SVRV Sachverständigenrat für Verbraucherfragen

Digital Sovereignty

Report by the Advisory Council for Consumer Affairs

June 2017

Berlin, June 2017
ISSN 2510-0084

Published by:
Advisory Council for Consumer Affairs
at the Federal Ministry of Justice and Consumer Protection
Mohrenstrasse 37
10117 Berlin

Tel.: +49 (0) 30 18 580 0
Fax: +49 (0) 30 18 580 9525
eMail: info@svr-verbraucherfragen.de
Website: www.svr-verbraucherfragen.de

This publication is available on the internet.

Members of the Advisory Council for Consumer Affairs

Prof. Dr. Lucia Reisch (Chairperson)
Professor for Intercultural Consumer Research and European Consumer Policy at Copenhagen Business School

Dr. Daniela Büchel (Vice Chairperson)
Member of the Management Board of REWE for the Areas of Human Resources and Sustainability

Prof. Dr. Gerd Gigerenzer
Director of the Center for "Adaptive Behavior and Cognition" and the Harding Center for Risk Literacy at the Max Planck Institute for Human Development in Berlin

Helga Zander-Hayat
Head of the Area of Market and Law at the North Rhine-Westphalia Consumer Organisation

Prof. Dr. Gesche Joost
Professor in the Department of Design Research at the Berlin University of the Arts and Internet Ambassador of the German Federal Government in the EU's "Digital Champions" Group

Prof. Dr. Hans-Wolfgang Micklitz
Professor of Economic Law at the European University Institute in Florence

Prof. Dr. Andreas Oehler
Professor of Finance at the University of Bamberg and Director of the Household Finance and Financial Literacy Research Center

Prof. Dr. Kirsten Schlegel-Matthies
Professor of Home Economics at the University of Paderborn

Prof. Dr. Gert G. Wagner
Professor of Empirical Economic Research and Economic Policy at the Technical University of Berlin, Executive Board Member of the Germany Institute for Economic Research and Max Planck Fellow at the Max Planck Institute for Human Development

Advisory Council Staff

Head of Secretariat:
Thomas Fischer, M.A.

Academic staff of the Secretariat:
Dr. Irina Domurath, Dr. Christian Groß

Contents

Foreword

Since its inception, the Advisory Council has approached the core topic of "consumers in the digital world" from various different angles. In its policy paper Verbraucherpolitik in der digitalen Welt: Standpunkte des Sachverständigenrates für Verbraucherfragen ["Consumer Policy in the Digital World: Position Paper by the Advisory Council for Consumer Affairs"] (SVRV, 2015), the Advisory Council advocates making the benefits of digitalisation available to as many consumers as possible by designing privacy-friendly technology, strengthening the digital literacy of consumers and introducing prudent regulations. The Advisory Council is in no way alone in this respect. Work is also being done within the sphere of international consumer policy on regulations for the digital world that are designed to serve the common good – one example being the efforts undertaken during the negotiations of the G20 Digital Ministers in 2017 (BMWi, 2017a).

Picking up on these core demands, the present report builds on several previous studies conducted by the Advisory Council in the fields of consumer empowerment and regulation, and goes on to discuss various technological aspects of digitalisation. In the area of consumer-friendly technology, the Advisory Council has set a clear agenda with studies entitled Der Wert der persönlichen Daten ["The value of personal data"]3 and Technologien für und wider Digitale Souveränität ["Technologies beneficial or detrimental to digital sovereignty"].4 In its policy paper Digitale Welt und Gesundheit. eHealth und mHealth – Chancen und Risiken der Digitalisierung im Gesundheitsbereich ["The digital world and health: e-health and m-health – opportunities and risks of digitalisation in the health sector"], the Advisory Council emphasises the point that if we do not strengthen digital literacy, we will squander the opportunities presented by digitalisation. The Advisory Council has already addressed questions of regulation in its earlier report entitled Verbraucherrecht 2.0 ["Consumer Rights 2.0"] as well as in its working paper entitled Personalisierte Preise ["Personalised Pricing"]. There, the Advisory Council discusses consent requirements, disclosure obligations on the part of providers, and the right to non-discriminatory access to services.

3 Retrieved on 20 June 2017 from URL http://www.svr-verbraucherfragen.de/wp-content/uploads/Open_Knowledge_Foundation_Studie.pdf.

4 Retrieved on 20 June 2017 from URL http://www.svr-verbraucherfragen.de/wp-content/uploads/Weis_Lucks_Grassmuck_Studie_.pdf.

Our special thanks go to Gesche Jost for coordinating the compilation of this report. Others who contributed to its preparation include: Daniela Büchel, Gerd Gigerenzer, Hans Micklitz, Lucia A. Reisch, Kirsten Schlegel-Matthies, Gert G. Wagner and Helga Zander-Hayat.

The Advisory Council would like to thank all the staff members of the Secretariat for their valuable support in compiling the report. We would like to extend special thanks to the Advisory Council's academic staff: Christian Groß, Irina Domurath and Mathias Bug.

In addition, the Advisory Council would like to thank Rüdiger Weis, Stefan Lucks and Volker Grassmuck (authors of the study Technologie für und wider Digitale Souveränität) as well as Walter Palmetshofer, Arne Semsrott and Anna Alberts (authors of the study Der Wert persönlicher Daten: Ist Datenhandel der bessere Datenschutz?) for contributing their expertise.

In conclusion, we would like to point out that the language in this text should be understood as being gender-neutral. In the interests of better readability, we have refrained from always specifying both genders.

Berlin, June 2017

For the Advisory Council for Consumer Affairs

Lucia Reisch
Chair of the SVRV

Gesche Joost
Member of the SVRV

Executive summary

With this report on Digital Sovereignty, the Advisory Council for Consumer Affairs is contributing to an ongoing debate which is redefining the concept of digital sovereignty from the perspective of consumer policy.

We understand the concept of digital sovereignty as meaning that consumers are empowered and autonomous to act in various roles in the digital world – namely as market participants, as consumer-citizens of society, and as "prosumers" within networks. The concept furthermore refers to the rights and obligations of citizens within the regulatory framework, emphasising the conditions which must be in place so that individuals are able to use digital media and services in an independent, proficient and responsible manner, thereby empowering them to actively participate as citizens of a digital society.

We identify four guiding principles in connection with digital sovereignty: freedom of choice, self-determination, self-control and security. In order to make these principles work in reality, we propose the following measures which need to be implemented in three different areas: consumer-friendly technology, digital literacy and regulation.

Technology

- **Creating a consumer-centric data portal:** The Advisory Council recommends the development of a consumer-centric data portal (dashboard) in order to make individual data sovereignty a viable reality.

- **Enforcing the principles of privacy by design and privacy by default:** The Advisory Council reiterates the demand for user-friendly, data-minimising and security-oriented default settings for communication systems (privacy/security by design and privacy/security by default as the guiding principles). State-funded projects must be aligned with these principles.

- **Improving security in the Internet of Things:** In the face of steadily worsening security problems in the Internet of Things segment, the Advisory Council recommends evaluating how we can ensure that products and services which appear on the market are mandatorily and continually protected throughout their entire life cycle by security updates – echoing the procedures in the healthcare field. Technological standards need to be developed in this area, while source codes (similar to recipes in the food sector) should be deposited into escrow.

- **Expanding the range of data-minimising products:** The Advisory Council recommends assessing whether it would be possible to grant consumers a right to use data-minimising digital products, meaning that there would always be a data-minimising version for consumers to choose.

Digital literacy

- **Establishing a qualification pact for "Digital Literacy in Teacher Training":** The Advisory Council recommends that a qualification pact be established for digital literacy in teacher training (similar to the Quality Pact for Teaching or the National Initiative to Improve Teacher Training).

- **Promoting services that improve digital literacy:** The Advisory Council recommends that both existing and future (institutional) services designed to improve digital literacy be sustainably funded and structurally integrated. At the same time, there should be a systematic expansion of services with a gatekeeping function, services for multipliers and services for consumers.

- **Developing measures to improve self-control in using digital media and services:** The Advisory Council recommends that the education ministries develop measures to improve self-control in the use of digital media and services.

- **Studying the effects of digitalisation on cognition, emotion and social life:** The Advisory Council recommends the targeted funding of interdisciplinary research into the effects of digitalisation on cognition, emotion and the social life of consumers. This applies to both "digital natives" and "digital migrants".

Regulation

- **Implementing T&C and privacy statements as one-pagers:** The Advisory Council reiterates its recommendation that before contracts are concluded, companies must inform consumers via one-pagers (500 words) about the relevant privacy requirements and about the terms and conditions. The Advisory Council recommends developing these one-pagers in a pilot project organised by the Federal Ministry of Justice and Consumer Protection (BMJV) and involving the relevant stakeholders.

- **Making algorithms transparent and open to scrutiny:** The Advisory Council reiterates its recommendation that legal requirements must be put in place to ensure that (a) algorithms take account of the requirements of consumer law, data protection law, anti-discrimination law and digital security, and that in cases where consumers are directly exposed to algorithms, the underlying parameters need to be made transparent, and that (b) based on standardised disclosure requirements, algorithms should be disclosed to a group of experts who carry out spot checks to see whether they are legally sound. The Advisory Council recommends that legal standards are developed and that source codes are deposited into escrow.

- **Improving the right of access to free-of-charge information:** The Advisory Council recommends that the right of access to information (section 34 of the Federal Data Protection Act) be guaranteed without limitations. It also recommends that companies be obligated to inform consumers about their right to free-of-charge information and about the option to rectify inaccurate data – in a clear, transparent and easily identifiable way when the products are offered (i.e. rectification, erasure and blocking).

- **Continuing to develop the minimum standards for interoperability:** The Advisory Council recommends developing minimum standards that ensure compatibility between digital services, thereby allowing for communication between user accounts independently of the service provider (i.e. interoperability – as already established in the mobile telecommunications sector).

- **Defining the right to data portability in more concrete terms:** The Advisory Council underscores its recommendation that the right to data portability be understood in terms of a right of termination. It also recommends establishing a framework for switching to different service providers (as is already established for digital payment transactions).

1. Current status of the debate

Digital products and services permeate the everyday lives of today's consumers and are presenting new challenges for consumer policy. Internet-enabled mobile devices are becoming ever more popular, particularly among young people: in a survey, virtually everyone aged between 12 and 19 reported using one (Feierabend et al., 2016). Usage is also high throughout the population as a whole, with around two thirds of the population in Germany currently using a mobile device (Initiative D21, 2016). Even among "silver surfers" (i.e. users over 60), around half of the under-70s and one quarter of the over-70s regularly access the internet from their mobile devices (Initiative D21, 2016; Destatis, 2016).

Clearly perceptible in this process is an increasing crisis of trust among consumers in online service providers: not only in terms of the utilisation of their data (trade in data, big data) and the security of their data (hacking, phishing) but also where the reliability of online content is concerned (targeted disinformation, "fake news"). For example, a study by Orange (2014) found that almost 80 percent of consumers distrusted online service providers and felt that the utilisation of their data was lacking in transparency. Nonetheless, the overwhelming majority of consumers was still prepared to share their personal data if, in return, they could make use of services (see Destatis, 2016 on the utilisation of data for advertising purposes). This points to asymmetric power relationships between companies and individuals, where the former have access to vast amounts of individual data, while the latter have no knowledge or control in this regard (World Economic Forum, 2014).

Utilisation of data: One possible reason for the above-mentioned crisis of trust is the growing number of online services whose business model involves the collection and processing of large volumes of data (see Christel & Spiekerman, 2016; Karaboga et al., 2014; on the distribution of utilisation in Germany: Destatis, 2016). This leads to a growing "digital footprint" which provides detailed information about an individual's consumer behaviour, social environment and preferences (Golder & Macy, 2014) or allows such predictions to be made via big data. One consequence is that information on the payment behaviour or payment willingness of consumers can be extrapolated, thereby allowing providers to implement personalised pricing (Schleusener & Hosell 2015; Zander-Hayat et al., 2016a; Zander-Hayat et al., 2016b). Given the nature of these developments, established online platforms such as Google, Facebook, Amazon and YouTube take on particular significance due to the considerable market power they have accumulated within the online segment. In the minds of consumers, alternative options are either non-existent or insufficiently attractive. Another fact of everyday life is that many consumers feel group pressure to network on these platforms and to engage in consumer behaviour there. While it would be technically possible to change service providers, it almost never happens in practice because interoperability between different providers is far from ideal, making it difficult and consumer-unfriendly to migrate user data to a new provider.

Security of data: From the consumer viewpoint, there is also a need for action in terms of creating an effective security architecture within the online marketplace. This is underlined by the fact that increasing numbers of people now have first-hand experience of online crime such as identity theft, the spread of computer viruses, and the fraudulent misuse of online banking data (Birkel et al., 2014; Rieckmann & Kraus, 2015; Bug et al., 2015, Bundeskriminalamt, 2016). Consumer trust in the security of devices has been further shaken by the fact that the Internet of Things – intelligent everyday appliances connected to the internet – has been the subject of recent denial-of-service attacks[3] (Möche, 2016; Weis et al., 2016).

Online content: The phenomenon of targeted disinformation appearing on social media and ideologically motivated websites is on the rise (the key phrase being "fake news"; see Kucharski, 2016; Spinney, 2017). As a result, each individual user must now have a basic ability to assess the credibility of any given source or content. Furthermore, nearly one in five German teenagers has personally experienced online harassment and hate speech in social media. This was

3 In a (distributed) denial-of-service attack, large volumes of queries are transmitted simultaneously from numerous different devices to one or more servers, thereby overloading them. These types of attacks are not rare; server providers and specialised companies are able to intercept a certain portion of them. But the stronger and longer the attacks become, the more difficult it becomes to block them (Kühl & Breitegger, 2016).

the result of a 2015 study conducted by YouGov and commissioned by Vodaphone.[4] Around one third of the respondents said that a friend or family member had been subjected to harassment on the internet. In light of these and other incidents, there has been a significant overall drop in the perceived level of security within this quasi-public space.

It is therefore unsurprising that one of the main concerns of digital consumer policy is to regain and strengthen consumer trust on all these levels. The best way to create and cultivate a legitimate sense of trust in the online environment is by empowering consumers to act in sovereign ways within the digital world. In Germany, the political discussion regarding the digital sovereignty of consumers has been in progress for at least ten years: it can be traced back to the Charta Verbrauchersouverenität in der digitalen Welt ["Charter of Consumer Sovereignty in the Digital World"] (BMELV, 2007) which was presented on World Consumer Day in 2007 in the midst of an exponential increase in all forms of digital business relationships. In that document, the authors applied the term "consumer sovereignty" to the digital context for the first time and drew up guidelines for a consumer-friendly structuring of the digital world. Reference was also made to the fundamental right to "informational self-determination".

Building on that paper issued by the BMELV, recommendations for strengthening digital sovereignty were gradually refined as the consumer policy discourse evolved. The Federal Government's Consumer Policy Report of 2008 took up the central arguments of the paper and described consumer literacy as a basic prerequisite for responsible decision-making in the digital world (Bundesregierung, 2008). Likewise, the Federal Government's "Digital Agenda 2014-2017" deemed the strengthening of media literacy among consumers to be a key consumer protection measure in the digital world – alongside market watchdogs, the right to file class actions, and default settings that protect the private sphere in digital applications (privacy by design and privacy by default) (Bundesregierung, 2014). The Federal Ministry for Economic Affairs and Energy adopted a similar position, deeming the acquisition of key skills in IT security and data protection to be preconditions for digital sovereignty (BMWi, 2015). In addition to the issues of identity security and protection against identity theft, the Federal Government's 2016 Consumer Policy Report identified the main goals of consumer policy as being to "strengthen self-determination and to guarantee freedom of choice, transparency, comprehensive and understandable consumer information, and security on the internet" (Bundesregierung, 2016).

In the present report, we build on this understanding of (individual) digital sovereignty and distinguish it from the digital sovereignty of nation states.[5] The concept of "data sovereignty"[6] – another central idea in the consumer policy discourse – is integrated within our approach as being an important aspect of digital sovereignty: namely the freedom enjoyed by consumers to make choices about the collection, processing and utilisation of their personal data. For instance, it should be for consumers themselves to decide whether their personal data can be donated for charitable purposes or sold, or whether their data should not even be collected in the first place. Taking this line of thought, digital sovereignty and data minimisation are not mutually exclusive opposites as

4 Retrieved on 14 June 2017 from URL http://docs.dpaq.de/9635-ppt_for_vodafone__cyberbullying_-_germany__060_9_9_15.pdf.

5 In the course of the debate over the disclosures by Edward Snowden, the term "digital sovereignty" was often used in the context of the nation-state's sovereignty over digital infrastructure (Friedrichsen & Bisa, 2016). After it became known that large-scale surveillance activities were being carried out by the U.S. intelligence services in particular, there were demands for the digital sovereignty of European states and their citizens to be strengthened, for example by installing independent digital infrastructures or by promoting national capacities for hardware production (BMWi, 2015). The Bitkom trade association also emphasises the nation-state aspect of digital sovereignty (Bitkom, 2015): the goal of digital sovereignty is described as being to create "independence from specific economic areas, states and companies in acquiring and using digital technologies and platforms". More as an afterthought to these business-oriented observations, Bitkom considers one aspect of digital sovereignty to be that consumers (in addition to companies and government administrations) use "digital technologies and solutions in a secure, independent and self-determined manner".

6 Heiko Maas (Maas, 2015) regards consent to the collection and processing of personal data as the key to data sovereignty and criticises the current situation where consent is often a meaningless ritual due to excessively long T&Cs and where self-determination is nothing more than an illusion. The Green Paper Digital Platforms – which is described as being based on a consultation process with industry, academia and society – uses the aforementioned "data sovereignty" term as a central motif. But no detailed explanation is provided, nor is there any attempt to differentiate the term from the concept of digital sovereignty. However, the paper does include a consumer policy component: for example, it emphasises the importance of safeguarding the ability of consumers to handle their data in a sovereign manner, including the power to decide who should be in possession of such data (BMWi, 2016). Building on that document, the BMWi's White Paper Digital Platforms approaches the topic within the context of the General Data Protection Regulation and examines data sovereignty in parallel with the issue of data portability, but without exploring the underlying concepts in greater detail (BMWi, 2017b). The Charter of Digital Fundamental Rights of the European Union (retrieved on 14 June from URL https://digitalcharta.eu/) refers to "data sovereignty" and takes it to mean inter alia the right to determine how one's personal data are used, as well as the requirement to give one's consent to the collection and use of personal data. It also mentions the challenges that digitalisation presents to the educational system; however, digital education per se is understood as being a right that enables people to live in the digital world in a self-determined manner.

is sometimes assumed (e.g. BMWi, 2015). Quite the contrary: it should be possible for data minimisation to be an aspect of digital sovereignty, one that is determined by consumers themselves.

We therefore understand the concept of digital sovereignty as meaning that consumers are empowered and autonomous to act in various roles in the digital world – namely as market participants, as consumer-citizens of society, and as "prosumers" within networks. The concept furthermore refers to the rights and obligations of citizens within the regulatory framework, emphasising the conditions which must be in place so that individuals are able to use digital media and services in an independent, proficient and responsible manner, thereby empowering them to actively participate in a digital society. Echoing the discourse on consumer sovereignty in the digital world (BMELV, 2007; Bundesregierung, 2016) as well as the paper by Mertz et al. (2016), we identify four guiding principles in connection with digital sovereignty: freedom of choice, self-determination, self-control and security. We suggest that these can be implemented via consumer-friendly technology, digital literacy on the part of consumers, and regulation.

With the present report, the Advisory Council for Consumer Affairs is contributing to an ongoing debate which is redefining the concept of digital sovereignty from the perspective of consumer policy. Based on our appraisal of the current situation, we outline recommendations for concrete action and address the different actors responsible for the ensuing implementation. The report is structured as follows: in Chapter 2, we identify four guiding principles of digital sovereignty (freedom of choice, self-determination, self-control and security) and argue that digital sovereignty should be encouraged by means of technology, digital literacy and consumer-friendly regulation (the "digital sovereignty triangle"). In Chapters 3 to 5, we provide brief descriptions of specific thematic issues in the each of the three fields of action, coupled with recommendations for action in consumer policy.

2. Conceptual framework: guiding principles and fields of action

2.1. Four guiding principles: freedom of choice, self-determination, self-control and security

Our understanding of digital sovereignty is based on the concept of consumer sovereignty (e.g. Hutt, 1940; Persky, 1993; Schwarzkopf, 2011). The concept includes both an empirical/descriptive level ("How sovereign are consumers?"; "What other factors interact with the sovereignty of consumers?") as well as a prescriptive/normative level ("How sovereign do consumers need to be?"; "What steps must be taken to ensure that consumers are empowered to act in sovereign ways?") and describes the relationship that exists – or should exist – between consumers and suppliers in the marketplace (Schwarzkopf, 2011).

The descriptive/empirical approach is taken by Mertz et al. (2016) in their article Digitale Selbstbestimmung ["Digital self-determination"]. In that article, they describe the aspects that are related to digital self-determination (identified as: digital literacy, awareness, values, choice, voluntariness, decision-making and action) and the factors that play a fundamental role in shaping digital self-determination (identified as: technical, socio-cultural and personal factors). Digital sovereignty is defined here as the "concrete development of a human personality in terms of being able to implement one's own strategies and decisions, where this involves a conscious use of digital media or is (co-)dependent upon the existence or functionality of digital media" (Mertz et al., 2016). The authors also draw numerous parallels between the concepts of digital self-determination and informational self-determination (Mertz et al., 2016).

In the present report, we contribute to the debate on the prescriptive/normative level and enquire as to which specific underlying conditions are required in order to ensure that consumers can act in self-determined ways in a world characterised by increasing digital interconnectivity (see Rau, 2016).

Drawing on the report by Mertz et al. (2016) and the political discourse on consumer sovereignty in the digital world (BMELV, 2007; Bundesregierung, 2016), we identify four guiding principles related to digital sovereignty: freedom of choice, self-determination, self-control and security.

Freedom of choice is understood in a broad sense as encompassing aspects of positive freedom ("freedom to do something") as well as negative freedom ("freedom to not do something"). According to this principle, consumers should be at liberty to decide whether to do something or whether to refrain from doing it (Mertz et al., 2016). Applied to the context of consumers in the digital world, this could for example mean that when buying an app, users are always given the choice between a free version which requires them to disclose their user data and a paid version which does not require them to disclose their data (Weis et al., 2016). Freedom of choice can also take the form of consumers not having to pay large transaction fees in order to switch providers. This helps to prevent the kind of lock-in effects which can occur when data portability is inadequate – the result of "data silos" and an absence of standards to ensure genuine interoperability (BMWi & BMJV, 2015). Consumers have particularly effective freedom of choice when they become the "active managers" of their own data: they can then reach independent decisions about whether to disclose, transfer, delete, donate or trade their data – insofar as there is no conflict with the legally enshrined interests of other stakeholders (see Palmetshofer et al., 2016). Freedom of choice also includes deciding whether or not third parties should be allowed to have access to one's personal data.

Self-determination when interacting with digital media means that users of hardware and software retain control over important decisions. It follows that consumers should never be the subject of automated decisions based on algorithms in cases where those decisions can have a significant impact on their lives. For example, if an automated and intransparent scoring system is used to decide whether credit should be awarded, consumers can encounter major problems if the relevant data and the algorithmic logic are not open to scrutiny since they would have no basis for exercising their right to object. These developments grow increasingly ominous as scoring methods are used on an ever broader scale for integrating different

types of data (Weis et al., 2016). Limiting the collection and use of personal data to a specific purpose is thus an important issue, as is the option of storing and analysing data in anonymous form. The principle of self-determination also includes consumers being able to evaluate the risk of manipulation (Mertz et al., 2016) which can result from activities such as the deployment of social bots[7] or the spreading of targeted disinformation ("fake news"). Apart from introducing the appropriate technological and regulatory safeguards, it is also essential to ensure that basic digital skills and data literacy are in place.

Self-control means that users are capable of setting their own limits on how they use digital services and can assess the consequences of their own behaviour. Confronted with thousands of different apps, the rise of the Internet of Things, and the possibility of being permanently online, it is increasingly important for people to have control over their own lives – rather than being controlled by (or even addicted to) the digital world. Self-control also means not having one's concentration interrupted by using a mobile phone while driving or having to deal with a constant stream of incoming mails (Helbing et al., 2017). Even more serious than potential lapses in concentration are the documented cases of people becoming dependent on digital media – otherwise known as "internet addiction".[8] For some people, this dependence on digital media can lead to elevated levels of "technostress" (Gigerenzer, 2010). Thus our understanding of digital sovereignty is not simply about creating the preconditions for sovereign behaviour within the digital world – it is also about individuals being required to exhibit sovereign behaviour in their interactions with the digital world in the sense of having the ability to control their use of digital services or devices such as smartphones, rather than having their behaviour controlled or significantly influenced.

Security means ensuring that consumer data and digital infrastructures are protected by the state, by corporations and by consumers themselves. To this end, there is a need for infrastructures which enable the secure acquisition, storage and controlled onward transmission of data. The rising number of cyber attacks on private computers and the numerous cases of customer data being stolen from international corporations underline the major importance of this issue for consumer policy. On this front, technical presets that comply with "privacy by design" and "privacy by default" principles can help to provide consumers with a secure and manageable basis for their everyday activities in the digital world. Meanwhile, the availability of easy-to-use encryption technologies and regular security updates are key factors in enhancing the security of consumers online. The task of raising public awareness about the main issues in online security must be tackled by an educational approach that spans different age groups and institutions.

2.2. Three fields of action: technology, digital literacy and regulation

Picking up on the Advisory Council's preliminary work mentioned at the outset of this report, we suggest that the described guiding principles for digital sovereignty should be implemented by consumer-friendly *technology*, by *digital literacy*, and by setting ground rules for the digital world via *regulation* that serves the common good. Digital sovereignty can thus be described from three different perspectives: one with a focus on the requisite technological framework for data-intensive products and services; one with a focus on how to teach the necessary skills and capabilities for dealing with online information, sources and data; and one with a focus on regulating the use of personal data and on strengthening consumer rights. Taken together, we refer to these three fields as the "digital sovereignty triangle".

In this context, we understand the umbrella term *technology* as specifically referring to technological enablers, i.e. the functionalities, principles and applications that enable sovereign behaviour in the digital world – or prevent it when they are missing. This includes aspects such as user-centric data management, data minimisation principles, and the use of encryption technologies and security updates.

7 Social bots are computer programmes capable of posting automatic answers in social media (Ferrara et al., 2016).

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

Digital literacy covers aspects such as how to deal with information and possible disinformation ("fake news"), how to interact with digital communications media, how to use digital tools, the ability to manage data and – related to this – a grasp of the current product and conceptual landscape, plus a willingness to engage in lifelong learning. By strengthening digital literacy skills, consumers are furthermore empowered to use digital media with self-control – an approach that can encompass anything from restricting oneself to moderate usage, to the self-determined decision to avoid using digital media altogether.

Regulation covers the rights and obligations of the individual consumer as well as the rights and obligations of corporate and government entities. The rights and obligations of the individual consumer include the right to deletion of data and the right to data portability, as well as the obligation to install security updates on Internet of Things devices. The rights and obligations of corporate and government entities particularly include transparency and purpose limitation in the collection and utilisation of data. They also include the obligation to make algorithms transparent and open to scrutiny – for example via algorithm auditing of the kind already performed in connection with credit scoring systems.

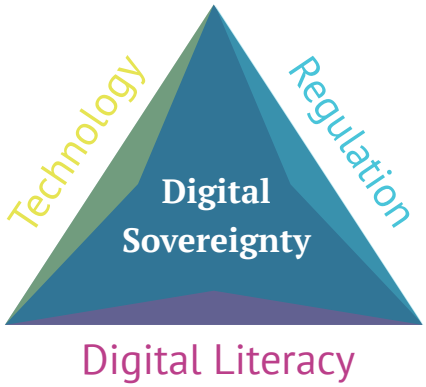


Figure 1: The digital sovereignty triangle:
Technology, digital literacy and regulation (our own model)

The model is designed to illustrate the *interdependencies* between the different fields of action for consumer policy. It shows that progress must be made in all three fields in order to make digital sovereignty a viable option for consumers. Consumers who recognise the value of their own data and who wish to exercise their rights on the internet are unable to act in sovereign ways if the technological landscape stops them from doing so – either because they are prevented from transferring their data to other service providers or because they have no choice in how their data are utilised. Meanwhile, the regulation of data markets will only work if the proper technological steps are taken and consumers are able to actively exercise their rights. Expanding on the concept of digital self-determination as formulated by Mertz et al. (2016), we therefore emphasise the ways in which the individual factors that constitute digital sovereignty interact and strengthen (or weaken) one another.

In similar fashion to the concept outlined here, De Mooy (2017) defines three areas that interact with one another in contributing towards the overall goal of enabling data sovereignty for the individual. According to De Mooy, the prerequisites for greater data sovereignty are education, data portability, industry self-regulation and state-regulated assessments. But our concept attaches broader objectives to the term of digital sovereignty. Likewise the fields of action are broader in scope.

In our understanding, digital sovereignty always emerges from a balance between technology, digital literacy and regulation – without prioritising any one of these factors and in the full knowledge that all three components can address both public and private entities as well as individuals. In the following section, we present our recommendations in these three fields for strengthening the digital sovereignty of consumers.

Technology

3. Technology

The following chapter covers some of the main technological aspects relevant to the digital sovereignty of consumers. These include data protection and data utilisation – as well as security aspects which are becoming increasingly significant in an ever more interconnected world.

3.1. Creating a consumer-centric data portal

The Advisory Council recommends the development of a *consumer-centric data portal (dashboard)* in order to make individual data sovereignty a viable reality.

The Advisory Council recommends the development of a consumer-centric data portal (dashboard) in order to make individual data sovereignty a viable reality. The dashboard would provide consumers with transparency regarding the utilisation (in terms of volume and content) of their personal data by the various providers on the internet. Furthermore, it would give consumers a centralised location from which they could manage their access rights and delete or edit their personal data.

The use of such a dashboard would need to be underpinned by a single enforceable law. In practice, a data portal of this type could be implemented by the government and corporations by means of a jointly funded initiative.

When developing a consumer-centric data portal, the main focus should be on providing transparency in the areas of data processing, data market decentralisation and the use of technological standards such as MyData[9] (see Jentzsch, 2017). MyData has formulated a set of rights that should apply to any interface gathering all the stored personal and customisable data that each individual consumer would be able to access. These are: the right to know which personal information is being held; the right to view the actual content of the personal data; the right to be able to rectify incorrect data; the right to check who has access to the personal data and why; the right to obtain personal data and use them freely; the right to share personal data with third parties or to sell the data; the right to delete personal data (Palmetshofer, Semsrott & Alberts, 2016). Similar approaches include vendor relationship management (VRM) and the Hub-of-All-Things (HAT) approach (Palmetshofer et al., 2016).

It is important to emphasise the core idea behind the creation of a consumer-centric data portal – namely, to empower consumers in taking control of their own data flow. By contrast, the possibility for consumers to trade their own data should not be a major focus in developing the data portal. This should merely be viewed as a potential scenario for consumers. In this regard, the Advisory Council notes that attempting to monetise data is not generally a worthwhile activity for consumers at present, and that data trading may in fact only benefit consumers with advanced levels of data literacy. Furthermore, the ethical aspects of online trading in personal data (e.g. body data) have not yet been adequately discussed. It should also be noted that it is currently difficult for consumers to determine a fair price for their data (SVRV, 2016). This means that when using online services, consumers often enter into commercial relationships without being able to estimate the value that can be created from the data they provide or the data they generate by using the service. Factors which influence the sensitivity of consumers towards the utilisation of their personal data include, on the one hand, easily measurable variables such as data type, service provider, device used, type of data collection and data utilisation, and on the other hand, subjective variables such as trust in the service provider and the resulting benefit – whether real or perceived – to the consumers themselves (World Economic Forum 2014). Cultural factors also play a role here: consumers in Scandinavian and Baltic countries appear to be less sensitive about their data than consumers in Germany, for example.

Attempts by researchers to develop models and standards concerning the value of individual data are currently only capable of producing approximate results (Palmetshofer et al., 2016; Jentzsch, 2016). However,

9 Retrieved on 14 June 2017 from URL http://mydata.org.

it does appear that the latest utilisation models underestimate the economic value of data and the attainable prices (Palmetshofer et al., 2016). There is also the question of whether data can be subsequently reutilised, and if so, who then actually owns the data. A further problem lies in the fact that data are frequently only valuable once they have been linked to other data. But the possibilities for tracing huge sets of generated data back to individual consumers are limited. Apart from that, consumers do not always have the technical option or the requisite authorisation to download their personal data from each of the services used. Even if they can download the data, advanced IT skills are usually required to process them or link them to other data.

Another approach which is designed to give consumers more control over their own data flow is the implementation of a context-sensitive recommender system (World Economic Forum 2014). This system would assume the role of mediator between consumers and the service providers who wish to utilise their data. Based on various factors such as user history, default settings and type of data utilisation, the recommender system would either recommend that the consumer takes advantage of the service or – if there are concerns regarding data protection – advise against it. The system could also include the ability to learn from the consumer's decisions. In general, recommender systems can help the consumer to determine whether terms and conditions and value creation models based on personal data are reasonable, thereby ultimately improving usability. However, this approach is still only at the conceptual stage. This is why we have suggested the consumer-centric data portal and the recommender system as development projects that could improve the digital sovereignty of consumers in the future.

3.2. Enforcing the principles of privacy by design and privacy by default

The Advisory Council reiterates the demand for user-friendly, data-minimising and security-oriented default settings for communication systems (privacy/security by design and privacy/security by default as the guiding principles). State-funded projects must be aligned with these principles.

According to the "privacy by design" principle, the issue of privacy must play a key role in the design of communication systems in order to protect the consumer's private sphere. The "privacy by default" principle means that the system's default settings will ensure the highest levels of privacy and data protection. From this starting point, consumers have the option of easily switching to communication modes with varying degrees of data minimisation.

The same applies to the principles of "security by design" and "security by default", but this time with regard to the security aspect in communication and the security aspect when using services. These principles should enable all users – particularly those without advanced levels of informational and digital literacy – to easily and effectively protect their data and to communicate in a secure manner.

It remains one of the Advisory Council's key objectives to establish sufficient privacy in communications and in the transfer of consumer data (see Reisch et al. 2015, SVRV, 2015). In this context, we consider it particularly important to ensure that even people without high levels of information literacy are easily able protect their data.10 The ePrivacy Directive from 2002 – which remains valid today – supports this notion. Recital 46 specifies the necessary measures, which require:

10 An overview of these "privacy-enhancing technologies" is provided by Domurath & Kosyra (2016).

> "manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected." (ePrivacy Directive 2002/58/EG)

The requirement also reflects the ideas set out in the EU General Data Protection Regulation (Article 25 I, II):

> "that appropriate technical and organisational measures are implemented in order to meet the requirements of this Regulation. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default." (EU Data Protection Regulation, Recital 78)

The principle of privacy/security by design requires that privacy and other security aspects are integral elements of communications systems. This means that certain features are implemented within – or developed for – the communications system in order to ensure privacy (Weis et al., 2016; Domurath & Kosyra, 2016). For example, the privacy by design principle states that data should be processed locally by the consumer, and that data should only be transmitted anonymously and using pseudonymisation (or aggregation), encryption and authentication (Weis et al., 2016).

Privacy/security by default means that consumers have the option of easily switching between more or less secure modes of communication – but the more secure communication mode is always selected by default. Privacy/security by default can therefore be viewed as a standard setting which ensures that personal data in IT systems or business models are automatically protected – without the user having to take measures to protect their privacy (Domurath & Kosyra, 2016).[11]

11 It is important to distinguish the principle of privacy by default from the principle of privacy by option: while the latter principle allows consumers to switch between more or less secure modes of communication, the more secure option does not necessarily have to be the default setting (Weis et al., 2016).

3.3. Improving security in the Internet of Things

In the face of steadily worsening security problems in the Internet of Things (IoT) segment, the Advisory Council recommends evaluating how we can ensure that products and services which appear on the market are mandatorily and continually protected throughout their entire life cycle by security updates – echoing the procedures in the healthcare field. Technological standards need to be developed in this area, while source codes (similar to recipes in the food sector) should be deposited into escrow.

To ensure sufficient levels of protection in the IoT segment, manufacturers should be obliged to develop security updates. One further possibility would be to consider ways in which a system's source code could be deposited with an escrow agent in the event that a manufacturer fails to comply with this obligation. In such cases, the option of disclosing the source code (open source) should also be considered. This would ensure at the very least that third parties could take over the development and distribution of security updates.

In order to enhance the security of consumers in the digital world, the IT industry has constantly developed and refined its security management systems, using frequent and in some cases automatic software updates, combined with hardware updates at relatively short intervals. While established products such as Adobe Flash or Microsoft Windows/Office – despite the best efforts of the manufacturers – have repeatedly come to the attention of security researchers, with vulnerabilities in the security architecture being criticised on a regular basis (BSI, 2016), the overall security situation in the relatively new IoT segment is even worse (Weis et al., 2016).

This is because the devices sold for and integrated into the IoT are often inexpensive products with low customer retention (e.g. internet-enabled light

bulbs or IP cameras) and their short product cycles mean that companies often feel no obligation to keep consumers informed about the requisite security updates (Weis et al., 2016). But even IoT devices with relatively long lifespans (e.g. smart heating control systems) occasionally exhibit major security loopholes, since their hardware and embedded software require long-term maintenance which a manufacturer may not be able to provide. Furthermore, consumers are often unaware that such devices require not only hardware maintenance, but software maintenance too (Weis et al., 2016). The industry therefore needs to devise consumer-friendly standards to ensure that the IoT operates within a secure infrastructure, the implementation of which is compatible with everyday usage.

Given the mounting evidence of a problematic security situation within the IoT sector, we advocate taking stronger and more effective measures to guarantee security in and around the IoT. This includes the obligation for manufacturers to develop security updates.

In addition, it would be possible to consider ways in which a system's source code could be deposited with an escrow agent in the event that a manufacturer fails to comply with this obligation. In such cases, the option of disclosing the source code (open source) should also be considered. This would ensure at the very least that third parties could take over the development and distribution of security updates. If the manufacturer failed to comply with the aforementioned obligations, or if the manufacturer ceased to exist, the escrow agent would arrange for the source code to be released as "open source" software.

3.4. Expanding the range of data-minimising products

The Advisory Council recommends assessing whether it would be possible to grant consumers a right to use data-minimising digital products, meaning that there would always be a data-minimising version for consumers to choose.

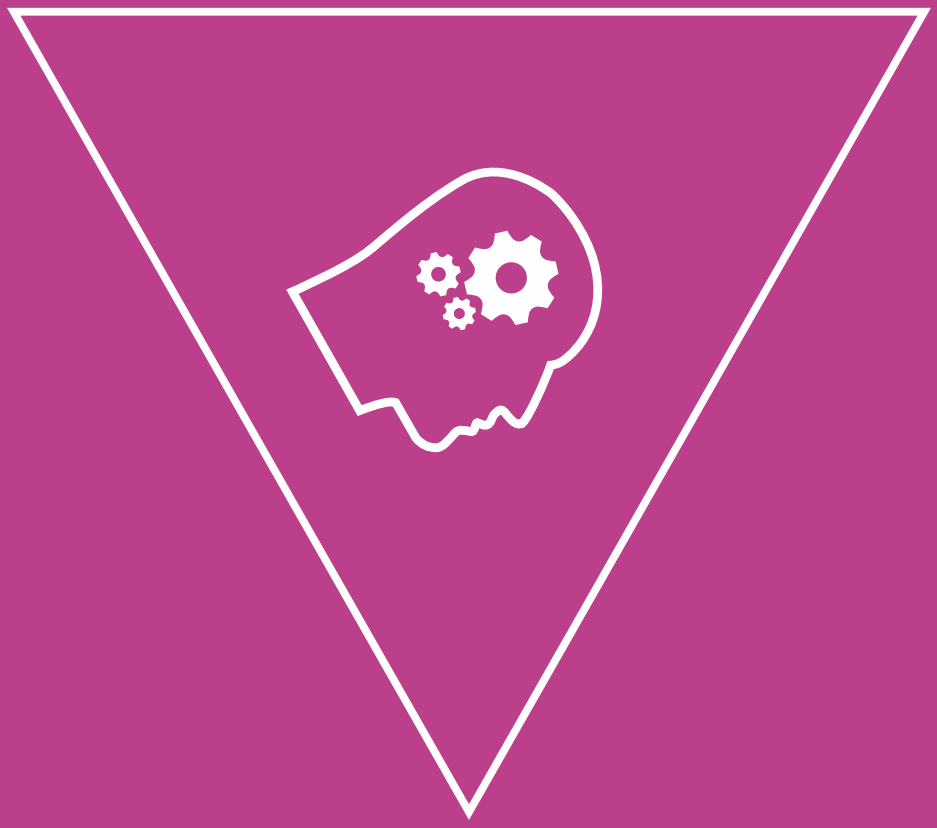
When using digital products and services, users should be able to decide whether they want to provide information about their own media use, or whether they wish to avoid providing such information (entirely or partially) without the essential functions of the digital product being limited as a result. Consumers who do not wish to provide data must not be disadvantaged in any way (in line with anti-discrimination law). Applying this principle to commercial transactions, it means that no negative consequences should arise from a consumer's decision to purchase products and services online without, for instance, creating a customer account or participating in other types of data disclosure (which are not directly required to perform the contract).

One key aspect of digital sovereignty is the ability to choose how digital content is displayed – on websites, for example. This includes the option of using ad blockers without limiting a particular website's usability.[12] While we are aware that services funded (exclusively) by advertising are losing revenue due to the growing popularity of ad blockers, we are against a ban because it is important to protect freedom of choice in how online services are presented. It would be in the advertising industry's own best interests to recognise that online advertising is often perceived as a considerable nuisance which is detrimental to the user experience. Online ads frequently take up large portions of screen space and can even be personalised to the individual user, appearing as pop-ups, increasing the sound volume, being difficult to remove and eating up significant amounts of data volume. If a website with journalistic/editorial content only

12 Ad blockers are browser add-ons that modify the content of a website for the benefit of the user. They are designed to display a website with as little advertising as possible and to limit the amounts of information about media usage that is transmitted to the website provider (see also Ofiera, 2016).

has a small part of its total content devoted to actual news, this represents an imbalance which must be rectified in the interests of the consumer. The understandable sense of frustration at being disturbed by advertising should be a focus of attention here, as should the ability of advertising to track our personal interests.

Furthermore, anti-discrimination law should apply to cases where an individual decides that she does not wish to (digitally) disclose her data. In the context of actual commercial transactions, this means that – as far as possible – no negative consequences should arise from a consumer's decision to purchase products and services online without creating a customer account or participating in other types of data disclosure (Becker, 2017).



Digital Literacy

4. Digital literacy

Digitalisation is profoundly changing the way information is produced, made available and distributed in society. But in order to make self-determined and empowered use of the new opportunities offered by the digital society, consumers have to develop new skills. Digital literacy is an essential prerequisite for freedom of choice, self-determination, self-control and security in the online environment.

Information and data literacy – which are the component parts of digital literacy – are new cultural proficiencies that have emerged alongside reading, writing and arithmetic. Consumers should ideally be capable of actively determining their own need for information, finding that information, evaluating it in terms of relevance, quality, scope and message, processing it for their own needs, restructuring it and making it accessible to other people if so desired (e.g. Süss, 2017). These are valuable skills, regardless of whether the information is available in analogue or digital form.

But in the context of digital media, entirely new phenomena have emerged which are important when it comes to using and assessing digitally stored information in proficient and empowered ways. One of these phenomena is the erasability (or not) of data. Another is the distinction between different types of content: editorial content, classic advertising formats, user-driven content (including influencer marketing on platforms such as YouTube and Instagram) and content that is automatically generated by social bots (see Wineburg et al., 2016). Apart from that, dealing with the information available on the internet has thrown up a new set of problems from the standpoints of data protection and copyright law. The rapid nature of technological development means that users have to be equally quick at developing their own skills.

In the following section, we outline key objectives designed to strengthen the digital literacy of consumers. These objectives include equipping teachers with the necessary qualifications and expanding the range of reliable consumer information. Beyond that, we believe that action is required in the field of digital self-control, and we also see a need for additional research into the effects of digitalisation on cognition, emotion and social life. Meanwhile, ethical questions have emerged with regard to issues such as data trading, loss of control in the Internet of Things, and the freedom of choice available to consumers. Each of these questions also has a legal dimension. There is a resulting demand for interdisciplinary research in the field of consumer policy, one which needs to be met through targeted funding.

4.1. Establishing a qualification pact for "Digital Literacy in Teacher Training"

The Advisory Council recommends that a qualification pact for "Digital Literacy in Teacher Training" be established (similar to the Quality Pact for Teaching or the National Initiative to Improve Teacher Training).

Establishing such a package of measures for "Digital Literacy in Teacher Training" – to be jointly funded by the Federation and the *Länder* – should guarantee that teachers acquire digital literacy skills during the first and second stages of their teacher training. It should also ensure that teachers are offered further training throughout their career, thereby enabling them to adapt to the ever-changing requirements of the digital world. The emphasis should be more on understanding the implications of digitalisation as an overall process, and less on the specific digitalisation of lessons or on the use of digital equipment.

Apart from equipping teachers with the skills to work with digital tools and media, as well as the confidence to utilise the formats and methodologies of digital teaching (including the setting of exams), teacher training courses and further training courses should also seek to ensure that both prospective and established teachers have the ability to grasp the opportunities and implications of digitalisation for individuals and society at large. In learning to cope with digitalisation in every field of life (not just in digital media but also in IoT, etc.), consumers need certain skills in dealing with freedom of choice, self-determination, self-control and security. These skills must be fostered through a range of training measures.

But if insufficient attention is devoted to this matter in teacher training, initiatives such as the "Education in the Digital World" strategy developed by the Standing Conference of the Ministers of Education and Cultural Affairs (Kultusministerkonferenz, 2016) – which involved the Länder agreeing on a framework to divide up the competencies for digital education – will remain incomplete. First, the matter needs to be addressed in science and humanities courses, in subject-related didactics courses, and in educational science courses at teacher training institutions. Second, it has implications for the second stage of teacher training (i.e. the practical phase) as well as for further training institutions that cater to teachers who are responsible for devising integrated concepts to strengthen digital literacy in teacher training programmes. As a result, there is a need to amend the Ländergemeinsame inhaltliche Anforderungen für die Fachwissenschaften und Fachdidaktiken in der Lehrerbildung ["Content requirements for subject-related studies and subject-related didactics in teacher training for all the Länder"] (Kultusministerkonferenz, 2008, cf. 2017[13]) so as to include digital skills in the compulsory standards for teacher training.

4.2. Promoting services that improve digital literacy

The Advisory Council recommends that existing and future (institutional) services designed to improve digital literacy be sustainably funded and structurally integrated. At the same time, there should be a systematic expansion of services with a gatekeeping function, services for multipliers and services for consumers.

(Institutional) services designed to improve digital literacy for multipliers and consumers can be empowering because they provide reliable and verified information, act as gatekeepers and can respond quickly to new developments in the digital world.

Gatekeepers such as the consumer organisation *Stiftung Warentest* offer reliable information on products and services in areas ranging from financial investment and education to household goods. This enables consumers to make informed choices without having to rely on biased sources. The health sector, for example, is plagued by the problem that most consumers are unable to tell the difference between neutral and biased information. This is an area where the Institute for Quality and Efficiency in Health Care [*Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen*, IQWiG] could assume a gatekeeping role by compiling, updating and distributing a list of recommended resources that provide evidence-based and easy-to-understand information.

One example of a service that performs a gatekeeping function for multipliers is the online platform *Materialkompass Verbraucherbildung* ["Guide to consumer education materials"]. Meanwhile, the *Weiterbildungs-Guide* ["Further education guide"] run by *Stiftung Warentest* and the *Medienkompetenz-Datenbank* ["Media literacy database"] provided by the Federal Agency for Civic Education are aimed directly at consumers themselves. Furthermore, initiatives and associations such as Initiative 21 and the Chaos Computer Club should be brought on board as additional stakeholders in order to embrace the current developments in digitalisation and to incorporate these trends in informational and educational services.

Given the rapid evolution of digital applications and the ever-changing behaviour of users, there is now a strong emphasis on the acquisition of digital literacy skills outside of the conventional education system. In order to make sense of complex issues, consumers need quick access to relevant and reliable information in all areas of consumption (see Gigerenzer et al., 2016). Gatekeeping services that provide meaningful and verified information can be of assistance here. The Advisory Council therefore recommends that more services with a gatekeeping function be established and funded in various fields of consumption – echoing the gatekeeping roles performed by Stiftung Warentest and IQWiG.[14] Reliable consumer informati-

13 Retrieved on 14 June 2017 from URL https://www.kmk.org/themen/allgemeinbildende-schulen/lehrkraefte/lehrerbildung.html.

14 Retrieved on 14 June 2017 from URL https://www.iqwig.de/.

on can be found on websites such as Mobilsicher.de[15] (an internet portal operated by iRights e.V. to promote safe mobile communication on smartphones and tablets), Marktwächter.de,[16] Checked4u.de[17] and Verbraucherzentrale.de[18] where consumer organisations offer information about digital services such as review sites, platforms and quantified self applications.

Such gatekeeping services are also useful for multipliers in various sectors. One example is Materialkompass Verbraucherbildung which evaluates teaching materials on consumer issues – including those covered by the media (on topics such as data protection, violence on the internet, basic knowledge and law) – and serves to verify the quality of teaching materials while also helping teachers with their lesson planning. The Advisory Council suggests making this service a permanent offering with the aim of providing teachers with guidance in choosing high-quality teaching materials in the field of digital education. Such guidance is important because the teaching materials used in classrooms are increasingly supplied by associations, publishing houses, non-governmental organisations, public authorities and companies, without being subject to any form of assessment.[19]

Besides activities aimed at improving digital literacy within the school setting, it is also important to expand and fund educational initiatives that promote digital literacy outside of school. Examples of these include the "Further education guide" offered by Stiftung Warentest[20] and the "Media literacy database" provided by the Federal Agency for Civic Education.[21] The database contains a list of media education projects designed to foster digital literacy. Users can search the database according to type of media or type of service. Other useful services are Digitalkompass.de[22] (a collaborative project to promote media literacy among older citizens) and "Watch your Web"[23] (ended in 2015 – an information portal that provides young people in social networks with information and media education with a focus on consumer protection).

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

4.3. Developing measures to improve self-control in using digital media and services

The Advisory Council recommends that the ministries of education and cultural affairs develop measures to improve self-control in the use of digital media and services.

Self-control – as opposed to outside control – is an integral part of digital literacy when using digital media and services. It means being able to control one's use of digital services or devices such as mobile phones, rather than being controlled by them. The consequences of insufficient control are becoming ever more apparent – as illustrated by the growing number of fatal road accidents caused by people using mobile phones while driving. Since such behaviour is formed at a very early age, measures to improve digital self-control should also begin early, i.e. at the pre-school stage.

In 2016, the Standing Conference of the Ministers of Education and Cultural Affairs focused on the topic of "Education in the Digital World". Its comprehensive strategy covering various different educational institutions and disciplines aims to address both pupils/students and educators. However, the approach fails to acknowledge the major relevance of digital self-control (as opposed to outside control) when using digital technologies. Self-control is an integral part of digital literacy. It means being able to control one's use of digital services or devices such as smartphones in accordance with one's own preferences. It also means being in control of one's behaviour in forums and social networks, as well as complying with the rules of netiquette (no hate speech, no cyberbullying, etc.; Underwood & Ehrenreich, 2017).

The consequences of lack of control are becoming increasingly apparent – as shown by the growing number of fatal traffic accidents caused by people using the internet while driving. Another example is when people are distracted by a constant stream of incoming emails, which can lead to lapses in concentration. In a representative survey conducted by Bitkom Research, it was found that 51% of car drivers read

text messages while driving and 8% watch videos on their smartphones.[24] The National Highway Traffic Safety Administration (2015) reported that one in seven crashes with documented driver distraction in the USA involved the use of mobile phones.

The growing need to use digital services while doing other activities (multitasking) can result in reduced cognitive control – such as a reduction in attention span and a decreased ability to remain focussed on specific everyday tasks – whereas the hypothesis that people can successfully adapt to multitasking is disputed (Ophir et al., 2009; van der Schuur et al., 2015). The use of digital services and social media during class has a negative effect on learning and examination performance (Ellis et al., 2010; Junco, 2012; Rosen et al., 2011; Wood et al., 2012). In 2012, 69% of American students reported that they texted during class, 28% used Facebook and 21% searched for content not related to class (Junco, 2012); 49% to 70% used Facebook at the same time as doing homework (Junco, 2015). Insufficient digital self-control can lead to dependency, also known as "internet addiction" (Helbing et al., 2017; Young & Abreu, 2011; cf. Kardefelt-Winther, 2014).

The development of self-control is an integral part of digital literacy, enabling the aforementioned negative consequences of digital technologies to be reduced. Digital self-control needs to be cultivated from the pre-school stage onwards and should be reaffirmed by the positive example set by parents (Gigerenzer, 2017). Given that almost no research yet exists on effective methods of self-control in the digital world, the Advisory Council sees a particular need for research in this area. Such research should strive to clarify (1) what type of interventions allow people to develop digital self-control; (2) how these interventions can be incorporated within (pre)school curricula; (3) what technical and legal options can help to compensate for insufficient self-control.

24 Retrieved on 14 June from URL https://www.bitkom.org/Presse/Presseinformation/Viele-Autofahrer-nutzen-waehrend-der-Fahrt-das-Smartphone.html.

4.4. Studying the effects of digitalisation on cognition, emotion and social life

The Advisory Council recommends the targeted funding of interdisciplinary research into the effects of digitalisation on cognition, emotion and the social life of consumers. This applies both to "digital natives" and "digital migrants".

At present, studies on digital literacy tend to focus on how people interact with technology. But only a limited amount of research has been conducted into how psychological and social behaviours are affected and what consequences can be expected. Scientists have speculated for years about whether digitalisation causes any systematic changes in the attention span, emotionality and social behaviour of humans, but there is a lack of systematic research particularly into the long-term effects of social media.

Meanwhile, ethical questions have emerged with regard to issues such as data trading, loss of control in the Internet of Things, and the freedom of choice available to consumers. Each of these questions also has a legal dimension. There is a resulting demand for interdisciplinary research in the field of consumer policy, one which needs to be met through targeted funding.

Given the popularity of digital media among children and adolescents, it is astonishing that the field of developmental psychology has produced so little research into the impact of digital media on development and behaviour (Underwood & Ehrenreich, 2017). With digital consumption inevitably reducing the level of interaction with adults, what effect does this have on child development (c.f. Barr, 2010)? What impact does shallow learning have on children's ability to think for themselves and make coherent sense of subject matter (Loh & Kanai, 2016)? Is the fact that many people now suffer from a reduced attention span – exacerbated by multitasking – a genuine problem or can people learn to perform at the same level despite constant interruptions? What relationships and forms of collaboration develop between humans

and machines and what are the consequences? The answers to these and other important questions are unknown.

Apart from the digital revolution's impact on cognitive skills, significant changes in emotional and social life can also be expected. Cases of cyberbullying are widely reported in the media and many young people certainly do get harmed online, but often in different ways than many adults imagine. Adolescents suffer from social exclusion when they constantly see pictures of their friends meeting up without them or going to parties which they were not invited to (Underwood & Ehrenreich, 2017). The obligation to be digitally available at all times – not only in social media but also in terms of professional availability – is described in the discourse as being a stress factor (Carstensen, 2015). Short-term abstention from digital media – whether voluntary or not – is also frequently experienced as a highly stressful situation, mirroring addictive behaviour. The Federal Commissioner for Drugs estimates that there are currently around 600,000 internet addicts and 2.5 million people with problematic internet behaviour in Germany (Stiftung Kind und Jugend, 2017). Excessive use of mobile phones and computers can cause sleep disorders and has mental health implications (e.g. Thomée, 2012; van der Schuur et al., 2015). In addition, the positive effects of real social interactions are endangered by smartphone use (Rotondi et al., 2017). There are also indications that the excessive media use of parents is correlated to developmental problems in their children – such as speech development disorders and hyperactivity in under-6-year-olds (Stiftung Kind und Jugend, 2017).

However, numerous positive developments can also be observed. Online communities that support civil society initiatives (e.g. Better Place, Code for Germany, Next Hamburg) have grown massively in terms of reach and exposure, enabling new forms of participation. There are corresponding online formats for political participation too (see the EU-funded MAZI project[25]) which encourages communities to grow.

For many people, the opportunity to share experiences on special interest forums that deal with sensitive personal issues (e.g. online self-help groups) is an important everyday resource that can be used anonymously (e.g. Döring, 2010). Interactions between people and networked systems are also playing an increasingly significant role in the professional world, where employees can be provided with real-time support via augmented reality applications,[26] thereby opening up new fields of activity, and where access to knowledge in the open source ecology can shift the parameters of production and – in the long term – possibly even change the structures of power (c.f. Rifkin, 2014). The resulting long-term ethical, legal and social questions need to be investigated.

In order to reach a better understanding of how digital technology changes all of us and how we can gain control over the negative implications while seizing and supporting the positive developments, it is essential that we conduct systematic research into how people are affected by the digital revolution. This research should focus not on whether cognitive development is influenced by digital media but on how users are affected by technology and what skills they require in order to better cope with the new environment (Gigerenzer, 2013; 2017). Above all, the research needs to ascertain (1) how child and adolescent development is affected by the use of digital services and what interventions are capable of promoting healthy usage; (2) how digital migrants are affected; (3) what institutional facilities and legal frameworks must be put in place to ensure that both "digital natives" and "digital migrants" are better capable of steering and controlling the mental, physical, social and economic implications of the digital revolution.

25 Retrieved on 14 June 2017 from URL http://www.mazizone.eu/.

26 See the SmartFactory project on Predictive Maintenance Data Analysis (retrieved on 14 June 2017 from URL http://dfki-3036.dfki.de/webNews/SF_Steckbrief_20151118_LabsNetworkIndustrie.pdf).

Regulation

5. Regulation

The thinking behind the regulatory approach is to make government and corporate entities assume responsibility for the provision and safeguarding of digital sovereignty. In the legal dimension, the concept of the digital sovereignty of consumers falls under the constitutionally protected right to informational self-determination in accordance with Article 2(1) sentence 1 of the German Basic Law.[27] The Federal Constitutional Court's census judgment couched the right to informational self-determination in concrete terms with reference to Article 2(1) and Article 1(1) of the Basic Law. It covers the right of each individual to decide about the disclosure and utilisation of their own personal data. Since that judgment, informational self-determination has been regarded as a necessary prerequisite for effective freedom in relations with both the state and private entities (Buchner, 2006). The protections offered by general privacy law also give consideration to the possibility that access to the system might be used to gain insight into key aspects of a person's biography or to obtain a meaningful idea of an individual's personality.[28]

Resulting from the government's responsibility to safeguard the informational self-determination of its citizens is an obligation to preserve and, where necessary, improve the legal framework that enables informational self-determination to be exercised. It is particularly important for the state to set a positive example because even derogations for internal security reasons must remain in strict compliance with the statutory framework, observing the transparency requirements for state action and adhering to the limits imposed by the highest courts.[29]

With this is mind, the following section contains recommendations for action in specific areas where the Advisory Council considers regulatory activity to be essential.

27 For a critical perspective on the concept of informational self-determination: Friedewaldt et al. (2017).

28 Federal Constitutional Court judgment of 27 Feb 2008 - file no. 1 BvR 370/07 - BVerfGE 120, 274, 314 (online searches).

29 Particularly significant here are the decisions concerning the nationwide state-ordered collection of digital communications data. For the German perspective on this issue: Federal Constitutional Court judgment of 2 March 2010, 1 BvR 256; CJEU judgment of 21 December 2016 in the joined cases C-203/15, Tele2 Sverige AB / Post- och telestyrelsen and C-698/15, Secretary of State for the Home Department / Tom Watson and Others, ECLI:EU:C:2016:970; CJEU judgment of 8 April 2014 in the joined cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, ECLI:EU:C:2014:238.

5.1. Implementing T&Cs and privacy statements as one-pagers

The Advisory Council reiterates its recommendation[30] that before contracts are concluded, companies must inform consumers via one-pagers (500 words) about the relevant privacy regulations and about the terms and conditions. The Advisory Council recommends developing these one-pagers in a pilot project organised by the Federal Ministry of Justice and Consumer Protection (BMJV) and involving the relevant stakeholders.

From the consumer's viewpoint, the obligation to produce one-pagers can help to increase the transparency of data transfer. In addition, one-pagers can help to increase acceptance of the T&Cs and privacy statements used in practice if they are drawn up in a collaborative process involving the BMJV or other government authorities on one side and stakeholders on the other.

The individual's consent to such data collection is a cornerstone of informational self-determination and is thus a key element of digital sovereignty for consumers. In practice, consent is obtained via standardised privacy statements. But according to a privacy sweep coordinated by the Global Privacy Enforcement Network (GPEN), statements explaining the collection and processing of consumer data – and the related consumer rights – were "alarmingly" inadequate in more than 300 of the Internet of Things devices that were analysed.[31] This was recently confirmed by a study carried out by the Market Watchdog for the Digital World entitled Wearables, Fitness-Apps und Datenschutz: Alles unter Kontrolle? ["Wearables, fitness-apps and data protection: everything under control?"].[32] Furthermore, an illustrative study that examined an app used in the Internet of

30 This proposal can be found in SVRV (2016, p. 46 et seq).

31 Further information can be found on the website of the Irish Data Protection Commissioner (retrieved on 14 June 2017 from URL https://www.dataprotection.ie/docs/23-9-2016-International-Privacy-Sweep-2016/i/1597.htm). In Germany, the Baden-Württemberg Commissioner for Data Protection and the Bavarian Office for Data Protection were involved.

32 Nine of the twelve wearables examined in the study were shown to incur such grave violations of data protection law that the North Rhine-Westphalia Consumer Organisation issued warnings to the manufacturers (Moll et al., 2017).

Things found that some clauses could be ineffective pursuant to sections 307 and 308 of the German Civil Code because they unilaterally oblige consumers to check and review amended clauses, and because they place consumers at an unreasonable disadvantage since they are not told that their data are being passed on to third parties (Domurath & Kosyra, 2016).

This means that action is urgently necessary with regard to the clarity and lawfulness of T&Cs and privacy statements. Making it a legal requirement to provide one-pagers can help to achieve the desired transparency and legality. Under the guidance of the BMJV, a text is currently being drafted in consultation with stakeholders. It goes further than the one-pager presented at the National IT Summit in 2015[33] which only contained data protection information.

5.2. Making algorithms transparent and open to scrutiny

The Advisory Council reiterates its recommendation[34] that legal requirements must be put in place to ensure that (a) algorithms take account of the requirements of consumer law, data protection law, anti-discrimination law and digital security, and that in cases where consumers are directly exposed to algorithms, the underlying parameters need to be made transparent, and that (b) based on standardised disclosure requirements, algorithms should be disclosed to a group of experts who carry out spot checks to see whether they are legally sound. The Advisory Council recommends that legal standards are developed and that source codes are deposited into escrow.

The disclosure of algorithms to a group of experts (e.g. at a digital agency of the kind proposed by the Advisory Council) is crucially important in order to ensure compliance with the statutory requirements for automated decision-making by algorithms. The primary focus here is on consumer law, anti-discrimination law and fair trading law, but there is also an emphasis on compliance with established principles of data protection law such as data minimisation and purpose limitation. From the consumer viewpoint, the most important thing is to have knowledge of the parameters underlying an algorithm (such as the different variables and their weighting) because without such knowledge, consumers are unable to file objections. These tasks could be brought together in a digital agency. Such an institution is needed in order to house the requisite expertise for the monitoring of compliance with statutory requirements.

In a world which is becoming ever more interconnected, the use of algorithms and the foreseeable evolution of self-learning algorithms have an impact on the deep-seated ethical principles woven into the fabric of our society. The law – which cannot avoid taking a regulatory stance on such ethical issues – reflects these questions in its normative framework. One challenge will be to work out the ways in which legislative instruments can be used to ensure that self-learning algorithms "act" in ethically responsible ways. While legal policy can obviously build on the expertise of those responsible for the development of artificial intelligence (AI) (BMWi, 2017b), adherence to regulatory standards should not be left entirely to market competition or to self-imposed ethical conduct within the commercial sector. But how can an autonomous, self-controlling process be embedded within a regulatory framework?

First, it is worth making the point that algorithms can be scrutinised on different levels. The mathematical formulae themselves can be scrutinised, as can the parameters that are critical for decision-making, as can the subsequent results of the underlying calculations or estimations. From the standpoint of consumer law, it would be possible to stipulate conditions for the scrutiny of an algorithm's parameters by drawing not only on the law of terms and conditions (see 5.1.) and the requirements of IT security (see 3.3.) but also on anti-discrimination law, fair trading law and data protection law. On one level, we are dealing here with parameters which can be analysed in order to

33 33 A template of this data protection one-pager was drawn up by the platform "Consumer protection in the digital world" which was headed by the Federal Ministry of Justice and Consumer Protection (BMJV) and comprised representatives from politics, business, academia, judicial institutions, and consumer and data protection organisations.

34 This proposal can be found in SVRV (2016, p. 67).

ascertain the legality of the decision-making carried out by algorithms. On another level, we are dealing with the human supervision of such decision-making.

The requirements of anti-discrimination law[35] and fair trading law[36] must be adhered to, especially where consumers are directly exposed to automated decisions. Because while algorithms make it possible to create apparently individualised advertising, offers, prices and ultimately even contracts, this individualisation may conceal elements of discrimination. Such discrimination is not necessarily aimed at any one individual. Rather, it can target a group of individuals who share common features that are determined via algorithms (Angwin & Parris, 2016).

Beyond that, the fundamental principles of data protection law – data minimisation (Article 5(1)(c) of the General Data Protection Regulation – GDPR) and purpose limitation (Article 5(1)(b) GDPR) – must continue to inform everyday practices whenever algorithms are used. This is essential if consumers are to develop trust in the handling of their personal data by government and corporate entities. It means that studies casting a critical light on big data's compatibility with these principles (Helbing, 2015) and voices demanding the right to products with no data collection (Becker, 2017) as well as the "right to an analogue world" (Maas, 2015)[37] will have to be taken seriously in the political debate. One approach would be to encourage the development of products and services whose underlying algorithms enable the automatic deletion of data (the key concepts here being: privacy by design and privacy by default).

In the case of self-learning algorithms, legal responsibility needs to be assignable. Research must be encouraged and carried out in this area. With self-learning algorithms in particular, lawmakers should draw on the specialist knowledge of companies in the information and communication technology (ICT) sector as well as experts in the associated research fields, applying this knowledge to draft a code of conduct on the use of personal data, artificial intelligence systems and big data analytics – without diluting the existing statutory requirements.

Compliance with these parameters can only be monitored, if at all, with the help of government agencies that oblige companies to disclose data and provide information.[38] In order to respect the private sector's interest in protecting trade secrets while also safeguarding the individual's right to information (section 34(1) sentence 4 of the Federal Data Protection Act [Bundesdatenschutzgesetz – BDSG]),[39] algorithms could be disclosed to a group of experts at a government authority (e.g. a digital agency) who then carry out spot checks to see whether the algorithms are legally sound. To this end, standardised software engineering procedures need to be developed.

In view of the fact that the largest and most innovative sections of ICT companies are located outside Germany, there is a need for concerted action at the international level. Ideally, the forum for seeking an adequate solution would be the European Union or – better still – the OECD and the United Nations.

35 e.g. the General Act on Equal Treatment [Allgemeines Gleichbehandlungsgesetz - AGG], section 19(1): "Any discrimination on the grounds of race or ethnic origin, sex, religion, disability, age or sexual orientation shall be illegal when establishing, executing or terminating civil-law obligations". As regards EU law: Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180/22, 19 July 2000 and Council Directive 2004/113/EC
of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, OJ L 373/37, 21 December 2004.

36 c.f. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149/22, 11 June 2005, which prohibits any misleading business practice if inter alia it "contains false information and is therefore untruthful or in any way [...] deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise".

37 Article 13 of the "digital civil rights" proposed by Heiko Maas (retrieved on 14 June 2017 from URL http://www.bmjv.de/SharedDocs/Interviews/DE/2015/Namensartikel/12092015_DieZeit_EN.html).

38 This proposal can be found in SVRV (2016, p. 71).

39 On this point, the Federal Court of Justice ruled in its "Schufa" judgment that the scoring formulae that are used to make credit assessments enjoy protection as trade secrets (BGH VI ZR 156/13). The case is currently before the Federal Constitutional Court. No date for the decision is currently foreseeable.

5.3. Improving the right of access to free-of-charge information

The Advisory Council recommends that the right of access to information (section 34 BDSG) be guaranteed without limitations. It also recommends that companies be obligated to inform consumers about their right to free-of-charge information and about the option to rectify inaccurate data – in a clear, transparent and easily identifiable way when the products are offered (i.e. rectification, erasure and blocking).

Data subjects wishing to exercise their right of access to information currently face considerable practical difficulties. These hindrances undermine the effectiveness of a right that is essential for the digital society. Consumers are not sufficiently informed about their rights and experience problems in asserting their right to free-of-charge information. To raise awareness among consumers about this right and other associated entitlements, websites must declare the right to information in a way that is transparent and easy to understand. Yet this is not sufficient on its own: there must also be a simple option for accessing free-of-charge information. The issue of liability for data controllers will therefore need to be discussed.

If public and non-public bodies gather data without the knowledge of the individual concerned, the applicable law stipulates that the individual must be informed about the storage, the relevant controller, and the purpose of the data processing (sections 19a and 33 BDSG, Article 15 GDPR). At the data subject's request, the controller must furthermore provide information about the stored data concerning that individual, the origins of such data, the recipients to whom the data have been transmitted, and the purpose of the storage (sections 19 and 34 BDSG, Article 15 GDPR).

For data subjects, the right of access to information provides a starting point for exercising further rights and forms the core of the right to informational self-determination. It also reflects the principle that decisions should ultimately be made by people, and that algorithms should be subject to continual human scrutiny with regard to decision-making. To this end, section 6(1) BDSG establishes that decisions of legal consequence should not be based solely on the automated processing of personal data that serve to evaluate individual personal characteristics. Articles 21 and 22 of the GDPR confer a right to object in such cases. In addition, the right of access to information provides individuals with an enforceable possibility to verify compliance with the principles of data minimisation and purpose limitation. The right thus makes a significant contribution to making automated decision-making more transparent. Only when data subjects learn of the nature and storage of personal data can they request that inaccurate data be rectified; that data be deleted when stored unlawfully or when the data are no longer necessary for the original purpose; and that data be blocked if the data subject asserts that they are incorrect but it cannot be established whether they are correct or incorrect (sections 20 and 35 BDSG, Articles 16 and 17 GDPR).[40]

Once again, the challenge here is to reconcile conflicting interests – the data subject's interest in erasure, the interest of those who seek information in accessing that information, and the commercial interests of businesses. The ECJ addressed this matter in its Google judgment,[41] stating that the right of data subjects to their data can indeed override the general public's interest in obtaining information. But due to legal and technical complications, it can be difficult in practice to exercise the right to erasure and the "right to be forgotten" as currently provided for in Article 17 GDPR. From a technical perspective, although erasing data is possible, it often involves a technically complex process (Weis et al., 2016). A further difficulty is that deletion is frequently performed only "partially". Even after deletion, data often remain available via other domains. Yet consumers are rarely aware of this limitation in the enforcement of their rights, so there is a fundamental need for clarification. Viable approaches to enforcing the right to erasure should be supported. If necessary, providers of social networks and other online services could be obligated to provide their customers with options for this purpose.

40 On rights to rectification: Becker (2017).

41 ECJ judgment of 13 May 2014 in Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, EU:C:2014:317.

In practice, data subjects are also often unaware of how they can exercise their right of access to information and the further rights that build upon it. Many consumers are uncertain as to which companies are processing their data. Spindler et al. (2016) report on a "serious discrepancy" between rights in theory and the actual situation in reality. In addition, the possibilities for obtaining free-of-charge information are not highlighted in prominent positions on websites. For example, in order to access personal information from Schufa (General Credit Protection Agency), consumers are first directed to a page where information is available upon payment (Korczak, 2016). There are also indications that requests for free-of-charge information often take longer than in cases where the information is being paid for (Korczak, 2016; Roßnagel et al., 2016).

Companies that gather and process data must offer free-of-charge options for accessing information in a prominent position on their websites and in other appropriate publications aimed at consumers. To guarantee this, there must be an obligation for companies to draw consumers' attention to the option of accessing information free of charge. A discussion is needed on whether liability should be introduced for this obligation in order to step up compliance with statutory requirements. Companies must also provide easily understandable information on this right and on the right to rectification, erasure and blocking. This ties in with the demand that consumers be provided with a privacy statement on a single page (see 5.1).

One further crucial element in this regard is algorithmic scrutiny (see 5.2). This helps consumers to acquire transparency regarding the data gathered about them as it can contribute to data minimisation in general. Scrutiny of algorithms can also assist consumers in tackling the difficulties they face in enforcing their rights.

5.4. Continuing to develop the minimum standards for interoperability

The Advisory Council recommends developing minimum standards that ensure compatibility between digital services, thereby allowing for communication between user accounts independently of the service provider (i.e. interoperability – as already established in the mobile telecommunications sector).

Interoperability – as well as user-friendly ways to migrate data between social networks or messenger services – is currently not supported in any systematic way. This leads to lock-in effects which always carry the danger of companies abusing their powerful market position – as can clearly be seen in the German market with providers such as Facebook and WhatsApp. Technical solutions for interoperability such as those implemented between various mobile phone providers could encourage competition.

The buzzword of "interoperability" goes to the very heart of the digital society. Interoperability essentially means the ability to transfer data between systems, applications and components (Palfrey & Gasser, 2012). It is concerned with reconciling two different aspects. On the one hand, a great deal of new infrastructure has been built to enhance connectivity and enable the flow of information between individuals, organisations and systems. On the other hand, we have not yet developed a suitable framework for identifying the (societal) goal of this interoperability and managing its inherent risks (Palfrey & Gasser, 2012). Interoperability is clearly about more than just technology and data flows. It is about a culture of human and institutional interaction. Four different but linked layers of interoperability can be identified (see Kominers, 2012; Gasser, 2012; Palfrey & Gasser, 2012). On the technical layer, interoperability means that technical systems can connect with one another, often through an agreed-upon interface. On the data (or semantic) layer, it aims to make data useful and readable once transferred via the interface. Thirdly, interoperability can only function if users have the necessary cognitive abilities and are willing to work

together. The final layer concerns cooperation in an abstract sense between societal systems, such as legal requirements. If interoperability is to be viable, societal considerations must take place on all of these layers at the same time.

In terms of the legal framework, interoperability is regulated in Germany and the EU by numerous instruments, mainly in the area of telecommunications. Since September, the relevant EU legislation has been undergoing revision as part of the Digital Single Market strategy with the aim of building a data economy and increasing competitiveness (European Commission, 2015). Standardisation plays a pivotal role throughout the initiative. According to Article 17 of the Framework Directive,[42] the European Commission has primary responsibility for drawing up non-binding standards as a basis for the harmonised provision of services. Together with the European Committee for Standardisation, one of the Commission's main objectives is to drive the development of standards – above all for interoperable financial, transport, administrative and e-Health services.[43] National regulatory authorities should create incentives for applying these standards (Article 5 of the Access Directive)[44] and encourage the implementation of international standards.

First and foremost, the task at hand is to put in place the technical groundwork necessary for interoperability. The standards required for this – and the resulting consequences for business, consumers and the state – are currently being discussed in relation to the entire market for digital products and services, particularly the Internet of Things (Zingales, 2015; Kominers, 2012). At present, however, there is little evidence of interoperability or user-friendly ways to migrate data between providers such as social networks and messenger services. This leads to lock-in effects which always carry the danger of companies abusing their powerful market position (Deutscher Bundestag, 2016), as can clearly be seen in the German market with providers such as Facebook and WhatsApp. Improved interoperability between over-the-top players such as WhatsApp and Skype would bring about tangible changes for consumers. As such, standard settings on interoperability would open up the market to new and innovative providers. By harmonising the regulations on over-the-top players with those for telecommunications providers, the market would also be made fairer and more open in areas extending beyond the issue of interoperability (BMWi, 2017b).

42 See recital 9 and Article 17 of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, OJ L 108, 24 April 2002, adapted by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services OJ L 337/37, 18 December 2009.

43 The European Committee for Standardisation provides information on standards that are currently in development or have already been approved (retrieved on 14 June 2017 from URL standards.cen.eu).

44 Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities, OJ L 108, 24 April 2002 adapted by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Access Directive).

5.5. Defining the right to data portability in more concrete terms

The Advisory Council underscores its recommendation that the right to data portability be understood in terms of a right of termination. It also recommends establishing a framework for switching to different service providers (as is already established for digital payment transactions).

Data portability – i.e. the transfer of data to the consumers themselves or to another service provider – largely depends on the implementation of the appropriate technical measures. This will require the establishment of a legal framework similar to that for digital payments. If consumers request that their data be transferred back to them, it is similar to exercising a right of termination. The current uncertainties concerning the wording in Article 20 GDPR should be overcome by explicitly granting consumers a right of termination.

The right of data portability was introduced in Article 20 GDPR following the ECJ's Google ruling.[45] Accordingly, the data subject has the right to receive personal data in a structured, commonly used and machine-readable format, as well as the right to transmit the data – or have the data transmitted – to another controller. The right to data portability should enable data subjects to transfer their social media profiles or email accounts to other service providers. This will necessarily involve data related to third parties (in the form of email conversations, shared pictures, etc.). Consequently, the right to data portability is highly relevant for digital sovereignty in terms of informational self-determination because it gives consumers the ability to choose digital services and switch between various providers.

At the same time, the right should also promote competition – although it is disputed whether it actually achieves this or not. The German and French competition authorities confirm that established companies enjoy greater market power because of their extensive client bases and data resources, which give them a competitive edge over other businesses that do not have such large volumes or such diverse types of data at their disposal (Birnstiel & Eckel, 2016). This imbalance of market power may result in lock-in effects (Deutscher Bundestag, 2016; Schantz, 2016; Swire & Lagos, 2013). Whether or not these effects are actually harmful to competition in light of changing consumer preferences and businesses models[46] remains to be seen at this point. What is clear is that the issue of data portability rights is a key component of the EU's strategy for the Digital Single Market (European Commission, 2015).

Implementation of the right to data portability is also contentious. From a technical point of view, some are confident that data portability is feasible with the help of the Semantic Web (Bojars, et al., 2008).[47] In the relevant technical literature, however, there is currently no simple standard that could help define what qualifies as a structured and "commonly used" data format and what does not (Swire & Lagos, 2013). Furthermore, data portability becomes problematic when third-party data are involved or when the degree of personalisation is unclear (see Schweitzer et al., 2016; BMWi, 2017b). The existing and proposed standards are still overly complicated (Swartz, 2013). To address these challenges, the Article 29 Data Protection Working Party has called upon trade and industry representatives to work towards a common set of interoperability standards and formats (Article 29 Data Protection Working Party, 2017). Yet the goal of interoperability should not simply be to enable one-off data transfers when consumers switch between service providers. Instead, social networks and chat services (for example) should enable common standards for interoperability between providers.

From a data security perspective, a discussion needs to take place on whether the right to data portability is a positive thing for consumers. One consequence of the right to data portability could be that, after one instance of illegal access, constant subsequent access is possible since far more data is made accessible in an automated process (Swire & Lagos, 2013). It is therefore necessary to strike a careful balance between data security and the right to data portability.

The situation in German data protection law is that the legislator can do no more than simply add further specification to the right to data portability within the meaning of Article 20 GDPR (Deutscher Bundestag, 2016). But in any event, it must be ensured that the right to data portability is provided for in an effective way. To this end, the right to data portability should be understood under contract law as a right to terminate the underlying consumer contract. This will allow consumers to request that their data be returned free of charge in a commonly used and machine-readable format or that their data be deleted. The data received can then be transmitted to other service providers, either by the consumers themselves or from one service provider to another (Article 20(2) GDPR). Despite contention over its effectiveness, this right is at least useful for consumers who wish to transfer their data to other providers and benefit from market competition.

45 ECJ judgment of 13 May 2014 in Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, EU:C:2014:317.

46 There are some isolated indications that consumers may in certain circumstances prefer limited interoperability (e.g. Apple products), see Zittrain (2009). Furthermore, companies seem to be already cooperating with the sharing of data between their platforms (e.g. the Facebook plug-in for websites), see Swire & Lagos (2013). On changing business models, see Pasquale (2015).

47 The first proposal is based on Berners-Lee (2000).

Bibliography

Angwin, J. & Parris, T. (2016). Facebook lets advertisers exclude users by race. ProPublica blog (28 October 2016). Retrieved on 21 June 2017 from 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 No. 242 rev.01. Retrieved on 14 June 2017 from 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 (December 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 (eds.), Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht: Arbeitsberichte (p. 1-134). Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht [Max Planck Institute for Foreign and International Criminal Law].

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) [German Association for Information Technology, Telecommunications and New Media].

BMELV (2007). Charta Verbrauchersouveränität in der digitalen Welt, Conference "Herausforderungen und Chancen in einer digitalisierten Welt: Beiträge der Verbraucherpolitik". Berlin: Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) [Federal Ministry of Food, Agriculture and Consumer Protection].

BMWi (2015). Leitplanken Digitaler Souveränität. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi) [Federal Ministry for Economic Affairs and Energy].

BMWi (2016). Green Paper Digital Platforms. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi) [Federal Ministry for Economic Affairs and Energy].

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) [Federal Ministry for Economic Affairs and Energy].

BMWi (2017b). White Paper Digital Platforms. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi) [Federal Ministry for Economic Affairs and Energy].

BMWi & BMJV (2015). Mehr Sicherheit, Souveränität und Selbstbestimmung in der digitalen Wirtschaft. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi) & Bundesministerium der Justiz und für Verbraucherschutz (BMJV) [Federal Ministry for Economic Affairs and Energy & Federal Ministry of Justice and Consumer Protection].

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 (May 2008), Innsbruck.

BSI (2016). Die Lage der IT-Sicherheit in Deutschland 2016. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI) [Federal Office for Information Security].

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 [Federal Criminal Police Office].

Bundesregierung (2014). Digitale Agenda 2014-2017. Berlin: Bundesregierung [Federal Government].

Bundesregierung (2008). Verbraucherpolitischer Bericht der Bundesregierung 2008, Berlin: Bundesregierung [Federal Government].

Bundesregierung (2016). Verbraucherpolitischer Bericht der Bundesregierung 2016, Berlin: Bundesregierung [Federal Government].

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. Retrieved on 16 November 2016 from 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 (ed.), Fachserie 15 Reihe 4 (p. 1-45). Wiesbaden: Statistisches Bundesamt (Destatis) [Federal Statistical Office].

Deutscher Bundestag (2016). Regulierung von Messengerdiensten: Datenportabilität und Interoperabilität. Wissenschaftliche Dienste No. WD 10 - 3000 - 060/16.

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

Domurath, I. & Kosyra, L. (2016). Verbraucherdatenschutz im Internet der Dinge. Sachverständigenrat für Verbraucherfragen Working Paper No. 3. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

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.

European Commission (2015). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe. COM(2015) 192 final.

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 (eds.), Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft (p. 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, Bundestag Committee Printed Paper No. 17(24)014-F.

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

Gigerenzer, G. (2017). Digital risk literacy: Technology needs users who can control it. Scientific American (25 February 2017). Retrieved on 20 June 2016 from 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. Publications of the Advisory Council for Consumer Affairs. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

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 February 2017). Retrieved on 20 June from 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 No. 4.1.

Jentzsch, N. (2017). Report: Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds. In: Stiftung Datenschutz (ed.), Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen (Part C – p. 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 (eds.), Schriftenreihe Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt (p. 1-48). Creative Commons 4.0 International License.

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 No. 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 [North Rhine-Westphalia Consumer Organisation].

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 October 2016). Retrieved on 14 June from 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 [Secretariat of the Standing Conference of the Ministers of Education and Cultural Affairs].

Kultusministerkonferenz (2016). Strategie der Kultusministerkonferenz "Bildung in der digitalen Welt". Bonn: Sekretariat der Kultusministerkonferenz [Secretariat of the Standing Conference of the Ministers of Education and Cultural Affairs].

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. Cologne: Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres).

Möchel, E. (2016). Machtvolle Rückkehr der DDoS-Attacken, ORF.at (4 October 2016). Retrieved on 14 June from 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 Nordrhein-Westfalen [North Rhine-Westphalia Consumer Organisation].

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. Retrieved on 27 February 2017 from 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. Retrieved on 14 June 2017 from 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? Publications of the Advisory Council for Consumer Affairs. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

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 (eds.), Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft (p. 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. Publications of the Advisory Council for Consumer Affairs. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

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 [North Rhine-Westphalia Consumer Organisation].

Rotondi, V., Stanca, L. & Tomasuolo, M. (2017). Connecting alone: Smartphone use, quality of social interactions and well-being. DEMS Working Paper Series No. 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. Publications of the Advisory Council for Consumer Affairs. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

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 No. 16-042.

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

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. Retrieved on 14 June from 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 (eds.), Medienpädagogik (p. 39-52). Baden-Baden: Nomos Verlagsgesellschaft.

SVRV (2015). Verbraucherpolitik in der digitalen Welt: Standpunkte des Sachverständigenrates für Verbraucherfragen. Publications of the Advisory Council for Consumer Affairs. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

SVRV (2016). Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt. Publications of the Advisory Council for Consumer Affairs. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

Swartz, A. (2013). Aaron Swartz's a programmable web: An unfinished work. In: J. Hendler & Y. Ding (eds.), Synthesis lectures on the semantic web: Theory and Technology (p. 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. Publications of the Advisory Council for Consumer Affairs. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

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 No. 2. Berlin: Sachverständigenrat für Verbraucherfragen (SVRV) [Advisory Council for Consumer Affairs].

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 No. 2015-026.

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

Advisory Council for Consumer Affairs

The Advisory Council for Consumer Affairs is an advisory body of the Federal Ministry of Justice and Consumer Protection (BMJV). It was set up in November 2014 by the Federal Minister of Justice and Consumer Protection, Heiko Maas. The Advisory Council for Consumer Affairs is tasked with using research findings and drawing on the Federal Ministry of Justice and Consumer Protection‘s practical experience to help shape consumer policy.

The Advisory Council is independent and is based in Berlin.

The chair of the Advisory Council is Professor Lucia Reisch.