: Technologie, Digitale Kompetenz, Regulierung

3. Technologie

3.1. Verbraucherzentriertes Datenportal schaffen

3.2. Prinzipien Privacy by Design und Privacy by Default durchsetzen

3.3. Sicherheit im Internet of Things erhöhen

3.4. Angebot an datensparsamen Produkten vergrößern

4. Digitale Kompetenz

4.1. Qualifizierungs-Pakt für „Digitale Kompetenz in der Lehrerbildung“ schließen

4.2. Angebote zur Förderung digitaler Kompetenz unterstützen

4.3. Maßnahmen zur Selbstkontrolle bei der Nutzung digitaler Medien und Dienstleistungen entwickeln

4.4. Auswirkungen der Digitalisierung auf Kognition, Emotion und soziales Leben erforschen

5. Regulierung

5.1. AGB und Datenschutzerklärungen als One-Pager umsetzen

5.2. Algorithmen offenlegen und überprüfbar machen

5.3. Unentgeltlichen Auskunftsanspruch nachbessern

5.4. Mindeststandards für Interoperabilität weiterentwickeln

5.5. Recht auf Datenportabilität konkretisieren

Literatur

Vorwort

Seit seiner Einsetzung bearbeitet der SVRV mit unterschiedlichen Schwerpunktsetzungen fortlaufend das Leitthema „Verbraucher in der digitalen Welt". In seinem Grundsatzpapier „Verbraucherpolitik in der digitalen Welt: Standpunkte des Sachverständigenrates für Verbraucherfragen" (SVRV, 2015) setzte sich der SVRV dafür ein, durch eine datenschutzfreundliche Gestaltung von Technologie, durch Stärkung der digitalen Kompetenz der Verbraucher und durch umsichtige Regulierung die Vorteile der Digitalisierung möglichst vielen Verbrauchern zugutekommen zu lassen. Damit ist der SVRV keineswegs alleine: Auch in der internationalen Verbraucherpolitik, wie 2017 im Rahmen der G20 Verhandlungen der Digitalminister, wird an Rahmenbedingungen für eine gemeinwohlorientierte Regulierung der digitalen Welt gearbeitet (BMWi, 2017a). Diese Kernforderungen aufgreifend, schließt das hier vorgelegte Gutachten an mehrere Vorarbeiten des SVRV in den Bereichen der Verbraucherkompetenz und Regulierung an und vertieft darüber hinaus technologische Aspekte der Digitalisierung. Im Bereich verbraucherfreundlicher Technologie setzt der SVRV Schwerpunkte durch die Studien „Der Wert der persönlichen Daten"[1] und „Technologien für und wider Digitale Souveränität"[2]. Ausgehend von dem Themenpapier „Digitale Welt und Gesundheit. eHealth und mHealth – Chancen und Risiken der Digitalisierung im Gesundheitsbereich" bekräftigt der SVRV die Position, dass ohne eine Stärkung der digitalen Kompetenz die Chancen der Digitalisierung vergeben werden. Fragen der Regulierung behandelte der SVRV bereits in dem Gutachten „Verbraucherrecht 2.0" sowie in dem Working Paper „Personalisierte Preise", in denen der SVRV beispielsweise auf Einwilligungserfordernisse, Offenlegungspflichten der Anbieter oder das Recht auf diskriminierungsfreien Zugang zu Angeboten verweist.

Besonderer Dank gilt Gesche Joost für die federführende Betreuung des Gutachtens. Bei der Erstellung des Gutachtens haben weiterhin mitgewirkt: Daniela Büchel, Gerd Gigerenzer, Hans Micklitz, Lucia A. Reisch, Kirsten Schlegel-Matthies, Gert G. Wagner und Helga Zander-Hayat.

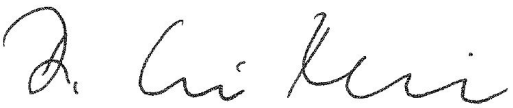
Der SVRV dankt allen Mitarbeitern der Geschäftsstelle des SVRV für die umfassende Unterstützung bei der Erarbeitung des Gutachtens. Wir danken insbesondere dem wissenschaftlichen Stab des SVRV, Christian Groß, Irina Domurath und Mathias Bug.

Daneben dankt der SVRV den Verfassern der Studie „Technologie für und wider Digitale Souveränität", Rüdiger Weis, Stefan Lucks und Volker Grassmuck sowie den Verfassern der Studie „Der Wert persönlicher Daten: Ist Datenhandel der bessere Datenschutz?", Walter Palmetshofer, Arne Semsrott und Anna Alberts, für das Einbringen ihrer Expertisen.

Abschließend sei darauf hingewiesen, dass die Sprache in diesem Text grundsätzlich geschlechterneutral gemeint ist. Auf eine durchgehende Nennung beider Geschlechter wurde zugunsten der besseren Lesbarkeit verzichtet.

Berlin im Juni 2017

Für den Sachverständigenrat für Verbraucherfragen



Lucia Reisch
Vorsitzende des SVRV

Gesche Joost
Mitglied des SVRV

1 Abgerufen am 20. Juni 2017 von URL http://www.svr-verbraucherfragen.de/wp-content/uploads/Open_Knowledge_Foundation_Studie.pdf.
2 Abgerufen am 20. Juni 2017 von URL http://www.svr-verbraucherfragen.de/wp-content/uploads/Weis_Lucks_Grassmuck_Studie_.pdf.

Executive Summary

Mit dem Gutachten „Digitale Souveränität“ leistet der Sachverständigenrat für Verbraucherfragen (SVRV) einen Beitrag zu der fortlaufenden Debatte zur Weiterentwicklung des Begriffs der Digitalen Souveränität aus verbraucherpolitischer Perspektive.

Unter Digitaler Souveränität verstehen wir die Handlungsfähigkeit und Entscheidungsfreiheit der Verbraucher, in der Digitalen Welt in verschiedenen Rollen zu agieren, nämlich als Marktteilnehmer, als Konsumentenbürger einer Gesellschaft sowie als „Prosumer“ in Netzwerken. Der Begriff verweist darüber hinaus auf die Rechte und Pflichten von Bürgern im staatlichen Ordnungsrahmen und unterstreicht die Rahmenbedingungen, unter denen das Individuum frei, kompetent und verantwortungsvoll digitale Medien und Dienste nutzen kann und somit in die Lage versetzt wird, aktiv als Bürger an einer digitalen Gesellschaft teilzuhaben.

Wir identifizieren vier Leitlinien, die im Zusammenhang mit Digitaler Souveränität stehen: Wahlfreiheit, Selbstbestimmung, Selbstkontrolle und Sicherheit. Um diese zu realisieren, schlagen wir die nachfolgenden Maßnahmen vor, die auf den Handlungsfeldern verbraucherfreundliche Technologie, digitale Kompetenz und Regulierung ergriffen werden sollten.

Technologie

- **Verbraucherzentriertes Datenportal schaffen:** Der SVRV empfiehlt die Entwicklung eines verbraucherzentrierten Datenportals (Dashboard) zur Realisierung der individuellen Datensouveränität.

- **Prinzipien Privacy by Design und Privacy by Default durchsetzen:** Der SVRV bekräftigt die Forderung nach einer nutzerfreundlichen, datensparsamen und gleichzeitig sicherheitsorientierten Voreinstellung von Kommunikationssystemen (Privacy / Security by Design und Privacy / Security by Default als Leitlinien). Staatlich geförderte Projekte müssen sich an diesen Linien orientieren.

- **Sicherheit im Internet of Things erhöhen:** Der SVRV empfiehlt zu prüfen, wie angesichts der sich immer mehr verstärkenden Sicherheitsprobleme im Internet-of-Things-Segment sichergestellt werden kann, wie – in Anlehnung an Verfahren aus dem Gesundheitsbereich – in den Verkehr gebrachte Produkte und Dienstleistungen über den gesamten Lebenszyklus hinweg durch Sicherheitsupdates verpflichtend kontinuierlich abzusichern sind. Hierzu sind technologische Standards zu entwickeln und Quellcodes (analog der „Rezeptur“ im Lebensmittelbereich) dauerhaft zu hinterlegen.

- **Angebot an datensparsamen Produkten vergrößern:** Der SVRV empfiehlt zu prüfen, ob Verbrauchern ein Recht auf die Nutzung datenerhebungsarmer digitaler Produkte eingeräumt werden kann, bei dem Verbraucher die Wahl haben, auf datenerhebungsarme Varianten digital zugreifen zu können.

Digitale Kompetenz

- **Qualifizierungs-Pakt für „Digitale Kompetenz in der Lehrerbildung“ schließen:** Der SVRV empfiehlt die Etablierung eines Qualifizierungs-Paktes für „Digitale Kompetenz in der Lehrerbildung“ (analog zum Qualitätspakt Lehre oder zur Qualitätsoffensive Lehrerbildung).

- **Angebote zur Förderung Digitaler Kompetenz unterstützen:** Der SVRV empfiehlt, bereits bestehende und neu zu etablierende (institutionelle) Angebote zur Förderung digitaler Kompetenz dauerhaft zu finanzieren und strukturell zu verankern. Dabei sollten Angebote mit Lotsenfunktion, Angebote für Multiplikatoren und Angebote für Verbraucher systematisch ausgebaut werden.

- **Maßnahmen zur Selbstkontrolle bei der Nutzung digitaler Medien und Dienstleistungen entwickeln:** Der SVRV empfiehlt den Kultusministerien, Maßnahmen zur Förderung der Selbstkontrolle bei der Nutzung digitaler Medien und Dienstleistungen zu entwickeln.

- **Auswirkungen der Digitalisierung auf Kognition, Emotion und soziales Leben erforschen:** Der SVRV empfiehlt die gezielte Förderung interdisziplinärer Forschung über die Auswirkung der Digitalisierung auf die Kognition, Emotion und das soziale Leben von Verbrauchern. Das betrifft sowohl „Digital Natives“ als auch „Digital Migrants“.

Regulierung

- **AGB und Datenschutzerklärungen als One-Pager umsetzen:** Der SVRV bekräftigt seine Empfehlung, dass der Unternehmer den Verbraucher auf je einer Seite (500 Wörter) über die relevanten datenschutzrechtlichen Vorgaben sowie über die AGB-Bestimmungen vor Vertragsschluss zu informieren hat. Der SVRV empfiehlt, diesen „One-Pager“ in einem vom BMJV organisierten Pilotprojekt mit relevanten Stakeholdern umzusetzen.

- **Algorithmen offenlegen und überprüfbar machen:** Der SVRV bekräftigt seine Empfehlungen, dass durch rechtliche Vorgaben sichergestellt werden muss, (a) dass Algorithmen die Vorgaben des Verbraucherrechts, des Datenschutzrechts, des Anti-Diskriminierungsrechts und der digitalen Sicherheit berücksichtigen, sowie die zugrundeliegenden Parameter bei Algorithmen mit direktem Verbraucherkontakt transparent zu machen, (b) dass Algorithmen durch standardisierte Offenlegungspflichten einem Kreis von Experten offengelegt werden, die per Stichprobe die rechtliche Unbedenklichkeit überprüfen. Der SVRV empfiehlt, rechtliche Standards zu entwickeln und Quellcodes dauerhaft zu hinterlegen.

- **Unentgeltlichen Auskunftsanspruch nachbessern:** Der Sachverständigenrat empfiehlt, den unentgeltlichen Auskunftsanspruch (§ 34 BDSG) ohne Limitierung zu gewähren sowie Unternehmen zu verpflichten, Verbraucher auf ihre kostenlosen Auskunftsrechte und auf die Möglichkeit der Berichtigung fehlerhafter Daten transparent, verständlich und leicht erkennbar beim Anbieten ihrer Produkte hinzuweisen (d. h. Berichtigung, Löschung und Sperrung).

- **Mindeststandards für Interoperabilität weiterentwickeln:** Der SVRV empfiehlt, Mindeststandards zu entwickeln, die eine Kompatibilität zwischen digitalen Diensten sicherstellen, so dass eine Kommunikation zwischen Nutzer-Accounts unabhängig vom Anbieter möglich ist (Interoperabilität – analog zum Mobilfunk).

- **Recht auf Datenportabilität konkretisieren:** Der SVRV bekräftigt seine Empfehlung, das Recht auf Datenportabilität als Kündigungsrecht zu verstehen und empfiehlt, einen Rahmen für einen Wechsel zwischen Anbietern festzulegen (analog zum digitalen Zahlungsverkehr).

1. Stand der Debatte

Digitale Produkte und Dienstleistungen durchdringen heute den Alltag von Verbrauchern und stellen die Verbraucherpolitik vor neue Herausforderungen. Internetfähige mobile Endgeräte finden eine immer stärkere Verbreitung und werden insbesondere bei Jugendlichen von nahezu allen Befragten im Alter von 12 bis 19 Jahren benutzt (Feierabend et al., 2016). Auch bei der gesamten Bevölkerung in Deutschland sind die Nutzerzahlen hoch und liegen gegenwärtig bei zwei Drittel der Bevölkerung (Initiative D21, 2016). Selbst bei den sogenannten „Silver Surfern" (d.h. User ab 60 Jahren) sind etwa die Hälfte der unter 70-Jährigen und ein Viertel der über 70-Jährigen regelmäßig mobil im Netz (Initiative D21, 2016; Destatis, 2016).

Dabei zeichnet sich eine wachsende Vertrauenskrise der Verbraucher gegenüber Online-Dienstleistern in Bezug auf die Nutzung (Stichwörter: Datenhandel und Big Data) und Sicherheit ihrer Daten (Stichwörter: Hacking-Angriffe und Phishing-Vorfälle) sowie den Wahrheitsgehalt von Online-Inhalten (Stichwort: Gezielte Desinformation bzw. „Fake News") ab. So misstrauen laut einer Studie von Orange (2014) fast 80 Prozent der Verbraucher Online-Dienstleistern und halten deren Nutzung von Daten für intransparent. Dennoch ist die überwiegende Zahl weiterhin gewillt, persönliche Daten zu teilen, wenn sie im Gegenzug dazu Dienstleistungen nutzen kann (zur Datennutzung zu Werbezwecken siehe Destatis, 2016). Dies zeugt von asymmetrischen Machtverhältnissen zwischen Unternehmen und Individuen: Erstere haben Zugriff auf die Menge der individuellen Daten, während den Verbrauchern das Wissen und die Kontrolle darüber fehlt (World Economic Forum, 2014).

Nutzung von Daten: Ein möglicher Grund für die beschriebene Vertrauenskrise liegt in der wachsenden Zahl an Online-Dienstleistungen, deren Geschäftsmodell auf der Sammlung und Auswertung großer Datenmengen beruht (siehe z. B. Christl & Spiekermann, 2016; Karaboga et al., 2014; zur Verbreitung der Nutzung in Deutschland: Destatis, 2016). Dies führt zu einem wachsenden „digitalen Fußabdruck", der detaillierte Aussagen über individuelles Konsumverhalten, soziales Umfeld und Vorlieben gibt (Golder & Macy, 2014) bzw. mittels Big Data deren Vorhersage ermöglicht. Als Folge können aus den Daten zum Beispiel Informationen über das Zahlungsverhalten bzw. die Zahlungsbereitschaft von Verbrauchern abgeleitet und somit personalisierte Preise gebildet werden (Schleusener & Hosell, 2015; Zander-Hayat et al., 2016a; Zander-Hayat et al., 2016b). Bei diesen Entwicklungen kommt etablierten Online-Plattformen wie Google, Facebook, Amazon und YouTube eine besondere Bedeutung zu, da diese im Online-Segment eine erhebliche Marktmacht erlangt haben und Alternativangebote aus Sicht der Verbraucher oft fehlen oder nicht attraktiv genug sind. Zur Realität gehört ebenso der von vielen Verbrauchern empfundene Gruppendruck, sich dennoch über die genannten Plattformen zu vernetzen und dort zu konsumieren: Obwohl ein Anbieterwechsel aus technischer Sicht zwar grundsätzlich möglich ist, wird dieser kaum praktiziert, da die Interoperabilität zwischen den Anbietern sehr lückenhaft ist und entsprechend die Datenportabilität von Nutzungsdaten hin zu einem neuen Anbieter sehr aufwändig und benutzerunfreundlich ist.

Sicherheit von Daten: Auf dem Online-Markt besteht aus Sicht der Verbraucher zudem Handlungsbedarf mit Blick auf die Schaffung einer wirksamen Sicherheitsarchitektur. Dies wird dadurch unterstrichen, dass persönliche Erfahrungen mit Online-Kriminalität – wie die Verbreitung von Computerviren, Identitätsdiebstahl und Missbrauch von Online-Banking-Daten – verstärkt auftreten (Birkel et al., 2014; Rieckmann & Kraus, 2015; Bug et al., 2015; Bundeskriminalamt, 2016). Zudem wurde das Vertrauen von Verbrauchern in die Sicherheit ihrer Endgeräte unter anderem durch jüngste Denial-of-Service Angriffe[3] auf Teile des Internet of Things – „intelligente Alltagsgegenstände", die mit dem Internet vernetzt sind – enttäuscht (Möchel, 2016; Weis et al., 2016).

Online-Inhalte: Ferner breitet sich das Phänomen der gezielten Desinformation auf sozialen Netzwerken und ideologisch motivierten Websites aus (Stichwort: „Fake News"; siehe z. B. Kucharski, 2016; Spinney, 2017), was zum jetzigen Zeitpunkt den einzelnen Usern ein grundständiges Einschätzungsvermögen hinsichtlich der Glaubwürdigkeit der Quellen und der Inhalte abverlangt. Darüber hinaus hat be-

3 Bei einem (Distributed) Denial-of-Service Angriff werden so viele gleichzeitige Anfragen von vielen verschiedenen Geräten auf einen oder mehrere Server geschickt, bis diese schlicht überlastet sind. Solche Attacken sind nicht selten; Serverprovider und spezialisierte Unternehmen können einen Teil von ihnen abfangen. Doch je stärker und länger die Angriffe dauern, desto schwieriger wird es (Kühl & Breitegger, 2016).

reits fast jeder fünfte deutsche Jugendliche persönliche Erfahrungen mit Online-Mobbing und Hetze in sozialen Medien gemacht. Zu diesem Ergebnis kam im Jahr 2015 eine Studie von YouGov, die im Auftrag von Vodafone durchgeführt wurde.[4] Dabei gab etwa ein Drittel der Befragten an, dass ein Freund oder ein Familienmitglied schon einmal im Internet gemobbt worden sei. Insgesamt hat sich durch diese und ähnliche Vorfälle die gefühlte Sicherheit in diesem quasi-öffentlichen Raum deutlich reduziert.

Die Rückgewinnung und Stärkung des Verbrauchervertrauens in all diesen Dimensionen steht damit nicht unerwartet im Mittelpunkt der digitalen Verbraucherpolitik. Ein solches berechtigtes Vertrauen in die digitale Welt kann am besten dann entstehen und stärker werden, wenn Verbraucher souverän in der digitalen Welt agieren können. Inzwischen reicht die verbraucherpolitische Diskussion über Digitale Souveränität in Deutschland mindestens zehn Jahre zurück: Sie lässt sich auf die „Charta Verbrauchersouveränität in der digitalen Welt" (BMELV, 2007) zurückführen, welche unter dem Eindruck der rasanten Zunahme aller Formen digitaler Geschäftsbeziehungen zum Weltverbrauchertag 2007 vorgelegt wurde. Hier übertragen die Autoren den Begriff der „Konsumentensouveränität" erstmalig auf den digitalen Kontext und definieren Leitlinien für eine verbraucherfreundliche Ausgestaltung der digitalen Welt. Bezug genommen wird außerdem auf das Grundrecht der „informationellen Selbstbestimmung".

Aufbauend auf dem Papier des BMELV wurden in der verbraucherpolitischen Debatte schrittweise Handlungsempfehlungen zur Stärkung der Digitalen Souveränität entwickelt. Der Verbraucherpolitische Bericht der Bundesregierung des Jahres 2008 greift die Kernaussagen der Charta auf und bezeichnet Verbraucherkompetenz als Grundvoraussetzung für eigenverantwortliche Entscheidungen in der digitalen Welt (Bundesregierung, 2008). Auch die „Digitale Agenda 2014 - 2017" der Bundesregierung sieht insbesondere in der Stärkung der Medienkompetenz der Verbraucher eine zentrale Maßnahme des Verbraucherschutzes in der digitalen Welt – neben den Marktwächtern, dem Verbandsklagerecht sowie Grundeinstellungen, welche die Privatsphäre bei digitalen Anwendungen schützen (Privacy by Design und Privacy by Default) (Bundesregierung, 2014). Ähnlich äußert sich das BMWi und sieht den Erwerb von Schlüsselkompetenzen, IT-Sicherheit und Datenschutz als Voraussetzungen für Digitale Souveränität an (BMWi, 2015). Neben Aspekten der Identitätssicherung sowie dem Schutz vor Identitätsdiebstahl nennt die Bundesregierung im Verbraucherpolitischen Bericht des Jahres 2016 die „Stärkung von Selbstbestimmung, die Gewährleistung von Wahlfreiheit und Transparenz, umfassende und verständliche Verbraucherinformationen und Sicherheit im Netz" als Zielsetzungen der Verbraucherpolitik (Bundesregierung, 2016).

In dem vorliegenden Gutachten knüpfen wir an dieses Verständnis von (individueller) Digitaler Souveränität an und grenzen diese von nationalstaatlicher Digitaler Souveränität[5] ab. Den Begriff der Datensouveränität[6], der ein weiteres zentrales Konzept in der verbraucherpolitischen Debatte beschreibt, integrieren wir als eine wichtige Ausprägung von Digitaler Souveränität in unser Konzept, nämlich als die Wahlfreiheit von Verbrauchern über Erhebung, Verarbeitung und Nutzung ihrer persönlichen Daten. Die Entscheidung darüber, ob beispielsweise persönliche Daten zu wohltätigen Zwecken gespendet, ob sie

4 Abgerufen am 14. Juni 2017 von URL http://docs.dpaq.de/9635-ppt_for_vodafone__cyberbullying_-_germany__060_9_9_15.pdf.

5 Der Begriff der Digitalen Souveränität wurde insbesondere im Zuge der Debatte um die Enthüllungen von Edward Snowden häufig auch in Bezug auf eine nationalstaatliche Souveränität der digitalen Infrastruktur genutzt (Friedrichsen & Bisa, 2016). Nach Bekanntwerden der massenhaften Überwachungstätigkeiten insbesondere des US-amerikanischen Geheimdienstes wurden Forderungen laut, die Digitale Souveränität der europäischen Staaten und ihrer Bürger etwa durch eine unabhängige digitale Infrastruktur oder durch nationale Produktionskompetenzen für Hardware zu stärken (BMWi, 2015). Auch der Branchenverbrand Bitkom betont den nationalstaatlichen Aspekt von digitaler Souveränität (Bitkom, 2015): Demnach ziele Digitale Souveränität darauf ab, „Unabhängigkeit von einzelnen Wirtschaftsräumen, Staaten und Unternehmen bei Bezug und Nutzung digitaler Technologien und Plattformen herzustellen". Eher als Annex zu diesen wirtschaftsorientierten Betrachtungen bezeichnet Bitkom als Bestandteil Digitaler Souveränität, dass auch Verbraucher (neben Unternehmen und Verwaltungen) „digitale Technologien und Lösungen sicher, selbständig und selbstbestimmt" einsetzen.

6 Heiko Maas (Maas, 2015) nennt die Einwilligung zum Sammeln, Verarbeiten usw. der persönlichen Daten den Schlüssel zur Datensouveränität und beklagt, dass die Einwilligung in Anbetracht überlanger AGB bisher eher Alibi-Charakter habe und daher Selbstbestimmung nur simuliert werde. Das nach Eigenaussage auf einem Dialogprozess mit Wirtschaft, Wissenschaft und Gesellschaft fußende „Grünbuch Digitale Plattformen" greift den bereits genannten Begriff „Datensouveränität" als Leitbild auf, ohne dies näher zu erläutern bzw. eine Abgrenzung zum Begriff Digitale Souveränität vorzunehmen. Allerdings hat das Papier auch eine verbraucherbezogene bzw. -politische Komponente: So wird betont, dass es wichtig sei, den souveränen Umgang der Verbraucher mit ihren Daten sicherzustellen, einschließlich der Verfügung darüber, wer im Besitz dieser Daten sein soll (BMWi, 2016). Das darauf aufbauende „Weißbuch Digitale Plattformen des BMWi" diskutiert im Rahmen der Datenschutzgrundverordnung Datensouveränität schließlich parallel zum Aspekt der Datenportabilität, ohne weiter auf die dahinterstehenden Konzepte einzugehen (BMWi, 2017b). Die „Charta der digitalen Grundrechte der Europäischen Union" (abgerufen am 14. Juni von URL https://digitalcharta.eu/) spricht von „Datensouveränität" und meint damit beispielsweise das Recht, über die eigenen Daten zu bestimmen oder auch das Einwilligungserfordernis für die Erhebung und Nutzung personenbezogener Daten. Die durch die Digitalisierung hervorgerufene Herausforderung für das Bildungswesen wird erwähnt; digitale Bildung als solche aber als Recht verstanden, um in der digitalen Welt selbstbestimmt leben zu können.

verkauft oder gänzlich in ihrer Erhebung vermieden werden, sollte demnach den Verbrauchern vorenthalten sein. Dieser Denkweise folgend sind Digitale Souveränität und Datensparsamkeit gerade keine sich ausschließenden Gegensätze, wie teilweise angenommen (z. B. BMWi, 2015) – im Gegenteil: Es sollte möglich sein, dass Datensparsamkeit zu einer von den Verbrauchern selbstbestimmten Ausprägung Digitaler Souveränität wird.

Unter Digitaler Souveränität verstehen wir demnach die Handlungsfähigkeit und Entscheidungsfreiheit der Verbraucher, in der digitalen Welt in verschiedenen Rollen agieren zu können, nämlich als Marktteilnehmer, als Konsumentenbürger einer Gesellschaft sowie als „Prosumer" in Netzwerken. Der Begriff verweist darüber hinaus auf die Rechte und Pflichten von Bürgern im staatlichen Ordnungsrahmen und unterstreicht die Rahmenbedingungen, unter denen die Bürger frei, kompetent und verantwortungsvoll digitale Medien und Dienste nutzen können und somit in die Lage versetzt werden, aktiv an einer digitalen Gesellschaft teilzuhaben. In Anlehnung an die Debatte zu Verbrauchersouveränität in der digitalen Welt (BMELV, 2007, S. 2; Bundesregierung, 2016) sowie das Papier von Mertz et al. (2016) identifizieren wir vier Leitlinien, die im Zusammenhang mit Digitaler Souveränität stehen: *Wahlfreiheit, Selbstbestimmung, Selbstkontrolle* und *Sicherheit*. Wir schlagen vor, dass sich diese mittels verbraucherfreundlicher *Technologie*, *digitaler Kompetenz* von Verbrauchern sowie *Regulierung* realisieren lassen.

Mit dem vorliegenden Gutachten leistet der SVRV einen Beitrag zu der fortlaufenden Debatte zur Weiterentwicklung des Begriffs der Digitalen Souveränität aus verbraucherpolitischer Perspektive. Aufbauend auf dieser Standortbestimmung skizzieren wir konkrete Handlungsempfehlungen, für deren Umsetzung unterschiedliche Akteure angesprochen werden. Es ist wie folgt aufgebaut: In Kapitel 2 leiten wir vier Leitlinien der Digitalen Souveränität (Wahlfreiheit, Selbstbestimmung, Selbstkontrolle und Sicherheit) her und argumentieren, dass Digitale Souveränität mittels Technologie, digitaler Kompetenz und verbraucherfreundlicher Regulierung („Dreieck der Digitalen Souveränität") gefördert werden sollte. In den Kapiteln 3 bis 5 stellen wir für die drei Handlungsfelder kurze themenspezifische Problemabrisse dar, ergänzt um verbraucherpolitische Handlungsempfehlungen.

2. Konzept: Leitlinien und Handlungsfelder

2.1. Vier Leitlinien: Wahlfreiheit, Selbstbestimmung, Selbstkontrolle und Sicherheit

Wir orientieren uns bei der Einordnung des Begriffs der Digitalen Souveränität an dem Konzept der Konsumentensouveränität (z. B. Hutt, 1940; Persky, 1993; Schwarzkopf, 2011). Das Konzept umfasst sowohl eine empirisch-deskriptive („Wie souverän sind Konsumenten?“ bzw. „Welche Determinanten wirken mit der Souveränität der Konsumenten zusammen?“) als auch eine präskriptiv-normative Ebene („Wie souverän sollten Konsumenten sein?“ bzw. „Welche Maßnahmen sollten ergriffen werden, um Konsumenten in die Lage zu versetzen, souverän zu agieren?“) und beschreibt, in welcher Position Nachfrager und Anbieter auf Märkten zueinander stehen bzw. stehen sollten (Schwarzkopf, 2011).

Einen deskriptiv-empirischen Ansatz verfolgen Mertz et al. (2016) in ihrem Artikel „Digitale Selbstbestimmung“. Sie beschreiben hier, welche Aspekte im Zusammenhang mit Digitaler Selbstbestimmung stehen (hier: Kompetenz, Informiertheit, Werte, Wahlmöglichkeit, Freiwilligkeit, Willensbildung, Handlung) und welche Faktoren grundsätzlich Digitale Selbstbestimmung determinieren (hier: technische, soziokulturelle und personenbezogene Determinanten). Digitale Souveränität ist hier definiert als die „[k]onkrete Entfaltung einer menschlichen Persönlichkeit bzw. die Möglichkeit der Realisierung von je eigenen Handlungsentwürfen und Handlungsentscheidungen soweit dies eine bewusste Verwendung digitaler Medien betrifft oder dies von der Existenz oder Funktionsweise digitaler Medien (mit-) abhängig ist“ (Mertz et al., S. 18). Die Autoren stellen zudem zahlreiche Parallelen zwischen dem Begriff der Digitalen Selbstbestimmung und dem Begriff der informationellen Selbstbestimmung her (Mertz et al., 2016).

In dem vorliegenden Gutachten führen wir die Debatte auf der präskriptiv-normativen Ebene fort und gehen der Frage nach, welche konkreten Rahmenbedingungen zu schaffen sind, damit Verbraucher selbstbestimmt in einer zunehmend digital vernetzten Welt handlungsfähig sind (siehe auch Rau, 2016).

In Anlehnung an das Gutachten von Mertz et al. (2016) sowie den verbraucherpolitischen Diskurs zu Verbrauchersouveränität in der digitalen Welt (BMELV; Bundesregierung, 2016) identifizieren wir vier Leitlinien, die im Zusammenhang mit Digitaler Souveränität stehen: *Wahlfreiheit, Selbstbestimmung, Selbstkontrolle* und *Sicherheit.*

Wahlfreiheit wird in einem weiten Sinne verstanden und umfasst sowohl Aspekte negativer Handlungsfreiheit („Freiheit *von* etwas“) wie auch positiver Handlungsfreiheit („Freiheit *zu* etwas“). Demnach sollten Verbraucher weitgehend frei darin sein, etwas zu tun oder auch zu unterlassen (Mertz et al., 2016). Übertragen auf den Verbraucherkontext in der digitalen Welt kann dies beispielsweise bedeuten, dass Nutzern grundsätzlich die Wahl überlassen ist, bei dem Kauf einer App je nach Präferenz zwischen einer Freeware-Variante (unter Preisgabe von Nutzerdaten) oder einer Bezahlvariante (ohne Preisgabe von Nutzerdaten) zu wählen (Weis et al., 2016). Wahlfreiheit kann sich auch darin äußern, dass Verbrauchern bei einem Anbieterwechsel kein erheblicher Transaktionsaufwand entsteht. So werden Lock-In-Effekte vermieden, die aufgrund mangelnder Portabilität von Daten – verursacht durch „Datensilos“ und fehlender Standards zur Ermöglichung einer echten Interoperabilität – entstehen können (BMWi & BMJV, 2015). Wahlfreiheit haben Verbraucher insbesondere auch dann, wenn sie zu „aktiven Verwaltern“ ihrer eigenen Daten werden: Dann können sie eigenständig über Weitergabe, Mitnahme, Löschung, Spende und Handel ihrer Daten entscheiden – insofern keine anderweitigen wichtigen und rechtlich klar verankerten Interessen anderer Akteure vorliegen (z. B. Palmetshofer et al., 2016). Zur Wahlfreiheit gehört ebenso die Entscheidung, ob die Einsicht in personenbezogene Daten anderen erlaubt sein soll oder nicht.

Selbstbestimmtheit im Umgang mit digitalen Medien bedeutet, dass die Nutzer von Hardware und Software Hoheit über wichtige Entscheidungen haben. Daraus folgt, dass Verbraucher grundsätzlich nicht das Objekt von automatisierten Entscheidungen auf der Grundlage von Algorithmen sein sollten, die von erheblicher Bedeutung für die Lebensführung von Verbrauchern sind. Beispielsweise kann ein vollau-

tomatisiertes, intransparentes Scoring-Verfahren bei der Entscheidung über eine Kredit-Vergabe für einen Verbraucher erhebliche Probleme verursachen, wenn die Datenbasis und die Logik des zugrundeliegenden Algorithmus nicht offen gelegt werden und damit die Grundlage für ein Widerspruchsrecht fehlt. Diese Entwicklungen werden umso brisanter, je weitreichender Scoring-Methoden in der Verknüpfung unterschiedlicher Datenarten eingesetzt werden (Weis et al., 2016). Die Zweckbindung bei der Erhebung und Verwendung personenbezogener Daten ist daher ein wichtiger Faktor, ebenso die Option, dass Daten anonymisiert gespeichert und ausgewertet werden. Der Grundsatz der Selbstbestimmtheit bedeutet auch, dass Verbraucher die Gefahren von Manipulationen abschätzen können (Mertz et al., 2016), die beispielsweise durch den Einsatz von Social Bots[7] sowie die Verbreitung gezielter Desinformation (sogenannte „Fake News“) entstehen. Neben geeigneten technologischen und regulatorischen Vorkehrungen sind hierbei eine digitale Grundbildung und Datenkompetenz unerlässlich.

Selbstkontrolle bedeutet, dass Nutzer in der Lage sind, selbst die Grenzen der eigenen Nutzung digitaler Angebote zu ziehen und die Konsequenzen ihres Verhaltens abzuschätzen. Angesichts hunderttausender verfügbarer Apps, des Internet of Things und der Möglichkeit, permanent online zu sein, wird es immer wichtiger, dass Menschen die Kontrolle über ihre Lebensführung haben – und nicht von der digitalen Welt gesteuert oder gar abhängig werden. Selbstkontrolle bedeutet auch, nicht vom Handy am Steuer oder permanent eingehenden E-Mails abgelenkt und in der Konzentration gestört zu werden (Helbing et al., 2017). Über mögliche Konzentrationsstörungen hinaus sind Fälle von Abhängigkeit von Menschen durch digitale Medien dokumentiert, welche auch als „Internet-Sucht“ bezeichnet werden.[8] Diese Abhängigkeit von digitalen Medien führt bei manchen Menschen mitunter zu erhöhtem Techno-Stress (Gigerenzer, 2010). Unser Verständnis von Digitaler Souveränität umfasst somit nicht nur die Gestaltung eines souveränen Agierens innerhalb der digitalen Welt, sondern fordert einen ebenso souveränen Umgang mit der digitalen Welt im Sinne der Fähigkeit, digitale Dienste oder Endgeräte wie das Smartphone bei der Nutzung kontrollieren zu können, nicht aber kontrolliert oder im Verhalten maßgeblich beeinflusst zu werden.

Sicherheit bedeutet, den Schutz von Verbraucherdaten und digitalen Infrastrukturen durch den Staat und Unternehmen sowie durch Verbraucher selbst zu gewährleisten. Zu diesem Zweck müssen Infrastrukturen verfügbar sein, die eine sichere Erhebung, Speicherung sowie eine kontrollierte Weitergabe von Daten ermöglichen. Die steigende Zahl von Cyber-Attacken auch auf private Rechner, wie auch die Fälle von Diebstahl der Kundendaten bei internationalen Konzernen, belegt die immense Bedeutung für die Verbraucherpolitik. Hierbei können technische Voreinstellungen wie Privacy by Design und Privacy by Default Verbrauchern einen sicheren und gleichzeitig komfortablen Alltag in der digitalen Welt erleichtern. Gleichzeitig sind die Verfügbarkeit einfach nutzbarer Verschlüsselungstechnologien wie auch regelmäßige Sicherheits-Updates maßgebliche Bausteine für die Sicherheit von Verbrauchern im Netz. Eine grundlegende Kenntnis zentraler Faktoren der Sicherheit im Netz ist dabei Aufgabe einer altersgruppen- und institutionenübergreifenden Bildung.

2.2. Drei Handlungsfelder: Technologie, Digitale Kompetenz und Regulierung

Anknüpfend an die eingangs beschriebenen Vorarbeiten des SVRV schlagen wir vor, dass sich die beschrieben Leitlinien für Digitale Souveränität mittels verbraucherfreundlicher *Technologie*, *digitaler Kompetenz* sowie einer Rahmensetzung durch *Regulierung* der digitalen Welt im Sinne des Gemeinwohls erzielen lassen. So lässt sich Digitale Souveränität aus drei Perspektiven beschreiben: Erstens, als Frage technologischer Rahmenbedingungen für datenintensive Dienstleistungen und Produkte; zweitens, als Frage der Bildung, die notwendigen Fähigkeiten und Fertigkeiten für den Umgang mit Informationen, Quellen und Daten online zu vermitteln; und drittens, als Frage der Regulierung der Nutzung personenbezogener Daten und als Stärkung der Verbraucherrechte. Diese drei Handlungsfelder zusammen bezeichnen wir als das Dreieck der Digitalen Souveränität.

7 Bei Social Bots handelt es sich um Computerprogramme, die in der Lage sind, in Sozialen Medien automatische Antworten zu setzen (Ferrara et al., 2016).

8 „Internet addiction is typically described as a state where an individual has lost control of the internet use and keeps using internet excessively to the point where he/she experiences problematic outcomes that negatively affects his/her life“ (Young & Abreu, 2011; cf. Kardefelt-Winther, 2014).

Unter dem Überbegriff *Technologie* verstehen wir hier im Besonderen technologische „Enabler“, also jene Funktionen, Prinzipien und Applikationen, die ein digital souveränes Verhalten ermöglichen – oder eben verhindern, wenn sie fehlen. Hier geht es zum Beispiel um nutzerzentriertes Datenmanagement, Prinzipien der Datensparsamkeit oder die Nutzung von Verschlüsselungstechnologien und Sicherheits-Updates.

Digitale Kompetenz umfasst Aspekte wie den Umgang mit Informationen und mit möglicherweise gezielter Desinformation („Fake News“), die Nutzung digitaler Kommunikationsmedien, die Nutzung digitaler Werkzeuge, die Fähigkeit zum Datenmanagement sowie – damit verbunden – die Verfügung über Produkt- und Konzeptwissen und die Bereitschaft zum lebenslangen, selbstständigen Lernen. Die Stärkung der digitalen Kompetenz versetzt Verbraucher darüber hinaus in die Lage, digitale Medien selbstkontrolliert zu nutzen, wovon eine maßvolle Nutzung bis hin zu einer selbstbestimmten Nicht-Nutzung eingeschlossen ist.

Regulierung umfasst sowohl Rechte und Pflichten des einzelnen Verbrauchers sowie Rechte und Pflichten von Unternehmen und Staat. Rechte und Pflichten des einzelnen Verbrauchers beziehen sich dabei beispielsweise auf das Recht auf Datenlöschung und Datenportabilität sowie die Pflicht zur Installation von Sicherheitsupdates auf Internet-of-Things-Geräten. Rechte und Pflichten von Unternehmen und Staat beziehen sich insbesondere auf Transparenz und Zweckbindung bei der Datenerhebung und Datenverwendung sowie Überprüfbarkeit und Offenlegung von Algorithmen beispielsweise im Rahmen von Algorithmen-Audits, wie sie heute bereits im Bereich des Kredit- und Bonitäts-Scorings praktiziert werden.

Abbildung 1: Dreieck der Digitalen Souveränität: Technologie, Digitale Kompetenz und Regulierung (eigene Darstellung)

Das Modell ist konzipiert, um die *Wirkungszusammenhänge* zwischen den beschriebenen Handlungsfeldern für die Verbraucherpolitik zu beschreiben. Daraus ergibt sich, dass ein Vorankommen auf allen drei Handlungsfeldern wichtig ist, um Digitale Souveränität für Verbraucher zu ermöglichen. Derjenige Verbraucher, der sich des Wertes seiner Daten bewusst ist und seine Rechte im Netz durchsetzen möchte, kann z. B. nicht souverän agieren, wenn die technologischen Rahmenbedingungen dies verhindern und seine Daten entweder nicht zu anderen Dienstleistern übertragen werden können oder er keine Wahlmöglichkeit bei der Nutzung seiner Daten hat. Gleichzeitig kann eine Regulierung der Datenmärkte nur dann wirksam sein, wenn die technologische Umsetzung erfolgt und der Verbraucher von seinen Rechten Gebrauch machen kann. In Ergänzung zu dem Modell der Digitalen Selbstbestimmung von Mertz et al. (2016) unterstreichen wir somit insbesondere das Zusammenwirken und die gegenseitige Verstärkung (oder auch Schwächung) der einzelnen Faktoren, die Digitale Souveränität konstituieren.

Ähnlich dem hier vorgestellten Konzept identifiziert De Mooy (2017) drei aufeinander wirkende Handlungsfelder, die auf das Ziel einer individuellen Datensouveränität hinwirken. De Mooy identifiziert hierbei Bildung, Datenportabilität, Selbstregulierung von Unternehmen und eine begleitende staatlich regulierte Überprüfung als Wegbereiter hin zu mehr Datensouveränität. Das hier vorgestellte Konzept fasst das Ziel mit dem Begriff der Digitalen Souveränität jedoch weiter. Entsprechend sind die Handlungsfelder weiter ausgelegt.

Digitale Souveränität resultiert in unserem Verständnis also immer aus der Balance zwischen Technologie, Digitaler Kompetenz und Regulierung – ohne einem der drei Faktoren Vorrang zu geben und wohlwissend, dass alle drei Komponenten sowohl Behörden und die Wirtschaft als auch das Individuum adressieren können. Im Folgenden stellen wir unsere Empfehlungen auf den drei Handlungsfeldern zur Stärkung der Digitalen Souveränität von Verbrauchern vor.

Technologie

3. Technologie

Im Folgenden werden zentrale technische Aspekte diskutiert, die für die Digitale Souveränität von Verbrauchern von Bedeutung sind. Dabei geht es insbesondere um Datenschutz und -nutzung sowie Sicherheitsaspekte, die in der zunehmend vernetzten Welt an Bedeutung gewinnen.

3.1. Verbraucherzentriertes Datenportal schaffen

Der SVRV empfiehlt die Entwicklung eines *verbraucherzentrierten Datenportals (Dashboard)* zur Realisierung der individuellen Datensouveränität.

Der SVRV empfiehlt die Entwicklung eines verbraucherzentrierten Datenportals (Dashboard) zur Realisierung der individuellen Datensouveränität. Darin hat der Verbraucher Transparenz über die Nutzung (Umfang, Inhalt) seiner individuellen Daten durch die unterschiedlichen Anbieter im Netz und kann sie zentral löschen, ändern und die Zugriffsrechte verwalten.

Der Zugang zu einem solchen Dashboard sollte durch ein individuelles durchsetzungsfähiges Recht gesichert werden. Praktisch umsetzbar wäre ein solches Datenportal beispielsweise durch eine von Staat und Unternehmen gemeinsam getragene Initiative.

Bei der Entwicklung eines verbraucherzentrierten Datenportals stehen die Transparenz bei der Datenverarbeitung, Dezentralisierung auf dem Datenmarkt und der Einsatz von technischen Standards wie zum Beispiel MyData[9] im Vordergrund (s. auch Jentzsch, 2017). MyData formuliert folgende Rechte für eine Schnittstelle zu sämtlichen gespeicherten persönlichen bzw. personalisierbaren Daten, auf die der individuelle Verbraucher Zugriff hätte: Das Recht zu wissen, welche persönlichen Informationen vorliegen; den tatsächlichen Inhalt der persönlichen Daten zu sehen; falsche Daten korrigieren zu können; zu prüfen, wer Zugriffe auf die personenbezogenen Daten hat und warum; persönliche Daten zu erhalten und sie frei zu verwenden; persönliche Informationen mit Dritten zu teilen oder sie zu verkaufen; persönliche Daten zu löschen (Palmetshofer, Semsrott & Alberts, 2016). Ähnliche Ansätze liefern das so genannte Vendor Relationship Management (VRM) sowie der Hub-of-All-Things-Ansatz (HAT) (Palmetshofer et al., 2016).

Es gilt zu betonen, dass der Leitgedanke bei der Schaffung eines verbraucherzentrierten Datenportals die beschriebene Lenkung des Datenflusses durch Verbraucher ist. Die Möglichkeit des Handels mit eigenen Daten hingegen sollte bei der Entwicklung des Datenportals nicht im Fokus stehen, sondern nur ein mögliches Szenario für Verbraucher sein. Hinsichtlich des Handels mit eigenen Daten stellt der SVRV fest, dass eine Monetarisierung von Daten für Verbraucher aktuell kaum sinnvoll realisierbar ist und möglicherweise nur diejenigen Verbraucher von Datenhandel profitieren, die über die nötige Datenkompetenz (Data Literacy) verfügen. Auch die ethischen Aspekte beim Online-Handel mit personenbezogenen Daten, wie zum Beispiel Körperdaten, sind bisher nicht hinreichend diskutiert. Außerdem ist festzuhalten, dass es derzeit für Verbraucher nur schwer möglich ist, einen fairen Preis für ihre Daten zu ermitteln (SVRV, 2016). Verbraucher gehen so bei der Nutzung von Online-Dienstleistungen in vielen Fällen eine Geschäftsbeziehung ein, ohne die Wertschöpfung, die auf der Grundlage ihrer übermittelten oder entstehenden Daten möglich ist, einschätzen zu können. Faktoren, die die Sensibilität der Verbraucher hinsichtlich der Nutzung ihrer Daten beeinflussen, sind dabei zum einen leicht messbare Variablen wie Datenart, Dienstleister, genutztes Endgerät, Art der Datensammlung und -nutzung, zum anderen subjektive Variablen wie Vertrauen in den Dienstleister und der empfundene oder reale Nutzen, der für Verbraucher entsteht (World Economic Forum, 2014). Auch kulturelle Faktoren spielen dabei eine Rolle. So scheinen beispielsweise die Verbraucher in skandinavischen und baltischen Ländern weniger datensensibel zu sein als deutsche.

Versuche, Modelle und Maßstäbe für den Wert individueller Daten zu entwickeln, sind derzeit für die Forschung nur näherungsweise möglich (Palmetshofer et al., 2016; Jentzsch, 2016). Es scheint sich je-

9 Abgerufen am 14. Juni 2017 von URL http://mydata.org.

doch herauszukristallisieren, dass bei den aktuellen Verwertungsmodellen der möglicherweise erzielbare Preis bzw. der ökonomische Wert der Daten mutmaßlich zu gering eingeschätzt wird (Palmetshofer et al., 2016). Zudem stellt sich die Frage nach der Wiederverwertbarkeit der Daten und damit zugleich danach, wem die Daten tatsächlich gehören. Hinzu kommt das Problem, dass viele Daten oft erst mit weiterer Verknüpfung wertvoll werden – die entstehenden großen Datensätze jedoch nur bedingt auf die jeweiligen individuellen Verbraucher rückführbar sind. Die Verbraucher haben auch nicht immer die technischen Möglichkeiten oder Optionen und Berechtigungen, ihre persönlichen Daten aus den jeweils verwendeten Diensten und Services herunterzuladen. Selbst wenn dies möglich ist, bedarf es meistens trotzdem noch fortgeschrittener EDV-Kenntnisse, um die Daten mit anderen zu verknüpfen oder aufzubereiten.

Ein weiterer Ansatz für eine verbrauchernahe Kontrolle des Datenflusses besteht in der Implementierung eines sogenannten kontextsensitiven Recommender-Systems (World Economic Forum, 2014). Ein solches System würde die Rolle eines Mittlers zwischen dem Dienstleister, der die Nutzung von Daten anfragt, und dem Verbraucher selbst einnehmen. Auf der Grundlage verschiedener Faktoren wie Nutzer-Historie, Grundeinstellung, Art der Datennutzung etc. würde das Recommender-System dem Verbraucher die Nutzung der Dienstleistung nahelegen oder aber abraten, wenn zum Beispiel Datenschutzbedenken vorliegen. Das System könnte zudem selbstlernend aufgebaut sein, so dass es aus den Entscheidungen des Verbrauchers lernt. Solche Systeme können den Verbraucher insgesamt bei der Entscheidung über die Angemessenheit von Geschäftsbedingungen und Wertschöpfungsmodellen auf der Grundlage von individuellen Daten unterstützen und dabei die Nutzbarkeit für ihn steigern. Jedoch ist auch dieser Ansatz bisher lediglich in der Konzept-Phase, so dass sowohl das verbraucherzentrierte Datenportal als auch das Recommender-System als zukünftige Entwicklungsprojekte für die Digitale Souveränität von Verbrauchern an dieser Stelle vorgeschlagen werden.

3.2. Prinzipien Privacy by Design und Privacy by Default durchsetzen

Der SVRV bekräftigt die Forderung nach einer nutzerfreundlichen, datensparsamen und gleichzeitig sicherheitsorientierten Voreinstellung von Kommunikationssystemen (Privacy / Security by Design und Privacy / Security by Default als Leitlinien). Staatlich geförderte Projekte müssen sich an diesen Linien orientieren.

Die Leitlinie *Privacy by Design* bedeutet, dass Vertraulichkeit natürlicher Bestandteil in der Konzeption und Gestaltung von Kommunikationssystemen ist, um die Privatsphäre von Verbrauchern zu schützen. Die Leitlinie *Privacy by Default* bedeutet, dass die Grundeinstellung ein Höchstmaß an Privatsphäre und Datenschutz gewährt und Verbrauchern von dieser Grundeinstellung ausgehend die Wahlmöglichkeit gegeben ist, leicht zwischen einem mehr oder weniger datensparsamen Kommunikationsmodus zu wechseln.

Analoges gilt für die Prinzipien *Security by Design* und *Security by Default* in Bezug auf die Sicherheit der Kommunikation und der genutzten Dienstleistungen. Hierdurch sollen alle Nutzer – insbesondere solche, die nicht über vertiefte informatorische und digitale Fähigkeiten verfügen – in die Lage versetzt werden, einfach und effektiv ihre Daten schützen sowie sicher kommunizieren zu können.

Die Herstellung von Vertraulichkeit (also „Privacy“) in der Kommunikation und die Weitergabe von Verbraucherdaten spielen für den SVRV weiterhin eine zentrale Rolle (s. bereits Reisch et al. 2015, SVRV, 2015). Hierbei ist es uns ein besonderes Anliegen, dass auch Laien, die nicht über vertiefte informatorische Fähigkeiten verfügen, besonders einfach ihre Daten schützen können.[10] Diese Vorstellung wird untermauert durch die noch gültige ePrivacy-Richtlinie aus dem Jahr 2002. Dort werden in Erwägungsgrund 46 Maßnahmen als notwendig erachtet,

10 Einen Überblick über diese sogenannten Privacy-Enhancing-Technologies bieten Domurath & Kosyra (2016).

> „mit denen die Hersteller bestimmter Arten von Geräten, die für elektronische Kommunikationsdienste benutzt werden, verpflichtet werden, in ihren Produkten von vornherein Sicherheitsfunktionen vorzusehen, die den Schutz personenbezogener Daten und der Privatsphäre des Nutzers und Teilnehmers gewährleisten." (ePrivacy-Richtlinie 2002/58/EG)

Darüber hinaus orientiert sich die Forderung an den Vorstellungen der EU Datenschutzgrundverordnung (Art. 25 I, II):

> „dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun." (EU Datenschutzgrundverordnung, Erwägungsgrund 78)

Privacy bzw. Security by Design bedeutet, dass Vertraulichkeit und andere Sicherheitseigenschaften natürliche Bestandteile von Kommunikationssystemen sind – in dem Sinne, dass entsprechende Funktionalitäten im Kommunikationssystem implementiert sind – oder entwickelt werden, um Vertraulichkeit herzustellen (Weis et al., 2016; Domurath & Kosyra, 2016). So besagt das Privacy-by-Design-Prinzip, dass Daten grundsätzlich lokal beim Verbraucher verarbeitet werden sollten bzw. dass Daten nur anonymisiert, pseudonymisiert (oder aggregiert) sowie verschlüsselt und authentisiert übermittelt werden dürfen (Weis et al., 2016).

Privacy bzw. Security by Default beschreibt die Wahlmöglichkeit, welche Verbrauchern gegeben ist, um leicht zwischen einem mehr oder weniger sicheren Kommunikationsmodus zu wechseln – voreingestellt („by Default") ist jedoch immer der sichere Modus. Privacy bzw. Security by Default kann also als eine Voreinstellung verstanden werden, die sicherstellt, dass personenbezogene Daten in IT-Systemen oder Geschäftsmodellen automatisch geschützt werden, ohne dass der Betroffene Maßnahmen zum Schutz seiner Privatsphäre ergreifen muss (Domurath & Kosyra, 2016).[11]

3.3. Sicherheit im Internet of Things erhöhen

Der SVRV empfiehlt zu prüfen, wie angesichts der sich immer mehr verstärkenden Sicherheitsprobleme im Internet-of-Things-Segment sichergestellt werden kann, wie – in Anlehnung an Verfahren aus dem Gesundheitsbereich – in den Verkehr gebrachte Produkte und Dienstleistungen über den gesamten Lebenszyklus hinweg durch Sicherheitsupdates verpflichtend kontinuierlich abzusichern sind. Hierzu sind technologische Standards zu entwickeln und Quellcodes (analog der „Rezeptur" im Lebensmittelbereich) dauerhaft zu hinterlegen.

Die Absicherung im IoT-Segment sollte eine Verpflichtung zum Schreiben von Sicherheitsupdates durch die Hersteller umfassen. Darüber hinaus besteht die Möglichkeit zu prüfen, in welcher Form der Quellcode eines Systems zum Beispiel bei einem Treuhänder hinterlegt werden kann, wenn der Hersteller seiner Verpflichtung, Sicherheitsupdates zu entwickeln, nicht nachkommt. In diesem Fall sollte auch die Variante geprüft werden, den Quelltext offen zu legen (Open Source). Damit soll sichergestellt werden, dass zumindest Dritte das Schreiben und ggf. Verbreiten von Sicherheitsupdates übernehmen können.

Im Sinne der Sicherheit von Verbrauchern in der digitalen Welt hat die IT-Industrie für Privatkunden und Unternehmen ein immer besseres Sicherheitsmanagement entwickelt, welches durch regelmäßige

11 Abzugrenzen von Privacy by Default ist Privacy by Option: Hier können Verbraucher zwischen mehr oder weniger sicheren Modi wechseln, ohne dass die Voreinstellung zwingend der sicherere Modus ist (Weis et al., 2016).

und teilweise automatische Updates von Software sowie durch verhältnismäßig kurze Updatezyklen der Hardware gestützt wird. Auch wenn trotz aller Bemühungen weit verbreitete Software-Produkte wie Adobe Flash sowie Microsoft Windows und Office wiederholt im Fokus von Sicherheitsforschern stehen und Schwachstellen in der Sicherheitsarchitektur kritisiert werden (BSI, 2016), ist die Sicherheitslage im verhältnismäßig jungen Internet-of-Things-Segment insgesamt als deutlich schlechter zu bewerten (Weis et al., 2016).

Begründen lässt sich dies damit, dass im Internet of Things oft niedrigpreisige Geräte mit geringer Kundenbindung verkauft und betrieben werden (zum Beispiel internetfähige Glühbirnen oder IP-Kameras), bei denen sich Unternehmen aufgrund eines kurzen Produktlebenszyklus oft nicht in der Verantwortung sehen, Verbraucher über nötige Sicherheitsupdates zu informieren (Weis et al., 2016). Es bestehen jedoch auch bei verhältnismäßig langlebigen Internet-of-Things-Geräten, wie zum Beispiel intelligenten Heizungssteuerungssystemen, mitunter gravierende Sicherheitslücken, da diese eine langjährige Wartung von Hard- und eingebetteter Software bedingen, welche ein Anbieter möglicherweise nicht zu leisten imstande ist. Oft fehlt es zudem auf Seiten der Verbraucher an Wissen, dass nicht nur die Hardware, sondern auch die Software derartiger Geräte gewartet werden muss (Weis et al., 2016). Von Seiten der Industrie sind hier verbraucherfreundliche Standards gefordert, die die alltagstaugliche Umsetzung einer sicheren Infrastruktur im Internet of Things gewährleisten.

In Anbetracht der vielen Anzeichen für eine angespannte Sicherheitslage im Internet-of-Things-Segment sprechen wir uns daher dafür aus, dass wirksamere Maßnahmen ergriffen werden müssen, um die Sicherheit im Internet of Things zu gewährleisten. Dazu gehört die Verpflichtung zum Schreiben von Sicherheitsupdates durch die Hersteller.

Darüber hinaus besteht die Möglichkeit zu prüfen, in welcher Form der Quellcode eines Systems zum Beispiel bei einem Treuhänder hinterlegt werden kann, wenn der Hersteller seiner Verpflichtung, Sicherheitsupdates zu entwickeln, nicht nachkommt. In diesem Fall sollte auch die Variante geprüft werden, den Quelltext offen zu legen (Open Source). Damit soll sichergestellt werden, dass zumindest Dritte das Schreiben und Verbreiten von Sicherheitsupdates übernehmen können. Kommt ein Hersteller den genannten Verpflichtungen nicht nach oder existiert der Hersteller nicht mehr, sorgt der Treuhänder für die Veröffentlichung der Quelltexte als Open Source.

3.4. Angebot an datensparsamen Produkten vergrößern

Der SVRV empfiehlt zu prüfen, ob Verbrauchern ein Recht auf die Nutzung datenerhebungsarmer digitaler Produkte eingeräumt werden kann, bei dem Verbraucher die Wahl haben, auf datenerhebungsarme Varianten digital zugreifen zu können.

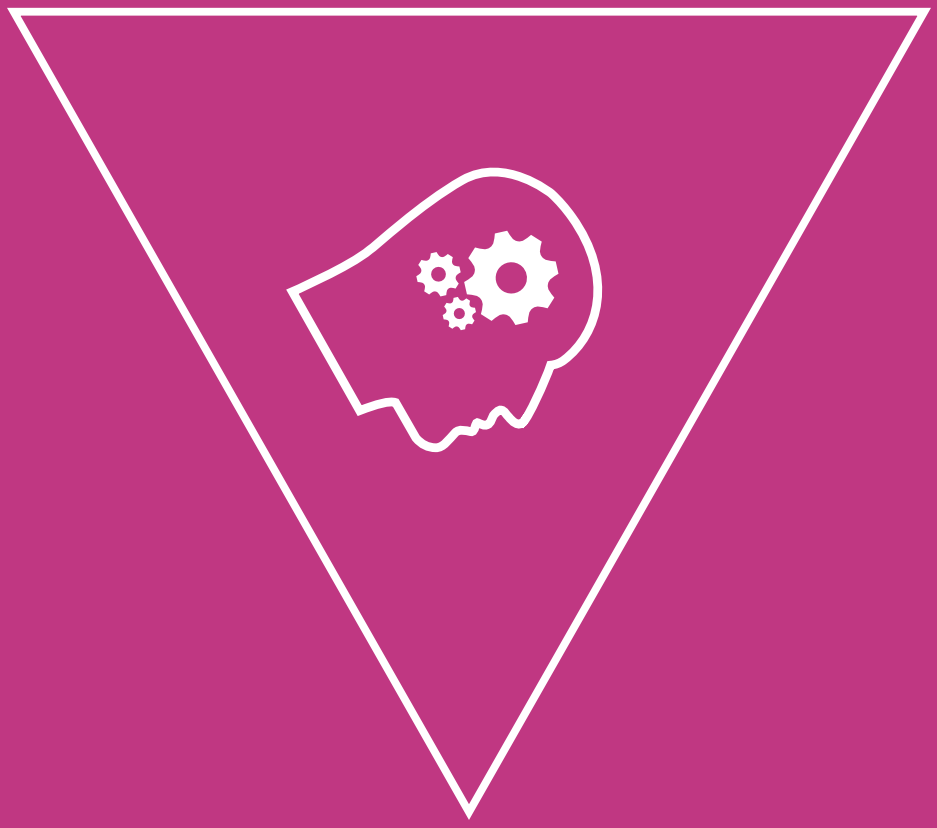
Nutzer sollten darüber entscheiden können, ob sie bei der Nutzung digitaler Dienste und Produkte Informationen über die eigene Mediennutzung preisgeben möchten oder ob sie hierauf teilweise oder vollständig verzichten möchten, ohne dass dabei die grundlegenden Funktionen eines digitalen Produkts eingeschränkt werden. Verbraucher, die keine Daten preisgeben wollen, dürfen nicht benachteiligt werden (analog zum Anti-Diskriminierungsrecht). Dies impliziert für den konkreten Geschäftsverkehr, dass keine negativen Folgen daran geknüpft sein dürfen, wenn eine Verbraucherin entscheidet, beispielsweise ohne das Anlegen eines Kundenkontos oder anderer Preisgabe von Daten (die nicht unmittelbar zur Vertragsabwicklung nötig sind) Produkte und Dienstleistungen online zu erwerben.

Ein wichtiges Merkmal der Digitalen Souveränität ist die Wahl der Darstellung von digitalen Inhalten beispielsweise auf Internetseiten. Darunter fällt die Möglichkeit, sogenannte Werbeblocker verwenden zu können, ohne dass die Nutzbarkeit der Internetseite eingeschränkt wird.[12] Obwohl wir uns darüber bewusst sind, dass (ausschließlich) werbefinanzierte

12 Bei Werbeblockern handelt es sich um Erweiterungen für den Browser, die Webseiteninhalte nutzergerecht verändern – mit dem Ziel, eine möglichst werbefreie Darstellung zu erreichen, sowie die Informationen über die Mediennutzung, die an den Webseitenanbieter übertragen werden, zu begrenzen (s. dazu auch Ofiera, 2016).

Angebote durch den zunehmenden Einsatz von Werbeblocker unter Umsatzeinbußen leiden, sprechen wir uns im Sinne der Wahlfreiheit der Präsentation von Online-Angeboten gegen ein Verbot von Werbeblocker aus. Die Werbeindustrie sollte in ihrem eigenen Interesse zur Kenntnis nehmen, dass – teils großflächige, möglicherweise sogar personalisierte – Werbung, welche oft im Pop-Up-Format oder mit unmittelbarer erhöhter Lautstärke erscheint, nicht abgestellt werden kann und erhebliches Datenvolumen in Anspruch nimmt, mitunter als eine erhebliche Belästigung und Einschränkung des Nutzungserlebnisses empfunden werden kann. Wenn die gewünschte Nachrichteninformation auf einer Internetseite mit journalistisch-redaktionellen Inhalten nur noch einen kleinen Teil des übertragenen Inhaltes ausmacht, ergibt sich ein Missverhältnis, das im Sinne des Verbrauchers verbessert werden sollte. Dem Aspekt der nachvollziehbaren Störung durch Werbung sowie dem Aspekt der Rückführbarkeit persönlicher Interessen durch die angebotene Werbung sollten dabei besondere Aufmerksamkeit gewidmet werden.

Darüber hinaus sollte das Anti-Diskriminierungsrecht auf solche Fälle Anwendung finden, in denen ein Individuum entscheidet, keine Daten (digital) preisgeben zu wollen. Dies impliziert für den konkreten Geschäftsverkehr, dass keine negativen Folgen daran geknüpft sein dürfen, dass ein Verbraucher entscheidet, beispielsweise ohne das Anlegen eines Kundenkontos oder anderer Preisgabe von Daten, Produkten und Dienstleistungen online zu erwerben, soweit dies möglich ist (Becker, 2017).



Digitale Kompetenz

4. Digitale Kompetenz

Die Digitalisierung verändert maßgeblich, wie in einer Gesellschaft Informationen produziert, bereitgestellt und verbreitet werden. Um die neuen Möglichkeiten und Chancen der digitalen Gesellschaft souverän und selbstbestimmt nutzen zu können, werden von den Verbrauchern zugleich neue Kompetenzen gefordert. Wahlfreiheit, Selbstbestimmung, Selbstkontrolle und Sicherheit im Netz bedürfen der Digitalen Kompetenz.

Information und *Data Literacy* beschreiben zusammengefasst als *Digital Literacy* eine neue Kulturtechnik neben Lesen, Schreiben und Rechnen. Verbraucher sollten in der Lage sein, ihren Bedarf an Informationen überhaupt zu bestimmen, Informationen zu finden, hinsichtlich ihrer Relevanz, Qualität, Reichweite und Aussagekraft zu beurteilen und zu bewerten, Informationen für sich zu verarbeiten und neu aufzubereiten und ggf. auch anderen zugänglich zu machen (z. B. Süss, 2017). Diese Kompetenzen sind unabhängig davon, ob Informationen analog oder digital vorhanden sind, bedeutsam.

Allerdings sind bestimmte Phänomene im Kontext digitaler Medien tatsächlich neu entstanden und für die kompetente Nutzung und Bewertung digital gespeicherter Informationen wichtig. Dazu zählen z. B. die (Nicht-) Löschbarkeit von Daten, die Unterscheidung zwischen redaktionellem Inhalt, klassischen Werbeformaten und durch Nutzer erzeugten Inhalten (einschließlich Influencer-Marketing auf Plattformen wie YouTube und Instagram) sowie automatisch generierte Inhalte durch Social Bots (dazu z. B. Wineburg et al., 2016). Darüber hinaus stellen Implikationen des Datenschutzes und des Urheberrechts im Umgang mit im Netz bereitgestellten Informationen ein neues Problemfeld dar. Diese schnellen technologischen Entwicklungen erfordern eine entsprechend schnelle Entwicklung der Kompetenzen der Nutzer.

Im Folgenden werden zentrale Ziele zur Förderung der digitalen Kompetenz von Verbrauchern formuliert. Diese umspannen eine notwendige Qualifizierung von Lehrkräften sowie den Ausbau des Angebots verlässlicher Verbraucherinformation. Darüber hinaus sehen wir Handlungsbedarf im Bereich der digitalen Selbstkontrolle und zudem weiteren Forschungsbedarf mit Blick auf die Auswirkungen der Digitalisierung auf Kognition, Emotion und das soziale Leben. Gleichzeitig stellen sich ethische Fragestellungen etwa in Bezug auf Datenhandel, Kontrollverlust im Internet of Things oder Wahlfreiheit von Verbrauchern, die jeweils auch juristische Dimensionen beinhalten. Hier ergibt sich ein interdisziplinärer Forschungsbedarf für die Verbraucherpolitik, der durch gezielte Förderung gedeckt werden sollte.

4.1. Qualifizierungs-Pakt für „Digitale Kompetenz in der Lehrerbildung“ schließen

Der SVRV empfiehlt die Etablierung eines Qualifizierungs-Paktes für „Digitale Kompetenz in der Lehrerbildung“ (analog zum Qualitätspakt Lehre oder zur Qualitätsoffensive Lehrerbildung).

Die Etablierung eines solchen von Bund und Ländern gemeinsam getragenen Maßnahmenpakets für „Digitale Kompetenz in der Lehrerbildung“ soll dazu beitragen, die Anbahnung von digitaler Kompetenz in der ersten und zweiten Phase der Lehrerbildung zu gewährleisten sowie im Rahmen von Fort- und Weiterbildungen auch zukünftig für die sich stetig wandelnden Anforderungen in der digitalen Welt zu sichern. Der Schwerpunkt sollte vor allem auf der inhaltlichen Auseinandersetzung mit der Digitalisierung liegen und sich weniger auf die Digitalisierung des Unterrichts oder der technischen Ausstattung fokussieren.

Neben Kompetenzen zum Umgang mit digitalen Medien und Werkzeugen sowie zur Anwendung von Formen und Methoden der digitalen Lehre (inklusive Prüfungen) müssen auch Kompetenzen angehender und bereits im Beruf stehender Lehrkräfte für den Umgang mit individuellen und gesellschaftlichen Chancen und Folgen der Digitalisierung Eingang in die Lehrer-aus-, -fort- und -weiterbildung finden. Wahlfreiheit, Selbstbestimmung, Selbstkontrolle und Sicherheit im Umgang mit Digitalisierung in allen Lebensbereichen (mit digitalen Medien aber auch mit IoT etc.) erfor-

dern Kompetenzen, die über unterschiedliche Bildungsmaßnahmen angebahnt werden müssen.

Ohne eine entsprechende Berücksichtigung in der Lehrerbildung sind jedoch Initiativen wie die KMK-Strategie „Bildung in der digitalen Welt“ (Kultusministerkonferenz, 2016), in der ein Kompetenzrahmen für digitale Bildung zwischen den Bundesländern vereinbart wurde, unvollständig. Adressiert sind hier zum einen Fachwissenschaften, Fachdidaktiken und Bildungswissenschaften an lehrerbildenden Hochschulen. Zum anderen betrifft dies die zweite Phase der Lehrerbildung, also die Zeit des Referendariats, sowie Fort- und Weiterbildungsinstitutionen für Lehrpersonen, die übergreifende Konzepte für den sukzessiven Aufbau von digitaler Kompetenz in der Lehrerbildung erstellen sollten. Daran anschließend müssten die „Ländergemeinsame[n] inhaltliche[n] Anforderungen für die Fachwissenschaften und Fachdidaktiken in der Lehrerbildung“ (Kultusministerkonferenz, 2008; cf. 2017[13]) angepasst werden, um so digitale Kompetenzen auch in den verpflichtenden Standards der lehrerbildenden Fächer abzubilden.

4.2. Angebote zur Förderung digitaler Kompetenz unterstützen

Der SVRV empfiehlt, bereits bestehende und neu zu etablierende (institutionelle) Angebote zur Förderung digitaler Kompetenz dauerhaft zu finanzieren und strukturell zu verankern. Dabei sollten Angebote mit Lotsenfunktion, Angebote für Multiplikatoren und Angebote für Verbraucher systematisch ausgebaut werden.

(Institutionelle) Angebote zur Förderung digitaler Kompetenz für Multiplikatoren und Verbraucher können zum Kompetenzaufbau beitragen, weil sie verlässliche und geprüfte Informationen vermitteln, als Lotsen fungieren und auf neue Entwicklungen in der digitalen Welt schnell reagieren können.

Lotsen, wie beispielsweise die Stiftung Warentest, stellen Verbrauchern verlässliche Informationen zu Produkten und Dienstleistungen u. a. in den Bereichen Geldanlage, Bildung und Haushalt zur Verfügung. Hierdurch werden Verbraucher in die Lage versetzt, Konsumentscheidungen frei von interessengeleiteten Informationen treffen zu können. Im Gesundheitsbereich besteht beispielsweise das Problem, dass die meisten Verbraucher verlässliche von interessengeleiteten Informationen nicht unterscheiden können. Hier könnte das Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen (IQWiG) eine solche Lotsenfunktion übernehmen, in dem es eine Positiv-Liste evidenzbasierter und verständlicher Quellen erstellt, regelmäßig aktualisiert und verbreitet.

Ein Angebot mit Lotsenfunktion für Multiplikatoren ist z. B. der Materialkompass Verbraucherbildung, während sich der „Weiterbildungs-Guide“ der Stiftung Warentest und die „Medienkompetenz-Datenbank“ der Bundeszentrale für Politische Bildung direkt an die Verbraucher richten. Zudem sollten Initiativen und Vereine, wie z. B. die Initiative D21 und der Chaos Computer Club, als zusätzliche Akteure gewonnen werden, um aktuelle Entwicklungen in der Digitalisierung aufgreifen und in Informations-, Aufklärungs- und Bildungsangebote umsetzen zu können.

Der Förderung digitaler Kompetenz außerhalb von Schule und anderen Bildungsinstitutionen kommt angesichts der schnellen Fortentwicklung digitaler Anwendungen und sich ändernder Nutzungsgewohnheiten eine zentrale Rolle zu. Zur Reduktion von Komplexität benötigen Verbraucher einen schnellen Zugang zu relevanten und verlässlichen Informationen in allen Konsumbereichen (siehe hierzu auch Gigerenzer et al., 2016). Angebote mit Lotsenfunktion, die geprüfte und wesentliche Informationen bieten, können hier eine sinnvolle Hilfestellung bieten. Der SVRV schlägt deshalb vor, dass, analog zur Lotsenfunktion bspw. der Stiftung Warentest oder des IQWiG[14], weitere Angebote mit Lotsenfunktion für Verbraucher in unterschiedlichen Konsumfeldern etabliert und gefördert werden sollten. Verlässliche Verbraucherinfor-

13 Abgerufen am 14. Juni 2017 von URL https://www.kmk.org/themen/allgemeinbildende-schulen/lehrkraefte/lehrerbildung.html.

14 Abgerufen am 14. Juni 2017 von URL https://www.iqwig.de/.

mationen werden u. a. bereitgestellt auf „Mobilsicher.de“,[15] ein Internetportal zur Förderung der Sicherheit mobiler Kommunikation über Smartphones und Tablets des iRights e.V., sowie auf Marktwächer.de[16], Checked4u.de[17] und Verbraucherzentrale.de[18], wo Verbraucherzentralen unter anderem Informationen zu digitalen Angeboten wie Bewertungsportalen, Plattformen und Quantified-Self-Diensten aufbereiten.

Solche Angebote mit Lotsenfunktion sind auch für Multiplikatoren in unterschiedlichen Bereichen eine Hilfe. Ein Beispiel ist der Materialkompass Verbraucherbildung; er bewertet Unterrichtsmaterialien zu Verbraucherfragen u. a. im Bereich Medien (zu Themen wie Datenschutz, Grundwissen und Recht sowie Gewalt im Netz) und dient sowohl der Qualitätssicherung von Unterrichtsmaterialien als auch Lehrkräften als Hilfestellung für die Gestaltung ihres Unterrichts. Der SVRV regt eine Verstetigung des Angebots an, um Lehrkräften eine Orientierung bei der Wahl qualitativ hochwertiger Unterrichtsmaterialien im Bereich der digitalen Bildung zu geben. Eine solche Orientierung ist bedeutsam, weil Unterrichtsmaterialien, die von Verbänden, Verlagen, Nichtregierungsorganisationen, der öffentlichen Hand sowie von Unternehmen angeboten werden, zunehmend im Unterricht genutzt werden, aber keinerlei Prüfung unterliegen.[19]

Neben Aktivitäten, welche die Förderung digitaler Kompetenz im schulischen Kontext zum Ziel haben, sollen Bildungsangebote ausgebaut und finanziert werden, welche digitale Kompetenz im außerschulischen Kontext fördern. Beispiele hierfür sind der „Weiterbildungs-Guide“ der Stiftung Warentest[20] oder die Medienkompetenz-Datenbank der Bundeszentrale für Politische Bildung[21]. In der Datenbank sind medienpädagogische Projekte aufgelistet, welche die Förderung von Medienkompetenz zum Ziel haben. In ihr kann entweder nach der Art der Medien oder des Angebots gesucht werden. Weitere hilfreiche Angebote sind Digitalkompass.de,[22] ein Verbundprojekt zur Förderung der Medienkompetenz älterer Menschen, sowie „Watch your Web“[23] (beendet im Jahr 2015), ein Informationsportal zur Vermittlung verbraucherschutzorientierter Jugendinformation und -medienbildung in sozialen Netzwerken

4.3. Maßnahmen zur Selbstkontrolle bei der Nutzung digitaler Medien und Dienstleistungen entwickeln

Der SVRV empfiehlt den Kultusministerien, Maßnahmen zur Förderung der Selbstkontrolle bei der Nutzung digitaler Medien und Dienstleistungen zu entwickeln.

Selbst- statt Fremdkontrolle bei der Nutzung digitaler Medien und Dienstleistungen ist ein wesentlicher Bestandteil von digitaler Kompetenz. Diese betrifft die Fähigkeit, digitale Dienste bzw. Endgeräte wie Handys zu kontrollieren statt von ihnen kontrolliert zu werden. Die Auswirkungen mangelnder Kontrolle werden in zunehmender Weise sichtbar, z. B. durch die wachsende Zahl von tödlichen Verkehrsunfällen aufgrund der Handynutzung am Steuer. Da derartige Verhaltensweisen sehr früh ausgebildet werden, sollten Maßnahmen zur Förderung der digitalen Selbstkontrolle entsprechend früh im Vorschulalter beginnen.

Die Kultusministerkonferenz widmete sich 2016 dem Thema „Bildung in der digitalen Welt“. Ihre Bildungsinstitutionen und Disziplinen übergreifende Strategie setzt gleichzeitig bei Schülern/Studierenden und Lehrenden an. Außer Acht gelassen wird bei diesem Ansatz die große Relevanz von digitaler Selbst- statt Fremdkontrolle bei der Nutzung von digitalen Technologien. Selbstkontrolle ist ein wesentlicher Bestandteil von digitaler Kompetenz. Sie betrifft die Fähigkeit, digitale Dienste oder Endgeräte wie das Smartphone bei der Nutzung gemäß eigener Präferenzen zu kontrollieren, aber auch das individuelle Verhalten in Foren und sozialen Netzwerken sowie die Einhaltung von Regeln der Netiquette (kein Hate Speech, kein Cybermobbing etc.; Underwood & Ehrenreich, 2017).

15 Abgerufen am 14. Juni 2017 von URL https://mobilsicher.de/.
16 Abgerufen am 18. Juni 2017 von URL www.marktwaechter.de.
17 Abgerufen am 18. Juni 2017 von URL www.checked4u.de.
18 Abgerufen am 18. Juni 2017 von URL www.verbraucherzentrale.de.
19 Abgerufen am 14. Juni 2017 von URL http://www.verbraucherbildung.de/artikel/lehrkraefte-wollen-unabhaengige-qualitaetstests-von-unterrichtsmaterial.
20 Abgerufen am 14. Juni 2017 von URL http://weiterbildungsguide.test.de/.
21 Abgerufen am 14. Juni von URL http://www.bpb.de/lernen/digitale-bildung/medienpaedagogik/206263/medienkompetenz-datenbank.
22 Abgerufen am 14. Juni 2017 von URL https://www.digital-kompass.de/.
23 Abgerufen am 14. Juni 2017 von URL http://www.watchyourweb.de/.

Die Auswirkungen mangelnder Kontrolle werden zunehmend sichtbar, z. B. durch die zunehmenden Fälle von tödlichen Verkehrsunfällen aufgrund von Internetnutzung am Steuer. Aber auch die Ablenkung durch permanent eingehende E-Mails und damit verbundene Konzentrationsstörungen sind zu nennen. Eine repräsentative Befragung von Bitkom Research hat ergeben, dass bereits 51 Prozent der Autofahrer am Steuer Kurznachrichten lesen und acht Prozent Videos auf dem Smartphone ansehen.[24] Die National Highway Traffic Safety Administration (2015) berichtet, dass einer von sieben Unfällen mit dokumentierter Fahrerablenkung in den USA mit Handynutzung verbunden war.

Das wachsende Bedürfnis, digitale Dienste während anderer Tätigkeiten zu nutzen (Multitasking) kann zu verringerter kognitiver Kontrollfähigkeit führen, wie z. B. der Verringerung der Aufmerksamkeitsspanne und der Fähigkeit, im Alltag fokussiert bei einer Aufgabe zu bleiben, wohingegen die Hypothese einer erfolgreichen Anpassung an Multitasking umstritten ist (Ophir et al., 2009; van der Schuur et al., 2015). Die parallele Nutzung digitaler Dienste und sozialer Netzwerke während Lehrveranstaltungen wirkt sich negativ auf Lern- und Prüfungsleistungen aus (Ellis et al., 2010; Junco, 2012; Rosen et al., 2011; Wood et al., 2012). Bereits 2012 gaben 69 Prozent amerikanischer Studenten an, während Lehrveranstaltungen Nachrichten zu schreiben, 28 Prozent nutzten Facebook und 21 Prozent suchten nach themenfremden Inhalten (Junco, 2012); 49 bis 70 Prozent nutzten Facebook parallel zur Erstellung von Hausarbeiten (Junco, 2015). Mangelnde digitale Selbstkontrolle kann in einer Abhängigkeit enden, welche als „Internet-Sucht“ bezeichnet wird (Helbing et al., 2017; Young & Abreu, 2011; cf. Kardefelt-Winther, 2014).

Um derartige negative Konsequenzen digitaler Technologien zu reduzieren, ist die Entwicklung von Selbstkontrolle ein wesentlicher Bestandteil digitaler Kompetenz. Diese digitale Selbstkontrolle sollte bereits im Vorschulalter entwickelt und auch von den Eltern vorgelebt werden (Gigerenzer, 2017). Forschung über wirksame Methoden der Selbstkontrolle in der digitalen Welt existiert bisher jedoch kaum, so dass der SVRV hier einen besonderen Forschungsbedarf sieht. Dieser sollte klären, (1) welche Interventionen Menschen helfen, digitale Selbstkontrolle auszubilden, (2) wie diese Interventionen bereits in (vor) schulische Curricula eingebaut werden können und (3) welche technischen und rechtlichen Mittel mangelnde Selbstkontrolle unterstützend kompensieren können.

24 Abgerufen am 14. Juni von URL https://www.bitkom.org/Presse/Presseinformation/Viele-Autofahrer-nutzen-waehrend-der-Fahrt-das-Smartphone.html.

4.4. Auswirkungen der Digitalisierung auf Kognition, Emotion und soziales Leben erforschen

Der SVRV empfiehlt die gezielte Förderung interdisziplinärer Forschung über die Auswirkung der Digitalisierung auf die Kognition, Emotion und das soziale Leben von Verbrauchern. Das betrifft sowohl „Digital Natives“ als auch „Digital Migrants“.

Derzeit wird digitale Kompetenz schwerpunktmäßig im Umgang mit Technik untersucht. Es wird dagegen nur bedingt erforscht, inwieweit psychische und soziale Verhaltensweisen sich verändern und welche Folgen davon zu erwarten sind. Über mögliche systematische Veränderungen der Aufmerksamkeit, der Gefühle, und des sozialen Verhaltens der Menschen durch die Digitalisierung wird seit Jahren spekuliert, aber es fehlt an systematischer Forschung, insbesondere zu den Langzeitauswirkungen sozialer Medien.

Gleichzeitig stellen sich ethische Fragestellungen etwa in Bezug auf Datenhandel, Kontrollverlust im Internet of Things oder Wahlfreiheit von Verbrauchern, die jeweils auch juristische Dimensionen beinhalten. Hier ergibt sich ein interdisziplinärer Forschungsbedarf für die Verbraucherpolitik, der durch gezielte Förderung gedeckt werden sollte.

Angesichts des Enthusiasmus von Kindern und Jugendlichen für digitale Medien ist es verblüffend, dass sich die entwicklungspsychologische Forschung mit deren Auswirkung auf Entwicklung und Verhalten bisher nur wenig befasst hat (Underwood & Ehrenreich, 2017). Wie wirkt sich die durch den digitalen Konsum notwendig verringerte Interaktion mit Erwachsenen auf die Entwicklung aus (vgl. Barr, 2010)?

Welche Folgen hat eine oberflächliche Informationsaufnahme („Shallow Learning“) auf die Fähigkeit zum eigenständigen Denken und zur Konsolidierung von Inhalten (Loh & Kanai, 2016)? Ist die reduzierte Aufmerksamkeitsspanne vieler Menschen, verstärkt durch Multitasking, ein Problem oder kann man lernen, auch mit ständigen Unterbrechungen die gleiche Leistung zu erbringen? Welche Beziehungen und Kollaborationen entwickeln sich zwischen Mensch und Maschine und was sind ihre Konsequenzen? Die Antworten auf diese und andere wichtige Fragen sind unbekannt.

Neben der Auswirkung der digitalen Revolution auf kognitive Fähigkeiten ist zu vermuten, dass das emotional-soziale Leben sich deutlich ändert. Es wird viel über Fälle von Cybermobbing berichtet, und viele Jugendliche werden tatsächlich online verletzt, aber oft anders als es sich viele Erwachsene vorstellen. Jugendliche leiden unter sozialem Ausschluss wenn sie ständig Bilder von ihren Freunden sehen, die sich ohne sie treffen, oder von Partys, auf die sie nicht eingeladen wurden (Underwood & Ehrenreich, 2017). Die erwartete ständige digitale Verfügbarkeit, nicht nur in sozialen Medien, sondern auch in der professionellen Rufbereitschaft, wird als sozialer Stressfaktor diskutiert (Carstensen, 2015). Kurzfristige Nichtnutzung von digitalen Medien, freiwillig oder nicht, wird ebenfalls häufig als eine Situation mit hohem Stress erlebt, ähnlich wie bei Suchtverhalten. Die Bundesdrogenbeauftragte geht zurzeit von etwa 600.000 Internetabhängigen und 2,5 Millionen problematischen Internetnutzern in Deutschland aus (Stiftung Kind und Jugend, 2017). Intensive Mobiltelefon- und Computernutzung sind Risikofaktoren für Schlafstörungen und mit psychischen Gesundheitsfolgen assoziiert (z. B. Thomée, 2012; van der Schuur et al., 2015). Des Weiteren sind positive Effekte realer sozialer Interaktionen durch Smartphone-Nutzung gefährdet (Rotondi et al., 2017). Zudem gibt es Hinweise auf Zusammenhänge zwischen intensiver Mediennutzung von Eltern und Entwicklungsstörungen der Kinder, etwa Sprachentwicklungsstörungen und motorischer Hyperaktivität bei unter 6-Jährigen (Stiftung Kind und Jugend, 2017).

Doch auch vielfältige positive Entwicklungen sind zu beobachten. So ist die Reichweite der Online-Communities, die zivilgesellschaftliches Engagement stärken (z. B. Better Place, Code for Germany, Next Hamburg), stark gestiegen und ermöglicht neue Formen der Teilhabe. Auch politische Partizipation findet im Netz komplementäre Formen (siehe hierzu beispielsweise das EU-geförderte Projekt MAZI[25]) und fördert Gemeinschaften.

Auch ist die Möglichkeit des Austausches auf themenspezifischen Foren zu sensiblen persönlichen Themen (z. B. Selbsthilfegruppen online) für viele eine wichtige Hilfe im Alltag geworden, die anonym genutzt werden kann (z. B. Döring, 2010). Die vielfältigen Beziehungen zwischen Mensch und vernetztem System werden auch immer stärker im Arbeitsumfeld in den Fokus rücken, wenn Beschäftigte durch Augmented Reality Anwendungen in Echtzeit unterstützt werden können[26] und sich somit neue Betätigungsfelder eröffnen, oder wenn der Zugang zu Wissen in der Open Source Ökologie Produktionsmöglichkeiten und langfristig potentiell auch Machtverhältnisse verschieben kann (vgl. Rifkin, 2014). Die langfristigen ethischen, juristischen und sozialen Fragestellungen, die sich daraus ergeben, gilt es zu untersuchen.

Um besser zu verstehen, wie die digitale Technologie uns alle verändert und wie wir negative Folgen unter Kontrolle bekommen können und gleichzeitig die positiven Entwicklungen begreifen und unterstützen können, ist es unerlässlich, die Auswirkungen der digitalen Revolution auf den Menschen systematisch zu untersuchen. Die zentrale Frage für die Forschung sollte dabei nicht sein, *ob* digitale Medien die kognitive Entwicklung beeinflussen, sondern *wie* Technologie die Nutzer verändert und welche Kompetenzen Nutzer brauchen, um besser damit umzugehen (Gigerenzer, 2013; 2017). Die Forschung sollte vor allem klären, (1) welche Auswirkungen die Nutzung digitaler Dienste auf die kindliche und jugendliche Entwicklung hat, und welche Interventionen ein gesundes Nutzungsverhalten fördern, (2) welche Auswirkungen sie auf „Digital Migrants“ hat, und (3) welche institutionellen und rechtlichen Rahmenbedingungen geschaffen werden sollten, damit sowohl „Digital Natives“ also auch „Digital Migrants“ die psychischen, gesundheitlichen, sozialen und ökonomischen Auswirkungen der digitalen Revolution besser steuern und kontrollieren können.

25 Abgerufen am 14. Juni 2017 von URL http://www.mazizone.eu/.

26 Siehe hierzu beispielsweise das Projekt smartFactory zu Predictive Maintenance Data Analysis (abgerufen am 14. Juni 2017 von URL http://dfki-3036.dfki.de/web-News/SF_Steckbrief_20151118_LabsNetworkIndustrie.pdf).

Regulierung

5. Regulierung

Die Handlungslogik der Regulierung zielt darauf ab, staatliche und privatwirtschaftliche Akteure für die Gewährleistung von Digitaler Souveränität in die Verantwortung zu nehmen. In der rechtlichen Dimension geht das Konzept der Digitalen Souveränität von Verbrauchern in dem verfassungsrechtlich geschützten Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 S. 1 GG auf.[27] Im Volkszählungsurteil des BVerfG wurde auf Grundlage des Art. 2 Abs. 1 und 1 Abs. 1 GG das Recht auf informationelle Selbstbestimmung konkretisiert. Es umfasst das Recht des Einzelnen, grundsätzlich „selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Informationelle Selbstbestimmung wird seither als die notwendige Vorbedingung tatsächlicher Freiheit, sowohl im Verhältnis zum Staat als auch im Verhältnis zu privaten Akteuren, betrachtet (Buchner, 2006). Der Schutzbereich des allgemeinen Persönlichkeitsrechts umfasst auch die Möglichkeit, durch einen Zugriff auf das System einen Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild der Persönlichkeit zu erhalten.[28]

Aus der staatlichen Verantwortung für die Gewährleistung der informationellen Selbstbestimmung der Bürger folgt die Pflicht, die juristischen Rahmenbedingungen für die Ausübung von informationeller Selbstbestimmung zu erhalten und ggf. zu verbessern. Der staatlichen Vorbildfunktion kommt besonders hohe Bedeutung zu, da sich auch Ausnahmeregelungen für Maßnahmen im Bereich der inneren Sicherheit strikt an den gesetzlichen Rahmen, die Ermöglichung der Transparenz staatlichen Handelns und der Einhaltung höchstrichterlich definierter Schranken[29] halten müssen.

In diesem Sinne finden sich im Folgenden Handlungsempfehlungen für konkrete Bereiche, in denen der SVRV regulatorische Handlung für unabdingbar hält.

27 Kritisch zum Begriff der informationellen Selbstbestimmung: Friedewaldt et al. (2017).

28 BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07 - BVerfGE 120, 274, 314 (Online Durchsuchungen).

29 Besondere Bedeutung kommt dabei den Entscheidungen rund um staatlich angeordnete, gesamtgesellschaftliche Speicherung von digitalen Kommunikationsdaten zu. Für die deutsche Ebene hierzu: BVerfG Urteil vom 2.3.2010, 1 BvR 256; EuGH, Urteil v. 21. Dezember 2016 in den verbundenen Rechtssachen C-203/15, Tele2 Sverige AB / Post- och telestyrelsen und C-698/15, Secretary of State for the Home Department / Tom Watson u. a ., ECLI:EU:C:2016:970; EuGH, Urteil v. 8. April 2014 in den verbundenen Rechtssachen C-293/12 und C-594/12 Digital Rights Ireland und Seitlinger u. a. ECLI:EU:C:2014:238.

5.1. AGB und Datenschutzerklärungen als One-Pager umsetzen

Der SVRV bekräftigt seine Empfehlung[30], dass Unternehmen die Verbraucher auf je einer Seite (500 Wörter) über die relevanten datenschutzrechtlichen Vorgaben sowie über die AGB-Bestimmungen vor Vertragsschluss zu informieren haben. Der SVRV empfiehlt, diesen „One-Pager" in einem vom BMJV organisierten Pilotprojekt mit relevanten Stakeholdern umzusetzen.

Die Verpflichtung zu einem „One-Pager" kann dazu beitragen, die Transparenz von Datenübertragungen für Verbraucher zu erhöhen. Außerdem kann der „One-Pager" dazu beitragen, dass die Akzeptanz von benutzten AGB und Datenschutzerklärungen erhöht wird, wenn er in einem kooperativen Prozess zwischen BMJV oder einer anderen staatlichen Behörde und Stakeholdern gemeinsam erarbeitet wird.

Die Einwilligung durch die Betroffenen in derlei Datenerhebungen ist ein Grundpfeiler der informationellen Selbstbestimmung und damit der Digitalen Souveränität von Verbrauchern. In der Praxis erfolgt die Einwilligung durch standardisierte Datenschutzerklärungen. Allerdings ist die Aufklärung über die Erhebung und Verarbeitung ihrer Daten und der entsprechenden Verbraucherrechte „alarmierend" schlecht, wie ein „Privacy Sweep" des Global Privacy Enforcement Networks GPEN bei über 300 der analysierten Internet-of-Things-Geräten festgestellt hat.[31] Dies zeigte jüngst auch die Untersuchung des Marktwächters Digitale Welt „Wearables, Fitness-Apps und Datenschutz: Alles unter Kontrolle?"[32]. Eine beispielhafte Analyse einer im Internet of Things benutzten App ergab außerdem, dass einige Klauseln gem. der §§ 307, 308 BGB unwirksam sein könnten, da sie den

30 Diese Forderung ist nachzulesen in SVRV (2016, S. 46f).

31 Weiterführende Informationen sind auf der Webseite des irischen Datenschutzbeauftragten zu finden (abgerufen am 14. Juni 2017 von URL https://www.dataprotection.ie/docs/23-9-2016-International-Privacy-Sweep-2016/i/1597.htm). In Deutschland haben sich der Landesbeauftrage für den Datenschutz Baden-Württemberg und das Bayerische Landesamt für Datenschutzaufsicht beteiligt.

32 Bei neun der zwölf untersuchten Wearables zeigten sich so erhebliche datenschutzrechtliche Verstöße, dass die Verbraucherzentrale Nordrhein-Westfalen die Anbieter abmahnte (Moll et al., 2017).

Verbrauchern einseitige Prüf- und Kontrollpflichten bzgl. Änderungen der Klauseln auferlegen und weil sie, wegen mangelnder Aufklärung über die Weitergabe von Daten an Dritte, Verbraucher unangemessen benachteiligen (Domurath & Kosyra, 2016).

Daraus folgt unbedingter Handlungsbedarf im Hinblick auf die Übersichtlichkeit und Legalität von AGB und Datenschutzerklärungen. Die regulative Forderung eines „One-Pagers", der im diskursiven Prozess mit Stakeholdern unter Führung des BMJV erarbeitet wird, kann dazu beitragen, die geforderte Transparenz und Legalität herbeizuführen. Er geht weiter als der im Rahmen des Nationalen IT-Gipfels 2015 vorgestellte One-Pager[33], der sich ausschließlich auf Datenschutzhinweise bezieht.

5.2. Algorithmen offenlegen und überprüfbar machen

Der SVRV bekräftigt seine Empfehlungen[34], dass durch rechtliche Vorgaben sichergestellt werden muss, (a) dass Algorithmen die Vorgaben des Verbraucherrechts, des Datenschutzrechts, des Anti-Diskriminierungsrechts und der digitalen Sicherheit berücksichtigen, sowie die zugrundeliegenden Parameter bei Algorithmen mit direktem Verbraucherkontakt transparent zu machen, (b) dass Algorithmen durch standardisierte Offenlegungspflichten einem Kreis von Experten offengelegt werden, die per Stichprobe die rechtliche Unbedenklichkeit überprüfen. Der SVRV empfiehlt, rechtliche Standards zu entwickeln und Quellcodes dauerhaft zu hinterlegen.

Die Offenlegung von Algorithmen für einen Kreis von Experten (z. B. in der vom SVRV geforderten Digitalagentur) ist maßgeblich für die Einhaltung gesetzgeberischer Vorgaben bei der automatisierten Entscheidung durch Algorithmen. Dabei geht es insbesondere um das Verbraucherrecht, Antidiskriminierung und das Lauterkeitsrecht, aber auch die Einhaltung datenschutzrechtlich festgeschriebener Grundsätze wie Datensparsamkeit und Zweckbindung. Für die Verbraucher selbst ist es vor allem wichtig, die den Algorithmen zugrundliegenden Parameter (wie die Variablen und ihre Gewichtung) zu kennen, weil sie nur so Widerspruch einlegen können. Diese Aufgaben könnten in einer Digitalagentur gebündelt werden. Diese ist notwendig, um dort Expertise für die Überwachung der Einhaltung gesetzgeberischer Vorgaben anzusiedeln.

Der Einsatz von Algorithmen und die absehbare Weiterentwicklung selbstlernender Algorithmen in einer ständig sich weiter vernetzenden Welt berühren tief verwurzelte ethische Grundsätze unseres gesellschaftlichen Zusammenlebens. Die ethischen Fragen strahlen in die Ordnungsfunktion des Rechts aus, welches sich einer normativen Stellungnahme zu diesen Fragen nicht verschließen kann. Eine besondere Herausforderung liegt in der Beantwortung der Frage, wie mit rechtlichen Mitteln sichergestellt werden kann, dass selbstlernende Algorithmen ethisch verantwortlich „handeln". Klar ist, dass die Rechtspolitik zwar auf die Expertise derjenigen, die die Entwicklung der Künstlichen Intelligenz (KI) vorantreiben, aufbauen kann (in diesem Sinne: BMWi, 2017b); jedoch sollte die Einhaltung regulativer Standards nicht allein auf dem Wettbewerb oder eigenverantwortlichem ethischem Handeln der Industrie beruhen. Aber wie kann ein sich selbst steuernder Prozess normativ eingebettet werden?

Zunächst muss klar gestellt werden, dass die Kontrolle von Algorithmen auf verschiedenen Ebenen stattfinden kann. Es können die mathematischen Formeln selbst, aber auch die für die Entscheidung erheblichen Parameter oder das Ergebnis der zugrundliegenden Berechnung oder Schätzung kontrolliert werden. Für das Verbraucherrecht können beispielsweise Bedingungen zur Kontrolle der Parameter von Algorithmen aufgestellt werden, die sich nicht nur aus dem Recht Allgemeiner Geschäftsbedingungen (siehe 5.1.) und Bedingungen der IT-Sicherheit (siehe 3.3.), sondern auch aus dem Antidiskriminierungs-, Lauterkeits- und Datenschutzrecht ergeben. Dabei geht es zum einen um die Parameter, an denen die

33 Ein Muster dieses Datenschutz-One-Pagers wurde erarbeitet von der vom BMJV geleiteten Plattform „Verbraucherschutz in der digitalen Welt", gebildet aus Vertreterinnen und Vertretern der Politik, Wirtschaft, Wissenschaft, Verbraucher- und Datenschutzorganisationen und Institutionen aus dem Justizbereich.

34 Diese Forderung ist nachzulesen in SVRV (2016, S. 67).

Rechtmäßigkeit der über Algorithmen getroffenen Entscheidungen gemessen wird, und zum anderen um die menschliche Kontrolle dieser Entscheidungen.

Die Anforderungen des Anti-Diskriminierungsrechts[35] wie auch des Lauterkeitsrechts[36] müssen beachtet werden, insbesondere wenn Verbraucher mit automatisierten Entscheidungen konfrontiert sind. Denn mit Hilfe von Algorithmen ist es möglich, Werbung, Angebote, Preise und letztlich Verträge scheinbar individuell zu gestalten, obwohl sich hinter der Individualisierung eine Diskriminierung verbergen mag. Diese Diskriminierung hat nicht notwendig ein bestimmtes Individuum im Blick, sondern eine Gruppe von Individuen, die bestimmte, über Algorithmen determinierte Merkmale aufweisen (Angwin & Parris, 2016).

Darüber hinaus müssen die datenschutzrechtlichen Grundsätze der Datensparsamkeit (Art. 5 Abs. 1 lit. c DSGVO) und Zweckbindung (Art. 5 Abs. 1 lit b DSGVO) handlungsleitende Grundsätze bleiben und beim Einsatz von Algorithmen beachtet werden. Nur so entsteht ein Grundvertrauen der Verbraucher in den staatlichen und privatwirtschaftlichen Umgang mit persönlichen Daten. Dies bedeutet, dass Untersuchungen, welche die Vereinbarkeit von Big Data mit diesen Grundsätzen kritisch beleuchten (Helbing, 2015), sowie Forderungen nach einem Recht auf datenerhebungsfreie Produkte (Becker, 2017) oder einem „Recht auf analoge Welt" (Maas, 2015)[37] auf politischer Ebene ernsthaft und nachdrücklich diskutiert werden müssen. Die Entwicklung von Produkten und Dienstleistungen, deren zugrundliegende Algorithmen eine automatische Löschung von Daten ermöglichen, könnten gefördert werden (Stichwörter: Privacy by Design und Privacy by Default).

Auch bei selbstlernenden Algorithmen muss die rechtliche Verantwortlichkeit zuzuordnen sein. Dazu sollten Forschungsprojekte verfolgt und ggf. angestoßen werden. Ohne die existierenden gesetzlichen Vorgaben abzuschwächen, sollte insbesondere im Fall von selbstlernenden Algorithmen der Gesetzgeber von dem Fachwissen der Informations- und Kommunikationstechnologischen Unternehmen sowie den Experten aus den jeweiligen Forschungsgebieten profitieren, und diese in einen Prozess zur Ausarbeitung eines Code of Conduct über die Verwendung von personenbezogenen Daten, künstlich intelligenter Systeme und der Big Data Analyse einbinden.

Die Einhaltung dieser Parameter kann nur, wenn überhaupt, mit Hilfe einer staatlichen Instanz überprüft werden, die Unternehmen zur Offenlegung von Daten und zur Auskunft verpflichtet.[38] Um dem Interesse der Unternehmen an ihren Geschäftsgeheimnissen auf der einen Seite und dem Auskunftsrecht der Betroffenen auf der anderen Seite gerecht zu werden (§ 34 Abs.1 S. 4 BDSG),[39] könnten Algorithmen durch standardisierte Offenlegungspflichten einem Kreis von Experten einer staatlichen Stellen wie z. B. einer Digitalagentur offengelegt werden, die per Stichprobe die rechtliche Unbedenklichkeit überprüfen. Hierzu sind standardisierte Verfahren des Software Engineering zu entwickeln.

In Anbetracht der Tatsache, dass die innovativsten und größten Teile der Informations- und kommunikationstechnologischen Unternehmen außerhalb Deutschlands angesiedelt sind, ist eine international konzertierte Aktion vonnöten. Idealerweise wäre das Forum für die Suche nach einer adäquaten Lösung die Europäische Union, besser noch die OECD und die Vereinten Nationen.

35 Zum Beispiel Allgemeines Gleichbehandlungsgesetz, § 19 Ab. 1: 'Eine Benachteiligung aus Gründen der Rasse oder wegen der ethnischen Herkunft, wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität bei der Begründung, Durchführung und Beendigung zivilrechtlicher Schuldverhältnisse (…) ist unzulässig'. Zum EU-Recht: Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft, OJ L 180/22, 19.7.2000 und Richtlinie 2004/113/EG des Rates vom 13. Dezember 2004 zur Verwirklichung des Grundsatzes der Gleichbehandlung von Männern und Frauen beim Zugang zu und bei der Versorgung mit Gütern und Dienstleistungen, OJ L 373/37, 21.12.2004.

36 Siehe Richtlinie 2005/29/EG des europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken) OJ L 149/22, 11.6.2005, welche irreführende Geschäftspraktiken verbietet, wenn sie u. a. „falsche Angaben enthält und somit unwahr ist oder wenn sie in irgendeiner Weise, …, selbst mit sachlich richtigen Angaben den Durchschnittsverbraucherin Bezug auf einen oder mehrere der nachstehend aufgeführten Punkte täuscht oder ihn zu täuschen geeignet ist und ihn in jedem Fall tatsächlich oder voraussichtlich zu einer geschäftlichen Entscheidung veranlasst, die er ansonsten nicht getroffen hätte.

37 Artikel 13 der von Heiko Maas vorgeschlagenen Digitalen Grundrechte (abgerufen am 14. Juni 2017 von URL http://www.bmjv.de/SharedDocs/Interviews/DE/2015/Namensartikel/12092015_DieZeit.html).

38 Diese Forderung ist nachzulesen in SVRV (2016, S. 71).

39 In dieser Hinsicht hat der BGH im Schufa-Urteil entschieden, dass die Score-Formel von Bonitätsbewertungen bei Krediten als Geschäftsgeheimnis geschützt sind (BGH VI ZR 156/13). Der Fall liegt jetzt dem Bundesverfassungsgericht vor. Ein Entscheidungstermin ist noch nicht absehbar.

5.3. Unentgeltlichen Auskunftsanspruch nachbessern

Der Sachverständigenrat empfiehlt, den unentgeltlichen Auskunftsanspruch (§ 34 BDSG) ohne Limitierung zu gewähren sowie Unternehmen zu verpflichten, Verbraucher auf ihre kostenlosen Auskunftsrechte und auf die Möglichkeit der Berichtigung fehlerhafter Daten transparent, verständlich und leicht erkennbar beim Anbieten ihrer Produkte hinzuweisen (d. h. Berichtigung, Löschung und Sperrung).

Die Durchsetzung des Auskunftsanspruchs ist im Moment mit erheblichen praktischen Schwierigkeiten verbunden, welche die Effektivität dieses für die Digitalgesellschaft grundlegenden Rechts schmälern. Verbraucher sind über ihre Rechte nicht ausreichend aufgeklärt und haben außerdem Probleme bei der Durchsetzung unentgeltlicher Auskunftsbegehren. Um Verbraucher über dieses und damit verbundene Rechte effektiv aufzuklären, müssen Auskunftsansprüche nicht nur leicht verständlich und transparent auf Webseiten platziert sein. Es muss außerdem auf einfache Weise möglich sein, unentgeltliche Auskünfte zu bekommen. Entsprechend sollte eine Haftung für verantwortliche Stellen diskutiert werden.

Wenn öffentliche und nichtöffentliche Stellen Daten ohne Kenntnis der betroffenen Individuen erheben, müssen diese nach geltendem Recht über die Speicherung, die verantwortliche Stelle sowie die Zweckbestimmungen der Datenverarbeitung unterrichtet werden (§§ 19a, 33 BDSG, Art. 15 DSGVO). Überdies hat die verantwortliche Stelle dem Betroffenen auf Verlangen über die zu seiner Person gespeicherten Daten, die Herkunft dieser Daten, die Empfänger, an die Daten weitergegeben werden, und den Zweck der Speicherung Auskunft zu erteilen (§§ 19, 34 BDSG, Art. 15 DSGVO).

Das Auskunftsrecht ist die Basis für die Ausübung weiterer Betroffenenrechte und damit der Kern des Rechts der informationellen Selbstbestimmung. Es spiegelt auch die Überlegung wider, dass Entscheidungen in letzter Instanz von Menschen getroffen werden bzw. dass eingesetzte Algorithmen auch unter kontinuierlicher menschlicher Kontrolle in Bezug auf ihre Entscheidungen stehen sollen. In diesem Sinne legt § 6 Abs. 1 BDSG fest, dass rechtserhebliche Entscheidungen nicht ausschließlich auf der automatisierten Verarbeitung personenbezogener Daten beruhen dürfen, wenn diese der Bewertung einzelner Persönlichkeitsmerkmale dienen. Artikel 21 und 22 DSGVO räumen diesbezüglich ein Widerspruchsrecht ein. Außerdem stellt das Auskunftsrecht eine individuell durchsetzbare Möglichkeit zur Kontrolle der Datenvermeidungs- und Zweckbindungsgrundsätze dar. Es dient damit maßgeblich der Transparenz automatisierter Entscheidungsfindung. Erst wenn Betroffene Kenntnis über die Identifikation und Speicherung von Daten erlangen, können unrichtige Daten berichtigt, unzulässig gespeicherte und für den Zweck nicht mehr erforderliche Daten gelöscht und, soweit ihre Richtigkeit vom Betroffenen bestritten wird, sich aber weder die Richtigkeit noch die Unrichtigkeit feststellen lässt, gesperrt werden (§§ 20, 35 BDSG, Arts. 16, 17 DSGVO).[40]

Hier geht es auch immer darum, das Spannungsfeld zwischen widerstreitenden Interessen – dem Löschungsinteresse des Betroffenen und dem Informationsinteresse der Informationssuchenden bzw. den Geschäftsinteressen von Unternehmen – aufzulösen. Diesbezüglich hat der EuGH in seinem Google-Urteil[41] ausgeführt, dass das Recht des Betroffenen an seinen Daten das Informationsinteresse der Allgemeinheit durchaus überwiegen kann. Allerdings ist die Umsetzung des Rechts auf Löschung der Daten bzw. das „Recht auf Vergessenwerden", wie es jetzt in Art. 17 DSGVO enthalten ist, in der Praxis aufgrund rechtlicher und technischer Schwierigkeiten problematisch. Aus technischer Sicht ist, auch wenn die Löschung von Daten grundsätzlich möglich ist, dies oft mit einigem technischen Aufwand verbunden (Weis et al., 2016). Problematisch ist auch, dass die Löschung oft nur „partiell" vollzogen wird. Daten sind auch nach Löschung über andere Domains oftmals weiterhin verfügbar. Über diese Einschränkungen in der Rechtsdurchsetzung herrscht bei Verbrauchern hingegen kaum Klarheit, daher besteht hier grundsätzlicher Aufklärungsbedarf. Plausible Ansätze, das Recht auf Löschen durchzusetzen, sollten unterstützt werden.

40 Zu den Korrekturrechten: Becker (2017).

41 EuGH Urteil vom 13. Mai 2014 im Fall C-131/12, Google Spain SL und Google Inc. v. Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, EU:C:2014:317.

Ggf. können Anbieter von sozialen Netzwerken und anderen Online-Diensten verpflichtet werden, ihren Kunden entsprechende Optionen anzubieten.

In der Praxis wissen Betroffene darüber hinaus oft nicht, wie sie ihr Auskunftsrecht sowie die darauf aufbauenden Rechte ausüben können. Verbrauchern ist häufig unklar, welche Unternehmen ihre Daten verarbeiten. Spindler et al. (2016) konstatieren eine „gravierende Diskrepanz" zwischen Rechten und gelebter Praxis. Außerdem werden kostenfreie Auskunftsmöglichkeiten nicht prominent auf Webseiten platziert und, ganz im Gegenteil, beispielsweise bei der Selbstauskunft der Schufa Verbraucher zunächst auf die bezahlte Auskunftsseite geleitet (Korczak, 2016). Es gibt auch Hinweise darauf, dass unentgeltliche Auskünfte oft länger dauern als entgeltliche (Korczak, 2016; Roßnagel et al., 2016).

Es muss aber sichergestellt sein, dass datenerhebende und -verarbeitende Unternehmen entgeltfreie Auskunftsmöglichkeiten prominent auf ihren Webseiten und in geeigneten sonstigen an Verbraucher gerichteten Veröffentlichungen platzieren. Daher sollten Unternehmen verpflichtet werden, auf die Möglichkeit der entgeltfreien Auskunft leicht auffindbar hinzuweisen. Es muss diskutiert werden, ob eine Haftung für diese Verpflichtung eingeführt werden soll, um die Einhaltung gesetzgeberischer Vorgaben zu verstärken. Außerdem müssen sie über dieses Recht sowie die Rechte auf Berichtigung, Löschung und Sperrung leicht verständlich aufklären. Hier sei auf die Forderung verwiesen, dass Datenschutzerklärungen den Verbrauchern auf einer Seite zur Verfügung gestellt werden sollen (s. Forderung 5.1).

Im Übrigen ist hier auch die Algorithmenkontrolle (s. Forderung 5.2) von entscheidender Bedeutung: Sie unterstützt Verbraucher dabei, Transparenz über die von ihnen erhobenen Daten zu erhalten, weil sie zur Minimierung von Daten überhaupt beitragen kann. Algorithmenkontrolle kann auch dabei helfen, die Probleme von Verbrauchern bei der Durchsetzung ihrer Rechte abzumildern.

5.4. Mindeststandards für Interoperabilität weiterentwickeln

Der SVRV empfiehlt, Mindeststandards zu entwickeln, die eine Kompatibilität zwischen digitalen Diensten sicherstellen, so dass eine Kommunikation zwischen Nutzer-Accounts unabhängig vom Anbieter möglich ist (Interoperabilität – analog zum Mobilfunk).

Die Interoperabilität – wie nutzerfreundliche Möglichkeiten der Datenportabilität zwischen sozialen Netzwerken oder Messenger-Diensten – ist derzeit nicht systematisch gegeben. Es kommt zu so genannten Lock-In-Effekten, die immer die Gefahr von Formen des Missbrauchs von Marktmacht bergen, wie sie auf dem deutschen Markt bei Plattformen wie Facebook und WhatsApp deutlich werden. Technische Lösungen der Interoperabilität, wie sie auch zwischen den verschiedenen Mobilfunkanbietern gefunden wurden, könnten neue Wettbewerbsanreize setzen.

Das Schlagwort „Interoperabilität" trifft das Mark der digitalen Gesellschaft. Im Kern bedeutet Interoperabilität die Möglichkeit, Daten über Systeme, Applikationen und Komponenten hinweg zu übertragen und nutzbar zu machen (Palfrey & Gasser, 2012). Es befasst sich mit dem Ausgleich zweier Dimensionen: Auf der einen Seite wurden mit hoher Geschwindigkeit viele neue Infrastrukturen entwickelt, die Konnektivität und Datenströme zwischen Individuen, Organisationen und Systemen erhöhen; auf der anderen Seite gibt es bisher keinen Orientierungsrahmen, der das (gesellschaftliche) Ziel dieser Interoperabilität definiert und ihre Risiken managt (Palfrey & Gasser, 2012). Dabei geht es also um mehr als Technik und Datenströme: Es geht um eine Kultur von menschlichen und institutionellen Interaktionen. Vier verschiedene und gleichzeitig miteinander verbundene Schichten der Interoperabilität können unterschieden werden (dazu Kominers, 2012; Gasser, 2012; Palfrey & Gasser, 2012): Auf der technischen Ebene geht es um die Möglichkeit technischer Systeme, sich miteinander zu verbinden, oft durch ein vereinbartes Interface; auf der Daten- bzw. semantischen Ebene geht es um die Nutzbarmachung und Lesbarkeit der Daten, die über das Interface über-

tragen werden; drittens, kann Interoperabilität nur funktionieren, wenn bei den Nutzern die kognitiven Fähigkeiten und die Bereitschaft vorhanden ist, zusammen zu arbeiten; zuletzt geht es im abstrakten Sinn um die Kooperationen zwischen gesellschaftlichen Systemen, wie z. B. rechtlichen Vorgaben. Wenn Interoperabilität effektiv nutzbar sein soll, müssen gesellschaftliche Überlegungen auf allen Ebenen gleichzeitig stattfinden.

Hinsichtlich der rechtlichen Rahmenbedingungen ist Interoperabilität in Deutschland und der EU durch mehrere Instrumente, hauptsächlich im Telekommunikationsbereich, geregelt. Seit September wird die EU-Gesetzgebung im Rahmen der Digitalmarktstrategie mit dem Ziel des Aufbaus einer Datenwirtschaft und der Steigerung der Wettbewerbsfähigkeit (Europäische Kommission, 2015) überarbeitet. Generell spielt Standardisierung dabei eine entscheidende Rolle. Gem. Artikel 17 der Rahmenrichtlinie[42] hat die Europäische Kommission die Federführung bei der Erarbeitung nicht bindender Standards als Grundlage für die harmonisierte Erbringung von Dienstleistungen. Insbesondere treibt sie, gemeinsam mit dem Europäischen Komitee für Standardisierung, die Entwicklung von Standards vor allem für interoperable Finanz-, Transport-, Verwaltungs- und eHealth-Dienstleistungen voran.[43] Nationale Regulierungsbehörden sollen Anreize für die Anwendung dieser Standards schaffen (Artikel 5 der Zugangsrichtlinie)[44] sowie die Implementierung von internationalen Standards vorantreiben. Grundlegend geht es zunächst darum, die technischen Voraussetzungen für Interoperabilität zu schaffen. Die dafür notwendigen Standards und daraus entstehende Konsequenzen für Wirtschaft, Verbraucher und Staat werden für den gesamten Markt der digitalen Dienstleistungen und Produkte und hier insbesondere auch für das Internet of Things diskutiert (Zingales, 2015; Kominers, 2012). Die Interoperabilität sowie nutzerfreundliche Möglichkeiten der Datenportabilität zwischen Anbietern, wie z. B. auch sozialen Netzwerken und Messenger-Diensten, ist derzeit jedoch kaum gegeben. Es kommt zu so genannten Lock-In-Effekten, was immer die Gefahr von Formen des Missbrauchs von Marktmacht birgt (Deutscher Bundestag, 2016), wie sie auf dem deutschen Markt bei Plattformen wie Facebook und WhatsApp deutlich werden. Unmittelbar spürbare Veränderungen für Verbraucher kann insbesondere eine verbesserte Interoperabilität für den Bereich der Over-The-Top-Player wie WhatsApp und Skype mit sich bringen. Dementsprechend wäre hier von Standardsetzungen in Bezug auf Interoperabilität eine Öffnung des Marktes auch für neue, innovative Anbieter zu erwarten. Eine Angleichung der Regulierung von solchen Over-the-Top-Playern an die Telekommunikationsanbieter würde entsprechend auch für Bereiche, die über die Interoperabilität hinausgehen, den Markt fairer und offener gestalten (BMWi, 2017b).

42 Siehe beispielsweise Erwägungsgrund 9 und Artikel 17 der Richtlinie 2002/21/EC des europäischen Parlaments und des Rates vom 7 März 2002 über einen gemeinsamen Rahmen für elektronische Kommunikationsnetzwerke und Dienstleistungen, OJ L 108, 24.4.2002, angepasst durch Richtlinie 2009/140/EG des europäischen Parlamentes und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste OJ L 337/37, 18.12.2009.

43 Informationen zu sich in Entwicklung befindlichen und bereits genehmigten Standards werden zur Verfügung gestellt vom European Committee for Standardization (abgerufen am 14. Juni 2017 von URL standards.cen.eu).

44 Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung, OJ L 108, 24.4.2002 angepasst durch Richtlinie 2009/140/EC des europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Zugangsrichtlinie).

5.5. Recht auf Datenportabilität konkretisieren

Der SVRV bekräftigt seine Empfehlung, das Recht auf Datenportabilität als Kündigungsrecht zu verstehen und empfiehlt, einen Rahmen für einen Wechsel zwischen Anbietern festzulegen (analog zum digitalen Zahlungsverkehr).

Das Recht auf Datenportabilität, verstanden als Übertragung der Daten zum Verbraucher selbst oder zu einem anderen Anbieter, ist maßgeblich von technischen Voraussetzungen abhängig. Hierzu muss ein rechtlicher Rahmen analog etwa zum digitalen Zahlungsverkehr festgelegt werden. Verlangt der Verbraucher den Rückübertrag der Daten auf sich selbst, kommt dies einem Kündigungsrecht gleich. Die bestehenden Unsicherheiten in Bezug auf die Formulierung in Art. 20 DSGV sind zu beseitigen, indem dem Verbraucher ausdrücklich ein Kündigungsrecht eingeräumt wird.

Das Recht auf Datenportabilität wurde im Nachgang des Google-Urteils des EuGH[45] in Artikel 20 DSGVO eingeführt. Danach hat der Betroffene das Recht, personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen zu übermitteln bzw. technisch übermitteln zu lassen. Das Recht auf Datenportabilität soll dem Betroffenen ermöglichen, Profile bei sozialen Netzwerken oder E-Mail-Konten auf andere Diensteanbieter zu übertragen. Dies muss notwendigerweise auch Daten Dritter umfassen (E-Mail-Konversationen, empfangene Bilder etc.). Damit ist das Recht auf Datenportabilität für die Ausübung digitaler Souveränität i. S. der informationellen Selbstbestimmung hoch relevant, weil es Verbrauchern die Möglichkeit gibt, zwischen verschiedenen Anbietern digitaler Dienstleistungen zu wählen und zu wechseln.

Gleichzeitig soll das Recht aber auch den Wettbewerb stärken, wenngleich dies nicht unumstritten ist. Die deutschen und französischen Wettbewerbsbehörden haben konstatiert, dass etablierte Unternehmen aufgrund ihrer großen Kunden- und Datenbasis u. a. eine Marktmacht und damit einen Wettbewerbsvorsprung gegenüber anderen Unternehmen, die nicht über ein vergleichbares Volumen oder vergleichbare Diversität von Daten verfügen, erlangen (Birnstiel & Eckel, 2016). Dadurch kann es zu sogenannten Lock-In Effekten kommen (Deutscher Bundestag, 2016; Schantz, 2016; Swire & Lagos, 2013). Ob diese Effekte wegen sich ändernder Präferenzen von Verbrauchern und Businessmodellen von Unternehmen[46] nachteilig für den Wettbewerb sind, soll an dieser Stelle dahin gestellt bleiben. Klar ist, dass die Zielsetzung des Rechts auf Datenportabilität einen unerlässlichen Teil der EU Strategie für einen digitalen Binnenmarkt für Europa darstellt (Europäische Kommission, 2015).

Die Umsetzung des Rechts auf Datenportabilität ist umstritten. Aus technischer Sicht sind einige mit Bezug auf das sog. Semantische Web zwar zuversichtlich, dass Datenportabilität machbar ist (Bojars, et al., 2008).[47] Allerdings gibt es in der technischen Fachliteratur im Moment noch keinen einfachen Standard, mit Hilfe dessen definiert werden könnte, was als strukturiertes und „gängiges" Datenformat gilt und was nicht (Swire & Lagos, 2013). Außerdem wird Datenportabilität problematisch, wenn sie auch Daten Dritter betrifft oder der Grad ihrer Personalisierung unklar ist (dazu Schweitzer et al., 2016; BMWi, 2017b). Existierende und angedachte Standards sind im Moment noch übermäßig kompliziert (Swartz, 2013). Vor diesem Hintergrund hat die Article 29 Data Protection Working Party die Industrie- und Handelsvertreter dazu aufgerufen, an einem gemeinsamen Set von Interoperabilitätsstandards und -formaten zu arbeiten (Article 29 Data Protection Working Party, 2017). Die Interoperabilität sollte jedoch nicht nur in diesem singulären Moment einer Datenübertragung im Rahmen des Anbieterwechsels dienen. Vielmehr sollten z. B. soziale Netzwerke oder Chat-Dienste gemeinsame Standards für die Interoperabilität zwischen den Anbietern ermöglichen.

45 EuGH Urteil vom 13. Mai 2014 im Fall C-131/12, Google Spain SL und Google Inc. v. Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, EU:C:2014:317.

46 Es gibt vereinzelte Anzeichen, dass Verbraucher beschränkte Interoperabilität u.U. bevorzugen können (z. B. Apple-Produkte), siehe Zittrain (2009). Außerdem scheinen Unternehmen auf dem Markt bereits ihre Daten über ihre Plattformen kooperativ austauschen (z. B. Facebook Plug-in für Webseiten), siehe Swire & Lagos (2013). Zu den sich ändernden Business-Modellen siehe Pasquale (2015).

47 Der erste Vorschlag beruht auf Berners-Lee (2000).

Aus datentechnischer Sicht muss diskutiert werden, ob das Recht auf Datenportabilität positiv für die Verbraucher ist. Das Recht auf Datenportabilität könnte dazu führen, dass nach einmaligem illegalem Zugriff auf die Daten weiterer ständiger Zugriff möglich ist, da viel mehr Daten in automatisierter Weise zugänglich gemacht werden (Swire & Lagos, 2013). Daher muss ein Ausgleich zwischen dem Recht auf Datenportabilität und Datensicherheit gefunden werden.

Im deutschen Datenschutzrecht kann das Recht auf Datenportabilität i. S. d. Art. 20 DSGVO nur noch konkretisiert werden (Deutscher Bundestag, 2016). Jedenfalls muss sichergestellt werden, dass das Recht auf Datenportabilität effektiv ausgestaltet ist. In diesem Sinne sollte schuldrechtlich das Recht auf Datenportabilität als Kündigung des zugrundeliegenden Verbrauchervertrages zu verstehen sein. Damit können Verbraucher die kostenfreie Rückübertragung der Daten in einem gängigen maschinenlesbaren und interoperablen Format oder ihre Löschung verlangen. So können die Daten dann an andere Dienstleister übertragen werden, entweder vom Verbraucher selbst oder von einem Dienstleister zum anderen (Art. 20 Abs. 2 GSDVO). Unabhängig von den Kontroversen um die Effektivität des Rechts, ist dies zumindest für Verbraucher sinnvoll, die vom Wettbewerb auf dem Markt profitieren und ihre Daten auf andere Anbieter übertragen wollen.

Literatur

Angwin, J. & Parris, T. (2016). Facebook lets advertisers exclude users by race. ProPublica blog (28. Oktober 2016). Abgerufen am 21. Juni von URL https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.

Article 29 Data Protection Party (2017). Guidelines on the right to data portability. 16/EN WP Nr. 242 rev.01. Abgerufen am 14. Juni von URL http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

Barr, R. (2010). Transfer of learning between 2D and 3D sources during infancy: Informing theory and practice. Developmental Review, 30, 128-154.

Becker, M. (2017). Ein Recht auf datenerhebungsfreie Produkte. JuristenZeitung, 72 (4), 170-181.

Berners-Lee, T. (2000). Semantic web on XML 2000 conference (Dezember 2000), Washington DC.

Birkel, C., Guzy, N., Hummelsheim, D., Oberwittler, D. & Pritsch, J. (2014). Der Deutsche Viktimisierungssurvey 2012. Erste Ergebnisse zu Opfererfahrungen, Einstellungen gegenüber der Polizei und Kriminalitätsfurcht. In H.-J. Albrecht & U. Sieber (Hrsg.), Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht: Arbeitsberichte (S. 1-134). Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Birnstiel, A. & Eckel, P. (2016). Competition law and data. Wettbewerb in Recht und Praxis, 10, 1189-1195.

Bitkom (2015). Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa. Berlin: Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom).

BMELV (2007). Charta Verbrauchersouveränität in der digitalen Welt, Konferenz „Herausforderungen und Chancen in einer digitalisierten Welt: Beiträge der Verbraucherpolitik. Berlin: Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV).

BMWi (2015). Leitplanken Digitaler Souveränität. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

BMWi (2016). Grünbuch Digitale Plattformen. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

BMWI (2017a). G20 Digital Economy Ministerial Conference: G20 Digital Economy Ministerial Declaration – Shaping Digitalisation for an Interconnected World. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

BMWi (2017b). Weißbuch Digitale Plattformen des BMWi. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).

BMWi & BMJV (2015). Mehr Sicherheit, Souveränität und Selbstbestimmung in der digitalen Wirtschaft. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi) und Bundesministerium der Justiz und für Verbraucherschutz (BMJV).

Bojars, U., Passant, A., Breslin, J.G. & Decker, S. (2008). Social network and data portability using semantic web technologies. In Proceedings of the BIS 2008 Workshop on Social Aspects of the Web (Mai 2008), Innsbruck.

BSI (2016). Die Lage der IT-Sicherheit in Deutschland 2016. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

Buchner, B. (2006). Informationelle Selbstbestimmung im Privatrecht. Tübingen: Mohr Siebeck.

Bug, M., Kraus, M. & Walenda, B. (2015). Analoge und digitale Unsicherheiten: Neue Perspektive auf Kriminalitätsfurcht. DIW Wochenbericht, 12/2015, 280-287.

Bundeskriminalamt (2016). Cybercrime: Bundeslagebild 2015. Wiesbaden: Bundeskriminalamt.

Bundesregierung (2014). Digitale Agenda 2014-2017. Berlin: Bundesregierung.

Bundesregierung (2008). Verbraucherpolitischer Bericht der Bundesregierung 2008, Berlin: Bundesregierung.

Bundesregierung (2016). Verbraucherpolitischer Bericht der Bundesregierung 2016, Berlin: Bundesregierung.

Carstensen, T. (2015). Neue Anforderungen und Belastungen durch digitale und mobile Technologien. WSI Mitteilungen, 68, 187-193.

Christl, W. & Spiekermann, S. (2016). Networks of control, Facultas. Abgerufen am 16. November 2016 von URL http://crackedlabs.org/en/networksofcontrol.

De Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data. Gütersloh: Bertelsmann Stiftung.

Destatis (2016). Wirtschaftsrechnungen: Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien. In Statistisches Bundesamt (Hrsg.), Fachserie 15 Reihe 4 (S. 1-45). Wiesbaden: Statistisches Bundesamt.

Deutscher Bundestag (2016). Regulierung von Messengerdiensten: Datenportabilität und Interoperabilität. Wissenschaftliche Dienste Nr. WD 10 - 3000 - 060/16.

Döring, N. (2010). Sozialkontakte online: Identitäten, Beziehungen, Gemeinschaften. In W. Schweiger & K. Beck (Hrsg.), Handbuch Online-Kommunikation (S. 159-183). Wiesbaden: VS Verlag für Sozialwissenschaften.

Domurath, I. & Kosyra, L. (2016). Verbraucherdatenschutz im Internet der Dinge. Sachverständigenrat für Verbraucherfragen Working Paper Nr. 3. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV).

Ellis, Y., Daniels, B. & Jauregui, A. (2010). The effect of multitasking on the grade performance of business students. Research in Higher Education Journal, 8 (1), 1-11.

Europäische Kommission (2015). Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) Nr. 192final.

Feierabend, S., Plankenhorn, T. & Rathgeb, T. (2016). JIM 2016: Jugend, Information, (Multi-) Media. Stuttgart: Medienpädagogischer Forschungsverbund Südwest.

Ferrara, E., Varol, O., Davis, C., Menczer, F. & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59 (7), 96-104.

Friedewaldt, M., Lamla, J. & Roßnagel, A. (2017). Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden: Springer Fachmedien Wiesbaden GmbH.

Friedrichsen, M. & Bisa, P. (2016). Einführung – Analyse der digitalen Souveränität auf fünf Ebenen. In M. Friedrichsen & P.-J. Bisa (Hrsg.), Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft (S. 1-6). Wiesbaden: Springer VS.

Gasser, U. (2012). Interoperability in the digital ecosystem, GSR Discussion paper. Cambridge, MA: The Berkman Center for Internet & Society at Harvard University.

Gigerenzer, G. (2010). Digitale Risikokompetenz. Enquete-Kommission Internet und digitale Gesellschaft, Ausschussdrucksache Nr. 17(24)014-F.

Gigerenzer, G. (2013). Risiko: Wie man die richtigen Entscheidungen trifft. München: C. Bertelsmann.

Gigerenzer, G. (2017). Digital risk literacy: Technology needs users who can control it. Scientific American (25. Februar 2017). Abgerufen am 20. Juni 2016 von URL https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

Gigerenzer, G., Schlegel-Matthies, K. & Wagner, G.G. (2016). Digitale Welt und Gesundheit. eHealth und mHealth – Chancen und Risiken der Digitalisierung im Gesundheitsbereich. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen.

Golder, S.A. & Macy, M.W. (2014). Digital footprints: Opportunities and challenges for online social research. Annual Review of Sociology, 40, 129-152.

Helbing, T. (2015). Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, Kommunikation & Recht, 145 (3), 145-150.

Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van der Hofen, J., Zicari, R. V. & Zwitter, A. (2017). Will democracy survive big data and artificial intelligence? Scientific American (25. Februar 2017). Abgerufen am 20. Juni von URL https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

Hutt, W.H. (1940). The concept of consumers' sovereignty. The Economic Journal, 50 (197), 66-77.

Initiative D21 (2016). 2016 D21-Digital-Index: Jährliches Lagebild zur Digitalen Gesellschaft. Berlin: Initiative D21.

Jentzsch, N. (2016). State-of-the-art of the economics of Cyber-Security and Privacy. IPACSO - Innovation Framework for ICT Security Deliverable Nr. 4.1.

Jentzsch, N. (2017). Gutachten: Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds. In: Stiftung Datenschutz (Hrsg), Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen (Teil C – S. 1-41). Leipzig: Stiftung Datenschutz.

Junco, R. (2012). In-class multitasking and academic performance. Computers in Human Behavior, 28 (6), 2236-2243.

Junco, R. (2015). Student class standing, facebook use, and academic performance. Journal of Applied Developmental Psychology, 36, 18-29.

Karaboga, M., Masur, P., Matzner, T., Mothes, C., Nebel, M., Ochs, C., Schütz, P. & Simo Fhom, H. (2014). White Paper Selbstdatenschutz. In P. Zoche, R. Ammicht-Quinn, J. Lamla, A. Roßnagel, S. Trepte & M. Waidner (Hrsg.), Schriftenreihe Forum Privatheit und selbstbestimmtes Leben in der

digitalen Welt (S. 1-48). Creative Commons 4.0 International Lizenz.

Kardefelt-Winther, D. (2014). A conceptual and methodological critique of internet addiction research: Towards a model of compensatory internet use. Computers in Human Behavior, 31, 351-354.

Kominers, P. (2012). Interoperability case study internet of things (IoT). Berkman Center Research Publication Nr. 2012-10. Cambridge, MA: Berkman Center for Internet and Society at Harvard University.

Korczak, D. (2016). Marktcheck Kostenloser Auskunftsanspruch von Verbrauchern bei Auskunfteien: Abschlussbericht der GP Forschungsgruppe. Düsseldorf: Verbraucherzentrale Nordrhein-Westfalen.

Kucharski, A. (2016). Post-truth: Study epidemiology of fake news. Nature, 540 (7634), 525-525.

Kühl, E. & Breitegger, B. (2016). Der Angriff, der aus dem Kühlschrank kam, Zeit online (24. Oktober 2016). Abgerufen am 14. Juni von URL http://www.zeit.de/digital/internet/2016-10/ddos-attacke-dyn-internet-der-dinge-us-wahl.

Kultusministerkonferenz (2008). Ländergemeinsame inhaltliche Anforderungen für die Fachwissenschaften und Fachdidaktiken in der Lehrerbildung. Bonn: Sekretariat der Kultusministerkonferenz.

Kultusministerkonferenz (2016). Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt". Bonn: Sekretariat der Kultusministerkonferenz.

Loh, K.K. & Kanai, R. (2016). How has the Internet reshaped human cognition? The Neuroscientist, 22 (5), 506-520.

Maas, H. (2015). EU-Datenschutz-Grundverordnung: Datensouveränität in der digitalen Gesellschaft. Datenschutz und Datensicherheit-DuD, 39 (9), 579-580.

Mertz, M., Jannes, M., Schlomann, A., Manderscheid, E., Rietz, C. & Woopen, C. (2016). Digitale Selbstbestimmung. Köln: Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres).

Möchel, E. (2016). Machtvolle Rückkehr der DDoS-Attacken, ORF.at (4. Oktober 2016). Abgerufen am 14. Juni von URL http://fm4v3.orf.at/stories/1773571/.

Moll, R., Schulze, A., Rusch-Rodosthenous, M., Kunke, C. & Scheibel, L. (2017). Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle? Düsseldorf: Verbraucherzentrale NRW.

National Highway Traffic Safety Administration (2015). Distracted driving 2015. Washington, DC.

Ofiera, J. (2016). Ein Ad-Blocker-Verbot ist keine Lösung – Ausgediente Geschäftsmodelle nicht künstlich am Leben erhalten. Abgerufen am 27.02.2017 von URL https://www.piratenfraktion-nrw.de/tag/digitalisierung/.

Ophir, E., Nass, C. & Wagner, A. D. (2009). Cognitive control in media multitaskers. Proceedings of the National Academy of Sciences, 106 (37), 15583-15587.

Orange (2014). The future of digital trust: A European study on the nature of consumer trust, and personal data. Abgerufen am 14. Juni von URL https://www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf.

Palfrey, J. & Gasser, U. (2012). Interop: The promise and perils of highly interconnected systems. New York: Basic Books.

Palmetshofer, W., Semsrott, A. & Alberts, A. (2016). Der Wert persönlicher Daten: Ist Datenhandel der bessere Datenschutz? Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV).

Pasquale, F. (2015). The back box society – The secret algorithms that control money and information. Cambridge, MA: Harvard University Press.

Persky, J. (1993). Retrospectives: consumer sovereignty. The Journal of Economic Perspectives, 7 (1), 183-191.

Rau, H. (2016). Der Souverän – wir haben ihn längst zu Grabe getragen. In M. Friedrichsen & P.-J. Bisa (Hrsg.), Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft (S. 79-92). Wiesbaden: Springer VS.

Reisch, L., Büchel, D., Joost, G. & Zander-Hayat, H. (2015). Digitale Welt und Handel. Ver-braucher im personalisierten Online-Handel. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV).

Riekmann, J. & Kraus, M. (2015). Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe. DIW-Wochenbericht, 82 (12), 295-301.

Rifkin, J. (2014). Die Null-Grenzkosten-Gesellschaft: Das Internet der Dinge, kollaboratives Gemeingut und der Rückzug des Kapitalismus. Frankfurt am Main: Campus Verlag Rosen.

Roßnagel, A., Nebel, M. & Geminn, C. (2016). Entgeltliche Auskunftsansprüche zu Score-Werten und ihr Mehrwert für den Verbraucher. Düsseldorf: Verbraucherzentrale Nordrhein-Westfalen e.V.

Rotondi, V., Stanca, L. & Tomasuolo, M. (2017). Connecting alone: Smartphone use, quality of social interactions and well-being, DEMS Working Paper Series Nr. 357.

Schantz, P. (2016). Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. Neue Juristische Wochenschrift, 26, 1841-1847.

Schleusener, M. & Hosell, S. (2015). Personalisierte Preisdifferenzierung im Online-Handel, Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV).

Schwarzkopf, S. (2011). The political theology of consumer sovereignty: Towards an ontology of consumer society. Theory, Culture & Society, 28 (3), 106-129.

Schweitzer, H., Fetzer, T. & Peitz, M. (2016). Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen. ZEW Discussion Paper Series Nr. 16-042.

Spindler, G., Thorun, C. & Wittmann, J. (2016). Rechtsdurchsetzung im Verbraucherdatenschutz. Berlin: Friedrich-Ebert-Stiftung.

Spinney, L. (2017). How facebook, fake news and friends are warping your memory. Nature, 543 (7644), 168-170.

Stiftung Kind und Jugend (2017). Gemeinsame Pressemitteilung zur BLIKK-Studie. Abgerufen am 14. Juni von URL http://www.stiftung-kind-und-jugend.de/fileadmin/pdf/2017-05-29_PM_Blikk.pdf.

Süss, D. (2017, April). Medienpädagogik–Trends und Herausforderungen aus Sicht der Positiven Psychologie. In D. Süss & C. Trültzsch-Wijnen (Hrsg.), Medienpädagogik (S. 39-52). Baden-Baden: Nomos Verlagsgesellschaft..

SVRV (2015). Verbraucherpolitik in der digitalen Welt: Standpunkte des Sachverständigenrates für Verbraucherfragen. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV).

SVRV (2016). Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV).

Swartz, A. (2013). Aaron Swartz's a programmable web: An unfinished work. In J. Hendler & Y. Ding (Hrsg.), Synthesis lectures on the semantic web: Theory and Technology (S. 1-54). San Rafael, CA: Morgan & Claypool.

Swire, P. & Lagos, Y. (2013). Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique. Maryland Law Review, 72 (2), 335-380.

Thomée, S. (2012). ICT use and mental health in young adults. Effects of computer and mobile phone use on stress, sleep disturbances, and symptoms of depression. Dissertation thesis. University of Gothenburg.

Underwood, M.K. & Ehrenreich, S. E. (2017). The power and pain of adolescents' digital communication: Cyber victimization and the perils of lurking. American Psychologist, 72, 144-58.

van der Schuur, W. A., Baumgartner, S. E., Sumter, S. R. & Valkenburg, P. M. (2015). The consequences of media multitasking for youth: A review. Computers in Human Behavior, 53, 204-215.

Weis, R., Lucks, S. & Grassmuck, V. (2016). Technologien für und wider Digitale Souveränität. Veröffentlichungen des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV).

Wineburg, S., McGrew, S., Breakstone, J. & Ortega, T. (2016). Evaluating information: The cornerstone of civic online reasoning: Executive Summary. Stanford History Education Group.

Wood, E., Zivcakova, L., Gentile, P., Archer, K., De Pasquale, D. & Nosko, A. (2012). Examining the impact of off-task multi-tasking with technology on real-time classroom learning. Computers & Education, 58 (1), 365-374.

World Economic Forum (2014). Rethinking personal data: Trust and context in user-centred data ecosystems. Geneva: World Economic Forum.

Young, K. & Abreu, C. (2011). Internet addiction. A handbook and guide to evaluation and treatment. Hoboken, NJ: John Wiley & Sons.

Zander-Hayat, H., Domurath, I. & Gross, C. (2016a). Personalisierte Preise. Sachverständigenrat für Verbraucherfragen Working Paper Nr. 2. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV).

Zander-Hayat, H., Reisch, L. A. & Steffen, C. (2016b). Personalisierte Preise: Eine verbraucherpolitische Einordnung. Verbraucher und Recht, 31 (11), 403-409.

Zingales, N. (2015). Of coffee pods, videogames, and missed interoperability: Reflections for EU governance of the internet of things. TILEC Discussion Paper DP Nr. 2015-026.

Zittrain, J. (2008). The future of the internet – and how to stop it. London: Allen Lane.

Notizen

Sachverständigenrat für Verbraucherfragen

Der Sachverständigenrat für Verbraucherfragen ist ein Beratungsgremium des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV). Er wurde im November 2014 vom Bundesminister der Justiz und für Verbraucherschutz, Heiko Maas, eingerichtet. Der Sachverständigenrat für Verbraucherfragen soll auf der Basis wissenschaftlicher Erkenntnisse und unter Berücksichtigung der Erfahrungen aus der Praxis das Bundesministerium der Justiz und für Verbraucherschutz bei der Gestaltung der Verbraucherpolitik unterstützen.

Der Sachverständigenrat ist unabhängig und hat seinen Sitz in Berlin.

Vorsitzende des Sachverständigenrats ist Prof. Dr. Lucia Reisch.

Berlin, Juni 2017
ISSN 2510-0084

Herausgeber:
Sachverständigenrat für Verbraucherfragen
beim Bundesministerium der Justiz und für Verbraucherschutz
Mohrenstraße 37
10117 Berlin
Telefon: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525
E-Mail: info@svr-verbraucherfragen.de
Internet: www.svr-verbraucherfragen.de
Diese Veröffentlichung ist im Internet abrufbar.